

JOeSandbox Cloud BASIC



ID: 484268

Cookbook: browseurl.jbs

Time: 06:27:03

Date: 16/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Sigma Overview	3
Jbx Signature Overview	3
Phishing:	3
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	5
Unpacked PE Files	5
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
Contacted URLs	6
URLs from Memory and Binaries	6
Contacted IPs	6
Public	6
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	27
No static file info	27
Network Behavior	27
Network Port Distribution	27
TCP Packets	27
UDP Packets	27
DNS Queries	27
DNS Answers	28
HTTP Request Dependency Graph	30
HTTPS Proxied Packets	30
Code Manipulations	164
Statistics	164
Behavior	164
System Behavior	164
Analysis Process: iexplore.exe PID: 5672 Parent PID: 792	164
General	164
File Activities	164
Registry Activities	164
Analysis Process: iexplore.exe PID: 1744 Parent PID: 5672	164
General	164
File Activities	165
Registry Activities	165
Disassembly	165

Windows Analysis Report https://www.bustle.com/enter...

Overview

General Information

Sample URL:

http://https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-cha

Analysis ID:

484268

Infos:

HTTP

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

48

Range:

0 - 100

Whitelisted:

false

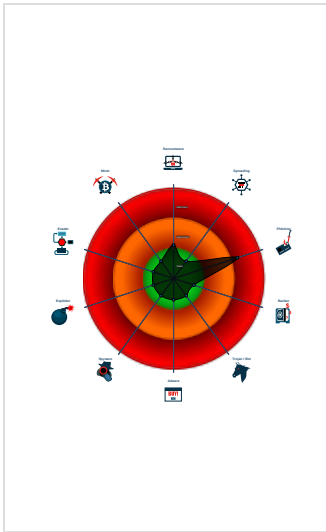
Confidence:

100%

Signatures

Missleading page title found

Classification



Process Tree

System is w10x64

iexplore.exe

(PID: 5672 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)

iexplore.exe

(PID: 1744 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5672 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)

cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

Phishing:



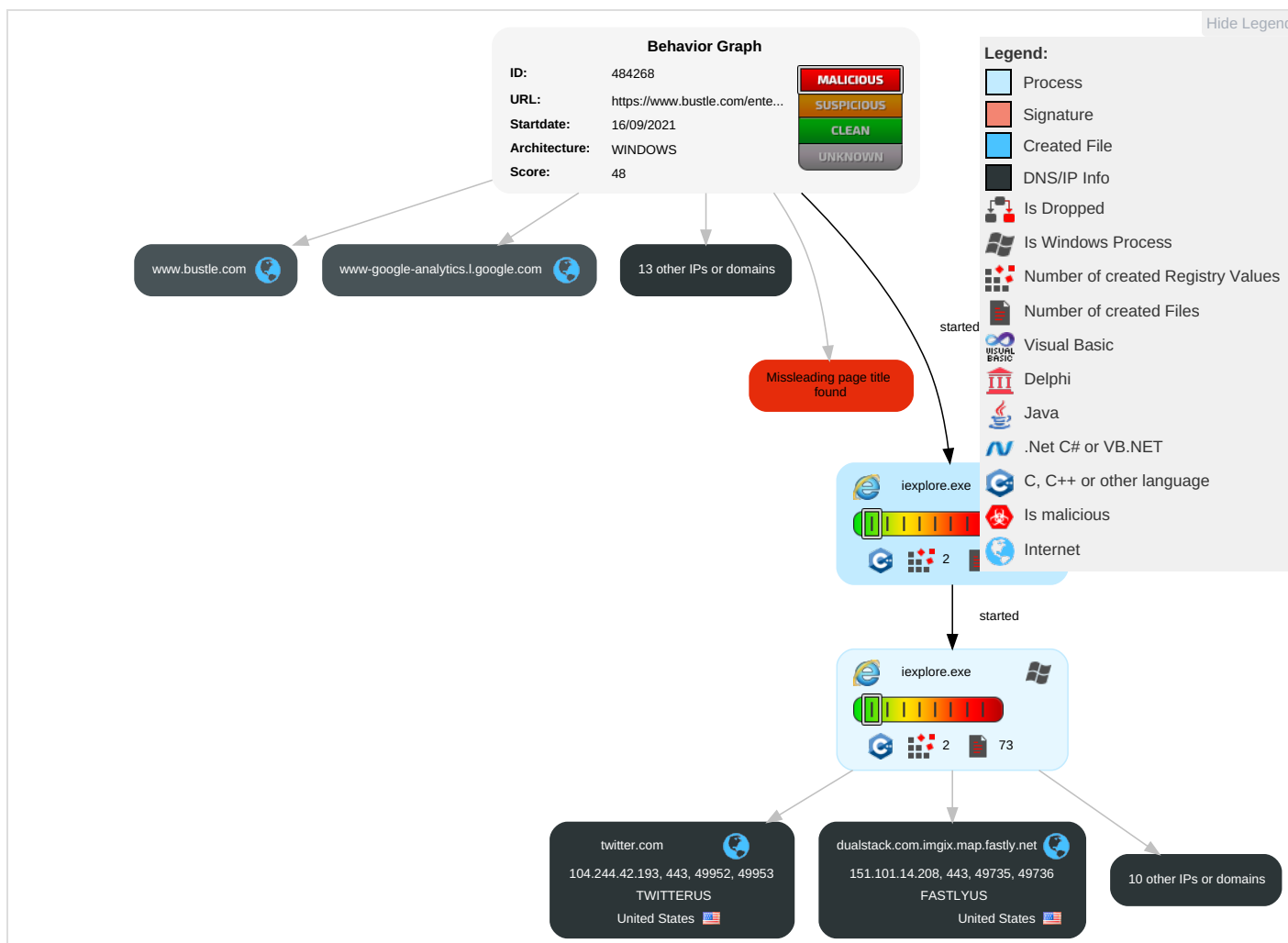


Missleading page title found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carrier Billing Fraud

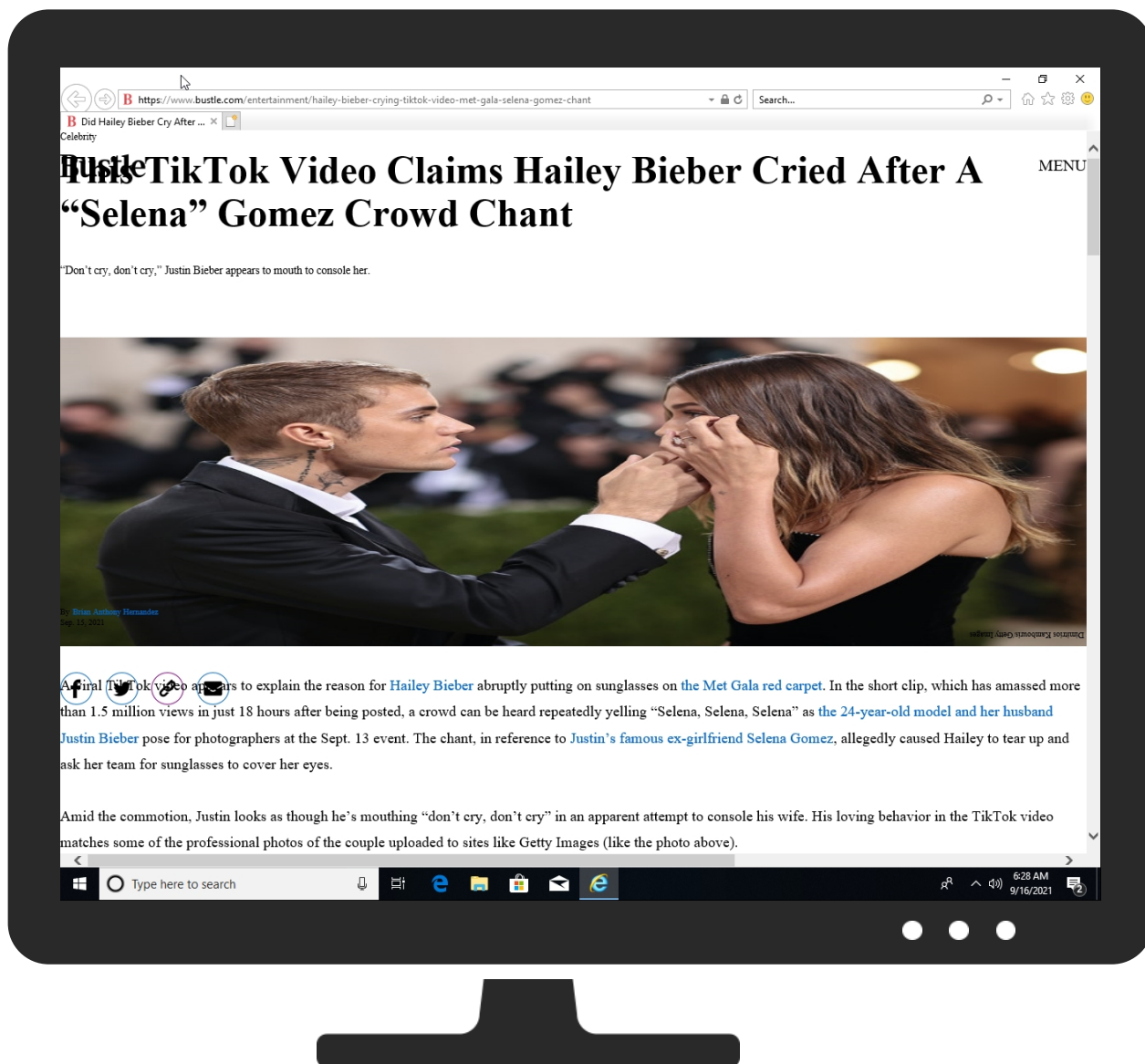
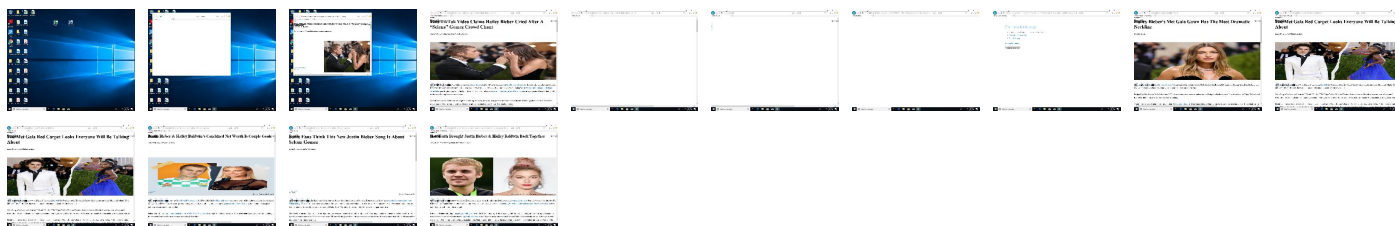
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
medallia.map.fastly.net	0%	Virustotal		Browse
twitterinc.tt.omtrdc.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bustl/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selenabustle.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
star-mini.c10r.facebook.com	157.240.9.35	true	false		high
twitter.com	104.244.42.193	true	false		high
medallia.map.fastly.net	151.101.2.133	true	false	• 0%, Virustotal, Browse	unknown
s.twitter.com	104.244.42.131	true	false		high
www-google-analytics.l.google.com	142.250.185.206	true	false		high
twitterinc.tt.omtrdc.net	18.203.190.43	true	false	• 0%, Virustotal, Browse	unknown
dualstack.com.imgix.map.fastly.net	151.101.14.208	true	false		unknown
www.bustle.com	52.222.214.86	true	false		high
cs41.wac.edgecastcdn.net	93.184.220.66	true	false		high
cs510.wpc.edgecastcdn.net	152.199.21.141	true	false		high
cooladata.kampyle.com	35.241.45.82	true	false		high
www.facebook.com	unknown	unknown	false		high
m.facebook.com	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
resources.digital-cloud-prem.medallia.com	unknown	unknown	false		high
cdn2.bustle.com	unknown	unknown	false		high
udc-neb.kampyle.com	unknown	unknown	false		high
help.twitter.com	unknown	unknown	false		high
imgix.bustle.com	unknown	unknown	false		high
platform.twitter.com	unknown	unknown	false		high
fonts.twitter.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.bustle.com/style/hailey-bieber-met-gala-2021-look	false		high
http://https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant	false		high
http://https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare	false		high
http://https://imgix.bustle.com/uploads/getty/2021/9/15/a0d3927a-fca0-49a6-8bd2-709fa0cfd3a-getty-1340178661.jpg?w=800&fit=crop&crop=faces&auto=format%2Ccompress	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.222.214.86	www.bustle.com	United States		16509	AMAZON-02US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
151.101.14.208	dualstack.com.imgix.map.fastly.net	United States		54113	FASTLYUS	false
157.240.9.35	star-mini.c10r.facebook.com	United States		32934	FACEBOOKUS	false
152.199.21.141	cs510.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
157.240.17.35	unknown	United States		32934	FACEBOOKUS	false
104.244.42.193	twitter.com	United States		13414	TWITTERUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	484268
Start date:	16.09.2021
Start time:	06:27:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browserurl.jbs
Sample URL:	http://https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.phis.win@3/59@14/6
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browsing link: https://www.bustle.com/ • Browsing link: https://www.bustle.com/profile/brian-anthony-hernandez-63990196 • Browsing link: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare • Browsing link: https://twitter.com/intent/tweet?url=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant&via=bustle • Browsing link: https://www.bustle.com/entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant • Browsing link: https://www.bustle.com/style/hailey-bieber-met-gala-2021-look • Browsing link: https://www.bustle.com/style/met-gala-2021-red-carpet-best-dressed • Browsing link: https://www.bustle.com/entertainment/justin-bieber-net-worth-hailey-baldwin-earnings-money • Browsing link: https://www.bustle.com/entertainment/is-justin-biebers-ghost-about-selena-gomez • Browsing link: https://www.bustle.com/entertainment/justin-bieber-hailey-baldwins-relationship-timeline-shows-how-this-couple-went-from-pda-to-rumored-engagement-so-fast-9692470 • Browsing link: https://twitter.com/arianalife0/status/1437939259609128967
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{E4E52F31-16F1-11EC-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8498435663427568
Encrypted:	false
SSDEEP:	48:lwJGcprUGwpl3G/ap8vGIpc03GvnZpvokGoZqp9odGo4RpmoHGw7h9o1jGWxhvo+:rPZsZ/2xWolto1foWRMolo1doCfodsX
MD5:	1A53EEF8C5214D3D06D164B5DBF3D2A9
SHA1:	6201C999E11615DA14F0CD027911B20F5873681F
SHA-256:	CA33FCCA2B5F7CDA251E59808BDD64A38EB4CD73CB9396EE4FE9BFCF6EDE3362
SHA-512:	D1E41BF3A2E14EADF025AABEC532889A39E7F591A81D481E4863D62AE01590EEA9C676D2AB7A712AB730C799858E7118CC081040C133A17E860FA71108BC148D
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E4E52F33-16F1-11EC-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	427366
Entropy (8bit):	2.870087666736812
Encrypted:	false
SSDEEP:	12288:U1r0KR1r0KR9+Pd+xo2cdfZnl+ZILOr0Qu4Vtly1y7yVy2yYyMyrykyCynryxo:U1r0KR1r0KR9+Pd+xo2cdfZnl+ZILOrg
MD5:	B294289A15B02F1586016A768C62585C
SHA1:	6EB93590E01941E1FCE14CA71926D2E32398750F
SHA-256:	CACEABD7BE57EACD9965AAE4F2F34D60FB1E9B00E22A11ADD93E8889B1A8C686
SHA-512:	9C3E630E127D1EA855165745CE184E82A5C1E154FCE00B14EDA323B64C085E2A5825CD74A7EB596462D2C24CF0AC1B9393EC4F1ABE3852A28E608906239156B
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{E4E52F34-16F1-11EC-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.565088816269626
Encrypted:	false
SSDEEP:	48:lwuGcprGwpaGG4pQGGrphSPGQpK1G7HpRMTGIpG:ryZlQ26lBSZAKTYA
MD5:	22F1E60A272A09BB997E06F342D59B6D
SHA1:	476AF707C7942E9711D9734DE5A1DA25B41A8B8C
SHA-256:	DEBB770214DC23407DF3226AF026FAABAC8722F06036C68EE177BF13AE589B66
SHA-512:	006BC6FC84C9B2ABF4663D53C0B2CF48C8E2EC7A5C78446C85F1A0014FC2A633383D69499584E5031CFA0761C4E8F55DCDA03CB33B69295E8EFE187CA1578C
Malicious:	false
Reputation:	low
Preview:	R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.06356110806806
Encrypted:	false
SSDEEP:	12:TMHdNMNxEbGNSnWiml002EtM3MHdNMNxEbGNSnWiml00ObVbkEtMb:2d6NxOCuSSZHKd6NxOCuSSZ76b
MD5:	672513530AB16AA8985622A7E61A1DF5
SHA1:	FFD9C3FF2DE4890FD44F15A98EF70DE6BEBD922F
SHA-256:	1D6D02D54FB2AF1F3C52EF694F2E704CF44031A3DEB9418D7BD1EE9C89DCB391
SHA-512:	DEE778082DDBCA6BFA4AC4BB2C87C198A63C192A4B5FE579B943C066E9C7384D088B4E9571AE06DB4DA AFC98CEB64E85E789DC50358B21EF51E9901648E12C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.071171919967232
Encrypted:	false
SSDEEP:	12:TMHdNMNxe2kBUNGNWiml002EtM3MHdNMNxe2kBUNGNWiml00Obkak6EtMb:2d6NxriyGSZHKd6NxriyGSZ7Aa7b
MD5:	9060B3A7E02C5D68789861F9846728F7
SHA1:	6A8C9077362EB029191E42522319415E59FD72C4
SHA-256:	F36055CEDE07BA3D02E20292AD82D9EC31BE9768FD3C2BF1EE8FD68DC9C5B5EC
SHA-512:	64D49E3EB80F6649E7DF527C3DD125F5C7873DAA6655AB377F30F1880628379EA536E1B0108479120510F5DC0C53E945A291EC5460E22EA57F047012380352E2
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbb90a161,0x01d7aafe</date><accdate>0xbb90a161,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xbb90a161,0x01d7aafe</date><accdate>0xbb90a161,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.082225983776254

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Encrypted:	false
SSDEEP:	12:TMHdNMNxxvLBgNSnWiml002EtM3MHdNMNxxvLBgNSnWiml00ObmZEtMb:2d6NxvtuSSZHKd6NxvtuSSZ7mb
MD5:	E0941F0FD07F34D61BBB5DC9B12FDC2D
SHA1:	121C1288CC1415C523C4578C9D5D23118676FD8D
SHA-256:	514E17BA11D247520B917643ED05158B0138F0BBA320DAC8C4DD95BFCE0320B
SHA-512:	81B524E7AACB0F561364D65F881F080FED59AD91CDB6223C562F8D5584AA4EE4EBAC7D366258540DBD13DCE74999035F22D6B844DE2E6F6CD456438CEA9D9E D3
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/" /><date>0xbb97c83b,0x01d7aafe</date> <accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/" /><date>0xbb97c83b,0x01d7aafe</date><accda te>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Wikip edia.url"/></tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.078892002371602
Encrypted:	false
SSDEEP:	12:TMHdNMNxiBgNSnWiml002EtM3MHdNMNxiBgNSnWiml00Obd5EtMb:2d6NxcuSSZHKd6NxcuSSZ7Jjb
MD5:	BDD133AD57580CD1ACA72F6F8224A7BB
SHA1:	B95869FF6D8997CDFE2C9C6A115D741BB6C187E8
SHA-256:	1BEE4F89D76259A9F7D495674AB9B13FB0169A01C8245955CFA1B67376332CE7
SHA-512:	DFA5A37724678DD03E74B8A85E6B63179DD0280488BBA58E63DF4537F84059E6BDE5AF4E64364DFA776731DE74817F0E960C3C4E5B537810F23A61D5A50A87Df
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/" /><date>0xbb97c83b,0x01d7aafe</date><acc date>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/" /><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c 83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Live.url"/></tile> </msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.090611493363248
Encrypted:	false
SSDEEP:	12:TMHdNMNxxhGwBgNSnWiml002EtM3MHdNMNxxhGwBgNSnWiml00ObK075EtMb:2d6NxQWuSSZHKd6NxQWuSSZ7YKajb
MD5:	20B8ED17370029552820C20F28838BAD
SHA1:	38EC105B8D59BD2C111B30B82CAF3AF97F9CAA57
SHA-256:	AAA001B97A471D5269890D7EA5A67A31AA2710E6A49C4932937A663CA1DC10C0
SHA-512:	FEABB4DAFB3C3FD179343C3FC3DE4D2FF0ADFCD6921AE8EB6359BF303F9EC95D3892414DE667C453C108010125EDC18A1C3CFA386F2A3759D930DAC3E04 7E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0xbb97c83b,0x01d7aafe</date>< accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/" /><date>0xbb97c83b,0x01d7aafe</date><accdate>0 xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user1\Favorites\Youtube.url"/> </tile></msapplication></browserconfig>..

C:\Users\user1\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0665905086084155
Encrypted:	false
SSDEEP:	12:TMHdNMNxnBgNSnWiml002EtM3MHdNMNxnBgNSnWiml00ObxEtMb:2d6Nx0BuSSZHKd6Nx0BuSSZ7nb
MD5:	C6BD55AE260408C401E4C2555AE2B74D
SHA1:	7A0BBEE740BAB7F71529973EBC7A39562DC4F72D

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
SHA-256:	FC32C3F838EA6A8CF24FE2D065EAC71082DC2F4335E26CAFA752A63E55362E21
SHA-512:	C0046EDB3FD9A39CA59ADC81079E8616D60FDDFFEDCEFC2D92C9A59D713FADC3B1B6548D878478B491F0974B38FA9A5D332989171212686C8B595B00A4596F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.103984809338757
Encrypted:	false
SSDEEP:	12:TMHdNMNxxBgNSnWiml002EtM3MHdNMNxxBgNSnWiml00Ob6Kq5EtMb:2d6NxfuSSZHKd6NxfuSSZ7ob
MD5:	387D146CBBB239B5F529639E7A0129E7
SHA1:	68E9FE19D4E8A5858FC9EF55C5E2C1BB741CCA8A
SHA-256:	B0454E0BE57AD567B5ED0BBBF4696C35F0C57D14EF75F5A8F2B5A3C67DF53806
SHA-512:	FD087F2FA427AA7B2DD1C1F7C38BCDC76D3DFE2E8B87B269E1E3A6F5624283CCB8F936A5961377F7A851CE454B92B6C43E34B3EEF6B8C6833C68C953F9F39D9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.07390133133069
Encrypted:	false
SSDEEP:	12:TMHdNMNxcBgNSnWiml002EtM3MHdNMNxcBgNSnWiml00ObVEtMb:2d6NxquSSZHKd6NxquSSZ7Db
MD5:	6AC4DFA73595FC518FD9F712AF8DFDBB
SHA1:	231C42058012C8A01E1AABB3D524F358333704C1
SHA-256:	1B7C514F417B192D921EE7F11687A03D94DE5EA729D78F529358E9F99932E442
SHA-512:	22572034CE9AB76FE3DA6E8523F68AD83A327D6EB77C6147B8FCE6D757DB380C58641DA3CE66F3376F5184A30A7DA3EE6C3AED7D8B9FAEA61466BDA6093AC149
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.064851724800326
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnBgNSnWiml002EtM3MHdNMNxfnBgNSnWiml00Obe5EtMb:2d6NxJuSSZHKd6NxJuSSZ7ijb
MD5:	3A60496FC8530C62649FD5A59E46332A
SHA1:	005D32D467C3B6FFC812CAFF2C7E10F1781948B8
SHA-256:	9F3639C92EF45AD739B1AB01C779B381D32D9A45A513C7126535E264E1AA3370
SHA-512:	E467494497B6CF55B1796B077D9213C5BA7FDC9239248F640A6458BEB8A9A8090EEF5DB479156222A2F84D0F5ABC2AA7DB7509BA2352BF92D0268665494707C6
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml

Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xbb97c83b,0x01d7aafe</date><accdate>0xbb97c83b,0x01d7aafe</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..
----------	--

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\lynfz0jx\imagestore.dat

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	1009
Entropy (8bit):	7.308541022593749
Encrypted:	false
SSDEEP:	24:xOVaWcQc2iiznkM0aA6TSkUUoJQU3T9hoQYDAQFu5EWD:xOVaWc1s0p6T5UUr4UQxr
MD5:	03A40F7EA81208DFA57CF743A3348C39
SHA1:	75A331CEF40A17916132F3954F3B56C42E72B59E
SHA-256:	AC7E85AB70AB12DACD8B48B1C531BE2FB1E3E884191E0B72CA8E645ADEC910A2
SHA-512:	44EECEEAE7869DE4D228B22758A62281290C8B2708928CA008DEF37379D9C36B2B3D445ED17FBA415335759CC115E5769751232BC99B682C31E84502528B0B4E
Malicious:	false
Reputation:	low
Preview:	"h.t.t.p.s://.w.w.w...b.u.s.t.l.e...c.o.m/f.a.v.i.c.o.n...i.c.o.....PNG.....IHDR... ..szz.....gAMA.....a...8eXIfMM.*.....i.....N@.....IDATX..MHTQ...wf."OG....*.cQ_@.E~.#.%.@.E..i...E.r.9...+.)\$V.3.R.m.y...s.A...~.s...;3...y...?Y.x...2.9.....0B.x.....*Mg..."h3.x.S...~.S%...9.....r....b....Py..V..L.XY.x6.wzT.B1U.t.m.b.....O:}...~O...f... ..l8..]o...J..{:3.....]3..NM.6.2..}...w..n....X..}P.Y&..;/5?..U.....n2j...U@.....Tx{.m!_\$.....f#..t.{{.M.b..L.....g.gy."1.Pg..0AQ.K'S..i.@.R..P.F.....+OB.p p..t..#.3V.U...}@..E..h...#<...a.RS..R...xId.Y.U.O.....p.....<.JE...i}..%F.....H.....f.L....D.8....&..Mjo...}.+....._kL...0W..m.@8'.6...p...l.Q.?..`=.....u...!l...;@...x...c..qe...!..rq*...97...ro^....<..l8..;C.....!..~...o.....N@8.ay^..PG....<.V. ...).....0....W..}o:...p#g w...(L[...lEND.B`...)JCa...

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\AuthorPage-aebfb1aad7[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1258
Entropy (8bit):	5.25935736530688
Encrypted:	false
SSDEEP:	24:MS6WMMbRNicaBdrZ1bN9Y+Ct+uJ5bYWpeoMA4ORSoc5j+peQr:MSxMb/iZdrZ7igJPDB+MK
MD5:	6357293C038EADFA6BE5170EDFF2AABA
SHA1:	3C1736CB78F0D031B8DD53D7FC184A3BC07AB328
SHA-256:	E842516DA49B88D623A2E1C0843C51D024C02897E3EC75000E7830A65ECDC17D
SHA-512:	D051BF0801893B66EDDA3B32AC7ABA77FC290024E86F82EBE5B615F41EF4307FA3D09C68723252D875BC76857B47FE5E849F3199D8DEE814480918029D5BDCB
Malicious:	false
Reputation:	low
Preview:	.lHf{background:var(--slot2);color:var(--slot1);min-height:100vh}.xDM{margin:2rem auto;max-width:var(--maxContainerWidth);padding:0 var(--pageGutter);position:relative;width:100%}.wS_{border-top:.5px solid #0003;color:inherit;display:flex;padding:1rem 0}.HOL{padding-left:var(--pageGutter)}.HOL p{margin:0 0 1rem}.khv{font-family:var(--fontFamilyHeading);font-size:.875rem;letter-spacing:-.15px;line-height:1.15}.dXp{color:var(--slot3);font-family:var(--fontFamilySansSerif);font-size:.625rem;font-weight:var(--fontWeightBold)}._dS,.koY{display:none}.cdn{flex:none;width:150px}@media (min-width:768px){.wS_{padding:var(--pageGutter) 0}.khv{font-size:1.5rem}._dS,.koY{display:block}._dS,.dXp{font-size:.8125rem}.koY{font-family:var(--fontFamilySansSerif);font-size:.875rem;letter-spacing:-.1px;line-height:1.5}.cdn{width:250px}}@media (min-width:1025px){.cdn{flex:none;width:175px}.wS_{padding:2rem 0}.HOL{display:grid;flex:1;grid-template-columns:1fr 175px;grid-template-rows:auto auto 1fr;padding-le

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\ListiclePage-a481cffd14[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	116930
Entropy (8bit):	5.531223715297272
Encrypted:	false
SSDEEP:	1536:fdN3pgbW1EiJS5L9tMy8GvTYrdjwTZ6z5jvkZqq3VBsYFqq/Ej7ZTdXMPYZ1dPk0:DU62HtJYZEaa9KTfoj2nyTV
MD5:	BC1832A379B8E5321C5086B4040B055C
SHA1:	D1BE810411508C89B3C37C7EAB7BD1B9BAD0ED47
SHA-256:	8BBF93B6912313D62EC9415FD72E4F726FE51ACD6039AFA96B9C1BC1709F5978
SHA-512:	EFED52FCC1790250F09BB55BB793248E6620DBF32D906CB9B0F2E43ECE43F241E8E2AE79DB4D3D2D0E6779624B584A74A2FB82A188FBB5291A428CE3AB0C06AC
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\ListiclePage-a481cffd14[1].js

Preview:	"use strict";(globalThis.webpackChunk=globalThis.webpackChunk []).push([([242],{7925:(e,t,r)=>{r.d(t,{Z:()=>{}});var o=r(2335);const a={sponsorHolder:"Jjo",sponsor:"KSr",sponsorName:"cCz",sponsorBy:"cAx",sponsorIntro:"IzZ",sponsorImage:"PgK",inHub:"FDR",inStorefront:"UJX",wrapped:"eFu"};var n=r(2779),i=r.n(n),s=r(3847).h,function l(e){const{className:t,inHub:r,inStorefront:n,modelID:l,sponsorText:c,wrapped:p}=e,d=i()(a.sponsorHolder,t,p&&a.inHub,n&&a.inStorefront);return c?s("div",{className:d},s("span",{className:a.sponsorBy},c)):s(o.RW,{className:d,style:a,modelID:l})}}),6550:(e,t,r)=>{r.d(t,{Z:()=>c});const o="wVs",a="yKE",n="OnM";var i=r(2779),s=r.n(i),l=r(3847).h,function c(e){const{parent:t,inFeature:r}=e [],{title:i,path:c,sponsored:p}=t {};return l("a",{className:s(o,r&&n),href:c},p&&l("div",{className:a},"Sponsored"),i))},7201:(e,t,r)=>{r.d(t,{Z:()=>c});const o="JAm";var a=r(9580),n=r(2779),i=r.n(n),s=r(3847).h;const l=["facebook","twitter","copyLink","mailto"];
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\NewErrorPageTemplate[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpActUzJD0IFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
Reputation:	low
Preview:	.body{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;.....mainContent{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;.....title{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;.....errorExplanation{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;.....taskSection{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;.....li{.. margin-top: 8px;.....diagnoseButton{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\la0d3927a-fca0-49a6-8bd2-709fa0fcfd3a-getty-1340178661[1].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x611, frames 3
Category:	dropped
Size (bytes):	80984
Entropy (8bit):	7.976756272543975
Encrypted:	false
SSDEEP:	1536:hhjE6GOjLIKY4vALwuY/liTVRqUJhCJiJYS9eX9kuLNfE+3nt6:hhFGuMhww/liTVUMCgYV9HLhpA
MD5:	3E8594FD9BD984E977D32D35B45031A9
SHA1:	61DBA760995E7A59AB2A1C1F6D5F4A70D503ACB0
SHA-256:	B5C40A502BA2B00DC7483045036915DFBF16AA238181B8C892BC3EA67EE8BA26
SHA-512:	82DB2AF20A0E2A45CC577A8BE7BE52DFFA94976938027776369F8D907613B97AFD2145C56C0142DCC7724BFEB30B4332E4A6C33620535006077C86AD86605887
Malicious:	false
Reputation:	low
Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino.....mnrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt...P...3desc.....lwtpt.....bkpt.....rXYZ.....gXYZ.....bXYZ...@.....dmnd...T...pdmdd.....vued...L.....view.....\$lumi.....meas.....\$tech...0.....TRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZ ..o...8.....XYZb.....XYZ\$.desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\favicon[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 32 x 32, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	903
Entropy (8bit):	7.525200976527568
Encrypted:	false
SSDEEP:	24:wcQc2iiznKM0aA6TSKUoUjQU3T9hoQYDAQFu5EWE:wc1s0p6T5UUr4UQxs
MD5:	237EA60A7CA62236AE8721B6B98214A3
SHA1:	AE68024A84932500FFBB9A512E6B0D9EC99F071D
SHA-256:	9F98CCAFD747D9364274610DFE1411CD28B177DA9CCF3FE8C919FB5B604B3417
SHA-512:	8E3284AE0426DB49271B68C41D0845D73118A74946A980955B45AE73D030EA87205ED12A1B6B90824E3B85626EA4E929A776DEF4EF392C72CA408DC9741C3134
Malicious:	false
Reputation:	low

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\favicon[1].png

Preview:	.PNG.....IHDR... ..szz.....gAMA.....a.....8eXIfMM.*.....i.....N@.....IDATX..MHTQ...wf."0G....,*cQ.@.E~.#.%.@.E..i...E.r.9...+..\$V.3.R.m.y....s.A....~.s...;3...y...?Y.x....2.9....0B.x.....*"....Mg...."h3.x.S.~.S%.9....r...b....Py..V..L.XY.x6.wzT.B1U.t.m.b.....O:}...~O..f .I8..]o...J..{:3.....}3..NM.6.2..)}...w..n....X.}.P.Y&../5?.U.....n2j...U@.....Tx{m!\$_\$....#f.t.{{.M.b..L.....g.gy."1.Pg..0AQ.K'S.i.@.R..P.F.....+OB.pl.p./t..#3V.U...}@..E..h...#<...a.RS..R...xld.Y.U.O...p.....<..JE...i}...%F.....H....f.L....D.8....&.Mjo...}.+....._kL....0W..m.@8'.6...p..l.Q.?..'=-.....u...!l...;@.....X....c.qe...!..rq*...97..r0^.....<...l8...;C....!l...~....O...N@8.ay^..PG....<..V. ...}.....0....W..}o:..p#g]w...(L..[....IEND.B`.
----------	--

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	46937
Entropy (8bit):	5.5403009125913485
Encrypted:	false
SSDEEP:	768:KqSR08h8YP7UcPAqTLZBNVDxkkJJi/eTYeL69kPTX3TgxFL/YYRF1mq:CBrx3i/eTnHTgxFLI
MD5:	115F229B9F255E22CEA23A4AE09D803
SHA1:	35E8A3CD3907522B85ED6D26455F2F2A87A2267B
SHA-256:	244E7BBA8EBBD8F299A1D1344BF1F0C0C2EE59416AEE332ABBD7A7EEC4B2AFD2
SHA-512:	EAAA4DD8E50EE4CA7A33644C6E6B9D28BDF62261A86487D5086E560FD04978B724F35E6A3C7A0B7887A6D994FEDA585AAB97D42539D64D37D66A293D9134E31F
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\is-justin-biebers-ghost-about-selena-gomez[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	43191
Entropy (8bit):	5.499174186143864
Encrypted:	false
SSDEEP:	768:KqSR08h8YP7UcPAqT3lBmNbukkPdL69kPCBUe9k5gl1mq:cBqu7YD9Y
MD5:	7486D8EBDD4BB71AE8EF5CF7AC8BD0D5
SHA1:	692DE674973DF2CAC5F28483E507BFE579A84207
SHA-256:	EF19A0DE551BB3BED2DB95673023A67E40046F35FA8FDB355BF2E7B6E22FFA93
SHA-512:	A930A8F29348DAFB2E0AD9738364C051D2FE7277F795C42FD2F5F69919F17ADEAB217010B86CD6EB19CF271C5BFA107210754DF6F11E8D2F20671195AD0DE52
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\vendors-d0e3a0e319[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	35797
Entropy (8bit):	5.309666495423084
Encrypted:	false
SSDEEP:	384:r8XBMeWUPW1Y1xKAhbQJ2PPjYQOZ9cn4z7cC5WDDWfxW9kOnU:9PbK2PWcRComfx8NnU
MD5:	AD8BFDf96C31BD5E49DF3E6D027E37B3
SHA1:	763B6C1F8F2551BEE070ECBE9477D9FB030399D5
SHA-256:	803521E42A807B979CF464C9D756F046131ACA355D7F87C19AF10FEDDDB2CC01
SHA-512:	FBC02AE7D60BA26B26D4B98B8CE7F8A4357153B6E2498F8C3E21C16E21A6688F9023DFC855564703F0CCFB4C7B1D5E2C17E09F806391B3429FF173CBA9823E1
Malicious:	false
Reputation:	low

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\vendors-d0e3a0e319[1].js	
Preview:	(globalThis.webpackChunk=globalThis.webpackChunk []).push([([216],[2779:(e,t)=>[var n;function(){“use strict”;var r={}.hasOwnProperty;function o(){for(var e=[],t=0;t<arguments.length;t++){var n=arguments[t];if(n){var i=typeof n;if(“string”===i “number”===i)e.push(n);else if(Array.isArray(n)){if(n.length){var u=o.apply(null,n);u&&e.push(u)}}else if(“object”===i){if(n.toString===Object.prototype.toString)for(var a in n)r.call(n,a)&&n[a]&&e.push(a);else e.push(n.toString())}}return e.join(“ ”)}e.exports?o.default=o,e.exports=o}:void 0===n=function(){return o}.apply(t,[])) (e.exports=n)}(),8755:(e,t,n)=>[“use strict”;Object.defineProperty(t,“__esModule”,{value:!0});var r=n(6264);t.default=function(e){var t=e.createElement,n=e.getCardComponent;return function(e){var o=e[0],i=e[1];return t(n(o)) r.throwError(“Unhandled card: `getCardComponent(“”+o+”)” did not return a corresponding component.”),[payload:i]}}},7002:(e,t,n)=>[“use strict”;Object.defineProperty(t,“__esModule”,{value:!0})

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\0W10PBUV\youtube-9689e80b6a[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	465
Entropy (8bit):	4.393086814780356
Encrypted:	false
SSDEEP:	6:tl9mc4sl3QOF9rBdVwvpkVm4CNALfCIORBvuVzIzTuR32/hbz0yL/f/MkC2jvnlQ:t41h/BXw+RCNaLj0wBlzaW5/TI40R6
MD5:	4656C1149BC199734B60E97760F364A1
SHA1:	F48417D77C3DF7D04712971C27BE3E513ADA9315
SHA-256:	DFC24BAF204D35339494C2B4FAD1EA328DC835D875E699FDAB250C48273709E6
SHA-512:	4F116435040FAE263744AECC13A72452692768ABA1C3D0227E69B03D0069E5BC5E6853643281BDE2BA535FE7148C77A27FDABD0FEA4C531BB6E389088DC8680
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 512 512"><path d="M490.2 73.9c-13.9-24.7-29-29.2-59.6-31-30.7-2-107.8-2.9-174.5-2.9-66.9 0-144 .9-174.7 2.9-30.6 1.8-45.7 6.3-59.7 31C7.4 98.6 0 181.1 0 255.9v.3c0 74.5 7.4 157.3 21.7 181.7 14 24.7 29.1 29.2 59.7 31.3 30.7 1.8 107.8 2.8 174.7 2.8 66.8 0 143.9-1.1 174.6-2.8 30.7-2.1 45.8-6.6 59.6-31.3 14.4-24.4 21.7-107.2 21.7-181.7v-.3c0-74.8-7.3-157.3-21.8-182zM192 352V160l160 96-160 96z" fill="#222"/></svg>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\870fc2cb-fef2-4933-98c0-a8f34bdf6849-met002[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x537, frames 3
Category:	dropped
Size (bytes):	101275
Entropy (8bit):	7.975943154233203
Encrypted:	false
SSDEEP:	1536:hzn/yROgz1PmkDgsyv6DcRnPSYbXb6vy3ps48E12UKZJ3/9PJKW3kDqLLTl:hznKJ5mItyvDdP+6hXLKhPxkDqLLTl
MD5:	1856D7F6EA1D20B517B68EF8BD692636
SHA1:	6C7C366D6760AF232B0AE5E46608B5FD2B5E8DC8
SHA-256:	BCF556789CC0E6EB268F68FC3F8714DC9256F7B853CFBB41ECF0053DAD82DEF1
SHA-512:	2EABB763275C18CADA926804CA452AF1C58B5AE716E04F8F069AC9092523CDA65ADB5DD886CE69A5DE327A0E0ADBF1866FC336A146BEB88E090BD8DBCE2FC9A2
Malicious:	false
Reputation:	low
Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino.....mnrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt...P...3desc.....lwtp... ..bkpt.....rXYZ.....gXYZ.....bXYZ...@.....dmnd...T...pdmdd.....vued...L...view.....\$lumi.....meas.....\$tech...0....rTRC...<...gTRC...<...bTRC...<...text...Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZo...8.....XYZb.....XYZ\$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\9d14445b-bac9-4822-9fdf-361d5b1e373a-justin-bieber-hailey-baldwin-bieber-net-worth[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x796, frames 3
Category:	dropped
Size (bytes):	80040
Entropy (8bit):	7.960115202241718
Encrypted:	false
SSDEEP:	1536:hoS+uluwHrAgjQFN4ZRyk+wMCpNbbWdjCXFt+toSp7lfbXuTADsDYv63UiF:hoDulFhjQ+yk0CTWxMt+ZpcxoBcUUc
MD5:	D889A86E3C5CCFECDD138B1DC6F1DD71D
SHA1:	DCAC11A5924B1BCDFA222985C12E65221487F019
SHA-256:	A6D725AB76C8D8A725657D65C8BD868E471B4000EE4B57D907E1AD11131E7421
SHA-512:	DBDE2333978FF902B999EDD8490C8546F8C5E1A1951414D8F6074A1397F6207E215FDE61F1AF373103547A66A8CF0BFC5F332CE690EB3712F94605430D5BA60E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\9d14445b-bac9-4822-9fdf-361d5b1e373a-justin-bieber-hailey-baldwin-bieber-net-worth[1].jpg

Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino....mnrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt...P...3desc.....lwtpt..bkpt.....rXYZ.....gXYZ.....bXYZ...@...dmnd...T...pdmdd.....vued...L....view.....\$lumi.....meas.....\$tech...0....rTRC...<...gTRC...<...bTRC...<...text... Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZo...8....XYZb.....XYZ\$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference V iewing Condition in IEC61966-2.1.....
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\brian-anthony-hernandez-63990196[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	49721
Entropy (8bit):	5.492277350441632
Encrypted:	false
SSDEEP:	768:KqSR08f8YP7UcPAQTq6BTeKtizrV3du5lIXOfL69kPOir8y761mc:OBXSMLS
MD5:	FAEC292F4296AF9F485A129413DD8127
SHA1:	663A56615C693ADA421853B402E0F07B25088F07
SHA-256:	111A48843BCF2AC559A3E6FBD1FBB5C584BFCE2243FC5D0784D42E93DD7B718F
SHA-512:	13CD4544B8869736FB420F6FEB175170A7F807B4DF9ABDA03B3954649A8E173E5457C07F52933DF217F4E68875A7ADBD354AE38116791F6ABCD96D2A358067EA
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /> <meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="art icle:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle .com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bu stle.com/bustle/2021/AuthorPage-aebfb1aad7.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular- 017

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\common-d9e5af7042[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	174091
Entropy (8bit):	5.35036814147841
Encrypted:	false
SSDEEP:	1536:9ppceL/7a+USE3ZvjTDx7hd6L/b1gXQJgl3ITGDw+S7QPlyxEPf:rrCZvjTD/d6L/b1GQJ23ISDw+S7QP5af
MD5:	FBF12C1E39BF073EAC6DB7AC459A1498
SHA1:	F60385283379602F27A0EC2EA4ADEEBB5FA2F80B
SHA-256:	8BA0629633E5A874F4E1AF251588AEDF9AFACEA1BADEA67B9A2D6654E3A5EDB6
SHA-512:	C91D3969D8DB84952D135026ACF20621EB3F952C2CEEC1EF5C5889597D4A6AE23EBDB280D3BDE201E08F1E63A4D456D9693A9A5E18309D13DD763F0811DEEE F
Malicious:	false
Reputation:	low
Preview:	.sqO{height:110px;margin:1rem auto;position:relative;text-align:center}body>div>.sqO{position:fixed;top:-50px}.wGs,body>div>.sqO{bottom:0;left:0;margin:auto;rig ht:0}.wGs{border:solid var(--slot3);height:55px;position:absolute;top:0;transform-origin:center center;width:65px}.ooy{animation:HHd 1.4s linear infinite;border-width:5px ;left:-50px;top:-50px}.EN_@animation:qlm 1.4s linear infinite;border-width:3px;left:50px;top:50px}@keyframes HHd{0%{transform:translateZ(0) scale(1)}25%{transfo rm:translate3d(25px,25px,0) scale(.75)}50%{transform:translate3d(50px,50px,0) scale(1)}75%{transform:translate3d(25px,25px,0) scale(1.5)}to{transform:translateZ(0) scale(1)}}@keyframes qlm{0%{transform:translateZ(0) scale(1)}25%{transform:translate3d(-25px,-25px,0) scale(1.5)}50%{transform:translate3d(-40px,-40px,0) sc ale(1)}75%{transform:translate3d(-25px,-25px,0) scale(.75)}to{transform:translateZ(0) scale(1)}}.VuB{position:relative}.Cgk{background:none;border:none;height: 100%;pointer-events:none;posit

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\ldnsserror[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBDBF35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\dnserver[1]

Preview:	.<!DOCTYPE HTML>..<html>..<head>..<link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css">..<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">..<title>Can’t reach this page</title>..<script src="errorPageStrings.js" language="javascript" type="text/javascript">..</script>..<script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">..</script>..</head>....<body onLoad="getInfo(); initMo reInfo('infoBlockID');">..<div id="contentContainer" class="mainContent">..<div id="mainTitle" class="title">Can’t reach this page</div>..<div class="taskSection" id="taskSection">..<ul id="cantDisplayTasks" class="tasks">..<li id="task1-1">Make sure the web address is correct ..<li id="task1-2">Search for this site on Bing ..
----------	---

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\down[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBIE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....ex....PLTE...W..W..W..W..W..W..W..W..W..W..U.....W..W..!Y.#Z.\$\].<r.=s.P..Q..U..o..p..r..x..z..~.....b.....\$.s...7tRNS.a.o(,.s...e.....q*.....F.Z....IDATx^%\$.@.C..jm.mTk...m.? ;.y..S....F.t.....D>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<q.kH....#+....l.z.....'.ksC...X<+.J>....%3BmqaV ...h..Z_<:Y_jG...vN^<>.Nu.u@.....M....?...1D.m-)s8..&....lEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\instagram-fb2dbe01f2[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	447
Entropy (8bit):	4.7444397133223
Encrypted:	false
SSDEEP:	12:trP13IDS4B4H9evfXdARMXYfhJgtCcvH3AdKwD96:tzdcV949QXdQMM8tCQ3CL6
MD5:	76B4CD8BD9AE37F9DA9C4553F49E1099
SHA1:	C523BE694C26B1F5D68DD531F8D68635D5A766C9
SHA-256:	989073A90E6DFE3899A5F1F6C3825E9A65E197DA6A43956352335A2C4AB5D703
SHA-512:	B4FD2E01E7C7317DCAD9D75FEB2D682532F98E2D9572A2D91CB5AEE3852C687ECF512136404C0C7D4FE6CEA43E6A4331A6BBFD52D2F11D13E2BF3F723289272
Malicious:	false
Reputation:	low
Preview:	<svg width="90" height="90" version="1" xmlns="http://www.w3.org/2000/svg"><path d="M9 26v38c0 9 8 17 17 17h38c9 0 17-8 17-17V26c0-9-8-17-17H26C17 9 17 9 26zm-9 0C0 12 12 0 26 0h38c14 0 26 12 26 26v38c0 14-12 26-26 26H26C12 90 0 78 0 64V26z" fill="#222"/><circle cx="69" cy="21" r="6" fill="#222"/><path d="M45 68c13 0 23-10 23-23S58 22 45 22 22 32 22 45s10 23 23zm0-8c-8 0-15-7-15-15s7-15 15-15 7 15 15-7 15-15 15z" fill="#222"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\logo46x38[1].png

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 46 x 38, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	1015
Entropy (8bit):	7.700668019695508
Encrypted:	false
SSDEEP:	24:T7/62CaaF2ugZ+dGeNFmTscIFYn93/ly/KU3tIl8eS:T7/6RaaF2K4TCY93wC18eS
MD5:	EEF9BFBF60E5A155561FD74258F34134
SHA1:	6060E49DD1EE6D67DABAA1295C50440A12DFAA0
SHA-256:	CC9E476C4F6128FE6ECC8C2FC704C3AC64CD38F6858B541E0004CDF956C93E91
SHA-512:	52B4CBD58FFDD271A24FD907E6E52314BA046CC29BE04D931FC8D519D3603A782B44C800A74ED25BE24AE6149A11BFD1D8A7837D27E8E9941F47DCD2F00F24B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....&.....Z....pHYs.....sRGB.....gAMA.....a....IDATx..XJRA..%o*....@n'..`Y/..N.T..D.;..jYV.]...T.....Q.X#J.....6mos;....=....le.....V=...x..C....\q.}.....<IG...&MZ....Kbm.3Gh<E...q.....A.....N.....6"6"N.....B..8>..>.G.x....>..W.Q.\$..4B..)......qj.....)a,z...l.5..C..mz.....8..[>.O.*...b'y.*\$..L.. d....>.,.50.Tc..%.f...Y6.*_j..h.*2...8IFD. .c...{...;..b.....EKM....>..jB..m6W..j.z...d...A_..V.x.^{.V.W....AZ.<....L.S..."U.kg..[.<j'PU...'.s...].:7+....Gxk8.....J.. ..Ny.1.9]?....C.n.. !:"'.....&...G...v..1@.....A..wC..L...1...3..j2.q..b....>...@.D....l..5.`....BX.V.Q..pAZ .W..1..ak....L>.2...).....L>.2...).Q*>...YY.U....y..P..J....*:...@..%.c0.yl.s...cH..Q..a.... .B....A..M...l..Y..4. .n...'.K.knt.>xQ.....n.)G-Q.....N&.%1l.(.Ga5Wa5.#5x.tG...'.Jp.'!.....R..W....j....*JY.....Fl.V....k.p.P.O.."vUJ.../..U.[F

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\pinterest-4aa4bba5df[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	758
Entropy (8bit):	4.173497071278891
Encrypted:	false
SSDEEP:	12:tcWD3lJwlsKUZCzbcZG75ud6nkU+Ec3bkskz1llhH7VuKO7S5U/OrjduImcA6:tcWwUxUZ4bc/Yn9iQr5Shbhh5U/O/d9
MD5:	B5DBABB411FCD0ECCB44FC67F2E8ECCA
SHA1:	D386ABBE3A2FAF02531FC231780C7BCE13BBDE54
SHA-256:	E3DFA30F8222ED7D179172C942CAA886FE4A6A7E895A478E8C5170CE9583A8D
SHA-512:	507C8360A3A8DD1BA3AE2EBF24881873886DFD79B358D50FDC3C78EEEC89A71CFFC39FC616C88361E23EF66DECCD53B24FE4A4D50B1BBC6E88F4421C18A7486
Malicious:	false
Reputation:	low
Preview:	<svg viewBox="0 0 32 32" xmlns="http://www.w3.org/2000/svg"><path d="M28.386 10.53c0 7.21-4.008 12.598-9.918 12.598-1.985 0-3.851-1.073-4.49-2.292 0 0-1.068 4.235-1.292 5.053-.796 2.888-3.137 5.777-3.318 6.015-.127.165-.407.113-.437-.105-.051-.368-.647-4.013.055-6.98612.364-10.016s-.586-1.174-.586-2.908c0-2.725 1.578-4.758 3.544-4.758 1.672 0 2.479 1.254 2.479 2.759 0 1.682-1.069 4.194-1.622 6.522-.461 1.95.978 3.541 2.901 3.541 3.482 0 5.827-4.474 5.827-9.773 0-4.028-2.712-7.044-7.648-7.044-5.574 0-9.049 4.158-9.049 8.803 0 1.602.473 2.732 1.213 3.605.339.402.387.563.264 1.025-.09.339-.29 1.152-.376 1.475-.122.466-.499.632-.92.46-2.567-1.048-3.764-3.861-3.764-7.022C3.614 6.261 8.017 0 16.75 0c7.019 0 11.636 5.077 11.636 10.53z" fill="#222"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\sharer[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	62458
Entropy (8bit):	5.4507025729600445
Encrypted:	false
SSDEEP:	1536:f9DklGtH+PQCX5Q68cgj2ILDYLaEavYd0SafjxBHIHck+vy9wEfYn54EO/9ielo5:3S
MD5:	750BCBE6963FA81DD0293CE18332F5C6
SHA1:	51B372429FE51BF40FB788E24214D983A0D51216
SHA-256:	10B643CC06A0011A418EBECFDF07A68E5782925D425FFE89CAF9BBA3ECBC0FBE
SHA-512:	C31B556DF4212641FF9DAEEB33C0166FB960A2DF6353BD12AF38921D21B44FDA1935B48B5310EA1A427E239AF96538076C86665BAF9BB9FE208CAF682324E1C
Malicious:	false
Reputation:	low
Preview:	<html><head><title>Redirecting...</title><script type="text/javascript" nonce="r2DCXqbv">/*!<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2911"+"&m="+m;},5000);if(top!=self){try{if(parent!=top){throw 1;}var si_cj_d=["a pps.facebook.com","apps.beta.facebook.com"];var href=top.location.href.toLowerCase();for(var i=0;i<si_cj_d.length;i++){if (href.indexOf(si_cj_d[i])>=0){throw 1;}}si_cj("3");}catch(e){si_cj("1 l");window.document.write("\u003Cstyle nonce="\u003Cqbv">body * {display:none !important;}\u003Cstyle>\u003Ca href="#" onclick="\u003Clocation .href=window.location.href" style="\u003Cdisplay:block !important;padding:10px!>Gehe zu facebook.com\u003Cva>");/*HB85UTqD*/}}()/)* */</script><script type="text/javascript" nonce="r2DCXqbv">window.location.replace("https://m.facebook.com/vsharer/vsharer.php?u=https://u00253A\u00252F\u00252Fwww.bustle.com\u00252Fentertainment\u

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\MEEXW4H4\sharer[2].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	62883
Entropy (8bit):	5.453045544367317
Encrypted:	false
SSDEEP:	1536:f8HcAjdr4sakNqNbKXgF3tXdGKrAV61jV+7Fg9qmaJsQpgOyVS6RiwDPfHwdpl5G:1
MD5:	5CB52243C3966706A4778D8B5B0B9DFA
SHA1:	539A285643F4897038EFC8DED17341B7559182FE
SHA-256:	415C16D1BE8743F75C155529E371A0D72C5B6DC454124DFC6A9033D284C1E036
SHA-512:	569BCA95C1081C0E31A68985059ABF52635ED6A2CB3CA5512EC54274E6542F68FD4FEEBA6D09B58C6EBF1AE8438FAE9DE7750A2A01820CB28F72A7719043372
Malicious:	false
Reputation:	low
Preview:	<html><head><title>Redirecting...</title><script type="text/javascript" nonce="4hOX1Exe">/*!<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2535"+"&m="+m;},5000);if(top!=self){try{if(parent!=top){throw 1;}var si_cj_d=["a pps.facebook.com","apps.beta.facebook.com"];var href=top.location.href.toLowerCase();for(var i=0;i<si_cj_d.length;i++){if (href.indexOf(si_cj_d[i])>=0){throw 1;}}si_cj("3 https://www.facebook.com/vsharer/vsharer.php?u=https://u00253A\u00252F\u00252Fwww.bustle.com\u00252Fentertainment\u00252Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant\u00253Futm_term\u00253Dshare");}catch(e){si_cj("1 https://www.facebook.com/vsharer/vsharer.php?u=https://u00253A\u00252F\u00252Fwww.bustle.com\u00252Fentertainment\u00252Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant\u00253Futm_term\u00253Dshare");window.document.write("\u003Cstyle nonce="\u003C1Ex

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\1d5c8fb4-91b5-470e-a6b4-97bdc1f03ac7-getty-139340878[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x639, frames 3

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\1d5c8fb4-91b5-470e-a6b4-97bdc1f03ac7-getty-139340878[1].jpg	
Category:	dropped
Size (bytes):	89178
Entropy (8bit):	7.976713483249943
Encrypted:	false
SSDEEP:	1536:hF749BtlWedAi2Bi8R9Lrha4dfquhMo1+sUU3U3wg10Q1mmqHmjJ6VG:hZ4XtlWIAi2E8LLrXYICTLw6Fj44
MD5:	D84A07E822C786011CCD7C38174EFF74
SHA1:	76EBC182EB3608088B7362C45FF5C4B036DEDCC3
SHA-256:	4AE2F2504B070304C992D84FD0E25E4B48B80215F41AE6291050A80B390D6284
SHA-512:	8AA4C7B37978E4925EEF00660A9D9CD9E2704B4C9E873CB5C3D794FFF67E48A380FD664D0A131FDDFF60D27F3A339A42ADBB78D62C2D3A86FF91B907243AC80
Malicious:	false
Reputation:	low
Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino....mntrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt...P...3desc.....lwpt..bkpt.....rXYZ.....gXYZ.....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....\$lumi.....meas.....\$tech...0....rTRC...<....gTRC...<....bTRC...<....text...Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZo...8.....XYZb.....XYZ\$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\8J5M6CLK.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	390494
Entropy (8bit):	5.461690997498249
Encrypted:	false
SSDEEP:	3072:bmCHE0r4zCONGD9UsjgCUdlFnKBD+jAP+N8SMHZcHabW7u2eSP:nERzCd9ljgCUdiBD+jAPpSX7u2eSP
MD5:	39A3A45AD499DDBC8B19272D78C15A6D2
SHA1:	BB3286F160C4AD74BDA084E125B600C3C24F7281
SHA-256:	656047689A4F8F5B0DD6C0A830367E5CC65EE3C2D2AAC91E7D1E78EC71005172
SHA-512:	64B09BE9ACBE2B6EF26781E0DD312BC0471006F20A112EE706670EB8E07B87B3380767C6D1E106A3C84E8E71D4AEF7BD2ADF249249279354C42BF73E8EEF40E7
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /> <meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="art icle:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle .com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bu stle.com/bustle/2021/HubPage-153fd9830e.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular- 017b0e

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\HubPage-153fd9830e[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.185480149629071
Encrypted:	false
SSDEEP:	24:/aDevLitqgVhtgmCUxpN+LhmYB5+fN7lrMgC+DhOcYPIN+qrITc97LkFc:/aD4xgtDPxaL1BYFUrMgRDhOcYN0TqFc
MD5:	E8149CBF266D3D9BEEAAAFD4621C67F9
SHA1:	D4FE0DC24DA4218DB6F452C2A568C3DBD436DE39
SHA-256:	11E4D5DD7A32CB36D589CE0311DAEAF7476EEDAD5E00A4F5F2099AE0188FF67
SHA-512:	00BD69AF651EBA08A834F44A6892996243D0009E7E0EA08C6F96D7FD0CA270F6844F498FF3B266CE26DC2A1A3FEF41EB9E92BEC5E60E183633012422123F56D7
Malicious:	false
Reputation:	low
Preview:	.Fzh{background-color:var(--slot2);color:var(--slot3);padding-top:var(--headerHeight)}.JDF.Fzh{padding-top:0}.EDs{color:inherit;font-family:var(--fontFamilyHeading);font- size:3.1rem;font-weight:var(--fontWeightRegular);line-height:1;margin:0 auto;max-width:calc(var(--maxContainerWidth) - var(--pageGutter)*2);padding:2rem 0 1rem; position:relative;text-align:right;width:calc(100% - var(--pageGutter)*2);z-index:var(--zIndexContent)}.EDs:after{background:currentColor;bottom:0;content:"";height:1px;p osition:absolute;right:0;width:100%}.FtB{pointer-events:none}.lZG.FtB{position:relative}.qCB{height:0;left:calc(var(--pageGutter) - 8px);pointer-events:all;position:absol ute;top:3.5rem;width:277px;z-index:var(--zIndexOverContent)}.qCB svg{fill:currentColor;left:0;position:absolute;right:0;top:0}.BfG{font-family:var(--fontFamilySansSerif); font-size:.625rem;left:calc(var(--pageGutter) - 8px);letter-spacing:-.1px;opacity:.6;position:absolute;text-transform:uppercase;top:2.25rem;z-index:var(--zIndex

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\ListiclePage-96bbf86d27[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\ListiclePage-96bbf86d27[1].css

Size (bytes):	1668
Entropy (8bit):	5.27502243202118
Encrypted:	false
SSDEEP:	24:oqgcitqgs7S6jiCSintdg56hxf6jzTSi4StkxxRrXCSKPytvOKuYE/t:3BDiChtd9hxxPh4DdCLPvKLO
MD5:	F8EFED3D0F49406C6151B4DFFB40A688
SHA1:	2E6E20A8E19E176A3176B3C038CDDC38AE31013F
SHA-256:	8AD461DB92F784A11A38E1B0B818DB1D17D058DED9E3D6E907531B01C9FB9527
SHA-512:	F796825D34A5E2B27CD913D2358024D33E397C66425AC295C7C46759EE8F678B0B41FE9B2DDCDCED763154FFFE7135776286249A3BA783DE68E0890C20223676
Malicious:	false
Reputation:	low
Preview:	.Kzu{background:var(--slot2);color:var(--slot1);overflow-x:hidden;position:relative}.hew{align-items:baseline;display:flex;flex-wrap:wrap;justify-content:space-between}.wMG{margin:1.5rem 0}.tRu{margin:0 auto;max-width:calc(var(--maxContainerWidth) - var(--pageGutter)*2)}.NW_{color:var(--slot1);display:grid;font-size:1.1rem;grid-template-columns:[full-start] var(--pageGutter) [main-start] minmax(calc(63% - 3.75rem),var(--maxBodyWidth)) [main-end] var(--pageGutter) [full-end];line-height:1.75;margin:-1px auto 0;position:relative;word-break:break-word}.WIN{margin:2rem 0 0}.NW_>{*{grid-column:main}.FLb{display:none}@media (min-width:768px){.hew.ds{flex-direction:row-reverse}.tRu{padding:0}.NW_{font-size:1.15rem;grid-template-columns:[full-start] minmax(var(--pageGutter),1fr) [main-start] minmax(65%,var(--maxBodyWidth)) [main-end] var(--pageGutter) [full-end];margin:0}}@media (min-width:1025px){.hew{left:0;margin:0 auto;position:absolute;right:calc(var(--maxContainerWidth) - 344px);width:34

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\errorPageStrings[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNIX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
Preview:	//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";...var L_REFRESH_TEXT = "Refresh the page.";...var L_MOREINFO_TEXT = "More information";...var L_OFFLINE_USERS_TEXT = "For offline users";...var L_RELOAD_TEXT = "Retype the address.";...var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";...var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";...var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";...var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";...//used by invalidcert.js and hstsцерterror.js...var L_CertUnknownCA_TEXT = "Your PC doesn't trust this website's security certificate.";...var L_CertExpired_TEXT = "The website's security certificate is not yet valid or has expired.";...var L_CertCNMismatch_TEXT = "The hostname in the website's security certificate differs from the website you are trying to visit.";...var L

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\facebook-a5deab0bdf[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	141
Entropy (8bit):	4.955724428205325
Encrypted:	false
SSDEEP:	3:tlsqDmJS4RKb5ykKcvUJWVH9urcHeTGI+Tn6Flcqdp4qGXb:tl9mc4sl3U4H0qFlsn6FWqR6
MD5:	A709A93BDDDDAA1D4FA3ABA5CE6C7607
SHA1:	88D86E12A2A11151BCCDD1D4B4C74F98C5AD6312
SHA-256:	687ACF1D718343C9219C2D04428B70FE060F40FB54B51A1CAAE069B067B83DD3
SHA-512:	E7EA383BEB0A974B74D5C93F96D28DCF39CF112F615B3284737D9654B15B5C5FEC895909508F73C80C39E7C9937D6F0FD07D539FEB47DF243435B2E7E810E041
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 16 30"><path d="M16 6h-6v4h6v6h-6v14H4V16H0v-6h4V8c0-4 4-8 8-8h4v6z" fill="#222"/></svg>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\main-944316c15d[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	139863
Entropy (8bit):	5.47836621807488
Encrypted:	false
SSDEEP:	3072:Y93FvSobz/hzXzy241UBuhUROnTrsirew3HwUpocgJ:C5bDDZsCMnTpyw3QUpocgJ
MD5:	F50421B97D5CD7B6D882C9CF09F006D7
SHA1:	07DB10D2E37E06F08B735ABCF62F1CC5A97BAEEF

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\main-944316c15d[1].js	
SHA-256:	F95AB662735B540EEB1F176E06E8380379843D6D5CF2BF9BE8F0B3DE800F0889
SHA-512:	5C664D365CF777C37609B10C374F2F8276D21F7B5C02AC604DBF09E7BFEDCE0E45A38F4AD1296857BC7F87CCBCE24F53C0A87D786D40C8CEF8D6F175039FC7C
Malicious:	false
Reputation:	low
Preview:	((=>{"use strict";var e,t,n,o,s={3920:(e,t,n)=>{n.d(t,{Z:()=>o});const o="47695f29abfbb904a1546b9d5f2c3dc60ef69bd0f4cb3d63e2ea539051911412"},2990:(e,t,n)=>{n.d(t,{Z:()=>c});const o="sqO",s="wGs",r="ooy",i="EN_";var a=n(2779),d=n.n(a),l=n(3847).h;function c(e){return l("div",{className:d()(o,e.className)}),l("div",{className:d()(r,s)}),l("div",{className:d()(i,s)}))}}},175:(e,t,n)=>{n.d(t,{Z:()=>s});var o=n(3847).h;function s(e){const{className:t,style:n={}}=e;return o("svg",{className:t,style:n,xmlns:"http://www.w3.org/2000/svg",viewBox:"0 0 2651 719"},o("path",{id:"M2637 572c-130.8 142.4-299.2 81.1-307.7-123H2643c11-89-25-269-205-269-149 0-242 121-242 265 0 155 106 274 246 274 79 0 169-56 209-130l-14-17zm-211-343c51 0 82 64 86 176h-182.2c6.1-101.9 45.1-176 96.2-176zM397 345v-2c79-22 142-82 142-167C539 80 459 9 309 9H1v32c61 5 68 8 68 42v554c0 33-7 36-69 40v32h338c150 0 231-74 231-180 0-81-47-157-172-184zM214 51h69c79 0 109 59 109 134 0 83-37 138-117 138l-61-1V51zm201 478c0 71-23 139-121

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\met-gala-2021-red-carpet-best-dressed[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	236174
Entropy (8bit):	5.555879100648826
Encrypted:	false
SSDEEP:	1536:YBMCWXzSWH//zAMzGTDJSQbyvfrSEZc/64hKLw7n0UhvQHLsek:YOyapzGTd7yvJ3pLVUhvQwek
MD5:	5565E8234AB409315965AC2E12C71EAC
SHA1:	6E265121344B9C054031A41CA23A077FE0C4EB42
SHA-256:	020FA03FD24FF4BD3B690DDD227101C723FAB79108E149EA20E5A1C093852903
SHA-512:	8D9362C7D494DD47AF54D1D959D5C7774D24BD2048F9B486D7D72A5498D8CEE9C581305309E316D49A8F15C9D3C818565212D724EDECD453C62F240047F5E22
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/ListiclePage-96bbf86d27.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-0

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\PSUEOSZZ\twitter-21b286c13f[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	613
Entropy (8bit):	4.180992365831918
Encrypted:	false
SSDEEP:	12:t41W0QRriSEgPFqXi/kGI3zVhKxScKnRacsUPxF6:t41PYNsi/kGI3Bn3R3F6
MD5:	791ACD3459133F4F68F920BAD15834BF
SHA1:	2F3734B8AFFC0B53F13D649F8D7D7B6292224076
SHA-256:	0B8FD1E2A134A0B66A7915498D2238744D52C5B3EC9C4D27FA9DE932B0BB4842
SHA-512:	DCFC75DC2AEFA59D18284F69B783737F111C8C32B09CFB6BF87D50B77E1DABAD55876C3FA3D11EF8408EF65A114F546D9E57DF9E14A7205BDDFBDAAA61AF693
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 300 265.5"><path d="M288.3 52.2c-10.1 4.5-20.9 7.5-32.2 8.8 11.6-6.9 20.5-17.9 24.7-31-10.8 6.4-22.8 11.1-35.6 13.6a55.92 55.92 0 0 0-40.9-17.7c-31 0-56.1 25.1-56.1 56.1 0 4.5 8.7 1.5 12.8-46.6-2.3-87.9-24.7-115.6-58.6-4.8 8.3-7.6 17.9-7.6 28.2 0 19.5 9.9 36.6 25 46.7-9.2-3-17.8-2.8-25.4-7v.7c0 27.2 19.3 49.8 45 55-4.7 1.3-9.7 2-14.8 2-3.6 0-7.1-.4-10.6-1 7.1 22.3 27.9 38.5 52.4 39-19.2 15-43.4 24-69.7 24-4.5 0-9-.3-13.4-.8 24.8 15.9 54.3 2 5.2 86 25.2 103.2 0 159.6-85.5 159.6-159.6 0-2.4-.1-4.9-.2-7.3 10.8-7.9 20.3-17.8 27.9-29.1z" fill="#222"/></svg>

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ812OL4\AuthorPage-2a82eded97[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19680
Entropy (8bit):	5.592829669492504
Encrypted:	false
SSDEEP:	384:+1Yp9umgAZMmfl1b5piVleYnMCAkKctPPnva607ZwqxHOFGJVA06IPoXtlwEKCpF:+19mg8HPjiVldnMCAk5i607ZwMuz0yoy
MD5:	CB65841BA1E2FF7C6A2BA748E93DF2BD
SHA1:	F1D247C354B60D95E8740B450EC3284E05D55745
SHA-256:	9ECF6E94F82C10234820D4F3D1E13B4AFBDB9C3C3868CBA6BA36154F0871C3D7
SHA-512:	66178563E643A8B32DD5E2E345D1ACF0F4763053AC39F259C0C47B3CF8593F4AF1B5EDDE74F419B3CE675A9D3FD8870B79ADCB3CC615D541C41043CEB7F22B5

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\AuthorPage-2a82eded97[1].js

Malicious:	false
Reputation:	low
Preview:	"use strict";(globalThis.webpackChunk=globalThis.webpackChunk []).push([[479],[2385:(e,t,a)=>{a.d(t,{Z:()=>Z});var r=a(565);const o="FxZ",n="uIY",s="rAj",l="wjn",i="yrZ",c="rCM",p="Ael",u="uQS",d="uTb",m="cRS",f="tBL",y="Kto",v="ZVN";var b=a(492),h=a(9023),g=a(2779),O=a.n(g),P=a(3847).h;var w=a(3847).h,C=Object.defineProperty,N=Object.defineProperties,j=Object.getOwnPropertyDescriptor,S=Object.getOwnPropertySymbols,x=Object.prototype.hasOwnProperty,k=Object.prototype.propertyIsEnumerable,l=(e,t,a)=>t in e?C(e,t,{enumerable:!0,configurable:!0,writable:!0,value:a}):e[t]=a;const z={author:{emphasizeName:function(e){const{card:t}=e,{author:a}=t [],{name:r,bio:g,twitter:w,instagram:C,facebook:N,primaryMedia:j,url:S}=a [],x={facebook:P("svg",{xmlns:"http://www.w3.org/2000/svg",viewBox:"0 0 16 30"}),P("path",{d:"M16 6h-6v4h6v6h-6v14H4V16H0v-6h4V8c0-4 4-8 8-8h4v6z"}))},twitter:P("svg",{xmlns:"http://www.w3.org/2000/svg",viewBox:"0 0 300 265.5"}),P("path",{d:"M288.3 52.2c-10.1 4.5-20.9 7.5-32.

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\CardPage-99d9dcad6b[1].css

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	dropped
Size (bytes):	1680
Entropy (8bit):	5.243081416671087
Encrypted:	false
SSDEEP:	24:ggkitqg11e7SBS3lGjC5intLKKyEz9s6jzTSi4SmkkaSmXCSKpNnLV:gLMiaCl6iChtLKJgzPh40S+CLPNLV
MD5:	757353D114C61E45487D6EEB66C9B90B
SHA1:	23E741436B64AA5D55FC58D85BD39502EBFC969
SHA-256:	E44B21F03F79C3C584211257DD0CBFA0D311B1F02332A63C1940D22C2270CF75
SHA-512:	EED49BEA8DCBED09E87056F69154DE38C4FE5995483A4F05D6F54A5E9631ECB70B115DCE96A72D5FA637913C679F7F8DE60DCF5BA948EA4D20000505ED8410B
Malicious:	false
Reputation:	low
Preview:	.oBg{background:var(--slot2);color:var(--slot1);position:relative}.UfH{align-items:baseline;display:flex;flex-wrap:wrap;justify-content:space-between}.lno{margin:1.5rem 0}.tnD{margin:0 auto;max-width:calc(var(--maxContainerWidth) - var(--pageGutter)*2);padding-top:1px}.AjL{color:var(--slot1);display:grid;font-size:1.1rem;grid-auto-rows:min-content;grid-template-columns:[full-start] var(--pageGutter) [main-start] minmax(calc(63% - 3.75rem),var(--maxBodyWidth)) [main-end] var(--pageGutter) [full-end];line-height:1.75;margin:-1px auto 0;position:relative;word-break:break-word}.AjL>*[grid-column:main].gia{display:none}.bHH{height:1px;width:1px}.DzI{grid-column:full;overflow:visible}.Gjd{grid-column:full;margin-bottom:var(--minAdSpacing);width:100vw}.DzI>div{max-width:300px;overflow-x:hidden}@media (min-width:768px){.UfH.qUD{flex-direction:row-reverse}.tnD{padding:0}.AjL{font-size:1.15rem;grid-template-columns:[full-start] minmax(var(--pageGutter),1fr) [main-start] minmax(65%,var(--maxBodyW

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\CardPage-e651e53eed[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	125406
Entropy (8bit):	5.521354177243122
Encrypted:	false
SSDEEP:	1536:edN3pgkc1dEI/V5L9tPy8GhU1Hdj+C6H5jfkZq8k3nP6AfqcCKEa9sYrjqK8fxKW:Bb6ycPnpKSTB4+uE/OfojRytV
MD5:	93D3853926205422301B2B98F7238C65
SHA1:	679BC637F8FB8E6D87153DDBB917DAA555CB7511
SHA-256:	615E6B509E7FB16804573EE2559D4580D356AE3899D41DAE86BE09E5993FA25A
SHA-512:	A58F241336FFFE0F14FC59FC665363DD5BA3E73FA5113F34B7BA8090B34AC0BA335FCDFDE8D95896E86730509681209FC7FFA0DE89DF943ADA283BF2553C5F3
Malicious:	false
Reputation:	low
Preview:	"use strict";(globalThis.webpackChunk=globalThis.webpackChunk []).push([[483],[7925:(e,t,r)=>{r.d(t,{Z:()=>});var o=r(2335);const a={sponsorHolder:"Jjo",sponsor:"KSr",sponsorName:"cCz",sponsorBy:"cAx",sponsorIntro:"lIz",sponsorImage:"PgK",inHub:"FDR",inStorefront:"UJX",wrapped:"eFu";var n=r(2779),i=r.n(n),s=r(3847).h,function l(e){const{className:t,inHub:r,inStorefront:n,modelID:l,sponsorText:c,wrapped:p}=e,d=i()(a.sponsorHolder,t,p&&a.wrapped,r&&a.inHub,n&&a.inStorefront);return c?s("div",{className:d},s("span",{className:a.sponsorBy},c)):s(o.RW,{className:d,style:a.modelID:l})}},6550:(e,t,r)=>{r.d(t,{Z:()=>c});const o="wVs",a="yKE",n="OnM";var i=r(2779),s=r.n(i),l=r(3847).h,function c(e){const{parent:t,inFeature:r}=e [],{title:i,path:c,sponsored:p}=t {};return l("a",{className:s()(o,r&&n),href:c,p&&l("div",{className:a},"Sponsored"),i)}),7201:(e,t,r)=>{r.d(t,{Z:()=>c});const o="JAm";var a=r(9580),n=r(2779),i=r.n(n),s=r(3847).h;const l=["facebook","twitter","copyLink","mailto"];

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\HubPage-537dd4e27b[1].js

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	146725
Entropy (8bit):	5.4797428685487315
Encrypted:	false
SSDEEP:	3072:W8JQL2J6s8XCCk9aguTudfwWNxvVHIUtajftl2:HGL2J6s8XCCFuOPZtjp
MD5:	13931017AE892A6E6C610F1EF2072A85
SHA1:	DBDC3D57FD43BFB5E5C678D5272AA577D0678AC9
SHA-256:	69ED2E23817E399431D37D8962D320772E0C47B93ED394DA54065E4335DEFCE2
SHA-512:	98790ED51CF979A137B4C4DB5F5C8EBA9C272425ABA4A6A3150814BC431CA0C5D87B3AF92E87BEF5A82E2C3A0BBD1E0B402EC8DEC35023CFB0C2155DBD412D7
Malicious:	false

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\HubPage-537dd4e27b[1].js	
Reputation:	low
Preview:	"use strict";(globalThis.webpackChunk=globalThis.webpackChunk []).push([([157],{7925:(e,t,r)=>{r.d(t,{Z:()=>{}});var a=r(2335);const o={sponsorHolder:"Jjo",sponsor:"KSr",sponsorName:"cCz",sponsorBy:"cAx",sponsorIntro:"IzZ",sponsorImage:"PgK",inHub:"FDR",inStorefront:"UJX",wrapped:"eFu"};var n=r(2779),i=r.n(n),s=r(3847).h,function l(e){const{className:t,inHub:r,inStorefront:n,modelID:l,sponsorText:c,wrapped:d}=e,p=i()(o.sponsorHolder,t,d&&o.wrapped,r&&o.inHub,n&&o.inStorefront);return c?s("div",{className:p},s("span",{className:o.sponsorBy},c)):s(a.RW,{className:p,style:o,modelID:l})}}),2368:(e,t,r)=>{r.d(t,{Z:()=>c});var a=r(2779),o=r.n(a);const n="laD",i="Neu";var s=r(3914),l=r(3847).h,function c(e){const{className:t,authors:r}=e;return l("div",{className:o()(n,t)},l("span",null,"By "),r&&(0,s.WD)(r.map((e=>const{path:t,url:r}=e,a=t r;return l(a?"a":"span",{key:a,href:a.className:i},e.name)))))),9240:(e,t,r)=>{r.d(t,{Z:()=>B});var a=r(2779),o=r.n(a),n=r(7991),i=r(7695);const s="fzx"

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\cdac0f30-47b2-40bb-aed0-56e8870a2265-screen-shot-2018-07-08-at-11127-pm-1[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x475, frames 3
Category:	dropped
Size (bytes):	64256
Entropy (8bit):	7.970513348077674
Encrypted:	false
SSDEEP:	1536:hlfX/Gc0o5Zfz/Kn25Bq2PN/pgLuauO6TLKbc+LcTW:hlWJo5Zfz/Kn2m22uaGTeuS
MD5:	3C6DE36C9E02F08893AD9F4BFB93C758
SHA1:	F29A807DA56AB58BCFB621D802473EDAA1C07DA1
SHA-256:	F561F477ACD0CCEC82327C59D8BFF9E6316A8D176913BFF40567338B25567857
SHA-512:	CDE12C63CAB3CA3409F1265DAE8870331DE4233955EE6100757C71E4FCC87C8900FD8768D3F95DA8F59C1A1138362411BB5212EC086DF26ED6656AC7A4B5566
Malicious:	false
Reputation:	low
Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino.....mnrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt..P...3desc.....lwtp..bkpt.....rXYZ.....gXYZ.....bXYZ...@....dmnd...T...pdmdd.....vued...L...view.....\$lumi.....meas.....\$tech...0....rTRC...<....gTRC...<....bTRC...<....text...Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZo...8.....XYZb.....XYZ\$.desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\lef1ae7f7-4dec-4534-b086-3c906f522c23-getty-1340147774[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, progressive, precision 8, 800x533, frames 3
Category:	dropped
Size (bytes):	69855
Entropy (8bit):	7.972345861494414
Encrypted:	false
SSDEEP:	1536:hYUefxMH59PHSebe3xD8287lmJI2YSUHmUm1tCBx9sLN2WkkKZx:hYUQxMZBQBy7IKIejDCBx9HkKZx
MD5:	697D95A6FD1D64534C470DAA16AFF7CC
SHA1:	C5E414D17A1CCB9B3FD49061A6BB872FC23AF2CE
SHA-256:	7F19488CB35A22A83E8D461F189EE743D6E23C83F495FD6307C2B5AA8358D1C7
SHA-512:	D43C00D43DDDEE20162D01902216852897CC4D449E024B56B847704FC3493B0721AA7BFFFC4FDFBADAe4BC213FF6D0B08D2F1283FC56CE9483428A3FC85FB90
Malicious:	false
Reputation:	low
Preview:	JFIF.....H.H.....XICC_PROFILE.....HLino.....mnrRGB XYZ1..acspMSFT....IEC sRGB.....-HPcprt..P...3desc.....lwtp..bkpt.....rXYZ.....gXYZ.....bXYZ...@....dmnd...T...pdmdd.....vued...L...view.....\$lumi.....meas.....\$tech...0....rTRC...<....gTRC...<....bTRC...<....text...Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZQ.....XYZXYZo...8.....XYZb.....XYZ\$.desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....Reference Viewing Condition in IEC61966-2.1.....Reference V iewing Condition in IEC61966-2.1.....

C:\Users\user1\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	46937
Entropy (8bit):	5.5403009125913485
Encrypted:	false
SSDEEP:	768:KqSR08h8YP7UcPAqTLZBNVDxkkJJi/eTyEL69kPTX3TgxFL/YYRF1mq;CBrx3i/eTnHTgxFLI
MD5:	115F229B9F255E22C6EA23A4AE09D803
SHA1:	35E8A3CD3907522B85ED6D26455F2F2A87A2267B
SHA-256:	244E7BBA8EBBD8F299A1D1344BF1F0C0C2EE59416AEE332ABBD476EEC4B2AFD2
SHA-512:	EAAA4DD8E50EE4CA7A33644C6E6B9D28BDF62261A86487D5086E560FD04978B724F35E6A3C7A0B7887A6D994FEDA585AAB97D42539D64D37D66A293D9134E3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant[1].htm

Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\hailey-bieber-met-gala-2021-look[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	32046
Entropy (8bit):	5.484291828390955
Encrypted:	false
SSDEEP:	768:KqSR08hYP7UcPAqTejBI+GjkkAP0L69kPx/p1mq;BijQWZ
MD5:	A380E81CE927040A7F221053310E4FAB
SHA1:	543D7F4E786214F95CF8FC7A476E1AE519C43A4D
SHA-256:	4EA79AE128A9DC742422B0235950CA32B1F5584F849848F88C556296A673CF40
SHA-512:	350D614DFC43455659FBFBE92794E73E088577C73A1CF8C471C9538A1A8622A1C371DB502FA19D4D32D8EC788DA903B2ACEA612E918C9A82D814309FC9BF69E
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8TAGGGVWvnyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFD8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
Preview:	...function isExternalUrlSafeForNavigation(urlStr){...var regEx = new RegExp("(http(s?)[fptp]file: / ", "i");...return regEx.exec(urlStr);...}.function clickRefresh(){...var location = window.location.href;...var poundIndex = location.indexOf("#");...if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))...{...window.location.replace(location.substring(poundIndex+1));...}.function navCancelInit(){...var location = window.location.href;...var poundIndex = location.indexOf("#");...if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))...{...var bElement = document.createElement("A");...bElement.innerText = L_REFRESH_TEXT;...bElement.href = 'javascript:clickRefresh()';...navCancelContainer.appendChild(bElement);...}.else...{...var textNode = document.createTextNode(L_RELOAD_TEXT);...navCancelContainer.appendChild(textNode);...}.function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\justin-bieber-hailey-baldwins-relationship-timeline-shows-how-this-couple-went-from-pda-to-rumored-engagement-so-fast-9692470[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	129639
Entropy (8bit):	5.41752825202691
Encrypted:	false
SSDEEP:	1536:hcBIKIU7xH90bTMijLcYgC4ENZ9Z03prCjQi2ZAE5+h:61xxH9uTMikjC4ENZ9Z03puQi2ZAES
MD5:	46C93786B0F16D48DD576125C5EF55EE
SHA1:	E6A2072A9FEE50F982E0DA9BBBC2D721C5229FDD
SHA-256:	453078B761A2C348DB23B219D9EB8E32AE53B9B7D862E4CBB9DFACE98BE25418
SHA-512:	D044668A43CB83FDE4BA11597C3CD86122931FC7D6FA566DF32EE382F55058582BCE9898C0592219873551AA7D18A3D48A343D078D67F65CE5C834A40307F346
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\justin-bieber-hailey-baldwins-relationship-timeline-shows-how-this-couple-went-from-pda-to-rumored-engagement-so-fast-9692470[1].htm

Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0
----------	--

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\justin-bieber-net-worth-hailey-baldwin-earnings-money[1].htm

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	67320
Entropy (8bit):	5.404785332269466
Encrypted:	false
SSDEEP:	768:KqSR08h8YP7UcPAqTsaBWcRjkk0QcZG15m/X8xyZNL69kP2YVIOiJj/CYUoOTVt:mBZjgZG15MXmksYVlz/dmXwBsBZ
MD5:	214A13E8FAC1C058F1BC09852C11D28C
SHA1:	9F911A3D749FC852DE54860C0947B74AEE17A6CC
SHA-256:	7A0FAF9BC52F0CE1E5FDD4CB9879DAED3EDA7A70A0253F4A97FB7E8B9978F9F9
SHA-512:	65349C2D88C1E1BE27A2BF6DD23C138A2E7546CD838DA534EE974ECDD7E1466C9CEB7937848B0E576F0BF640F2215655BA51527B79E08FC3DE4EBF380FDBB5D5
Malicious:	false
Reputation:	low
Preview:	<!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><meta property="og:site_name" content="Bustle" /><meta property="article:publisher" content="https://www.facebook.com/bustledotcom" /><link rel="apple-touch-icon" href="https://cdn2.bustle.com/bustle/2021/icon-c030f451b3.png" /><link rel="alternate" type="application/rss+xml" href="/rss" /><link rel="preconnect" href="https://cdn2.bustle.com" crossorigin /><link rel="preconnect" href="https://imgix.bustle.com" crossorigin /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/common-d9e5af7042.css" /><link rel="preload" as="style" href="https://cdn2.bustle.com/bustle/2021/CardPage-99d9dcad6b.css" /><link rel="preload" as="font" type="font/woff2" href="https://cdn2c.bustle.com/bustle/2021/untitled-sans-web-regular-017b0

C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\WJ8I2OL4\search-f909203196[1].svg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	326
Entropy (8bit):	4.699122630329575
Encrypted:	false
SSDEEP:	6:tnrRNAojo9mc4slmYjvt9TG6k9pDsoHTP4SxVWuSluCc0VuSfFEzSkFE5RBuBKf:trrijYIIIT648TP4SxVXu8QSKzkDBue
MD5:	1D915DCC4CFAD34232B64B4487850F7B
SHA1:	9F9865227678E8F7D81AA87B6EB532973E3F90E0
SHA-256:	2605332E392A83121026DEF03C3279AF6C91D71E0ECF74AA358740D765481EBB
SHA-512:	8570BCA2AE08C6518C19B2042F3A3D05F53E3CCAB6F301BF50765B4630383C00A5A64E5617EFF6C3C45D603A84C7AB9C7B864710F018A4E24CC425AB813C6B9
Malicious:	false
Reputation:	low
Preview:	<svg width="27" height="26" xmlns="http://www.w3.org/2000/svg"><path d="M10.5 0C16.299 0 21 4.701 21 10.5c0 2.23-.695 4.297-1.88 5.998l7.047 7.048-2.121 2.121-.977-6.975A10.456 10.456 0 0 1 10.5 21C4.701 21 0 16.299 0 10.5S4.701 0 10.5 0zm0 3a7.5 7.5 0 1 0 0 15 7.5 7.5 0 0 0 0-15z" fill="#2A2A2A" fill-rule="evenodd"/></svg>

C:\Users\user\AppData\Local\Temp\~DF6842BD4B25F7601B.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	440547
Entropy (8bit):	1.0414870972026575
Encrypted:	false
SSDEEP:	12288:hKr0KRKr0KRAa0KrmjESS9UUYYUUUUUy0Qu4VAUUUUUUUUUUUUUUUUUUUUUw:hKr0KRKr0KRAa0KrmjESS9UUYYUUUUH
MD5:	401AEC06BA97D812AD300E4A78CEA6E8
SHA1:	5EF855255CC5741BBF481B248DB07A9CDFA695BC
SHA-256:	EB3340F8C9C0087D0456C7E9591871E7EE5089DD3C2667699B0ABD658557987F
SHA-512:	DEC14C18B852EE02B10D551168F5B6DFB95A66277D7335BC7E557A874DD593B2E0304FF91E2B1A8A32754BC5420E5F85AEC50AC98B2CD8429A72BC69C34E36E
Malicious:	false
Reputation:	low

C:\Users\user1\AppData\Local\Temp\~DF6842BD4B25F7601B.TMP

Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....
----------	--

C:\Users\user1\AppData\Local\Temp\~DF699F1BF376DA715F.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.4753324855706353
Encrypted:	false
SSDEEP:	24:c9lH9lH9lIn9lIn9lofF9lo99lWINYyGDADh6Cy6X:kBqolGYllc0kX
MD5:	5507547DC2CFEFE32C6B743EA1276687
SHA1:	EA99744F1886A5F1FA50E9CA2C50C0C14B8875D0
SHA-256:	248461C5363E1E83A0464A256F7DC81083013904B28780536643CE77EDD7BA17
SHA-512:	D38CA33EA5F9397733EBBBCDDC8195CB6F7D2B9111274E37B9D6813F0AF08EFC057E29612779950ADE2697D2FA2DB570BA4E077B23346FEC0791F705BE86DE 5
Malicious:	false
Reputation:	low
Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....

C:\Users\user1\AppData\Local\Temp\~DF8FB3155CF03C945B.TMP

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lH9lH9lIn9lIn9lRx/9lR.J9lTb9lTb9lISSU9lSSU9laAa/9laA:kBqoxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	*%..H..M..{y..+0...(.....*%..H..M..{y..+0...(.....

C:\Users\user1\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\28c8b86deab549a1.customDestinations-ms (copy)

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	3440
Entropy (8bit):	3.1939275463746135
Encrypted:	false
SSDEEP:	48:/di1PUIJC9GrIoVAsASFUdi1PUIJh683GrIoVAczH:wPUB9S1AJSPUY3S1AG
MD5:	6ABB7FDC15219BCB78254ABB332889D0
SHA1:	05C13167AD04B889F86313ED153BC8067A42BA11
SHA-256:	123C04FF6D4F9E4EABE4B087DF5284DA21AF16737CF16F1CCE06AC6D8B3186BA
SHA-512:	82DC80A6E12D6DA2BB3ED6E806BF378308C2E14F997CE4E2CB94529DBB3D9E9AFE7C496A564759E51120584BA707AF31FAC5415F70B1E9F57DF0CC16C40E48 A
Malicious:	false
Reputation:	low
Preview:	FL.....F.@.....@.>....@6.....?c.....P.O. :i.....+00.../C:\.....1.....>Q=w..PROGRA~1.t.....L>QCw...E.....J...P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.1....l.1.....L.J..INTERN~1.T.....L.0Sjk.....i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r....f.2.....L.9 .iexplore.exe..JL.J0S{k....R.....x.....i.e.x.p.l.o.r.e...e.x.e.....^.....-.....]......k.#1.....C:\Program Files\internet explorer\iexplore.exe....-p.r.i.v.a.t.e...C:.\W.i.n.d.o.w.s.\S .Y.S.T.E.M.3.2.\I.E.F.R.A.M.E...d.l.l.....%SystemRoot%\SYSTEM32\IEFRAME.dll.....%S.y.s.t.e.m.R.o.o.t.%\S.Y.S.T.E.M.3.2.\I

C:\Users\user1\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\9WZVNGXXHWL1MKW36ILF.temp	
Process:	C:\Program Files\internet explorer\explore.exe
File Type:	data
Category:	dropped
Size (bytes):	3440
Entropy (8bit):	3.1939275463746135
Encrypted:	false
SSDEEP:	48:/di1PUIJC9GrIoVAsASFUdi1PUIJh683GrIoVAczH:wPUB9S1AJSPUY3S1AG
MD5:	6ABB7FDC15219BCB78254ABB332889D0
SHA1:	05C13167AD04B889F86313ED153BC8067A42BA11
SHA-256:	123C04FF6D4F9E4EABE4B087DF5284DA21AF16737CF16F1CCE06AC6D8B3186BA
SHA-512:	82DC80A6E12D6DA2BB3ED6E806BF378308C2E14F997CE4E2CB94529DBB3D9E9AFE7C496A564759E51120584BA707AF31FAC5415F70B1E9F57DF0CC16C40E48A
Malicious:	false
Reputation:	low
Preview:	FL.....F.@..@>...@6.....?c.....P.O.+00.../C:\.....1.....>Q=w.PROGRA~1.t.....L>QCw...E.....J...P.r.o.g.r.a.m. .F.i.l.e.s...@.s.h.e.l.l.3.2...d.l.l.,-2.1.7.8.1.....l.1.....L.J..INTERN~1..T.....L.0Sjk.....i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r.....f.2.....L.9 .i.e.p.l.o.r.e..JL.J0S{k....R.....X.....i.e.x.p.l.o.r.e...e.x.e.....^.....-.....]......k.#1....C:\Program Files\internet explorer\explore.exe....-p.r.i.v.a.t.e...C:\.W.i.n.d.o.w.s\..S .Y.S.T.E.M.3.2\..I.E.F.R.A.M.E...d.l.l.....%SystemRoot%\SYSTEM32\IEFRAME.dll.....%S.y.s.t.e.m.R.o.o.t.%\..S.Y.S.T.E.M.3.2\..l

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 16, 2021 06:27:55.819098949 CEST	192.168.2.3	8.8.8.8	0xe2dc	Standard query (0)	www.bustle.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:56.882074118 CEST	192.168.2.3	8.8.8.8	0x97b3	Standard query (0)	cdn2.bustle.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:56.883378029 CEST	192.168.2.3	8.8.8.8	0x16c	Standard query (0)	imgix.bustle.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:24.202480078 CEST	192.168.2.3	8.8.8.8	0x7d9b	Standard query (0)	www.bustle.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:33.361450911 CEST	192.168.2.3	8.8.8.8	0xe05e	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:33.673270941 CEST	192.168.2.3	8.8.8.8	0x5b3f	Standard query (0)	m.facebook.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:09.280736923 CEST	192.168.2.3	8.8.8.8	0x34ee	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:09.525863886 CEST	192.168.2.3	8.8.8.8	0x454f	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:16.877465963 CEST	192.168.2.3	8.8.8.8	0xc996	Standard query (0)	help.twitter.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.442914963 CEST	192.168.2.3	8.8.8.8	0x8339	Standard query (0)	platform.twitter.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.854393959 CEST	192.168.2.3	8.8.8.8	0x6fe1	Standard query (0)	twitterinc.tt.omtrdc.net	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.083219051 CEST	192.168.2.3	8.8.8.8	0x410f	Standard query (0)	fonts.twitter.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 16, 2021 06:29:19.506810904 CEST	192.168.2.3	8.8.8.8	0x86f1	Standard query (0)	resources.digital-cloud-prem.m edallia.com	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:19.818598986 CEST	192.168.2.3	8.8.8.8	0xc565	Standard query (0)	udc-neb.kam pyle.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 16, 2021 06:27:55.852236032 CEST	8.8.8.8	192.168.2.3	0xe2dc	No error (0)	www.bustle.com		52.222.214.86	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:55.852236032 CEST	8.8.8.8	192.168.2.3	0xe2dc	No error (0)	www.bustle.com		52.222.214.69	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:55.852236032 CEST	8.8.8.8	192.168.2.3	0xe2dc	No error (0)	www.bustle.com		52.222.214.53	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:55.852236032 CEST	8.8.8.8	192.168.2.3	0xe2dc	No error (0)	www.bustle.com		52.222.214.36	A (IP address)	IN (0x0001)
Sep 16, 2021 06:27:56.918745995 CEST	8.8.8.8	192.168.2.3	0x97b3	No error (0)	cdn2.bustle.com	cdn2.bustle.com.cdn.clou dfare.net		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:27:56.920298100 CEST	8.8.8.8	192.168.2.3	0x16c	No error (0)	imgix.bustle.com	typeset-beta.imgix.net		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:27:56.920298100 CEST	8.8.8.8	192.168.2.3	0x16c	No error (0)	typeset-be ta.imgix.net	dualstack.com.imgix.map. fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:27:56.920298100 CEST	8.8.8.8	192.168.2.3	0x16c	No error (0)	dualstack. com.imgix. map.fastly.net		151.101.14.208	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:24.246489048 CEST	8.8.8.8	192.168.2.3	0x7d9b	No error (0)	www.bustle.com		52.222.214.36	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:24.246489048 CEST	8.8.8.8	192.168.2.3	0x7d9b	No error (0)	www.bustle.com		52.222.214.86	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:24.246489048 CEST	8.8.8.8	192.168.2.3	0x7d9b	No error (0)	www.bustle.com		52.222.214.53	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:24.246489048 CEST	8.8.8.8	192.168.2.3	0x7d9b	No error (0)	www.bustle.com		52.222.214.69	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:33.388415098 CEST	8.8.8.8	192.168.2.3	0xe05e	No error (0)	www.facebo ok.com	star- mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:28:33.388415098 CEST	8.8.8.8	192.168.2.3	0xe05e	No error (0)	star-mini. c10r.faceb ook.com		157.240.9.35	A (IP address)	IN (0x0001)
Sep 16, 2021 06:28:33.704857111 CEST	8.8.8.8	192.168.2.3	0x5b3f	No error (0)	m.facebook.com	star- mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:28:33.704857111 CEST	8.8.8.8	192.168.2.3	0x5b3f	No error (0)	star-mini. c10r.faceb ook.com		157.240.17.35	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:09.307554007 CEST	8.8.8.8	192.168.2.3	0x34ee	No error (0)	twitter.com		104.244.42.193	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:09.307554007 CEST	8.8.8.8	192.168.2.3	0x34ee	No error (0)	twitter.com		104.244.42.1	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:09.560168028 CEST	8.8.8.8	192.168.2.3	0x454f	No error (0)	abs.twimg.com	cs510.wpc.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:09.560168028 CEST	8.8.8.8	192.168.2.3	0x454f	No error (0)	cs510.wpc. edgecastcdn.net		152.199.21.141	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:16.904156923 CEST	8.8.8.8	192.168.2.3	0xc996	No error (0)	help.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:16.904156923 CEST	8.8.8.8	192.168.2.3	0xc996	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:16.904156923 CEST	8.8.8.8	192.168.2.3	0xc996	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 16, 2021 06:29:16.904156923 CEST	8.8.8.8	192.168.2.3	0xc996	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:16.904156923 CEST	8.8.8.8	192.168.2.3	0xc996	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.493457079 CEST	8.8.8.8	192.168.2.3	0x8339	No error (0)	platform.t witter.com	cs472.wac.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:17.493457079 CEST	8.8.8.8	192.168.2.3	0x8339	No error (0)	cs472.wac. edgecastcdn.net	cs1-apr- 8315.wac.edgecastcdn.n et		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:17.493457079 CEST	8.8.8.8	192.168.2.3	0x8339	No error (0)	cs1-apr-83 15.wac.edg ecastcdn.net	wac.apr- 8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:17.493457079 CEST	8.8.8.8	192.168.2.3	0x8339	No error (0)	cs1-lb-eu. 8315.ecdns.net	cs41.wac.edgecastcdn.ne t		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:17.493457079 CEST	8.8.8.8	192.168.2.3	0x8339	No error (0)	cs41.wac.e dgecastcdn.net		93.184.220.66	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		18.203.190.43	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		52.18.150.20	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		34.252.166.160	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		34.247.157.93	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		34.249.52.209	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		54.170.22.84	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		3.248.102.201	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:17.885945082 CEST	8.8.8.8	192.168.2.3	0x6fe1	No error (0)	twitterinc .tt.omtrdc.net		63.33.35.188	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.118908882 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	fonts.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:18.118908882 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.118908882 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.118908882 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.118908882 CEST	8.8.8.8	192.168.2.3	0x410f	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:18.345155001 CEST	8.8.8.8	192.168.2.3	0xcf66	No error (0)	www-google- analytics .l.google.com		142.250.185.206	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:19.537277937 CEST	8.8.8.8	192.168.2.3	0x86f1	No error (0)	resources. digital-cloud- prem.m edallia.com	medallia.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:19.537277937 CEST	8.8.8.8	192.168.2.3	0x86f1	No error (0)	medallia.m ap.fastly.net		151.101.2.133	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:19.537277937 CEST	8.8.8.8	192.168.2.3	0x86f1	No error (0)	medallia.m ap.fastly.net		151.101.66.133	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:19.537277937 CEST	8.8.8.8	192.168.2.3	0x86f1	No error (0)	medallia.m ap.fastly.net		151.101.130.133	A (IP address)	IN (0x0001)
Sep 16, 2021 06:29:19.537277937 CEST	8.8.8.8	192.168.2.3	0x86f1	No error (0)	medallia.m ap.fastly.net		151.101.194.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 16, 2021 06:29:19.844125032 CEST	8.8.8.8	192.168.2.3	0xc565	No error (0)	udc-neb.kampyle.com	cooladata.kampyle.com		CNAME (Canonical name)	IN (0x0001)
Sep 16, 2021 06:29:19.844125032 CEST	8.8.8.8	192.168.2.3	0xc565	No error (0)	cooladata.kampyle.com		35.241.45.82	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bustle.com - https: - imgix.bustle.com - m.facebook.com - www.facebook.com - abs.twimg.com - twitter.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:56 UTC	0	OUT	GET /entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:27:56 UTC	0	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 46937 Connection: close Date: Thu, 16 Sep 2021 04:27:56 GMT content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Cache-Control: max-age=3600 Apigw-Requestid: FvQn-hc9oAMEP7g= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 f3e00d74aa4544d776f78a159416d17b.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: QXxXderMcSAhbRIwlsndYKdEkZnEgWkCV7FhUpMmbK4nHTnCcRdlTw==
2021-09-16 04:27:56 UTC	0	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:27:56 UTC	8	IN	Data Raw: 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 61 30 64 33 39 32 37 61 2d 66 63 61 30 2d 34 39 61 36 2d 38 62 64 32 2d 37 30 39 66 61 30 66 63 66 64 33 61 2d 67 65 74 74 79 2d 31 33 34 30 31 37 38 36 36 31 2e 6a 70 67 3f 77 3d 38 30 30 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 31 36 30 30 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 61 30 64 33 39 32 37 61 2d 66 63 61 30 2d 34 39 61 36 2d 38 62 64 32 2d 37 30 39 66 61 30 66 63 66 64 33 61 2d 67 65 74 74 79 2d 31 33 34 Data Ascii: etty/2021/9/15/a0d3927a-fca0-49a6-8bd2-709fa0fcfd3a-getty-1340178661.jpg?w=800&fit=crop&crop=faces&auto=format%2Ccompress&q=50&dpr=2 1600w, https://imgix.bustle.com/uploads/getty/2021/9/15/a0d3927a-fca0-49a6-8bd2-709fa0fcfd3a-getty-134
2021-09-16 04:27:56 UTC	20	IN	Data Raw: 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 63 37 33 35 38 61 36 66 2d 37 64 31 63 2d 34 37 66 38 2d 39 39 62 39 2d 37 38 65 34 33 63 32 32 65 37 38 33 2d 67 65 74 74 79 2d 31 33 34 30 31 38 34 34 33 31 2e 6a 70 67 3f 77 3d 33 30 30 26 61 6d 70 3b 68 3d 33 36 30 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 36 30 30 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 63 37 33 35 38 61 36 66 2d 37 64 31 63 2d 34 Data Ascii: x.bustle.com/uploads/getty/2021/9/15/c7358a6f-7d1c-47f8-99b9-78e43c22e783-getty-1340184431.jpg?w=300&h=360&fit=crop&crop=faces&auto=format%2Ccompress&q=50&dpr=2 600w, https://imgix.bustle.com/uploads/getty/2021/9/15/c7358a6f-7d1c-4

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:57 UTC	51	IN	Data Raw: 3c 06 89 c8 d0 8d 71 6a 97 4f 66 ba 82 46 bc 66 ca 1d c5 08 aa 29 12 3e 9a 8b 08 d4 cd 86 28 4c e0 a1 4c c6 df 1a 29 c6 ef fb 31 d0 36 7c f4 f9 f0 b0 f5 21 f0 12 7a c5 95 fd 43 bd bd ef 7c e4 10 38 a5 72 c1 37 40 eb 7c eb 14 64 f6 85 ae 33 5b 14 74 93 79 1a 96 4b 65 6e d2 25 d0 53 b6 46 9a 94 2d 24 d5 27 c7 e9 4c 75 95 b4 56 81 93 d6 38 e7 37 81 41 72 8d 1f 67 9f 02 ac e0 71 4f a8 38 97 33 36 70 4a 8c 3e 40 6b 92 6b ca cc 64 62 93 fd 78 df c9 83 8f 3e 4b b9 aa 3c b0 96 91 19 2e 53 1f a9 7a 7a 35 8b 51 04 94 c6 af 5b e6 c8 bd 79 99 73 2d 13 ac f4 de 0e d6 86 43 4f 3d 14 bd 6c a2 c8 93 2c eb aa 66 b6 90 cd ea f6 6a 93 a1 99 c7 e7 75 13 a9 6e f5 39 23 2f 37 81 31 17 ce ea b6 07 4d d1 71 4d b1 f3 da a8 40 a9 14 96 4a 44 89 e1 c1 e1 80 cb ee 3b d6 59 5f df 6b Data Ascii: <qjOfff>(LL)16 !zC 8r7@ d3 tyKen%SF-\$!LuV87ArgqO836pJ>@kkdbx>K<.Szz5Q ys-mCO= ,fkjun9#//71MqM@JD;Y_k
2021-09-16 04:27:57 UTC	53	IN	Data Raw: c9 75 54 3c f7 89 2d bf d6 c8 d3 bc 2c 6f 2c 5e d7 62 6b 7b cc f8 45 33 52 5e 7a eb d9 23 e0 ed 59 36 b4 c8 aa 62 c6 ac f2 57 69 4c ba 63 f4 67 4f b9 45 28 81 a2 ba b4 d7 cc 8d 9d 32 f8 5d 6b 43 d5 d2 77 a6 79 98 32 ac ad 97 d8 30 a7 82 53 20 9e dc b9 aa 32 f1 7a 4a 23 74 dd 2c dc 17 79 24 f6 f9 a3 6e 6b 49 72 a9 d5 9f 30 74 51 5a e6 1c 36 ca 6b a0 1e e7 ef 0c a4 fd 15 be de 73 a5 1e 9d ff 00 55 df ae 8f 2d f5 ea eb a5 3b 86 18 f8 81 63 58 2c b4 f5 72 a5 70 de 66 a7 98 bb 42 6e e9 25 73 1b d1 f5 75 9f a1 fe 23 fd 52 74 f8 43 7f 47 25 59 76 e1 2b 39 4a 9e 6a 8b 4d 89 6c 72 5e ca 82 f3 b9 b2 6c 3a cd d0 32 3a df 3c 51 29 84 53 ac f6 f7 cf 16 cd 8e f1 31 b3 ac e9 9b 99 f5 16 4f c5 d6 d6 a1 49 9f 25 4f 6b 6e 6b f2 3a cb b2 e9 5c c7 3a bd af 87 59 2c 8d be 3a Data Ascii: uT<-o,*bk[E3R^z#Y6bWlCgOE(2)kCwy20S 2zJ#t,y\$nk1r0tQZ6ksU;-X,rpfBn%su#rCG%Yv+9JjMlr^!2:<Q)S1OmA%Oknk:\Y,;
2021-09-16 04:27:57 UTC	54	IN	Data Raw: 1c b0 31 06 22 36 71 27 70 58 e3 20 5a 76 88 d6 98 33 e7 dd 3a d8 d0 94 91 aa f0 17 bb a1 33 f4 9a 6d 88 54 79 ab e6 d6 3b fa 10 cf 32 b9 25 b6 ac ad a3 e6 95 43 8b 3e a4 45 71 7c c6 05 56 58 b6 44 bc 98 cb 33 a3 65 91 3a 8d 5c 79 bf 31 c4 db af 5d 1b 28 ab b3 94 0a 40 73 2a 42 50 37 21 4f de cf ac f0 8d 14 eb f4 73 ad 32 66 7e 05 06 66 a5 c9 f8 2f 92 07 b5 b5 22 e7 7d f1 f4 46 dc 6e cb f8 af 0f d6 11 76 d4 65 a8 34 00 f1 7f 63 7e 87 57 f6 1c ba 21 0e cd 58 52 e5 9f 4c ac cb 2a 57 2b 8f cb b4 b3 7e 5f 7d ca a1 3e 7a 38 2f ae ec f3 a4 93 7b 06 cd b0 e1 f0 33 69 9b 2d 21 f3 6f 09 eb b6 ff 00 73 aa e8 ea f2 40 12 9a d0 b6 a0 4a a0 c4 ba 14 4e aa da 9b a6 ff 00 a3 3d 6d 9a 72 cd 35 6c e7 71 d2 75 94 33 d8 bd 91 ce f6 fb 17 b2 2d d0 d5 d9 73 e7 0e 7b a4 db da Data Ascii: 1"6q'pX Zv3:3mTy;2%<C>Eq VXD3e:ly1 (@s*BP7!Os2f-f"/)Fnve4c-W!XRL*W+~_)>z8{3!ls@JN=mr5lqu3-s{
2021-09-16 04:27:57 UTC	55	IN	Data Raw: 0a ee b6 d0 45 56 32 7c 41 f2 fd 30 75 d1 3a 60 d9 75 c5 28 c4 38 f6 b0 80 c9 a7 f7 e9 57 1d a1 28 97 48 1e 8d 4c 9e 3e d6 d2 98 6c 54 49 b0 8a ee b5 80 40 7d 2b 58 e4 4a 11 44 58 99 59 88 1a 83 c4 e8 b9 b9 a5 88 b5 8e 8b 0b ea 5b 93 f5 1d f9 6a b5 eb d6 ff 00 22 40 6a c9 13 a0 5b c8 78 5e 5b 1b 4a 39 27 ea 8a 78 bd 48 fd 5d 61 bf 8d 15 da 5f 5b 16 66 a8 71 9a dc 72 8c 27 9b 33 aa 67 59 ed f2 7e 99 92 3b 39 bb be 94 94 2d 09 19 7d d6 5a 39 2d 59 0e ac 6b 18 4a c9 eb 8a 92 03 00 68 65 6b 46 11 f0 3d 35 c9 e3 c4 80 45 a0 4e 8a 31 33 d2 5b f7 e7 0c aa 1a 53 62 41 3d ca 94 a2 60 02 b7 53 12 21 68 b7 f5 c7 d0 9d ea a3 bc 03 2f e7 8f 17 b4 72 7d 66 6e 61 4d ed 9b d7 6e 0d 19 66 62 81 4e 8a d1 57 19 4a dc d5 88 a4 cd cd e8 d3 78 e6 bc bc 6c 2a 9b 88 51 8c 92 1b Data Ascii: EV2 A0u: u(8W(HL>ITI@)+XJXDXY j"@ jx^[J9^xH]a_[fqr]3gY~;-9;)Z9-YkJhekF=5EN13[SbA= `S!h/r]fn aMv@fbNWJxl*Q
2021-09-16 04:27:57 UTC	57	IN	Data Raw: 3b be 77 f7 73 72 45 6f 0e bd f1 e7 bf c5 17 5d 00 81 55 96 b2 ba bd aa 2d 31 52 d0 a1 22 52 40 dc db 71 1a 98 2b 9d 62 db e1 d6 c6 95 d8 d6 6c e2 23 93 34 95 98 ed 02 85 b3 b4 14 cd f2 33 26 8b 9c 39 c3 42 a2 8b a3 46 dc e6 f6 e2 e2 af aa 5c 94 55 10 e1 38 88 b2 d3 f8 83 d4 10 01 29 10 c5 e0 09 63 9b a3 a1 a1 01 e6 b4 31 a9 d3 96 85 35 97 7a b6 4a 6a 18 94 ad 89 7a 24 e5 36 d8 4f 9d 48 47 17 b9 46 76 fc 8e 73 34 98 d8 b6 29 19 37 59 4f d8 ab 48 6b 11 4d d8 1b e6 c7 bb cf 28 7d be 1a 63 c9 fa 47 1d 1e 9e fa ca b9 cd 5c 06 04 9f ca 56 04 bf 16 93 aa c4 5f 0d 30 67 28 52 a8 c3 55 ad 52 77 44 9a 3c 25 cc 16 24 05 c3 8e ea fb 5a ca da f8 04 c9 65 83 92 27 ea 53 15 3b 87 4c d8 52 c9 34 ea 55 62 2e a2 35 da ca e2 b4 87 12 5e 5d f9 1e 47 79 e1 28 b2 ec 38 d3 3f 15 Data Ascii: :wrEoJ-U-1R"R@q+bl#43&9BFU8)c15zJz\$6OHGFvs4)7YOHkM(c gV_0g(RURwD<%\$ZeS;LR4Ub.5^)Gy(8?
2021-09-16 04:27:57 UTC	58	IN	Data Raw: 02 a6 94 a2 b2 2e f8 ba 42 78 69 e5 24 48 49 ca 15 84 23 18 95 f5 ba 8b 4a 10 8b dd ef 3c 31 77 9e e7 bd ee 8c db 99 4a bb 7e ff 00 ba 65 c3 2c 92 86 b3 e4 1f bc 99 09 0a a3 0c dc e7 3d c1 29 e2 25 6a 7a 58 5a 51 70 5d 17 4b 08 0a 50 49 fd 39 a0 83 5e 75 c5 c7 99 23 c2 2c de a4 21 2a a5 e7 96 11 2a 38 e0 c9 29 1a d8 3c ef bd e1 0c 42 18 39 cf 73 dd ea 9b 4d 74 83 42 e9 8b 85 c8 a4 a9 09 31 5f c6 ef 16 85 18 96 b0 31 91 ce fb a2 52 83 8b 8d 19 00 6d 46 58 fd d1 16 22 89 3c 9e 9c 73 41 4a 35 b5 eb 5e 55 2d c3 4c 10 27 09 2a 15 9c 5f 3a a4 42 e6 86 c6 35 e9 7c f7 bc 61 85 f7 87 87 9d f7 83 ee aa b3 d7 4c 35 0e 97 b4 cc 28 84 a9 4d 3b ff c4 00 1b 01 00 02 03 01 01 01 00 00 00 00 00 00 00 00 02 04 01 03 05 00 06 07 ff da 00 08 01 02 10 00 00 00 ca 09 63 Data Ascii: .Bxi\$H#J<1wJ-e,=)j%zXZQp KPI9^u#;,*8<<B9sMtB1_1RMfX"<sAJ5^U-L*W:B5 aL5(M;c
2021-09-16 04:27:57 UTC	59	IN	Data Raw: 07 a0 ec 99 9b 4b ba b4 aa d6 10 e8 ae 7c b6 74 58 8a 95 89 33 95 ce fd 21 8e c4 5f 56 33 16 4d 4f 6c c1 14 40 c7 59 61 91 94 0c 77 18 d4 31 93 e6 c8 56 b7 3a ae 7b 3d 66 7e 87 a3 3d e6 1c 6b 3d 5a 2b 0f 56 dc cd 7c 5d 5f 15 d3 61 97 0c 41 0d 3c 87 8f b4 e0 2a 42 a0 8a ee f7 ba f3 11 e2 f5 77 33 93 48 2b f4 3a 53 31 5c c1 c5 73 65 96 59 d0 13 d1 5a be 22 2d 1b ec 59 15 44 2e f6 fb 9d dd 47 8a d7 f4 12 ae 4e 7d 1a 9e 8e 66 78 62 38 84 38 ad e2 93 1e 1f 1c 97 1d 2c 5f d9 0b 07 7b 7d de ee ec bf 38 fe ed ea e6 4d d6 c7 ac 32 28 8e e1 0e 98 09 32 b0 a2 70 b0 a0 2c a8 af 6f 05 2b fd 9e cc 4f 77 62 61 35 ae c0 66 a1 c1 eb 2e 22 ee ee 80 18 99 8a e5 91 35 3c b4 40 49 73 0f d9 4e c5 f3 d1 31 38 5e 65 a7 ac e5 a7 a7 75 b3 29 9e e1 af a3 ba e8 a7 86 8c 1a 8b a0 66 Data Ascii: K tX3!_V3MOI@Yaw1V:{=f-=k=Z+V]_aA<*Bw3H+:S1lseYZ"-YD.GN)fxb88,_}82(2p,o+Owba5f."5<@IsN 18^eu)f
2021-09-16 04:27:57 UTC	61	IN	Data Raw: 9b 85 14 7c ff 00 34 81 04 04 10 45 a9 c9 a4 b0 94 51 3a 99 1a 7e b7 6a 2e 3e ef 55 58 5f 7d 5a 72 51 f3 fe 92 4c 0e 5d cd 04 b4 00 52 48 c5 28 6b 81 44 38 82 dd 1f 5e b4 28 b6 fc 36 2c 8f 2e e4 ae aa 5d a9 c8 c2 0c 45 12 1a 9a 92 0d 4e 63 ca 28 94 18 eb be c3 6c d8 8a 07 5b 77 29 e4 c1 c5 bb 17 07 3a 8b 09 29 06 a4 10 29 44 f7 10 49 0d 61 9f d9 6f bc c9 4e fb f2 bc 66 a2 73 d4 fb 96 78 f4 e4 02 28 a0 c4 92 28 22 91 29 ac 0e 97 d6 76 e7 8e 1b 56 29 f8 ee 3a 44 be 4d 9d 1e 2d 3d 04 50 4e 21 81 24 92 29 12 18 d4 5f e9 9d 64 8f 7b eb 79 2f 3a 92 29 49 7f 6f 8f 71 40 12 92 0e 49 ad 21 24 e4 8c 41 22 fe e7 bc b8 d3 0f 96 73 08 12 e6 a3 67 6b 9a 32 35 a9 02 91 04 90 10 69 21 18 c3 9c 87 4f e9 76 8c 7e 61 cb 24 93 8a 0a d6 af 3e 1c 40 08 a0 4a 48 90 98 88 45 8d Data Ascii: 4EQ:-;.>UX_}ZrQL RH(kD8^(6, ENc([w:))DlaoNfsx((")vv):DM=-PN!\$)_d y/ loq@!!\$A"sgk25! Ov~a\$>@JHE
2021-09-16 04:27:57 UTC	62	IN	Data Raw: 5f 2b 8f 80 f2 d9 f1 39 cd d9 13 13 1f 99 c9 c8 64 5c a1 ba d1 73 c5 df b7 be de 73 ff 00 13 3d c1 41 7b 7b 1c b0 6c ab 63 5e f5 b6 ec 38 6e 8b 7d 68 89 d7 cf 68 c7 c3 61 bd 2a ec 29 35 4c d6 84 d3 fa a1 5f e8 9d 64 bf ef eb af f7 13 13 25 60 f6 6e e4 0f a1 62 9d ca f7 6c 6c f6 bb b7 b7 d3 26 7b d3 d7 a1 51 75 19 52 f5 1b 35 57 ad ad 43 6d bd 29 ea 43 af 4a e9 52 7e bf d7 52 5d 4d ab d5 b4 09 ad 7e 2c f5 f7 38 8e ff 00 1c de 77 bb 19 19 8f 13 e2 66 72 72 72 73 d8 58 16 fe 78 2f 05 33 3e d0 70 7e dd 4a 5f 5b 67 57 71 4d 63 c7 15 cc 79 00 6b 1d aa 2d 52 f5 e1 50 17 f0 55 5d a8 5d 43 5a 02 4a ab 57 9f 4a 35 f6 c2 c5 9e 13 b4 9c ee 24 8a d3 36 8d dd 60 e2 e2 c6 e2 de ed 96 02 20 4d 6c 14 8e 91 3a f4 aa bb 6b 5b ab 76 a6 8d 3b bd c6 08 48 fc 70 29 4d 25 39 26 Data Ascii: _+9d!ss=A{!lc^8n]hha*)JL_d%`nbl!g& QuR5WCm)CJR-R JM~.8wfrxxsX3>p-J_[gWqMcyk-RPU ]CZJWJ5\$6`. Ml:k[v;Hp)M)%9&

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:57 UTC	63	IN	Data Raw: ab b4 dc 65 90 13 4d 5a f2 3f 25 25 d1 9f 48 07 e5 e6 d8 d8 ea b5 14 28 ef f8 ee c0 b6 0f f9 13 60 5c 73 6c f3 af 5f 51 ca 96 93 77 ec a4 b4 b4 55 5e 13 7a b3 f3 5a 8b 55 7f e3 d6 fe 61 6b 80 23 8b 6b 78 b9 22 f2 d6 fd 8c 54 c4 2c 4c 4a 31 aa 66 4b 2e c2 9a 48 44 b4 59 1a 77 98 da 73 dc b6 a6 20 5d 16 65 a6 52 b2 53 01 d5 db 50 eb 5d af 6f e6 74 92 ab a2 aa d7 12 12 ab 0b bb 3b 4b 76 48 e1 99 5e 17 00 5f 28 d8 22 87 53 30 97 e5 e6 29 2a 2d 39 01 4c 59 4b b5 76 6a 71 23 50 9c 73 2e 23 7c 27 29 80 03 32 d0 f5 11 03 31 d2 c0 0e bb 92 de 39 62 18 0c be 6d 9d 16 89 d5 f8 fe af be 49 ca 74 b4 b6 56 f5 97 48 91 16 54 59 ac 67 24 ab aa be c2 64 ba 6c c2 d6 9b 76 72 bc a0 a0 75 02 c0 d8 b2 66 b4 56 57 a3 a2 ee 30 b2 24 18 0d ac ca 6d af 66 ad b5 5a f9 46 51 08 c1 Data Ascii: eMZ?%H("\sl_QwU^zZUak#kx"t,LJ1fK.HDYws]eRSP]ot;KvH^_("\$0)*-9LYKvjq#Ps.#])219bmltVHTYg \$dlvruVW0\$mIZFQ
2021-09-16 04:27:57 UTC	65	IN	Data Raw: 32 ac 09 89 2b 17 9f 88 55 77 6c a5 66 13 4a dd 77 03 7d 80 a7 24 cd c0 67 51 f4 79 08 bc c9 92 ff 00 9f df cc e5 72 a2 df 9a d9 5c 91 67 f1 bd 5f 3d d7 6a b4 b6 6e 3f 61 ab d8 61 42 98 f5 ae 29 b4 f1 23 b4 2d 0e 6a 64 0c 91 02 c8 bb 2b c1 7e e3 04 b6 eb 9c 5e 57 85 e2 01 ab a5 61 79 69 37 cc cd 90 bc a3 14 71 04 c7 59 b5 19 d4 c7 5d b5 93 85 33 39 1e 35 da fd 87 1d fe 39 c4 b6 9a 7e 4b a9 a2 96 28 28 9d 78 d7 05 3a 74 76 48 d8 2e 9d a4 d9 4d e1 b8 9b 60 e0 2f 59 4d 7a 65 17 8b 95 1b 64 e6 7c 44 c4 f7 dc e2 4a 99 cb ac 32 e6 29 5c 53 55 15 58 5c b5 55 c6 e6 c4 a6 8b ee ae bb 53 95 0e 32 be 5d 8e 23 5e b5 8b ad a5 5a 15 72 5d 5a d2 d8 c2 cd 3c 58 ad 66 aa 8d 8a d6 90 45 a4 9a 28 b8 d5 67 1e 32 6b 9a 13 4e 45 96 2c 5b b8 11 eb 31 e6 72 64 a6 73 be fb ac 2b Data Ascii: 2+UwlfJw}\$gQyr!g_ =jn?aaB)#-jd+-^Wayi7qY]u3959~K((x:tvH.M/!Ymzed[DJ2])SUX!US2)~#?zJc~XfE(g2kNE, [1rds+
2021-09-16 04:27:57 UTC	66	IN	Data Raw: a3 5e a6 2b 64 3b b5 7d 66 26 56 35 d7 ae 2d 6b 2b 7a 7f 3e 6c e2 4a b9 1c c1 cc 94 dd b1 b2 b2 a4 68 db 31 d8 e5 29 f7 e4 73 b2 09 1a 71 ae 7e be c6 c2 6a 2d 10 b4 d5 ae a5 d6 52 85 63 11 39 26 c3 22 61 3e 39 2a 28 1f 5a 53 76 5f 3b ac 64 a2 1e a1 49 a0 eb cd 55 d4 0a 95 aa d3 a9 7e c9 c4 84 c4 c4 0c e7 7d be a8 9c 16 3f 0b 3f 94 73 ce a2 7a 5d 7f ee 9c 5f c7 a8 ae 60 4d 92 51 42 be 9a bd 32 69 df 2b 95 a3 5e 5a a6 6a d7 ad fa 47 5a d5 37 54 e0 e0 9a e6 b5 e4 10 c4 32 db ed 30 c1 91 ac 29 cf 55 65 4c 66 73 3b 3b e4 49 55 9d 6b 13 9b 02 11 ac 35 14 81 48 a4 42 02 3b 99 6b 18 44 4c c6 65 e4 55 00 0d 4c 36 76 59 74 f1 51 2b f4 95 fc 5f 02 eb 85 7a 09 bd 7c f0 a3 d4 f3 da 48 a7 da 19 0c 38 95 01 58 c2 8d 46 db 8b 72 3c 1c 89 fe bd 22 22 95 d7 80 24 ca cc 17 Data Ascii: ^+d;f&V5-k+z>Jh1)sq-j-Rc9&"a>9:(ZSv_dIU-)??szl_`MQB2i+^ZjGZ7T20)UelFs;IUK5HB;kDL6 vYtQ+ _z]H8XFr<"\$
2021-09-16 04:27:57 UTC	67	IN	Data Raw: 40 04 46 00 94 33 0e 67 0a 30 f1 85 69 b4 d1 85 2d cd d0 56 8d 3b eb d8 76 df 6d b4 b9 68 23 da 48 ca 25 c4 65 33 e6 73 bf 6e fd 7e 1f af f5 be 08 88 28 60 ba 1b ed 33 eb 4e dd 9d 54 af 5d 6a c2 60 9a 79 1e 27 c7 b0 94 99 1f bf 6b 07 d9 33 eb af c1 4c 95 6b 7c 3b 93 d9 68 a7 fa a0 4e 4e 70 f6 c9 46 2b 2b ca 0a fc 7f 44 aa 53 5d 1a ba 55 96 b1 0c 11 1c 2c 64 99 cc c9 4c 99 dd b1 ae 10 3f 7e dc 78 56 a9 d9 6b 3e 5b c7 36 86 7b 99 9c 9c 71 4c f7 e6 73 ac f7 87 c5 98 b5 f6 be cf cb ee 4c 9b 1f 38 ac 11 31 ed ab dc 6c 02 e6 91 67 52 c2 5a cc 8c 88 c2 28 29 28 27 3b 9b 00 70 c4 79 8f 13 26 51 93 3c 0f 9a d7 ba 8b 3f d5 ae 4c f7 c5 1b 05 ec 89 ae 75 ca c4 7f 42 a5 9c 1e 9d 6c ad 81 2a c1 c2 c2 96 99 4f b4 cc cb 0e d3 d4 00 f8 6f c9 b5 b1 b9 d8 5f 49 a0 Data Ascii: @F3g0i-V;vmh#H%e3sn-(`3NTj`y`k3Lk];hNnpF++DSJ)u,dL?~xVk~[6[qlsL81lgRZ()?"=py&Q<?LuBI*O`o_!`
2021-09-16 04:27:57 UTC	69	IN	Data Raw: 57 47 79 3e 7a c9 8c ee 0b 5c 43 2b 8f 8e 55 30 2c 16 1b 7e 56 d8 01 d9 ec f7 9b bf f0 8c a3 04 45 2c c3 c9 f3 ed ee b2 5c 89 47 88 c8 86 c1 67 5e 9f 1c 2b d3 08 a6 7c 4e 75 19 07 0c eb ac 89 ef c7 7d f7 13 05 ec bc f5 29 f6 f6 71 44 91 09 67 7e 0b c4 e4 e5 24 4f ea 72 73 b9 f1 18 b6 0b 2b c5 60 34 b1 70 e2 7c d9 96 a9 7b 2d 96 f7 7b fe 11 91 9a f8 9c 29 2c 2c 2c 9f c0 4a a7 23 20 62 33 a7 0e 77 ed ef 27 33 eb eb 39 11 d4 fe 20 a1 9e 7b ef cf 7e de cb 64 d8 36 c9 41 1c e2 0b 26 66 7b c2 ce b2 ba 70 a6 67 c7 7d e4 c4 8c c6 46 1e 69 1b 5c a8 64 a9 95 ee d4 2a c3 4c 11 b2 d9 6f 77 bf e5 19 ab 59 78 2c 28 98 9f c4 62 88 66 06 3c 47 8b 83 3f 98 ce f3 e3 98 99 f1 d7 9e e1 9f 8e fb f3 df 7f 95 4c c4 c7 92 c9 8e 92 13 33 3e 3b ef 23 c4 c4 e4 f9 e2 e4 49 d0 b0 bb Data Ascii: WGY>zLC+U0,-VE,IGg^+ Nu))qDg-\$Ors+^4p[(-),,,J# b3w'39 {-d6A&f[pg]Fid^LowYx,(bf<G?L3>;#NI
2021-09-16 04:27:57 UTC	70	IN	Data Raw: e6 be d2 33 f6 af a8 dd 57 6d 7c 13 f1 7b 66 40 c7 f1 06 95 ef 0b 16 2c fc 43 41 dc ea fd 40 5c ab 84 20 47 89 a8 e1 d6 1e e2 b0 33 52 3c 5c 39 1f bc 81 56 9e d0 b0 32 0f 33 95 dc d6 54 4e 08 aa fa 3e 91 f4 4d 68 a0 46 7c 43 23 1b ca 8b 09 84 64 6d 1a 0f 4d 6e 6d a4 33 20 b6 55 95 8a b9 45 ce a2 71 bd 34 44 34 15 25 2c d3 ee 44 36 a6 a0 77 28 18 68 e9 63 1f c4 17 27 48 fc ac c5 40 e7 70 0e aa e4 e8 46 d6 26 2b 9a 00 2a 5c 4f 60 d5 41 24 65 e2 68 c0 fc 44 0f aa 8e 33 43 23 34 ad ab a7 b9 62 27 69 74 4c 2f 03 5a 7f 54 f6 75 81 1c c0 fa 3a 2a 21 c5 02 75 55 5b 28 73 5f 55 98 a1 45 45 4e 7a 8e 6b 15 72 af cf 89 c5 c0 c7 36 17 36 b7 a8 da a8 ee 52 c4 d1 24 fd 13 9a 6c 68 2e 3b 6f 45 c8 98 51 96 b0 e7 60 be 7a 9a 7b d7 27 46 63 60 05 ae a6 66 96 3a 94 ec a2 9a Data Ascii: 3Wm {f@.CA@^\G3R<I9V23TN>MhF[C#dmMnm3 UEq4D4%,D6w(hc'H@pF&+^*IO^A\$ehD3C#4b!tL/ZTu:*!uU[(s_UEENzkr66R\$!h,:oEQ`z'[Fc'f:
2021-09-16 04:27:57 UTC	71	IN	Data Raw: a7 78 2a 2c 4c e5 98 7c 4c ac a7 5a 29 2e 3c 14 72 4a 58 ea 36 4d 72 d6 a0 f6 83 e5 59 50 15 90 1b a3 34 a9 ad 01 59 6c a6 c6 0d d0 15 ba 7b ca ed 5d a8 f1 4e 91 c1 1c a1 14 42 a7 39 c5 e2 03 45 ee b9 23 91 30 85 ce 8a 21 89 dc d0 2e 3f 45 8b c4 3c 87 3f 78 b0 d1 3a 57 38 f1 45 5d 5d 1d 56 64 69 f0 46 94 3d ca bf 2f 7a 21 cc 73 bb 8a 31 4c 0d ff 1f 7a cc f6 bc 53 89 a7 6a a3 68 2e d1 b4 d3 f8 4a ce cc a0 6d 03 b2 7e 34 f1 bc 52 b2 4f 13 f5 08 43 27 4c 2e 1f d2 56 76 f4 c4 44 cc 0e 22 4a bb fd 17 7b 43 87 90 c6 72 6c 9d de 89 cd 52 0d eb 15 84 c4 36 58 de 41 07 72 e4 dc 5c 41 b8 87 88 a4 ed ea 95 83 7b 6a d9 a3 23 b1 c1 72 4e 15 b5 93 13 18 ec 06 a7 e0 8b da e8 f0 40 b4 7b 67 5f 0e 1e 8c 90 ae 4a e8 54 8f 71 2b 94 f1 7c a8 1d 34 2e 6c 2d 89 ee ab b5 75 Data Ascii: x*,L[LZ).<rJX6MrYP4Yl[[]NB9E#0!.`E<?x:W8E]]VdiF=/zls1LzSjh.Jm~4EOC'L.BvoLD'J[CrlR6XAraAj #rN@[g_JTq+]4.I-u
2021-09-16 04:27:57 UTC	73	IN	Data Raw: af 39 96 96 fe c1 5f e6 83 7d b6 d3 c5 11 3b 40 14 1f aa 2d c2 c6 c1 d6 74 84 7b 85 53 8c 71 87 53 31 8f 38 29 a2 26 ec fe 11 dc b2 b0 37 71 ab 7e aa 37 d1 da e6 63 6b 55 99 cd 78 3b 80 fa 5d 35 f1 3c 3a ce b1 09 bd 01 63 ba ae 15 3e 36 34 52 f9 cc 2b dd b6 d3 56 9e d1 bf c5 39 d4 76 e7 b6 8e 59 8d 0d 38 15 b1 50 0e ba 1f 92 30 4e 4e b5 da 1f a2 0e 65 09 75 29 b3 dc ab c7 c7 f7 9b f3 04 d4 dc a5 32 67 ed e6 2d f6 5b ab 8f 01 de 84 18 76 46 32 30 50 e7 6c 7d 51 7e a8 e2 78 9d e8 cd 82 64 8e b3 db 8a 14 02 d5 07 44 24 78 ad 83 41 3e fe 2b a2 73 a3 75 aa ef 81 4e 10 e6 17 3c 0f ac 3b 7b 42 c1 3c 53 69 bf 10 a2 8c dd fb 3a 5c 54 78 ea a0 63 aa d1 94 fb 4d b8 3d be 0b 05 8d 85 ce 23 cf 0f 59 a6 ce ec 2a 38 a4 a1 63 86 e3 5f a1 1f 55 0c 95 ca 6a 69 a5 40 77 b8 Data Ascii: 9_];@-t{SqS18)&7q~7ckUx;]5<:c>64R+V9vY8P0NNeu)2g-[vF20P]Q~xdD\$xA+suN<;[B<Si^TxcM=#Y*8 c_Uji@w
2021-09-16 04:27:57 UTC	74	IN	Data Raw: f3 87 f4 44 e2 de 29 d5 73 0f c1 66 c4 b5 d5 b3 9a 37 6f aa e9 20 ad aa 1a 50 fb ac 47 7b 32 bd bd db d0 1c a3 8d c3 8f 5d b9 9a 3b d3 86 53 e1 4e f0 ba 3e 50 8d da 93 b2 87 dc 4b 00 a8 69 39 7b 90 fb bb 98 e4 f9 30 a6 33 d7 8f 5e d0 84 8c d9 ae 60 2d dd c1 10 ab e9 e9 bd 50 ea bb 57 6a a9 d5 56 8b 65 59 58 ad a2 ae a9 ca 50 3a b4 a3 c1 1d fb 90 7e 0e b4 cb 57 e6 d7 7b 8d 77 af 33 19 ae cb 9c f7 78 04 ef f1 18 1c 05 1a 1b 4f 05 d2 36 6c df fc 4c a7 bc 68 a5 7e 07 0f 88 06 b2 64 0c 93 b4 b7 42 7b ea 9e e8 98 da 54 16 0d 92 75 14 b0 3d a8 fd ed f1 b6 94 7d 1d 19 a5 8e 6e 2a 07 bb a7 89 95 86 60 73 c5 ec bc 0b d1 10 ca b1 fd 34 06 c0 4a 2c e1 ae 57 52 ed 2b 3c 85 84 38 d3 da eb b3 b3 37 ac 11 9f 49 5f 41 23 74 e3 fd 42 39 ae e2 37 1e e5 01 6d 01 07 ba ce f7 Data Ascii: D)s7fo PG{2};SN>PKi9(03^'-PWjVeYXP:~W{w3xO6lH~-dB[Tu=]n^*s4J,WR+<87_A#tB97m

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:57 UTC	75	IN	Data Raw: bb 72 bd be 20 d5 30 e1 7a 42 3a cc a9 1d e3 37 ea a9 34 b1 d6 f9 5b f0 3a af fa c0 75 3f d0 a7 f2 92 10 93 05 8a 6e f0 2b e1 bf e4 bc c4 b1 6a 18 01 1e 28 9c a0 9a 51 c1 a3 de 87 dd 31 4d 1a c7 89 a8 ee 4d 7e 1a 58 eb fb 39 5c 3f 85 fb 41 10 3b ee 3e 6b 2b bb 33 82 3c 53 a5 8e 46 d4 82 cc a7 fa a6 4f 03 9a fb 39 ba d3 e6 a6 c2 bd a0 d6 96 ee 23 88 4c 93 0d 9d be 1d 84 6e fd 11 63 9d 97 47 6d 53 e6 9a e6 9e cd 3b 3f a6 04 a6 d1 0a 21 45 74 73 ad 80 ac aa 10 7b b4 41 ae d1 65 70 d9 ad f4 41 f0 80 4d 48 75 49 0a 9e 2e 4e f3 6f e2 3e 21 46 e6 12 34 d4 76 1e 08 16 59 00 6b ba 94 29 cc 97 35 05 40 da 1c 53 43 40 17 61 24 81 ec 9e 0a 2e 92 a7 78 d4 71 3b ff 00 55 4a b7 d4 75 cb 78 2c ae a0 77 03 ee fa 84 43 9c c0 6a 0d 6d de 9d 95 bd ea a6 57 70 6a fb c3 1e Data Ascii: r 0zB:74[u?n+j](Q1MM~X9)?A;>k+3<SFO9#LncGmS;?!Ets[AepAMHul.No>!F4vYk)5@SC@a\$.xq;UJux,wCj mWpj
2021-09-16 04:27:57 UTC	77	IN	Data Raw: 93 05 81 8a 29 0f 49 28 19 a4 77 17 9d 53 70 dc 9d 3e 21 c3 f6 51 b9 ff 00 ca 2a a4 93 ef 12 bf ac e7 66 90 77 9b fb aa 83 e1 7d 69 9d 82 b4 e2 34 21 53 13 24 44 54 39 a1 e2 bd f4 44 87 eb a0 3e fd ca 98 b6 83 fe a1 cb ef 14 59 36 eb 76 48 c7 fe ab ee b8 f7 c4 05 aa ec bd d5 a8 41 91 b3 37 54 82 c3 e2 83 31 6c de 00 a1 ee ad d0 12 42 e3 ea cb 97 f4 28 47 2d 0e 99 95 25 75 7d 66 8f 82 18 de 4f e8 ab 47 b6 8d af 03 b8 a7 06 b4 bc 51 c0 64 70 f9 f8 a6 cb 43 5d bb 8a fc 8f bd 66 7b bb 5b 99 1c ee 8f 42 0e bf 14 1d 33 ad d6 04 15 26 62 29 a1 fa 2a 38 3c e8 d6 97 05 d2 4a 1e 3d 68 c1 5e 69 12 55 95 15 b9 af e4 dd 68 8d 79 ac aa 81 28 21 cf 6e 6b 15 52 50 91 b9 4e a0 d5 bf 55 43 45 98 1a 77 f8 15 6a 83 db e2 b4 23 c4 76 a3 63 e0 7f 55 57 54 6e 15 1d a9 d2 3a c3 Data Ascii:)(wSp>!Q*fwj)4!\$SDT9D>Y6vHA7T1lB(G-%u)fOGQdpCj[f[[B3&)*8<J=h^iUhy(InkRPNUCEwj#vcUWTn:
2021-09-16 04:27:57 UTC	78	IN	Data Raw: 6f 10 32 d7 f1 33 eb 44 5d 9a 27 d1 a6 95 07 41 98 5d 66 e4 fa b7 d5 71 af 74 83 f5 5d 16 25 fc 4b 3d fb d0 18 be 8a 9e d3 11 ca f6 fe 20 e4 22 e5 38 a5 f5 4e 49 29 db 4c a5 37 0f ca 8d 99 83 61 ef 3f f0 ab 80 79 de c3 f5 fe a8 44 f6 1d d9 b2 b9 32 5c 28 91 be a6 d0 af b0 77 78 15 a6 5f 55 c4 77 54 56 8a 3c d1 6b 9e 00 b5 fa 27 b6 1e 8e 97 d0 ff 00 ea 51 12 35 e3 5a d0 ae 99 8c 90 10 09 1a f0 3b 97 de 18 c7 b6 8d 94 13 97 75 c6 ad 28 09 36 6a 2b b8 ea 0a 20 db 77 58 21 23 21 0e 3d 9e f4 79 3f 94 64 89 f5 ca e7 53 f8 4a e8 31 1d 13 87 54 96 a3 ad 75 15 1d aa 8a 81 55 55 5f ca 25 51 c8 a3 cd 45 a7 35 50 a2 b2 b1 5a ac d2 2b ab 2a b7 38 f1 5f 34 1a d5 6b 20 fa 11 a8 54 4e 74 40 13 a0 b1 09 9c a7 80 e8 4f ed e2 16 ed 0a 29 e0 74 12 6a 2f 43 be 8a 6c 4e 37 29 Data Ascii: o23Dj]Aqfj%kK="8NI)L7a?yD2l(wX_UwTV<[?Q5Z;u(6j+ wX!#!=y?dSJ1TuUu_%QE5PZ+*8_4k TNt@O)ij/CIN7)
2021-09-16 04:27:57 UTC	79	IN	Data Raw: 78 f7 1c c3 e4 a8 f8 9d dc 0f ba 8b ef 1c 94 c7 df a4 89 e0 3b c2 df 25 f7 4c 5d ff 00 65 23 5c d7 5a d7 d4 8b 34 32 1d 87 58 3b 80 ff 00 8f 92 90 e5 91 cd a3 d8 32 49 4e cd ea b2 65 79 bd 28 1d c0 8d 3b d0 0e d0 75 05 ff 00 95 dc 7b 5a 77 a9 22 ab e9 b2 6c e1 a8 af 15 47 54 5d bc 37 85 a4 8d 3e e4 0b db 43 07 03 ba c6 4e 91 98 7a c5 16 c2 c3 e3 85 7e 8b ef d1 97 31 dd 1c ec dd 5b 7f c2 c4 31 ee 2e cc 2f 76 bf 50 78 21 a8 57 f2 2a 55 68 bb 39 85 15 49 57 f2 8b 4a b2 b6 aa ab 31 54 56 e6 aa 2f 13 45 dc e0 86 9c 55 a8 83 db 7f ea 13 9a ea 81 e0 9b 98 58 84 28 8e 55 09 78 19 86 6d c1 72 84 31 42 5b 88 64 4e cb 70 fb 7c 7e 89 8c c1 7d d8 4c 25 73 a5 e9 65 73 7a b5 02 80 57 7d 15 1b 95 13 75 53 50 aa 74 e6 72 71 b2 26 9b a8 b2 e8 83 23 24 e8 b1 9c a8 09 9a 67 Data Ascii: x;%L]e#ZM42X;2lNey{u[Zw*!GT]>CGjil-1[1./vPx!W*Uh9lWJ1TV/EUX(Uxmr1B[dNp]-)L%seszWj)uSPtrq&#Sg
2021-09-16 04:27:57 UTC	81	IN	Data Raw: 01 b7 a3 da 3d 61 c5 45 89 8a ce a5 b6 5f c1 4c fa b6 9e 73 47 0d d5 fe f4 28 b4 96 b9 bb fb 93 b1 18 4a 1b 16 71 22 d5 e3 c4 2c 0c 9c 9f 95 d3 12 f8 0f a8 37 6e d7 82 81 f4 25 86 bb ea ed fc 47 61 51 76 8f 15 6a 83 50 af cd c2 b2 a0 f4 f3 63 a7 e8 d8 e6 3a 7a cf 7e 8d 0b 0d 83 fd a6 36 a0 f5 5e d8 8e 43 e2 a0 f7 24 03 ba c6 4e 91 98 7a c5 16 c2 c3 e3 85 cd f8 05 81 e5 4c 0b b0 f3 b2 a0 d0 b4 ef 6b 86 84 77 2e 52 c2 72 93 e0 c4 f9 ba fe cd c3 aa f6 fb 40 ff 00 74 52 be 9d 23 9f 41 bc b3 30 f9 a2 e9 72 43 1b 5c 35 cf 0b b2 95 70 5f 84 73 8f 19 65 aa 9b 28 6b 3a 06 d7 86 aa 60 68 e9 1b 33 eb d4 00 96 8e f4 3a 31 50 2b 4d da 29 b1 1c a1 3b a5 64 4e ca ea 66 68 b5 42 39 1c ca 15 d0 39 ae 1a 26 b8 0a a6 34 2a e8 ed de f5 c0 df 72 d5 02 ad 74 4e f5 5b 26 d4 12 Data Ascii: =aE_LsG(Jq",7n%GaQvjPc4z~6^C*KNz<Lkw.Rr@tR^A0rC\5p_se(k'h3:1P+M);dNfhB99&4*rtN[&
2021-09-16 04:27:57 UTC	82	IN	Data Raw: 29 f7 17 d1 0c 3f 2a c7 23 b4 39 9a ef e0 3a fb 90 06 56 ee a8 f8 59 64 c1 44 5d a8 21 be f0 8b f9 22 47 01 5f 30 e7 7f 29 4d 97 96 71 1f f7 63 8d be f1 5a ac 8f 6b 77 b4 ba be 0b fc dc ad 36 ce 2b fc d6 4e 18 31 f9 80 f7 22 f8 ac 2e a0 31 67 23 57 13 96 b4 75 46 a7 b9 62 63 74 72 44 4b 9c 1a 7b f6 93 25 b3 c3 e1 71 1b ba c6 4e 91 98 7a c5 16 c2 c3 e3 85 5e 87 e2 b0 f2 53 3e 1a 56 5a 95 1b 5f 24 f8 85 03 84 82 94 21 d6 24 15 3e 0e 42 e8 f6 a0 7e ad 75 88 ec 3f aa 9a 17 d9 c5 c2 c6 bb e8 3e a1 19 30 42 58 8d e3 76 6b ef 1b c2 8d 81 a4 5e 37 7c 15 5a e8 8d da 76 81 f9 15 ca 1f 76 7c cf ab c3 03 85 4e 85 b5 b2 97 17 fb 20 49 02 84 ad 9e 90 eb a3 9b db b8 f8 ad a5 a2 b0 56 56 2a a7 9c 7a 20 e9 9c f3 ea 0f 89 55 2b b3 98 ae 53 e4 9c 7c 78 bc 14 c6 39 99 bf 50 e1 Data Ascii:)?#9:VYdDj]"G_0)MqcZkw6+N1".1g#WuFbctrDK{[%q#]#FaK^S>VZ_\$!\$>B~u?>0BXvk^f[Zw N lVVv~ U+S Xp9P
2021-09-16 04:27:57 UTC	83	IN	Data Raw: c5 34 02 e7 d0 00 35 dc ba 59 0e 1a 10 44 a0 d5 d5 14 2e fe 9c f5 75 10 d9 41 b1 84 10 01 0a 20 42 0e 69 43 3a a4 45 5c fa 10 d8 71 b3 52 ee 91 8d af 63 45 7e aa 94 65 7b 56 79 15 82 20 2a 9b ab 00 9a e8 eb b2 d9 3f a3 2c 1b ec a7 8b 19 2b 5c d2 28 f2 8e 27 07 04 8e d5 cd a3 bf 33 6c 51 6e df 8a 2e c3 a7 b2 55 b1 44 10 ff 00 0b 6c 7a ae 67 b8 d3 8e 46 e6 5f e4 a4 a7 58 82 7b a8 50 2d 9b 0a ef 5d a4 b7 dd a2 cb f6 b6 28 9e 34 95 f4 3d c3 7a e9 71 8d 6e 63 7c 3c ce 15 ec 7d 17 47 c9 d8 57 7b 18 99 1a 7b 8f fc a7 42 f7 b3 70 c4 bb ff 00 23 4f a2 02 62 de 05 6b f8 1a e6 af 33 16 dd 0f 15 8d 81 dd 21 73 64 f5 36 b8 0e ed eb 95 39 40 d0 b8 35 ba 51 89 f8 9c 4e 69 6a 1b 5d 37 9e fe 0a 28 98 1a d6 80 07 04 02 d1 59 0e 0a ea 19 a3 20 80 a7 c0 39 d3 e0 1a e7 42 6f Data Ascii: 45YD@.uA BiC:E\qRcE~e[Vy *?,+l(3lQn.UdltgF_X{P-}(4=zqnc<)<GW[[Bp#Obk3!sd69@5QNIij7(Y 9Bo
2021-09-16 04:27:57 UTC	85	IN	Data Raw: 37 f7 29 31 53 e4 6d 50 8d 92 40 37 52 8b 16 dc 63 eb 5a 3a e0 f6 2b aa 38 2d 90 88 88 a6 3a 6c 31 3e ab ee c3 1d 62 9d 26 0d 81 c3 6e 02 61 7f 1a 03 b2 ba 4c 33 01 3a 1d 7e 08 39 ae 27 6a d7 8b 7c 11 97 91 f0 98 81 7e 8d cf 8d c7 b5 a5 0f bd e1 dc 48 a1 c3 36 be 16 2b fe 9d 1b 4d 4f 43 3b da 3c 01 a2 73 b1 2d 65 2b 97 5f 9a ce f1 5f 70 46 38 88 6f 58 d8 01 c5 64 63 5b ad 05 ca aa d1 5a dc e0 15 6b a0 42 15 e7 2c c5 61 f1 2d f6 b2 95 2c 13 39 cc 71 b1 f8 26 b9 81 c1 ac 1b 57 05 b5 16 d4 54 5d 74 91 87 51 b5 d5 0c b5 a2 66 5c b7 a2 d5 6d 73 36 c8 51 1e 72 51 2a a9 e4 80 d1 52 74 01 37 93 f0 3d 15 47 4d 20 db 3c 07 00 8b 9d 54 ea f9 1a a0 f1 42 9f 19 ab 6e 15 79 c9 5b 08 60 71 23 91 b1 b2 53 0f 2b ff 00 cb 3d df e9 bc fa 9f 95 db b8 1e 78 31 50 3a 29 5b 99 Data Ascii: 7)1SmP@7RcZ:+8-.l!>;b&nal3:-9'j]-H6+MOC;<s-e+__pF8oXdc[ZkBa,-a,q&WT]lQf\ms6QrQ*Rt7=GM <T Bny[q#S+=x1P:)]
2021-09-16 04:27:57 UTC	86	IN	Data Raw: cd 5d 4d 7b a8 8d 69 7c db d3 5b 1b 46 83 57 27 e2 1e 65 3b f4 54 6a ba b8 54 f2 49 1b 90 3a f3 5d 6f 56 41 bc b9 98 f5 5e 07 bf 54 06 1c 76 1d e8 fd f2 62 ed 5c c6 1f 75 95 1a 6c 28 aa ee 6d be 6a aa 73 80 b3 38 0a d3 b5 17 d8 75 46 83 b1 1a f3 92 8d 51 e6 6e 95 43 87 30 4d 41 1e 63 4a 6a 10 70 f3 7f ca 53 81 a1 14 3c cc 8f 93 7f c2 31 a5 ce 96 21 fe 50 fb 4c ff 00 6c 9f c3 bb b1 63 b9 43 14 d6 0e b9 f5 77 34 71 58 3f b2 d8 0f b8 e0 a4 6b f9 4a 51 ae bd 10 f6 9d db c0 27 48 04 f5 24 b8 ed 93 a9 3d a9 bd 61 a1 e6 08 20 af cd 44 10 a2 14 56 d5 04 53 d3 d4 9c 51 29 c8 a9 a6 95 b1 c6 c7 3d ef 20 35 ad 15 24 9d c0 2e 5c c3 c8 27 c4 e1 1f 1b 87 54 48 e0 dd 7b 17 28 d6 b4 8e bf 9d 63 e2 71 2f 84 86 f1 17 1f 04 d7 13 bd 44 0e 95 4d 71 bd 13 34 68 1d c8 61 70 ef Data Ascii: jM[i][FW'e;TjTl:]oVA^Tvb\ul(mjs8uFQnCOMacJjpS<1!PlLcCw4qX?kQJH\$=a DVSQ)=5\$.!TH{[(cq/DMq4hap
2021-09-16 04:27:57 UTC	87	IN	Data Raw: 04 d6 88 e6 35 25 15 65 f6 97 ec f1 6b 21 9b a6 c2 ff 00 f1 e6 25 cd fe 13 ab 57 20 fd a4 66 48 5e 62 c5 01 57 61 a4 eb 77 b7 da 1d de 4e 07 94 b0 12 e1 31 51 87 c3 23 68 e0 7e 63 81 1b 96 37 ec e7 29 f4 32 d5 f0 3e a6 09 bd b1 c0 fe 21 bc 73 0a dd 39 8f 0e 1b 97 49 ca f9 ff 00 ed 9b 22 8d 55 0e bc d5 6a cd 84 94 21 f7 6c 4c de dd 47 53 e2 8b 23 6b bf 09 71 ec a9 4c a1 02 f7 41 a7 66 ee 3a 21 17 58 d5 c4 d4 a2 6e 55 1b cd 6e 6a 5d 54 57 9e ca de 5e 4e 4f 88 03 ac e3 e0 0a 8c 65 8a 6f d9 cd 56 1a e8 1d fd 54 b8 0c 6b a1 90 56 27 5a bf 22 8c 67 a6 63 bc d9 d1 fb bc 78 27 34 df 7a 73 5c 41 e6 35 f2 6c 3d 09 08 a6 70 51 fb 29 9e ca 6f 04 d2 98 77 05 1f b2 14 7e ca 8b d8 51 a8 9e 2e 2a 83 9b 4a d7 e6 11 63 e8 9d 1b c3 c7 71 1c 41 dc 98 28 e6 dd 8e 19 9a 7b 3f Data Ascii: 5%ek!%W fH^bWawN1Q#h~c7)2>ls9l"Uj!lNGS#kqLfA:IXnUnj]TW^NOeoVTKvZ"gcx'4zs\A5l=pQ)ow~Q.* JcqA{(?>

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:57 UTC	89	IN	Data Raw: 88 a6 d4 58 88 b2 96 9d 04 83 aa ff 00 0d ea 5c 1f 23 47 8c e5 1c 5e 26 67 bc 67 70 6d 5c 19 5b 86 e4 1d ea 2c 4e 11 b3 46 76 5d 61 df 5a 2c 3c df 69 c4 71 90 4c 18 66 46 f3 f8 b5 a7 87 3b bf f5 03 1b d2 35 f4 c0 be 99 46 97 16 3c f7 5a 5d 39 13 18 5d 2f 22 4b 25 2f 09 12 7d 0a b0 5d 37 2c f4 a7 48 58 5d fc 46 c1 52 81 6f 54 d1 5d 5e 88 2a 2d 69 cc 39 a8 a8 17 4f 88 ca 0d 81 4d 6b 00 e0 9b cf 4c 24 80 6f 19 7d e9 bd 30 8d bd 48 ee e3 f4 cf 48 ed 6a 5a 7b 37 a7 3a 42 f3 a9 2a 47 52 a5 0e 6d af 27 60 ab fa 27 79 4e 28 a6 a6 85 44 4d ce 89 d2 77 27 15 ca 78 81 58 a0 79 6f b5 4a 37 de 56 03 93 5d 9f 15 88 0f 77 fb 50 9c de f7 68 98 2c d1 2b 69 4b ba b6 ee 4f 8b 94 73 e1 98 4c 52 3b 3c 59 45 45 f7 78 2e 57 c2 01 8a 93 09 3c 71 93 d6 2d b7 bd 74 c2 a3 Data Ascii: X\iG^&ggpm[,NFv]aZ,<iqLfF;5F<Z]9[/^"K%/)]7,HX]FRoTJ^*-i9OMkL\$0)0HNHj^{\7:B*GRm`yN(DMwx XyoJ7V]wPh,;k)KOSLR;<YEEEx.W<q-t
2021-09-16 04:27:57 UTC	90	IN	Data Raw: 5b f6 72 8c a7 c0 e9 cc 0a 2c 76 64 1e d5 b2 a8 da 79 52 3a cd 04 a9 5f b1 42 50 8a 20 df 2b a1 e5 86 3b 20 76 6d 2a 69 4a 5e ab 5e f4 1e d6 bc 68 56 e4 e0 ad cc 08 54 35 5f f5 c9 fb 58 c5 60 85 15 1a b4 46 aa 85 66 54 28 2f f1 1c 5f dd e0 77 f9 78 9d a8 f5 dd c7 b8 6e f2 f2 e1 99 e4 90 79 ad e8 3c e9 e6 21 57 c8 bf 90 3d 09 f2 07 a0 da 5a 7b 52 36 17 61 64 39 98 74 05 72 4b 5c 58 dc 45 1e 0e 85 09 a3 86 e3 af 4b 2b 22 88 37 e6 08 16 15 95 c5 aa ca 8e f2 68 d2 9a 22 c8 ed 0d d3 63 91 c1 ba 56 be 59 2d 63 80 bb 5c 11 7b 2a 37 81 f1 40 58 2b f3 5d 68 86 54 0b 17 49 cb 98 93 c0 30 2b 0a a1 94 22 85 8a a9 e6 a0 40 2e 89 8e e4 fc 33 bc e3 87 9d 70 f5 41 f5 7b ce ff 00 2c b9 c0 0d eb 2b 40 e0 15 7d 37 9c f2 ed cf 4e 60 7d 08 f4 56 54 2b 44 58 f6 b8 6e 54 c7 c8 Data Ascii: [r,vdyR:_BP +; vm*iJ^*hVT5_X'FFT(/_wxny<!W=TpR6ad9trk\XEK+~7h"vY-c{*7@X+}hTIO+~@.3pA{, +@}7N}VT+DXnT
2021-09-16 04:27:57 UTC	91	IN	Data Raw: f2 0f 35 91 25 52 e7 5f dc fc f1 fd d7 6c 77 ab 73 92 aa ab e4 8f 43 b0 7f fe 0a 35 10 8f 04 d5 d2 1a 36 e5 48 37 15 2b 8d 9a 57 46 2a 75 fd d3 cf 1f dd 6e 15 b9 ef e4 84 10 41 0f 41 7f 4d 6f 4b b3 cf 7e 6b f3 b2 39 ea 77 8a 27 91 51 74 e0 6f fb a1 11 9a 22 5c 49 fd d6 ea ac 07 b3 9a ea ab 4f dc 28 f3 e9 ad cd 7f 47 b3 cf b5 cd 7e 72 00 4d c4 c3 94 9d a0 a3 9a 33 9a 80 f1 4e 82 42 d3 fb 85 f9 fa 7c 40 6e e5 14 5c a5 2b 18 28 01 fd db 60 77 73 55 cb 45 60 ad e8 6f e5 6d 78 7a 6b 7a 5d 9f 26 fc f8 73 0b 2b 1b 74 0a 18 fa ac 01 62 1a 6c f7 04 f7 c3 57 1a f3 5b f7 11 75 ff 00 52 9f f3 7e ed b0 3b b9 b6 82 16 42 ca de 83 ff c4 00 30 11 00 02 01 03 04 01 02 05 05 00 01 05 00 00 00 00 01 02 03 10 11 12 20 21 31 41 04 71 13 22 30 32 51 33 40 42 61 81 05 14 23 Data Ascii: 5%R_lwsC56H7+WF*unAAMoK~k9wQto"IO(G~rM3NB]@nl+(`wsUE"omxz&z&s+tblIW[uR~;:B0 !1Aq"02Q3@B a#
2021-09-16 04:27:57 UTC	93	IN	Data Raw: bf ea cb 62 1b f9 0c 5a 3f 72 1b cb 3b 69 7f 58 29 f0 ff 00 c3 52 43 9b 64 e4 3e 48 d3 1c 30 67 04 79 f7 39 5d 11 93 f2 88 d9 4d 5d c9 0a 3a b7 c2 58 25 14 c9 7a 6f 9d 63 a1 c5 63 8b d3 96 07 3e 0a 7c bb 54 5c 5f 36 af fa 8e ca d1 43 79 7e c3 79 18 bb 47 81 7d e7 9f f4 93 1b e0 64 57 22 e8 94 b8 19 1e c5 f7 11 20 31 54 3e 31 2a c5 27 2a 93 c2 30 92 c2 de c8 48 68 5d 9a 90 99 a8 d6 52 9a 3e 22 2b 56 47 c4 3e 21 ac f8 85 77 f3 5d 0d e2 25 3b af b9 09 f8 23 e4 d5 cd 9b b4 6d 27 78 f6 22 04 ad 93 96 51 a4 a9 c3 1e 7c ed c1 8d 89 e5 12 c7 fe 09 c9 c6 58 62 a8 3a 87 c4 23 50 75 99 2a af 27 c4 35 9a 88 46 72 f0 54 a5 5b 39 d2 ec 84 3c 91 78 95 d7 68 7f 71 ce 09 77 b1 33 3b 17 68 c0 87 7f 4b 0c cf 3f 8d fc 99 ba 78 67 7c 9e aa 9f 0a 56 46 0c 99 7b 22 b2 f0 42 2a Data Ascii: bZ?r;iX)RCd>H0gy9]M]:X%zocc>[T_6Cy~yG)dW" 1T>1**0Hh]R>"+VG>lw]%;#m"x"Q]Xb:#Pu*5FrT[9<xhqw3;hk?xg]VF["B*
2021-09-16 04:27:57 UTC	94	IN	Data Raw: c2 24 18 8a d1 bc 44 87 a1 98 52 d0 99 05 76 53 81 38 e8 4b 49 0a 42 65 08 de 45 4a 76 3b 08 96 0f 6c 1e 82 63 dc 8b b4 8a 72 ba e9 df 0a 84 56 a8 5e 43 5e 64 22 02 dc 7a a1 d3 b4 d9 56 36 c2 ce c4 ae 53 f3 14 e4 4f 62 b4 6c f0 85 ce 19 58 92 bc 49 0b 61 f9 87 e6 3b 0f 64 32 2f 62 43 28 d4 64 65 75 cb 7c 61 44 74 55 89 2b 3c 27 82 f2 af 6c 7b 89 62 88 46 e4 63 62 52 48 f1 ac 26 e4 ef 62 ad ac 42 2a e3 82 b1 59 58 4c 74 52 d0 66 84 b5 28 a1 0d 65 7a 09 37 bb 27 1b 4b 06 4b b3 3b 0f c8 b1 96 c2 d8 a6 f2 c8 8b ee 66 2f 84 a4 29 89 97 29 b5 62 45 58 dc b5 86 8c a4 1d e1 8d 84 b9 28 b1 8e 26 78 a7 a2 19 5a 5a 14 ea 6a 3a 8a c5 59 5d e0 9d 99 1a a4 ea 0b 72 84 ec c9 79 a3 ee 57 8c af 78 b3 c3 a8 e3 77 b8 a9 49 b2 4b 53 78 10 d8 8f 95 9d 97 b9 12 3a ab 11 Data Ascii: \$DRvS8KlBeEJv;icrV^C^d"zV6SOblXla;d2/bC(deu aDtU+< l FcbRH&bB*YXLTRf(Aez7KK;f))bEX(&x ZZj:Y]ryWxwlKSx:
2021-09-16 04:27:57 UTC	95	IN	Data Raw: 66 54 a9 29 cd c9 f3 44 8e df 42 e1 dd e9 47 db 16 37 76 45 61 39 c6 31 bb d8 e2 2b ba b3 f4 ed ce 88 bf a1 70 4e f4 b1 68 4b 09 49 25 76 71 5c 4b ab 2b 2f 2f 41 11 62 7f 41 e0 1e 92 42 c6 e3 76 57 67 15 c5 3a 8e cb cb ff 00 7a 48 8f d0 78 27 6a b6 fb a1 3c 5b 49 1c 5f 14 ea 3c b1 f2 ff 00 de a4 7e 83 c3 bd 2d 68 e3 3a 91 84 6e dd 91 c4 f1 52 ab a2 d2 3c eb 05 1b 9e 19 90 b1 1f a1 53 e3 aa 45 59 ab 92 fd 42 7d a2 8a 95 67 37 79 3e 82 c2 26 83 48 b7 d3 56 11 f9 bb ff 4 6c 64 79 73 7a f5 62 ba 0b e4 98 b7 e9 4f fb 68 fb f2 f7 e7 44 79 7f ff c4 00 28 10 01 00 02 02 02 02 02 03 01 01 01 00 00 00 01 00 11 21 31 41 51 61 71 10 81 91 a1 b1 d1 20 c1 f0 e1 f1 30 ff da 00 08 01 01 00 01 3f 10 49 50 41 05 cb a6 c8 05 ec 63 07 30 86 28 4a 43 31 e8 74 90 8c 3b e6 Data Ascii: fT)DBG7vEa91+pNhKl9%vq\K+//AbABvWg:zHx'<[l_<--h:nR<SEYB]g7y>&HvldyszbOhDyDy(!1AQaq 0?IPAC0 (JC1t;
2021-09-16 04:27:57 UTC	97	IN	Data Raw: b8 11 50 d5 e7 1a bd 29 2c 56 6c 84 b3 95 7f c1 10 56 80 b5 a4 0a 52 59 8d dc 18 be 68 0b 51 91 2d bc 77 2d 38 a5 10 0e 96 cf f6 f3 15 88 ce e1 74 03 4f 23 ee 22 38 b1 15 c5 c0 32 a7 57 dc 3a 11 0d 80 2e d5 52 f4 36 75 10 3a 2c 8f 5d 83 15 f7 4c b4 84 2a a2 fd 21 9f e4 94 73 6c 5b b8 62 af 92 b8 9b 93 70 61 85 b5 eb 92 18 8c 62 cb 97 2e 0c ba 86 20 07 3f 00 31 5e 52 c4 41 38 06 f0 c5 cc 22 05 4d f3 28 33 29 2a 91 e9 b8 7d cc f4 ce 62 5f b4 c6 e6 0b 05 60 15 03 9c 63 77 f7 2d a9 e2 ab d0 b4 ac f7 b9 73 3c 03 6b c6 c5 3a 63 56 60 44 08 b9 46 81 d7 30 d5 80 22 3c 05 0d 78 23 d3 9d 31 5e a5 05 c1 b4 b6 e3 88 cc 79 5f 91 97 8e 2b 2c 7d 4a bc fe 65 f2 39 36 4e cc 18 b8 e1 73 cd b9 39 22 24 29 d2 78 64 84 66 cb 6f 67 64 26 c0 52 e3 b6 20 ae c0 b6 2f 8c 3c f7 Data Ascii: P),VIVRYhQ-w-8tO#"82W:.R6u:;]L*sl[bpab. ?1^RA8"M(3)*]b_`cw-s<k:cV'DF0"<x#1^y_+;J)e96Ns9"\$)xdfogd& R /<
2021-09-16 04:27:57 UTC	98	IN	Data Raw: 86 13 83 97 aa 99 b5 e3 2b c7 27 d4 45 25 03 b0 be 1f bd c3 1a d9 4d 57 ff 00 09 5a ba ca 2c 2e 08 86 c8 79 e4 54 45 6d aa a8 f6 89 82 8d 61 cb 67 d6 c9 4c a8 ca 01 80 2d fa 1a 7d c2 ae 68 25 64 ee 5f 46 d7 51 b2 01 23 86 28 64 1e a1 86 06 67 4b d3 f3 1c ca 41 58 b5 d9 d2 38 f7 2b fe 0b 19 a6 04 43 08 40 51 0d 8d b4 ce f8 3e 71 c1 8a 2f c0 a2 8c 89 8a 25 e9 24 21 45 50 26 52 fb 8a f3 18 bf 20 79 4f 3f c0 5a 17 94 b5 2c 28 9a 14 b9 5f 30 5a 94 be fd c3 58 ce 0e 91 59 de 97 cc 00 9b d8 70 e8 0b 49 79 e5 17 85 19 45 77 fb 40 d6 d8 a0 a4 ac 0a 9e e5 17 06 08 17 d8 29 02 07 84 14 c3 cd b8 af b9 42 65 d5 bb ac 88 b2 c7 6d 5d e5 cd b9 47 02 e5 a1 fd ae c4 49 73 0a a4 72 0d 74 47 c7 4f b8 b1 c9 61 87 dc 2e 31 68 25 8d 0f 9f 30 f5 72 1d 1a 72 0e de 65 30 02 e1 b1 Data Ascii: +!E%MMWZ;.yTEmagL~h%d_FQ#(dgKAX8+C@Q>q/%\$!EP&R yO?Z,(_OZXyPlEw@)Bem]GlsrtGOa.1%h0rre0
2021-09-16 04:27:57 UTC	99	IN	Data Raw: e7 ed ef 71 90 c0 f0 64 18 3f 9f cc 45 7b 62 1a bb af 03 fa 8d 3c 88 80 69 27 53 d1 aa f8 38 be 0b 17 e0 51 47 14 da 73 f1 5f 00 1b 86 77 3b 13 b3 18 ee 1a e2 3c 67 72 ce 60 10 25 cd e8 25 70 06 6f c4 0b 74 51 51 55 5a 56 0b c7 35 6a 06 b1 69 42 da fc 36 ad ba fe 98 cd a4 28 cb 34 d9 5a 77 33 59 4d c5 8f ba 32 be 3a 6a ed b1 7a 1a 8b f2 23 8b 6c 2f 97 f7 14 72 94 0a ac d6 fa 5e 7e 86 36 28 6f 0f b2 73 1e 72 4b ac 12 14 36 78 1a cf 0f e2 23 41 6d 5e c3 71 93 84 f7 28 49 28 c2 86 45 af dd 67 be e1 10 a0 25 b5 78 f1 af 71 31 46 d2 18 87 93 60 f0 c4 0b 55 42 a1 6a d6 5f 62 53 e2 0d 9c da c9 ad e2 63 ec 83 89 ca 57 7b 23 94 f0 fd 45 0d f9 c3 09 5a 4f 35 de fd cb 56 14 e0 51 7e 15 62 56 7c 91 c8 2c ef 5a 62 bb 17 ce e6 48 b2 50 8a db ab 2e e0 70 80 20 57 d7 72 e0 Data Ascii: qd?E{b<i'S8QGs_w;~gr"%%potQQUZV5jiB6{4Zw3YM24zj#lr^~6(osrK6x#Am^q((Eg%x1F`UBj_bScW{#EZ O5VQ~bVj,ZbHP.p Wr

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:57 UTC	101	IN	Data Raw: bf 28 32 0f 92 18 cd 2a 81 e3 4f c6 0f cc 67 60 27 77 52 b4 d0 04 b4 73 09 cf 89 4e 80 ec 47 a8 54 0f 6e 96 e1 d3 dc 55 e2 be 00 88 80 8b e0 aa 79 e2 3b 96 f3 09 66 bf 17 55 0c 81 65 a2 0c e6 dc ec 60 4b 62 3b 47 0c cb 88 19 96 ef 32 c8 09 61 17 e8 d2 3c eb 51 b9 a0 ac c5 6c 1f f6 66 e6 90 67 42 35 ea f7 28 c3 53 0f a0 b9 77 82 dc db b3 11 ac 8a 10 0e a9 4e 18 10 2c 9b 72 52 ef 35 68 cd 46 0d 08 da db d7 26 53 98 e4 8e a7 60 54 16 90 50 39 33 08 03 50 9c 74 e7 91 ca eb d4 2f 20 e8 6c 12 d4 38 2e c3 83 58 9a 6b ce 59 39 73 5c 0c 23 00 29 e9 38 c6 ef f8 81 94 c5 af 6d c8 f9 4b 0a e0 59 b1 e3 0d a0 f8 b0 82 03 c0 18 5d f3 77 8f 2c 47 18 cc 07 35 28 71 88 74 bb 5b c1 67 f1 51 a3 22 e7 8b 5b af 51 20 a6 aa c6 9a 2b ad d4 0e 0d 0e 4b 3c bf 72 f6 d5 6c bc ff 00 Data Ascii: (2*Og`wRsNGTnUy;fUe`Kb;G2a<QlfgB5(SwN,rR5hF&S`TP93Pl/ l8.XkY9sW)8mKYjw.G5(qtfgQ`l[Q +K<rI
2021-09-16 04:27:57 UTC	102	IN	Data Raw: bb b9 e7 09 0c 85 60 9b c3 f8 1f 98 cc a2 8a fd 16 ff 00 10 c6 e3 67 87 2b 3c d6 30 71 23 53 9c e7 dd dc b0 28 50 46 c4 7e 90 bf b8 57 1c 47 92 96 9e f7 51 b6 d3 cd 93 9f 54 91 18 a5 fa c1 8d 5b 06 00 34 70 bc d1 f9 16 fd b3 aa fe b3 4f a8 24 2a b6 9c bf ca b0 90 73 0c 41 da 56 3e a5 0c e5 4a ec d8 3f 71 14 6e 1e fa 0f 7f cc 15 2c b2 a0 6b 45 b6 9e f4 78 8e 16 ee 97 a9 46 f0 70 e6 3a 8d a0 15 4e 54 76 f1 2e 2b 14 29 c0 36 35 b2 00 2a c2 9f 72 d7 72 f2 62 88 e0 cd d9 8d 9c c7 bd c5 b9 a3 32 80 cc bd 33 06 91 43 30 53 72 f2 5c a5 86 28 35 14 85 e2 02 6a 1a ea 5e 71 0c 38 88 2a 07 e6 53 8f b9 bc aa 02 d8 06 ec 78 6c b8 68 12 75 34 67 f1 fa 33 43 2e 8f 59 31 fc 47 a4 5b b2 ce a1 51 ba bd ac 79 7a 80 09 68 ba f4 b0 2f 57 89 be 99 35 45 38 03 b4 fb 25 16 71 68 Data Ascii: `g+<0q#S(PF-WGQT[4pQ\$*sAV>J?qn,kExFp:NTv.+)65*rb23C0S0r(5j^q8*Sxlhu4g3C.Y1G[Qyzh/W5E8%qh
2021-09-16 04:27:57 UTC	103	IN	Data Raw: 41 cc 51 95 10 65 92 c8 0e a5 0c 10 dc d4 e7 19 be 83 0c 24 87 f3 2c 62 1e e2 fa c4 0c ea df d8 33 32 37 b3 c4 5e 17 91 c1 0c e7 dc 0f 48 cc e7 a5 01 a3 c4 27 99 5e b9 14 c3 90 c5 65 05 17 c8 2b e2 0f 81 95 97 5c 4e 58 dc 39 37 68 f2 c6 71 6b 6a cd 28 3e 53 1e 60 44 05 1e 4a 05 2b aa 34 f7 00 04 7a 63 d6 a3 b7 3b a6 30 40 38 b1 4b 5f f6 8a 6a 0b 68 de 41 e1 29 fc 42 06 a9 0c 80 83 2e 2c 6b 8d fc c3 22 60 09 5d 2c 3e c8 4b 6f 6d 39 89 ee 03 ee 19 83 d8 a9 72 b2 15 ed 0f c9 2a ba d5 7b 2e c4 f2 53 5e 60 14 0b 79 ef ef 1f cb 11 b9 a7 d7 84 63 3e 07 ef 72 91 29 b3 8a 5e 4f 4c 55 b0 65 1b 9e fa 72 f6 4c 42 5b 0f af 85 8a 6f b2 5b 60 d0 2d a1 ab ae 40 df 88 39 62 a5 98 f2 f3 7b 23 b2 dc 61 ae c9 e2 b6 40 26 52 e3 66 8c 35 c6 62 21 54 42 39 0a b5 80 58 cc 80 34 5d 3e 2e ff 00 dc 79 b2 bb 22 Data Ascii: AQe\$,b327^H^*e\NX97hqkj(>S`DJ+4Jsm;0@8K_jhA).B.,kom`Kob9B[R?JVjUH@t*#]-H%AWxE4`%kBd&28n @
2021-09-16 04:27:57 UTC	105	IN	Data Raw: e6 25 01 03 db 60 34 e2 2f 39 77 d4 ba 38 b7 68 28 b6 bc 0a b6 1f 83 51 5a 25 ae 80 73 d4 a6 84 82 4c 10 25 28 bc 4b 68 18 ac 7f 30 bb 22 2c 60 69 1f 64 df c9 9c 87 f4 22 4b 05 93 83 17 11 61 51 ca c8 a3 c5 e9 f7 16 82 06 88 12 ad 7a 46 e9 fa 8a aa a0 1d 97 cf 72 34 2c b0 e7 6a 2b b3 88 2f 52 1b d9 2a fa a6 62 3b 29 86 d6 4b 84 25 4c 9b e2 ce 4f 0e a1 bf d2 43 74 2f ec 06 a2 08 25 a9 6b 8d fc c3 22 60 09 5d 2c 3e c8 4b 6f 6d 39 89 ee 03 ee 19 83 d8 a9 72 b2 15 ed 0f c9 2a ba d5 7b 2e c4 f2 53 5e 60 14 0b 79 ef ef 1f cb 11 b9 a7 d7 84 63 3e 07 ef 72 91 29 b3 8a 5e 4f 4c 55 b0 65 1b 9e fa 72 f6 4c 42 5b 0f af 85 8a 6f b2 5b 60 d0 2d a1 ab ae 40 df 88 39 62 a5 98 f2 f3 7b 23 b2 dc 61 ae c9 e2 b6 40 26 52 e3 66 8c 35 c6 62 21 54 42 39 0a b5 80 58 cc 80 34 5d 3e 2e ff 00 dc 79 b2 bb 22 Data Ascii: %'4/9w8h(QZ%\$sL%(Kh0`,`id"KaQzFr4,j+/R*b;)K%LOCt/%k"]`,>r+*{.S^`yc>r)`OLUerLB[o]`-@9b{#a@&Rf5b!TB9X4}>.`y"
2021-09-16 04:27:57 UTC	106	IN	Data Raw: 36 e4 bf 30 cd c3 f5 d9 02 0b b4 5c 2a a5 35 8f 7b 21 d0 04 21 07 84 65 11 f9 8d aa f2 ec ae 5a d4 47 24 a7 25 a7 d8 a8 78 62 96 68 c6 ec 54 72 d8 96 40 b2 e6 71 8f 2f 58 88 1b 68 3d d6 98 d1 d8 30 3c 56 63 71 70 19 71 75 fe c4 60 08 82 b2 9a 07 74 1f 88 39 7a 38 6b 8a c5 f5 28 c8 02 d0 36 5f a1 fa 89 ba f4 64 b3 d8 0f 00 a8 c9 38 36 79 d3 42 be e5 b1 c1 2f a6 2c 08 34 7f b7 b1 71 e2 5a d2 8b 6f b0 f8 ad a8 bb 61 77 36 25 cd 9c 41 11 b9 66 01 e0 42 60 d6 50 a1 e1 e0 74 c5 5a 30 d3 cd f9 3a e1 8b 51 40 80 03 05 8e 1c 61 bd f3 15 90 58 de 6c 57 4f 1c 8c 47 e0 39 76 1c 23 df 89 93 31 4d f1 b4 68 50 f4 40 ac 20 83 13 81 c3 48 2d 63 fe 18 08 35 07 ab 88 37 17 94 6c dc 48 e2 02 5a 44 29 6b 5e 20 a8 ab a5 01 7f b6 22 d0 51 7c 44 ca 35 61 75 b1 fe a1 02 95 Data Ascii: 60!5!(!eZG\$%xbhTr@q/Xh=0<Vcqppqu`t9z8k(6_d\$86yB/,4qZoaw6%AfB`PtZ0:Q@aXIWOg9v#1MhP@ H-c57IHZD)k^`QJD5au
2021-09-16 04:27:57 UTC	107	IN	Data Raw: 36 b1 5f ea 58 43 8d 32 f5 17 75 bb 8b 2b 8b 5f fc 86 94 06 e6 00 17 57 07 23 92 f1 6c 84 70 06 46 50 01 a8 5a 50 db cd 59 43 ec aa 40 46 82 5e ef 49 ea 9b 22 c0 0e ca dd d1 93 c6 23 b4 d5 ec c8 a7 18 ea 73 52 e4 34 9f e4 c4 cd ea 05 77 42 c2 b9 31 29 59 72 51 4a df dc 06 0c 58 3c 22 27 ea 30 8e f2 bd 86 3f 30 d7 2f 33 5c a7 e1 82 b1 c0 6a ec 13 7e 11 29 9e 0f b5 9c 70 92 dc 78 93 a7 72 db 14 61 7a f8 f5 fa 81 2c d4 b7 0d e5 7d 73 0c 26 44 0a 09 fb f9 e6 52 de 3f 18 1d 89 cd 75 d4 6b 09 a7 80 6e ee fc 3c 23 94 96 57 86 db 0e af 92 2a 05 06 29 32 03 c0 a4 a1 ea 60 52 b0 cb 1d 7f 11 62 9a 1f 7f b8 a5 8e 61 51 34 e6 ba 81 70 50 2d b2 93 98 45 e6 2b 00 21 24 48 4b 8b e6 14 da 10 c5 74 d2 5a ba 60 7f b9 42 52 f7 90 f6 1c 31 ea 1e db b0 12 d1 77 90 ea 55 b4 bb Data Ascii: 6_XC2u+_W#lpFPZPYC@F^!`#sR4wB1)YrQJX<""0?0/3j\`)>pxraz.s&DR?ukn<#W*)2`RbaQ4pP-E+!\$HKtZ`B R1wU
2021-09-16 04:27:57 UTC	109	IN	Data Raw: db db 0c 8c 1f 30 db a2 a8 d5 ff 00 ec 6c df 48 19 23 16 75 37 7e 43 d7 51 f2 0f 99 09 fa 12 2f 2b 93 dc 1c 6d a4 16 64 cd 9e e3 52 1c ef dd 41 1a 17 fa 09 6b 17 45 54 47 a8 bc 7c 17 73 1f 43 de 19 af 40 24 75 2a 82 53 79 2a 78 47 f2 43 5e ab 86 9c a3 72 08 6a 9d a5 60 0d bd 47 78 e5 db 16 36 be b5 f5 08 90 00 81 d5 87 d4 5a 58 6b f0 f0 80 ef 0a f7 77 6e bf 5f 88 92 5a 40 aa 4a d8 fc 20 e2 5c d9 16 c7 01 90 85 50 e1 6d ad 1f d4 7d 62 57 6b 77 a0 46 f7 10 1a 8b d8 a8 69 c2 aa 3f 3b 6b cc 67 70 1b a5 7d 14 06 52 9d 96 af a0 ac 29 a8 32 d0 23 bb 2d 40 d4 6e e8 46 8c 0e 4c 71 3a c0 30 20 e3 57 81 ea 1a 4a e5 0e 7b 41 c5 3c f1 29 66 14 41 2e 47 b7 92 05 95 25 59 47 6d 34 0d 9d cc 70 0a 59 f2 29 65 f7 10 22 ee 87 79 d7 ee 04 a3 fd 9d 90 0c 58 3e a2 0e 66 4f Data Ascii: 0lH#u7-CQ/+mdRAKETGjS@C@`\$u`Sy*xGC^rj`Gx6ZXkwn_Z@J lPm)bWkwFi?;kgp)R)2#-@nFLq:0 WJ{A<})fA.G %YGM4pY)e`yX>fO
2021-09-16 04:27:57 UTC	110	IN	Data Raw: ae bf f9 42 2d 62 a3 1a ac 67 9c ab fe c4 2a 38 5f f2 42 0b b4 f7 13 b6 98 9c ee 3f cc ba e9 cc c2 5b bb 91 22 5e 02 4a c8 64 fe 6e 0b 60 94 15 60 03 c0 fe 2e 29 a2 a6 68 a0 fe 15 88 a8 0a 34 ac 5d 07 e2 c9 6f 90 af 1f c0 59 70 5a 3f 8d da bf 3c 4a 84 50 0d 16 d4 d7 09 c3 34 28 c2 da 2c d4 06 9b 8a ab c9 fd 7f 30 24 01 49 2e 9d 85 e7 59 a9 40 20 55 e3 a9 4d 49 5e ae e6 50 3d 4a 80 11 ae 71 70 4c 6b 18 ff 00 bb 97 a4 45 ac f5 16 38 d4 14 75 8b c4 b3 56 2f f9 8c c6 a2 86 5e 01 aa 5e 58 2d f8 fd d1 ba 3d 38 49 5b 82 d1 0f e5 3e 4b 22 dc b5 18 c1 d9 b8 cd 79 05 01 f7 62 ca e6 51 29 48 6f 37 ea 11 b6 cb e6 00 e3 30 16 6e 54 81 64 48 aa 46 10 94 10 e9 0e e2 69 05 94 f4 39 fb 81 56 69 cb 1d 4b f2 c7 15 87 27 35 0f 56 4b e2 fd 7b 9c 64 56 da ec 3a 65 d5 89 cc 30 Data Ascii: B-bg*8_B?["^Jdn`.)h4JoYpZ?<JP4(,0\$!.Y@ UMI^P=JqpLkE8uV/^^=-8l[<"ybQ)Ho70nTdHf9ViK`5VK{dV:e0
2021-09-16 04:27:57 UTC	111	IN	Data Raw: 3a 94 51 32 14 2a b6 c4 bf 1e aa b5 10 b0 f0 dc bc d1 f7 eb b9 5e c5 0b 7c 4b 59 a3 9b 25 ce ed f3 01 5d 6b 89 81 da 4b bc b3 fa 61 3d 56 d4 75 81 0c 12 b5 35 79 1a ff 00 ec 17 8b 74 06 8c 3c fb 9e 59 ba 95 0c ba de 3f 88 8a f9 80 a8 48 0e 09 8b 30 2a 3b 15 d2 66 31 0e 8c 46 30 40 00 b5 5d 04 cd e3 11 46 c0 fe 4e cc 70 d5 39 bf d4 2d 39 65 d7 a8 41 82 a5 8e 33 14 77 e6 1a 37 d3 02 04 00 ce a5 a9 36 af 0f b9 63 4b cf fa 65 47 75 83 dc ca 3c cd 81 ca 3f 73 ce db f9 80 a2 08 b7 ec 86 af a3 11 1c 62 a9 15 c3 2a 23 5c 8c 53 e1 60 30 0b 5f fa b2 59 16 e0 97 50 27 11 4d 44 a8 df 00 ab ad 98 cf d3 18 b1 32 3d 46 24 b5 b2 e6 b0 4c dd 67 05 22 5e 30 c5 30 86 c9 0d a9 b0 c2 f2 d5 d7 d4 50 32 9b ea d0 f4 a7 70 ab ec a5 1c 67 b8 aa 0e db 32 87 fa 9b 1a f3 46 58 84 17 Data Ascii: :Q2*^lKY%)kKa=Vu5yt<Y?H0*`;f1F0@]FNp9-9eA3w76cKeGu<?sb*#S_0_YP'MD2=F\$Lg""00P2pg2FX

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49768	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	571	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvHdw
2021-09-16 04:28:34 UTC	571	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvsU0; expires=Wed, 15-Dec-2021 04:28:33 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: eO8QIDtAiZXU518PzKJeWkp/talxhtGy+SuKNpeqPIQyia/SrF33egNH/RteYe/JNjzGlc95iwawwVRg5k/Hw== Date: Thu, 16 Sep 2021 04:28:34 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
100	192.168.2.3	49857	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	780	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf_AWVfEUScgKE
2021-09-16 04:28:47 UTC	781	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf_AWVfEUScyfc; expires=Wed, 15-Dec-2021 04:28:46 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: /Ty03kKsOWimNmSl5Ows14ZltsOP5uTHMXvaUosI+IQoAHQ4klX2RuzJOyUHWJRJ6IH90AlxNDOTA XE+K2P/w== Date: Thu, 16 Sep 2021 04:28:47 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
101	192.168.2.3	49858	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	782	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf__AWVfEUScYfc
2021-09-16 04:28:48 UTC	782	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: o1rihH+x6MCqWuv7OVnnW8Kwqn8fRFBjuJYUnPNFZIXEphBLMmynS2OzyHQtlmKy2s5/3/+yCpM5A Wzn0cjg== Date: Thu, 16 Sep 2021 04:28:48 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:48 UTC	783	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 41 71 6e 36 4e 61 62 42 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="Aqn6NabB">*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:48 UTC	784	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 41 71 6e 36 4e 61 62 42 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 62 53 38 74 63 30 35 30 2a 2f 7d 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="Aqn6NabB">body * {display:none !important;}\u003Cstyle>\u003Ca href="#" onclick="\"top.location.href=window.location.href\" style="display:block !important;padding:10px!>Gehe zu facebook.com \u003C/a>);/*bS8tc050*/})();/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
102	192.168.2.3	49859	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	784	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf__AWVfEUScYfc
2021-09-16 04:28:48 UTC	785	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5iMM; expires=Wed, 15-Dec-2021 04:28:47 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: pAtw0rFdHOCpRMw9gr44c2ZGp4IUIYJmjq3MhVobJgF4wYool8TwVdRA61a4gQbMvXZIZlyz/gDM2 F/F9vHQA== Date: Thu, 16 Sep 2021 04:28:48 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
103	192.168.2.3	49860	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	786	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5iMM
2021-09-16 04:28:48 UTC	787	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: ocpyqqGsxlQxx1ghL+Zek8EREP4vfSCDYoEOc9Cpa56+qq14WVPZPXC3cwwtc0YV44R3SRurXLN9ma5/vwQmQ== Date: Thu, 16 Sep 2021 04:28:48 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:48 UTC	787	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 67 55 72 53 4b 51 47 4f 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 39 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="gUrSKQGO">/*!<[CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=9
2021-09-16 04:28:48 UTC	788	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 67 55 72 53 4b 51 47 4f 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4c 34 4e 69 56 Data Ascii: ow.document.write(""+u003Cstyle nonce="\gUrSKQGO!">body * {display:none !important;}}u003Cvstyle>u003Ca href="\#\" onclick="\top.location.href=window.location.href\" style="\display:block !important;padding:10px!>Gehe zu facebook.com/u003C/a>");/*L4NiV

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
104	192.168.2.3	49861	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	789	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5iMM

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	794	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5ZdY
2021-09-16 04:28:48 UTC	794	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5BVM; expires=Wed, 15-Dec-2021 04:28:47 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: P168m8vgtXAXltvMF2pcMxyJcqFm657HWG1j77TelarfsGpPv+mlXs3h5RastvnX80G3194GfEOLgN irDPk3Vw== Date: Thu, 16 Sep 2021 04:28:48 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
107	192.168.2.3	49864	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	795	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5BVM
2021-09-16 04:28:48 UTC	796	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 9hDNBXxMgu/wJddAygno+OJwz8t5S6X28A3Kr4OLWYfj8LoE24aD1/FrTlmadkmM00QKl7hdm6NCX86lzsslyA== Date: Thu, 16 Sep 2021 04:28:48 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:48 UTC	797	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 0 6e 6f 6e 63 65 3d 22 4f 44 68 72 70 56 50 6a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 36 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ODhrpVPj">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=6
2021-09-16 04:28:48 UTC	798	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4f 44 68 72 70 56 50 6a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 59 54 44 45 32 2d 6f 77 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="ODhrpVPj">body * {display:none !important;}u003C/style>u003Ca href="\"#\" onclick="\"top.location.href=window.location.href\" style="display:block !important;padding:10px!>Gehe zu facebook.com/u003C/va>");/*YTDE2-ow*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
108	192.168.2.3	49865	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:48 UTC	798	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgA.AWXJVzq5BVM
2021-09-16 04:28:49 UTC	799	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGVbfU; expires=Wed, 15-Dec-2021 04:28:48 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 53CjnRs2QP0QD7IZOUTZJb8QPecZLknlZEmnF0uP/YPsMlvT3xK5o5clQeDk6YQ20GG1A3xfpY38lt vBsVWsog== Date: Thu, 16 Sep 2021 04:28:49 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
109	192.168.2.3	49866	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	800	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGVbfU
2021-09-16 04:28:49 UTC	801	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: im0o5he04Udk+w/IvAenHjAmqGLoAWIFhPzAhgVkTXGybUh49A1CNdMj+F6RvEZWxf3+6s/GExs2j4CateEJw== Date: Thu, 16 Sep 2021 04:28:49 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:49 UTC	801	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4a 48 74 6f 68 6f 51 54 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="JHtohoQT"/>*<![CDATA[*](function){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	802	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4a 48 74 6f 68 6f 51 54 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 52 4a 65 54 39 4e 68 56 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="JHtohoQTV">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003Cva>");/*RJeT9NhV*}}})/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49766	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	572	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvsU0
2021-09-16 04:28:34 UTC	573	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: PHGq+psAMKIAJfly7IRUeDQ+3Q2zdg7mJXA9xmbnEzLUxxf5Jr5GUOCdhd+ZbH7PkEIIIVEJMNJI ts2Hj3vA== Date: Thu, 16 Sep 2021 04:28:34 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:34 UTC	574	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 53 5a 30 68 32 64 59 63 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="SZ0h2dYc"/><![CDATA]*{(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:34 UTC	575	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 53 5a 30 68 32 64 59 63 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6b 7a 53 33 57 48 6f 74 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="SZ0h2dYc">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003Cva>");/*kzS3WHot*}}})/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
110	192.168.2.3	49867	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	803	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGvbfU

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	804	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGv9Wo; expires=Wed, 15-Dec-2021 04:28:48 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: zRID0Lrw8jUX6pFJCTy4hlsZdA6Ecdt1iLipNxNisJU7eTJFoWSzE02tW8ff1vrZNz9EqFiwexig+p mehYaRUw== Date: Thu, 16 Sep 2021 04:28:49 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
111	192.168.2.3	49868	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	805	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGv9Wo
2021-09-16 04:28:49 UTC	805	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: KzwPz6rcog3Z9NfZe9oY+IgUi/8Ks8H458EYFeWQLco2Fgcwt92KABHj6BGbnJg+9j41iqHF5+cSOqfX2B2H7Q== Date: Thu, 16 Sep 2021 04:28:49 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:49 UTC	806	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4e 68 35 32 63 32 61 39 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="Nh52c2a9"> /*<![CDATA["(function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:49 UTC	807	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4e 68 35 32 63 32 61 39 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 68 47 5a 66 6e 36 47 68 2a 2f 7d 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="Nh52c2a9">body * {display:none !important;}u003Cstyle>u003Ca href="#">onclick="\top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003C/a>");/*hGZfn6Gh*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
112	192.168.2.3	49869	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	808	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGv9Wo
2021-09-16 04:28:49 UTC	808	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGvNU8; expires=Wed, 15-Dec-2021 04:28:48 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: FbJHZkZAsJmBM8Bhv3MvFKDsQQI3VMXxY+bT134+D72yq68NeNY0Uvv4qeyJ7+I+BkSONep+DmxrZ0 JKRPSpYQ== Date: Thu, 16 Sep 2021 04:28:49 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
113	192.168.2.3	49870	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	809	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGvNU8
2021-09-16 04:28:49 UTC	810	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: pVKSh/pHAJVKUdeC3XVgvsgOI5muxRiZrIC+TX0WKiHWLpOfBAMq7xXQH/dtT8dKETWazkiRSchrMmqCUTSGA== Date: Thu, 16 Sep 2021 04:28:49 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:49 UTC	811	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 62 4c 4d 61 62 42 54 62 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="bLMabBTb">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:49 UTC	812	IN	Data Raw: 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 62 4c 4d 61 62 42 54 62 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 59 69 58 4b 6d 4b 67 63 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a 2f Data Ascii: "u003Cstyle nonce="\bLMabBTb\ ">body * {display:none !important;}u003C/style>u003Ca href="\#\" onclick="\top.location.href=window.location.href\" style="\display:block !important;padding:10px\ ">Gehe zu facebook.com\ u003C/va>");/*YiXKmKgc*}}{}}/*...*/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
114	192.168.2.3	49871	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	812	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgB.AWUQXDGVNU8
2021-09-16 04:28:50 UTC	813	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0to; expires=Wed, 15-Dec-2021 04:28:49 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: Ucb7gpmjYAVL+qz2EqX/JahDwZKoRQy7uYX0Z5lLh1O++wa4SiQboalsLjzvspFo9rjKxnal5/HL7w h9P6xfAA== Date: Thu, 16 Sep 2021 04:28:50 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
115	192.168.2.3	49872	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	814	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0to
2021-09-16 04:28:50 UTC	815	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: nCew8tmZTWCy58d7mBgg87PQSzfg7xvb+4cok6HvdfqLnn8viFYIy1/5ua2I94oMUXWlLqTw1mHF3 xE3O6xxQ== Date: Thu, 16 Sep 2021 04:28:50 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	815	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 61 66 48 4b 71 48 68 77 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="afHKqHhw">/*!CDATA[*/(function(){}function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3
2021-09-16 04:28:50 UTC	816	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 61 66 48 4b 71 48 68 77 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 42 4c 72 59 7a Data Ascii: ow.document.write("u003Cstyle nonce="afHKqHhw">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003C/a>");/*BLrYz

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
116	192.168.2.3	49873	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	817	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0to
2021-09-16 04:28:50 UTC	818	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0-U; expires=Wed, 15-Dec-2021 04:28:49 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: jqSckslITgK4EzP3zbhSDJOvr+e0KXcJK8SFzkKh+HqRivHsxRzY+OgnuyAxiqdu17awCM7vQG6rQ2 BfrhCbfg== Date: Thu, 16 Sep 2021 04:28:50 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
117	192.168.2.3	49874	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	819	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0-U

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	819	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: eydBqxX9vfko4DHvvpap2xxNu3UtBJzidTSleuXDWmusjuPf5PVghja6fFIU5BMI9EYZSGRr3RI/uxeHzggNiQ== Date: Thu, 16 Sep 2021 04:28:50 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:50 UTC	820	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 50 4b 49 6e 30 42 47 5a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="PKIn0BGZ"> /*<![CDATA[*(function() {function si_cj(m) {setTimeout(function() {new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3
2021-09-16 04:28:50 UTC	821	IN	Data Raw: 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 50 4b 49 6e 30 42 47 5a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 33 49 31 63 46 41 41 66 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a 2f Data Ascii: "u003Cstyle nonce="\u003Cstyle>\u003Cbody * {display:none !important;}u003Cvstyle>\u003Ca href="\u003Conclick="\u003Ctop.location.href>window.location.href" style="\u003Cdisplay:block !important;padding:10pxl">Gehe zu facebook.com\u003Cva>");/*31cFAAf*}})}/*...*/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
118	192.168.2.3	49876	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	822	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0-U
2021-09-16 04:28:50 UTC	822	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdK0YAQ; expires=Wed, 15-Dec-2021 04:28:49 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: Qx9ermys3ZhWXJRs96akmmzCt3s1UvrRVi4/SrbK3Ut5nSno2lcC8elUQpbDGtcZr6wxcmjF+EKhLz9kMJTK7g== Date: Thu, 16 Sep 2021 04:28:50 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
119	192.168.2.3	49877	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	823	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdKYAQ
2021-09-16 04:28:50 UTC	824	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 3heBpv7/cpHAM2Lj8VZR2Clf3XMjmsLPsqJfXh9bldCalhNyUgnudMPqej1E4reTZE/mezRFAWNIEcwtVWmlkQ== Date: Thu, 16 Sep 2021 04:28:50 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:50 UTC	825	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 7a 42 55 58 56 36 42 34 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="zBUXV6B4">*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:50 UTC	825	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 7a 42 55 58 56 36 42 34 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 69 73 56 68 4d Data Ascii: ow.document.write("u003Cstyle nonce="zBUXV6B4\">body * {display:none !important;}u003Cvstyle>u003Ca href=\"#\" onclick=\"top.location.href=window.location.href\" style=\"display:block !important;padding:10px!>Gehe zu facebook.comu003Cva>)/\";isVhM

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49769	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	575	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvsU0

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	576	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvNII; expires=Wed, 15-Dec-2021 04:28:33 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: pBZES45BWJ6RAAWDUqTdapA8vHC+jAU/BITS5CmkZRxSVpWT0S18poGnHGmm89nl2RXU ne1Mi9PYEHYBj4DOpw== Date: Thu, 16 Sep 2021 04:28:34 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
120	192.168.2.3	49878	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	826	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdKYAQ
2021-09-16 04:28:50 UTC	827	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdKZDc; expires=Wed, 15-Dec-2021 04:28:49 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: g06FTs8EFN16NgjzVRWb9vO3N0uNb7YrVQ7UKFx37IUZsqsSu2b70b6Vq3XKJDIkjlWEFR+sg+y0 TNB13xNg== Date: Thu, 16 Sep 2021 04:28:50 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
121	192.168.2.3	49879	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:50 UTC	828	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdKZDc

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	829	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: xs3nJsLtGRaZQscipcZpGtxrdm14MvX7uEweWhOraTX4u80lR3DR5OVPIDgdlvslIFRXCNxXfXnZBfvB5rNOGaQ== Date: Thu, 16 Sep 2021 04:28:51 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:51 UTC	829	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 52 4a 69 70 57 71 32 61 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 37 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="RJipWq2a">*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=7
2021-09-16 04:28:51 UTC	830	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 52 4a 69 70 57 71 32 61 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 58 51 70 69 35 Data Ascii: ow.document.write("\u003Cstyle nonce="RJipWq2a">body * {display:none !important;}\u003Cvstyle>\u003Ca href="#" onclick="\u003Ctop.location.href=window.location.href\u003C" style="\u003Cdisplay:block !important;padding:10px\u003C">Gehe zu facebook.com\u003C/a>");/*XQpi5

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
122	192.168.2.3	49881	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	831	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgC.AWU6DZdKZDc
2021-09-16 04:28:51 UTC	832	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnL3k; expires=Wed, 15-Dec-2021 04:28:50 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 9JaE4jkmZ5uCRr97B+78szPH8P+QqutRJH9pbTzLj5ZEMBk0cHzrhezLTwa4DDtKIFUXZMj6Ylui5tv6DKAniw== Date: Thu, 16 Sep 2021 04:28:51 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
123	192.168.2.3	49882	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	833	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnL3k
2021-09-16 04:28:51 UTC	833	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: ZivGHwva70eWWB0TeFmgC/z9Vsvl0BgX+UT1m5yuBgSp+9hMg+fx8B3elthB823G5p/TqP4Gemjj+Cw5cJZSw== Date: Thu, 16 Sep 2021 04:28:51 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:51 UTC	834	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 69 69 51 33 70 33 6b 38 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="iiQ3p3k8">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:51 UTC	835	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 69 69 51 33 70 33 6b 38 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 48 7a 4a 54 72 Data Ascii: ow.document.write("u003Cstyle nonce="iiQ3p3k8">body * {display:none !important;}u003C/vstyle>u003Ca href="#" onclick="location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003C/va>);/*HzJTr

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
124	192.168.2.3	49885	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	836	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnL3k

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	836	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUntpM; expires=Wed, 15-Dec-2021 04:28:50 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: pOGd4LwSy4VMR0P+dZCPA+typI8NPdt7fqoeZ7XII0x3MjJB+cfYDgQzchQklXo8Ln232yokigXkk M1/xYoyw== Date: Thu, 16 Sep 2021 04:28:51 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
125	192.168.2.3	49884	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	837	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUntpM
2021-09-16 04:28:51 UTC	838	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: JTUUXGhUmY5of2VpBmx6Yy+QNR0au4mysdciUoTrkepfP/Qnrpx59/GH11hXFrDOaWm+FqljOOTuya a+83aC/Q== Date: Thu, 16 Sep 2021 04:28:51 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:51 UTC	838	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6f 64 35 6a 63 37 7a 35 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="od5jc7z5">*<![CDATA[*(function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:51 UTC	839	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6f 64 35 6a 63 37 7a 35 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 30 68 59 6c 33 Data Ascii: ow.document.write("<u003Cstyle nonce="od5jc7z5">body * {display:none !important;}<u003Cvstyle><u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px;">Gehe zu facebook.com<u003C/a>");/*0hYI3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
126	192.168.2.3	49887	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	840	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUntpM
2021-09-16 04:28:51 UTC	841	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUn0Hk; expires=Wed, 15-Dec-2021 04:28:50 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: P4gHBcKpn8fKqRSRzQW0sv4/GrMsAnArcGKRYX2aR7OQUGaM03XLN/w2ssg202NzOMR/vQYDzIEUyzg2+oPuzg== Date: Thu, 16 Sep 2021 04:28:51 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
127	192.168.2.3	49888	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	842	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUn0Hk
2021-09-16 04:28:51 UTC	843	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: fUvJ/PzGnNy5/tH84i1raU9hMmcBM1uULFcwvPQRowcptGhWUcb0IZykrVot1bPBjMTMXyJ9mV7rD+fg8xwoA== Date: Thu, 16 Sep 2021 04:28:51 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:51 UTC	843	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 66 74 6c 77 64 66 31 38 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ftlwdf18">*<![CDATA[*]](function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	844	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 66 74 6c 77 64 66 31 38 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4b 70 51 76 79 Data Ascii: ow.document.write("u003Cstyle nonce="ftlwdf18">body * {display:none !important;}\u003C/style>\u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003C/a>");/*KpQvy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
128	192.168.2.3	49891	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:51 UTC	845	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUn0Hk
2021-09-16 04:28:51 UTC	846	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnYck; expires=Wed, 15-Dec-2021 04:28:50 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: bHzFCnvQRLb+gQe8cUeEmVQZiMOA8+P8WYcV6kQwFW32pUjOIETzjOGsswEM9RInceLP91PX1QPr2D3FGZO0KQ== Date: Thu, 16 Sep 2021 04:28:51 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
129	192.168.2.3	49892	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	847	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnYck
2021-09-16 04:28:52 UTC	847	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: zStuzcJCjQ9+4sBMA7zE4NPn3c91Q/xMcoXaGsDLLtiECYfSimmdquOusrkYQxhDt7V6RwGGA2wOtcsMdNixg== Date: Thu, 16 Sep 2021 04:28:52 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	848	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 66 50 73 48 72 5a 31 66 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="fPsHrZ1f">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:52 UTC	849	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 66 50 73 48 72 5a 31 66 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 48 54 68 48 6d Data Ascii: ow.document.write("<u003Cstyle nonce='fPsHrZ1f'>body * {display:none !important;}<u003Cvstyle><u003Ca href='\"#\"' onclick='\"top.location.href=window.location.href\"' style='\"display:block !important;padding:10px!>Gehe zu faceb ook.com<u003Cv>\">\";/*HTHm

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49770	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	577	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvNII
2021-09-16 04:28:34 UTC	578	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: gG734LXHnmBNzgLwkCDaL1ydpCArPylhRvnnVypcTRvrYULqaD5Mw0sQdVG1Cyi0qovcYmDJFed0M+z9kBZ6uw== Date: Thu, 16 Sep 2021 04:28:34 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:34 UTC	578	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 70 78 69 46 35 54 59 4d 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 39 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="pxiF5TYM">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=9
2021-09-16 04:28:34 UTC	579	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 70 78 69 46 35 54 59 4d 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 57 53 78 71 31 Data Ascii: ow.document.write("<u003Cstyle nonce='pxiF5TYM'>body * {display:none !important;}<u003Cvstyle><u003Ca href='\"#\"' onclick='\"top.location.href=window.location.href\"' style='\"display:block !important;padding:10px!>Gehe zu faceb ook.com<u003Cv>\">\";/*WSxq1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
130	192.168.2.3	49894	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	850	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgD.AWVMSWUnYck
2021-09-16 04:28:52 UTC	850	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXNFENNLY; expires=Wed, 15-Dec-2021 04:28:51 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: UN0BTG14oBuM1s7rbNksCdbbAHaZU+/706k/sEpE6BMLRCVUXOUj02PanW7BH0RwdJBRYLANw9MDyhI6lX6elw== Date: Thu, 16 Sep 2021 04:28:52 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
131	192.168.2.3	49895	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	851	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXNFENNLY
2021-09-16 04:28:52 UTC	852	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: jhEs4QuaSoqJ8QFYUn94W/z64ZwnAi4fL+VMnovudK80tOccaty3SWuUQOW0FYilrXbe0uoba/HkQcbJYbbRA== Date: Thu, 16 Sep 2021 04:28:52 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:52 UTC	852	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 0 6e 6f 6e 63 65 3d 22 72 4f 4e 46 5a 4e 77 75 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="rONFZNwu">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:52 UTC	853	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 72 4f 4e 46 5a 4e 77 75 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 75 32 32 59 78 66 62 5a 2a 2f 7d 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="rONFZNwu">body * {display:none !important;}}u003C/style>u003Ca href="#" ononclick="\top.location.href=window.location.href" style="\display:block !important;padding:10px!">Gehe zu facebook.com\u003C/va>");/*u22YxfbZ*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
132	192.168.2.3	49897	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	854	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXxNFENNLy
2021-09-16 04:28:52 UTC	855	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXxNFENKEc; expires=Wed, 15-Dec-2021 04:28:51 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: cEJZTGDe5qrt4hj/y9Vk+v+HSAplI8PboNo1ydNU8tBF8xfek0ITxY3+aChKmv27P9bAWOAMAd5trnhi9VHw== Date: Thu, 16 Sep 2021 04:28:52 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
133	192.168.2.3	49898	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	856	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXxNFENKEc
2021-09-16 04:28:52 UTC	857	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: NjWpCs+59jayh3VhaCvkCEk9DaM8oOMYWtLq8o5KKFWgDZm4aB6LTboznnrlog57J0rWspuTE5PGRL5oSby+3g== Date: Thu, 16 Sep 2021 04:28:52 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:52 UTC	857	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6e 6b 37 68 6e 50 42 71 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="nk7hnPBq">*<![CDATA]*!(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	858	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6e 6b 37 68 6e 50 42 71 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6c 59 67 57 71 69 31 33 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="nk7hnPBq">body * {display:none !important;}u003Cstyle>u003Ca href="#" onclick="\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003C/a>");/;YgWqi13*}})}()*/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
134	192.168.2.3	49900	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	859	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXNFENKEc
2021-09-16 04:28:52 UTC	859	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXNFENVbw; expires=Wed, 15-Dec-2021 04:28:51 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: G5D6BLR/95gvKGVWmyAgw8/apHpJzoSMOx+QiGsKwQLNaTy+sAQCI2nf17Mw1fDf4BowM24MyhPOAGd1OJRbhw== Date: Thu, 16 Sep 2021 04:28:52 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
135	192.168.2.3	49901	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	861	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXNFENVbw
2021-09-16 04:28:52 UTC	861	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: J8QylLW4cuB4lj7lBtWqLCLD+j3Dgll4plKh2QsJNTnspG2hsXF+MtkCUOaKbD0rx9KSi93rm91t0xzR8CD/w== Date: Thu, 16 Sep 2021 04:28:52 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	862	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 68 76 62 42 65 4c 57 74 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="hvbBeLWt">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:52 UTC	863	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 68 76 62 42 65 4c 57 74 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 53 59 37 6a 47 56 45 32 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="hvbBeLWt">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003Cv>");/*SY7jGVE2*/}})}/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
136	192.168.2.3	49903	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:52 UTC	863	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXnFENVbw
2021-09-16 04:28:53 UTC	864	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXnFENLfw; expires=Wed, 15-Dec-2021 04:28:50 GMT; Max-Age=7775998; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: h+iwVNx8bfs23bvknAYavrAZmwaRPpDL4k2dPrkys0R4isdCm2nPBgDA84iEGA0ZWYfc+Q6i0gx5Ok4//qJobQ== Date: Thu, 16 Sep 2021 04:28:53 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
137	192.168.2.3	49904	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	865	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXXnFENLfw

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	866	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html;charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: GcbDIMFcQwFiye7tr8LnemirnbicyAoLF+EHwJHPcnkkyflAudReWAs6lo3kJIVCdLEfHWclUaDFNP EcePsgxA== Date: Thu, 16 Sep 2021 04:28:53 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600,h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:53 UTC	866	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 52 62 67 37 41 32 71 4e 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="Rbg7A2qN"/>*<!CDATA[*]/(function(){function si_cj(m){setTimeout(function(){})(new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3
2021-09-16 04:28:53 UTC	867	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 52 62 67 37 41 32 71 4e 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 70 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 72 71 56 76 36 Data Ascii: ow.document.write("\u003Cstyle nonce="\u003Cstyle>\u003Ca href="#\" onclick="\u003Cstyle>\u003Cscript>\u003Cbody * {display:none !important;}</script>\u003C/a>" style="\u003Cscript>\u003Cbody * {display:none !important;padding:10px}>Gehe zu facebook.com\u003C/a>");/*rqVv6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
138	192.168.2.3	49906	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	868	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgE.AWXxNFENLfw
2021-09-16 04:28:53 UTC	869	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWW6Cq9feA8; expires=Wed, 15-Dec-2021 04:28:52 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: TRQ/dNXMHbJiXThwSISdkq61F/X6yf9nvmfctgUab32ahH5QXZcOPBBOPityFUJNCw2u7ymeVLxm31 PqAUHJiQ== Date: Thu, 16 Sep 2021 04:28:53 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
139	192.168.2.3	49907	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	581	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMbVlWw; expires=Wed, 15-Dec-2021 04:28:33 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: Dq++X377d5bK/klWrEQUS7Q170KLe17bNQ5I7FQ6+8K2QZfunRNQEOBL0JofX19N2JYz1bXTInVMhrBZ8Ltcw== Date: Thu, 16 Sep 2021 04:28:34 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
140	192.168.2.3	49909	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	873	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWV6Cq9feA8
2021-09-16 04:28:53 UTC	873	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWV6Cq9fn0E; expires=Wed, 15-Dec-2021 04:28:52 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 3RS78rJQP1aeVzEt7JvAU25mIG0u6tmli/oQ30Ki0sVICzToRk3ky7EA/dWzHCFRd3hZbfB8Lv3mD05X7CxFnw== Date: Thu, 16 Sep 2021 04:28:53 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
141	192.168.2.3	49910	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	874	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWV6Cq9fn0E

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	875	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: cFTY63UD5TC2+rqV6od2UEGNFEo67Fpl/OraJj1NV3wWmLYUAAOgCQ1h1OZ8ukMO38dFbhx5c9P++R3aSXmCHA== Date: Thu, 16 Sep 2021 04:28:53 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:53 UTC	876	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 33 4b 4f 50 6f 35 75 70 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="3KOPo5up"/>*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:53 UTC	877	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 33 4b 4f 50 6f 35 75 70 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 35 59 75 77 4f Data Ascii: ow.document.write("\u003Cstyle nonce="\u003COPo5up"/>body * {display:none !important;}\u003Cvstyle>\u003Cahref="\u003C/a>")/*5Yuwo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
142	192.168.2.3	49912	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	877	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWW6Cq9fn0E
2021-09-16 04:28:53 UTC	878	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWW6Cq9ffLs; expires=Wed, 15-Dec-2021 04:28:52 GMT; Max-Age=7775999; path=/; domain=facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: o/DrCPXYy6AHGZcuT6wnbi+uk918jSYhfsZQOXzJn6Y3MSySuxS6rMhu5OiYp2ri7gq16um+ip1OatRrqES9Ow== Date: Thu, 16 Sep 2021 04:28:53 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
143	192.168.2.3	49913	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:53 UTC	879	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWW6Cq9ffLs
2021-09-16 04:28:53 UTC	880	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: WSR7PV4LuR11sy5c0Zc3rpU0rjArqotP/3z2dCV5TdOvsbV/3deYA5ZWrmY9VSeRAC+MOtrkAkU2/QcC0tBhJw== Date: Thu, 16 Sep 2021 04:28:53 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:53 UTC	880	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6a 55 35 58 79 72 31 42 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="jU5Xyr1B">/*!CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3
2021-09-16 04:28:53 UTC	881	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6a 55 35 58 79 72 31 42 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6f 6f 59 58 4d 57 57 76 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="jU5Xyr1B">body * {display:none !important;}}u003Cvstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comu003Cv>");/*ooYXMMWWw*}}{}})/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
144	192.168.2.3	49915	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:54 UTC	882	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWW6Cq9ffLs
2021-09-16 04:28:54 UTC	883	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgF.AWUUIWcZhS_w; expires=Wed, 15-Dec-2021 04:28:53 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: ybFRFS+4phKDjRQsIJ5cjoQHf3mmZ+P7dQUdXkI6JdZdVa4W1zMm7g0kOgeduS6cugdVd6XykSHOCwvgN1D2Hg== Date: Thu, 16 Sep 2021 04:28:54 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
145	192.168.2.3	49916	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:54 UTC	884	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsgG.AWUIWcZhS_w

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
146	192.168.2.3	49921	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:55 UTC	884	OUT	GET /entertainment/hailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:28:55 UTC	885	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 46937 Connection: close Date: Thu, 16 Sep 2021 04:27:56 GMT content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Cache-Control: max-age=3600 Apigw-Requestid: FvQn-hc9oAMEP7g= Vary: Accept-Encoding X-Cache: Hit from cloudfront Via: 1.1 7abd55cee48606340f570b45718202b6.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: wrapHFHBWRyhyf0x02-rSGY3rdbdPTlotcjxRxEW73RK70ahQM5g== Age: 59
2021-09-16 04:28:55 UTC	885	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:28:55 UTC	901	IN	Data Raw: 61 69 6e 6d 65 6e 74 2f 6a 75 73 74 69 6e 2d 62 69 65 62 65 72 2d 6e 65 74 2d 77 6f 72 74 68 2d 68 61 69 6c 65 79 2d 62 61 6c 64 77 69 6e 2d 65 61 72 6e 69 6e 67 73 2d 6d 6f 6e 65 79 22 3e 57 68 61 74 20 49 73 20 4a 75 73 74 69 6e 20 26 61 6d 70 3b 20 48 61 69 6c 65 79 20 42 69 65 62 65 72 e2 80 99 73 20 4e 65 74 20 57 6f 72 74 68 3c 2f 61 3e 3c 2f 65 6d 3e 3c 2f 68 33 3e 3c 70 3e 48 61 69 6c 65 79 2c 20 77 68 6f 20 77 6f 72 65 20 61 20 53 61 69 6e 74 20 4c 61 75 72 65 6e 74 20 62 6c 61 63 6b 20 73 74 72 61 70 6c 65 73 73 20 73 68 65 61 74 68 20 67 6f 77 6e 20 77 69 74 68 20 61 20 70 6c 75 6e 67 69 6e 67 20 65 6d 62 65 6c 6c 69 73 68 65 64 20 6e 65 63 6b 6c 69 6e 65 20 61 6c 6f 6e 67 73 69 6 4 65 20 61 20 73 75 69 74 65 64 20 42 69 65 62 65 72 2c 20 77 61 Data Ascii: ainment/justin-bieber-net-worth-hailey-baldwin-earnings-money">What Is Justin & Hailey Biebers Net Worth Hailey, who wore a Saint Laurent black strapless sheath gown with a plunging embellished neck line alongside a suited Bieber, wa
2021-09-16 04:28:55 UTC	903	IN	Data Raw: 36 32 37 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 39 30 30 77 22 20 73 69 7a 65 73 3d 22 28 6d 69 6e 2d 77 69 64 74 68 3a 37 36 38 70 78 29 20 34 35 30 70 78 2c 20 33 30 30 70 78 22 20 61 6c 74 3d 22 43 61 6e 61 64 69 61 6e 20 73 69 6e 67 65 72 2d 73 6f 6e 67 77 72 69 74 65 72 20 4a 75 73 74 69 6e 20 42 69 65 62 65 72 20 61 6e 64 20 68 69 73 20 77 69 66 65 20 55 53 20 6d 6f 64 65 6c 20 48 61 6 9 6c 65 79 20 52 68 6f 64 65 20 42 61 6c 64 77 69 6e 20 42 69 65 62 65 72 20 61 72 72 69 76 65 20 66 6f 2e 2e 2e 22 20 63 6c 61 73 73 3d 22 45 64 73 22 20 2f 3e 3c 2f 6e 6f 73 63 72 69 Data Ascii: 627&fit=crop&crop=faces&auto=format%2Ccompress&q=50&dpr=2 900w" sizes="(min-width:768px) 450px, 300px" alt="Canadian singer-songwriter Justin Bieber and his wife US model Hailey Rhode Bald win Bieber arrive fo..." class="Eds" /></noscri

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:55 UTC	918	IN	Data Raw: 20 61 6c 6f 6e 67 73 69 64 65 20 61 20 73 75 69 74 65 64 20 42 69 65 62 65 72 2c 20 77 61 73 20 73 65 65 6e 20 73 6d 69 6c 69 6e 67 20 61 74 20 68 69 6d 20 61 73 20 74 68 65 79 20 61 72 72 69 76 65 64 20 66 6f 72 20 22 5d 2c 5b 30 2c 5b 38 5d 2c 31 2c 22 74 68 65 20 61 6e 6e 75 61 6c 20 63 68 61 72 69 74 79 20 65 76 65 6e 74 22 5d 2c 5b 30 2c 5b 5d 2c 30 2c 22 20 62 65 66 6f 72 65 20 61 70 70 65 61 72 69 6e 67 20 74 6f 20 62 65 20 76 69 73 69 62 6c 79 20 73 68 61 6b 65 6e 20 61 66 74 65 72 20 74 68 65 20 61 70 70 61 72 65 6e 74 20 63 68 61 6e 74 69 6e 67 2e 20 22 5d 5d 5d 2c 5b 31 30 2c 31 5d 2c 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 48 61 69 6c 65 79 20 74 68 65 6e 20 70 72 6f 63 65 65 64 65 64 20 74 6f 20 70 75 74 20 6f 6e 20 74 68 65 20 73 Data Ascii: alongside a suited Bieber, was seen smiling at him as they arrived for "[0,[8],1,"the annual charity event"),[0,[],0," before appearing to be visibly shaken after the apparent chanting. "]]],[10,1],[1,"p",[[0,[],0,"Hailey then proceeded to put o n the s
2021-09-16 04:28:55 UTC	919	IN	Data Raw: 67 6f 6f 64 20 73 70 69 72 74 73 20 77 68 65 6e 20 4b 65 6b 65 20 50 61 6c 6d 65 72 20 69 6e 74 65 72 76 69 65 77 65 64 20 74 68 65 6d 20 66 6f 72 20 22 5d 2c 5b 30 2c 5b 37 5d 2c 31 2c 22 56 6f 67 75 65 20 22 5d 2c 5b 30 2c 5b 5d 2c 30 2c 22 74 68 6f 75 67 68 22 5d 2c 5b 30 2c 5b 37 5d 2c 31 2c 22 2e 22 5d 5d 5d 2c 5b 31 30 2c 34 5d 5d 7d 2c 22 62 6f 64 79 5a 6f 6e 65 73 22 3a 5b 7b 22 69 64 22 3a 22 38 34 34 30 30 33 39 22 2c 22 63 61 72 64 22 3a 7b 22 69 64 22 3a 22 38 34 34 30 30 30 37 35 22 2c 22 74 79 70 65 22 3a 22 6f 65 6d 62 65 64 22 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 74 72 65 61 74 6d 65 6e 74 22 3a 6e 75 6c 6c 2c 22 65 66 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 74 65 22 3a 6e 75 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e Data Ascii: good spirts when Keke Palmer interviewed them for "[0,[7],1,"Vogue "[0,[],0,"though"),[0,[7],1,". "]]],[10,4]]),"bodyZones":[{"id":"","84400039","card":{"id":"","84400075","type":"oembed","settings":{"treatment":"null","effect":"null","palette": null},"palette":n

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
147	192.168.2.3	49931	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:56 UTC	931	OUT	GET /style/hailey-bieber-met-gala-2021-look HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:28:57 UTC	931	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 32046 Connection: close Date: Thu, 16 Sep 2021 04:28:57 GMT content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Cache-Control: max-age=3600 Apigw-Requestid: FvQxbjoioAMEMvA= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 5c79308f72e53cdf81a950b478a7e144.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: zruB5zk4GdNRhhbauLcyxuhNMWWpIGFtZIS1LPH5mCNvIB86c6hJWw==
2021-09-16 04:28:57 UTC	932	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:28:57 UTC	947	IN	Data Raw: 65 63 6b 62 6f 78 22 20 74 79 70 65 3d 22 63 68 65 63 6b 62 6f 78 22 20 2f 3e 3c 6e 61 76 20 63 6c 61 73 73 3d 22 7a 77 58 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 4b 46 43 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 68 63 6f 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 6f 6c 22 3e 3c 69 20 63 6c 61 73 73 3d 22 69 4b 46 22 3e 3c 2f 69 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6a 4f 63 22 3e 3c 6c 61 62 65 6c 20 63 6c 61 73 73 3d 22 56 75 42 20 77 66 5f 22 20 66 6f 72 3d 22 73 65 61 72 63 68 43 68 65 63 6b 62 6f 78 22 3e 3c 73 70 61 6e 3e 53 45 41 52 43 48 3c 2f 73 70 61 6e 3e 3c 62 75 74 74 6f 6e 20 61 72 69 61 2d 6c 61 62 65 6c 3d 22 6f 70 65 6e 20 73 65 61 72 63 68 22 20 63 6c 61 73 73 3d 22 43 67 6b 22 20 74 79 70 65 3d 22 62 75 74 74 6f Data Ascii: eckbox" type="checkbox" /><nav class="zwX"><div class="KFC"><div class="hco"><div class="sol"><i class="iKF"></i></div><div class="jOc"><label class="VuB wf_ " for="searchCheckbox">SEARCH<button aria-label="open search" class="Cgk" type="butto
2021-09-16 04:28:57 UTC	956	IN	Data Raw: 4d 65 74 20 47 61 6c 61 20 32 30 32 31 20 6c 6f 6f 6b 20 69 6e 63 6c 75 64 65 64 20 61 20 76 65 6c 76 65 74 20 62 6f 64 69 63 65 20 61 6e 64 20 61 20 64 72 61 6d 61 74 69 63 20 70 6c 75 6e 67 69 6e 67 20 6e 65 63 6b 6c 69 6e 65 2e 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 4d 69 6b 65 20 43 6f 70 70 6f 6c 61 2f 4f 65 74 74 79 20 49 6d 61 67 65 73 20 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2f 4f 65 74 74 79 20 49 6d 61 67 65 73 22 7d 2c 22 69 6d 61 67 65 22 3a 7b 22 69 64 22 3a 22 38 34 33 35 38 32 36 30 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 34 2f 62 33 32 38 63 31 32 36 2d 62 30 62 30 2d 34 34 65 64 2d 39 37 38 38 2d 61 Data Ascii: Met Gala 2021 look included a velvet bodice and a dramatic plunging neckline.", "attribution": "Mike Coppola/Getty Images Entertainment/Getty Images"), "image":{"id":"","84358260","url":"https://imgix.bustle.com/uploads/getty/2021/9/14/b328c126-b0b0-44ed-9788-a

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	962	IN	Data Raw: a6 17 fe ba 1d 56 2e 11 38 10 40 00 35 19 a0 c2 18 bb 9e 67 4b 24 1b 0a d5 68 56 ac da 3c 9e 99 b7 ca 2a da 05 07 fc 47 d5 63 bb ab 06 ab 88 a7 29 77 3a 1d 4a b7 a7 c3 70 08 8f 43 6b e3 bd fd db 74 12 ed 4e 93 65 01 50 19 04 80 80 71 73 62 3d a8 f1 b4 48 d9 f7 33 bd 03 d0 74 aa f4 4f d0 8d 43 32 bc 8c bc 60 cc ee d5 bd a2 25 27 d4 dc 99 89 f3 d1 d8 ac f8 5d f9 fe 97 d6 52 89 3e ed 29 56 6d 1e e5 9c 4b 79 ab 04 c2 6d a2 e3 bb f9 a5 56 30 f8 32 02 8c d9 a5 2b 6e 35 1b 89 64 09 8a 68 34 1c 7e d8 87 6b d7 51 8c 12 5d e3 b5 98 56 28 61 c0 58 44 28 33 74 d4 2d 6b 4d 59 4b 14 0a 51 ce d4 5d 6a 3b a9 fe 87 6a 3b 2d 82 45 80 f4 75 a4 90 80 b2 2f da 54 6c c5 85 45 b6 63 24 dd 4b f3 de 3b eb 69 70 85 7b 99 88 4f e4 62 2b f0 33 af e4 f9 89 88 af bc 90 52 b7 17 ae 04 Data Ascii: V.8@5gK\$hV<*Gc)w:JpCktNePqsb=H3tOC2`%jR>)VmKymV02+n5dh4~kQjV(aXD(3tM-kMYKQjji;-Eu/TIEc \$K;ip[Ob+3R
2021-09-16 04:28:57 UTC	964	IN	Data Raw: e3 fa 0d b3 41 bf 17 19 a7 45 94 8a 22 6e 3a 55 44 93 4d 9b 28 b8 94 fd e1 dc 8f 68 37 f9 b4 2f c2 ca 0c 42 7d 28 af ad d9 b7 fa ef a1 8d 04 96 a3 01 00 ae b7 24 41 28 4f 77 52 0b 86 23 96 41 05 34 76 be d9 96 7b 26 4d c4 c3 d9 4a be cc c9 4c 65 72 8d ba d3 66 33 68 13 f1 d2 f3 22 f5 16 03 5f ca 3b 21 ef d0 dd 17 7a 42 83 ef 65 80 e5 22 ae 83 a5 d4 76 d5 aa 71 91 4d 58 3b 78 c7 ae be 49 a7 7d 34 12 c7 c5 c4 45 35 f1 4f 9a 32 6f cd c7 49 11 ad 51 62 f1 b5 29 95 90 b2 61 9d 4e a2 20 05 53 5c b6 6a ff 00 51 ec 0d 18 46 9d cf b8 58 23 67 a5 69 5c c4 6c 8a c5 b6 eb 74 fc 95 a0 f7 a0 2e 2e 10 82 12 e2 dc e5 fa f3 62 bc 64 11 bf e8 8a c1 26 47 51 10 f2 9a b4 a7 dd bb 6a cf 98 ba f3 5f 25 24 91 60 c9 b7 88 fb f7 c1 67 be 37 6b 1b 03 18 83 46 6d fc 20 68 ab ec 8d Data Ascii: AE"n:UDM(h7/Bj)\$A(OwR#A4v{&MJLerf3h"_:!zBe"vqMX;xl)E5O2oQlbaN SijQFXhgi!t..bd&GQj_%\$ g7kFm h
2021-09-16 04:28:57 UTC	965	IN	Data Raw: ae 2f 3a 4a 92 69 3b 1a 1a 5a c2 24 cb 35 e6 0d a3 63 ab 10 91 52 92 8b 37 85 eb ce dc 2b 2a b7 99 c7 af 7d f3 9f 94 5f bf 11 e9 e2 4d 9d d9 39 63 6c 21 5e 2d 32 fa cf f4 46 34 29 32 40 33 f8 3d a8 51 c0 83 99 1c 7b fa 5a 96 0b c5 5b 2b 4d d8 03 e6 7f c3 3d 81 b9 a6 8a c4 ee b3 f5 48 99 79 00 87 71 f8 af f4 07 f3 c7 6f 12 31 31 26 d7 66 88 d1 fd d9 2e 36 b1 36 12 62 cd 18 aa ac 33 09 59 6f 5b c4 35 5d 5f 96 70 eb 8c e7 ef 5d 7b cf aa ae e3 96 9d 48 4b 3c 75 23 21 21 31 65 b6 4f 9a f7 52 a2 85 8c ad 96 fb da f1 d5 9a 6e 7a 13 42 0f ff 00 45 00 1f 94 82 bd b8 21 44 b6 9f ce 22 37 e8 14 8a 47 1b 4a 32 16 d8 91 70 54 12 0d 2a b0 d1 82 91 14 8d f2 52 34 fd c5 f6 ec e8 90 20 fc de 88 f6 36 0a 3d 83 97 89 f0 c5 9f 6b 28 ac 57 5e 80 7d ef bf 7e fb b5 de 74 cb Data Ascii: /:Ji;Z\$5cR7+*)_M9c!!^~2F4)2@37Q{Z[+M=Hyqo11&f.66b3Yqo5[_p][HK<u##!1eORnzBEmlD"7GJ2pt*R4 6=k(W^)-t
2021-09-16 04:28:57 UTC	966	IN	Data Raw: cd 86 56 41 5e 7c 69 57 1e ba 32 db 6c b3 36 1c 63 f9 e4 dc 5a 39 d4 a2 ca 3d 57 d5 4d 5f a5 9b cf 2b 67 42 b1 0f 76 da e5 de 4b b3 4a 1c 37 9b 74 b4 3e 44 d5 98 db f1 ee 99 74 fd 2d 18 e1 8d 37 fa d6 4a 12 0a a4 dd 48 b8 91 82 c1 48 b1 49 1f 53 8f 8f 53 85 ba 02 79 e7 9f 76 b2 10 31 cb b9 b2 12 c8 76 99 32 85 08 e7 1d 3f 37 26 f7 df 10 4e 9d 9c e8 7a 60 97 6f 05 7e 73 02 51 bd b4 a4 93 b9 a9 47 b2 e3 d7 3b bb f4 c4 63 29 49 fd 18 b1 5a 26 25 99 42 54 a9 22 c7 86 71 ee 74 fc 48 1b 71 f2 a7 fb c0 1f f5 cc ef 53 12 3b 9b 91 94 91 92 c3 54 6b 9a f4 9f 2c 62 fb 59 45 33 47 9e 79 f2 cb 33 83 8a 79 21 68 27 90 a7 af 47 3a e5 c6 b7 2b 21 24 f5 7e 5b fd 4d cd d9 93 51 5a 70 f8 0d b7 3d 3d e1 9c 9c 8d 7f df 7a 4b 97 1f a2 df a1 42 29 4d 8d 7a b7 59 65 52 af 50 6b Data Ascii: VA^jW2l6cZ9=WM+_gBvKJ7t>Dt:7JHHISSyv1v2??7&Nz'o~sQG;c)lZ&%BT"qtHqS;T,bYE3y3h'hG:~+!\$-[MQ Zp==zKB)MzYeRpk
2021-09-16 04:28:57 UTC	968	IN	Data Raw: eb b5 98 cf 96 16 9a 5f 41 ce e1 20 c1 b5 4a d8 f0 12 95 67 86 bb 83 52 c1 cd eb a0 d0 8f d0 c2 47 de e5 59 60 b4 8f 96 67 a8 7c d7 cc 5d a8 f9 68 0b 4f d0 53 9e cf d3 67 75 b1 cc b5 1d 62 a1 63 ca ea 62 6f a1 13 63 fa 22 51 85 5e a1 15 8e 6e 4c 86 a7 0e 2f 71 62 bf 9c 2e aa f2 98 67 c4 57 cd 26 cf 06 21 00 d1 48 02 d5 0b 5a 44 62 4b a0 9f d0 33 b7 b5 50 2a f2 0f ad 72 3a 9f b2 05 8a ac 5e 5d e5 8a e5 a4 ce 02 1d af 36 98 4e 79 35 95 2f 1b d2 bd b0 01 34 62 ba 8f d0 3e f5 96 44 60 6e ef 60 b0 a7 f4 e1 c2 58 80 33 4e 80 ec 97 af ab cf 75 99 6a 46 48 c0 45 a3 5f 79 ac 16 8a c1 8a 62 3f 42 47 9c ec f8 37 21 c1 28 29 8e 7b 04 c9 5a 0f 37 8e 81 01 23 81 57 b4 ee c5 ce ac 5c 72 e5 d4 30 2c a3 aa aa ce ad f7 e8 ef 72 31 ef 68 8f 13 e4 14 37 d9 7c c0 7f 01 32 09 Data Ascii: _A JgRGY`g][hOSgubcboc"Q^nL/qb.gW&!HZDbK3P*r:~j6Ny5/4b>D`n`X3NjFHE_yb?BG7!()([Z7#Ww0,r1h7 2
2021-09-16 04:28:57 UTC	969	IN	Data Raw: 26 7e ad 98 ca c6 ac dd 3d 43 39 1a 2c 47 a1 4e 76 b2 74 4c 94 1c cc f8 70 f1 95 a3 57 f0 d8 55 6c c1 b0 49 dc 85 f4 0b cc ee 19 da 62 64 a3 2b 96 fb 67 06 c1 b8 ad 8e d5 ad 86 f3 53 45 34 68 39 1a 96 f2 ab 1a 65 6c 96 01 ab dc 85 dc da e5 73 56 da c2 63 e8 b9 c6 9f ad 7c 90 52 5a e9 2e 66 20 b1 30 af 62 34 38 fa 74 6f 2b 10 ab c4 24 6e 45 44 3e a1 b9 b0 e9 35 0e ce 66 80 92 65 ea a5 b9 83 5d 2c a9 e9 9f c1 69 67 31 a3 c4 57 89 9c 82 43 22 15 e3 56 b2 45 a4 6a e5 ba d1 16 8e 91 a3 99 a2 d3 57 8e 73 a2 69 a5 48 4a 7c 06 96 4b 9c df 3f ad 13 58 c6 38 88 85 54 ee e5 4e 90 d6 8d 6d 65 57 44 19 f4 b7 b7 35 a8 e3 1e da 43 9d 4d 89 bc 3c a3 47 cb 66 e2 04 6d 6b 88 ad 90 d4 ee 54 ee 49 2f 0c 4e 90 dd 1e ea 2b 65 92 ba 5d 1d dc db 19 28 b9 cc c1 ee ac 1f 18 1e Data Ascii: &~-=9,GnvtLpWUllb+gSE4h9elsVc RZ.f 0b48to+\$nED>5fej.ig1WC"VEjWsiHJk?X8TNmeWD5CM<GfmkTI/ N+e)[
2021-09-16 04:28:57 UTC	970	IN	Data Raw: 06 04 29 44 84 8b ea 9c 64 e4 e2 73 4e 8a 35 ab d6 b3 52 fd 4d ad 67 d5 b7 5b 62 87 40 c8 f8 f6 ab 83 22 7f 46 bd 27 58 2b d6 0a c5 5d b5 92 8a a0 8c 12 5b 04 ff 00 78 c8 c8 fe 9b 1b 96 ef 01 6d 1b 5b 17 75 16 99 97 c5 61 a6 cd b8 6c 19 03 51 fa ee 4b 65 9b 7a 88 b1 af bc d5 c4 cc 94 37 08 92 e4 3d 2f 53 81 9e de 13 77 36 42 41 0a a4 86 20 97 23 b0 4c f8 9c a9 1a 40 a2 a4 2d e9 bf 5f 74 ab 53 7e 6e 65 bf 03 30 c0 2a 25 11 db 5d f4 ac dd 78 20 05 72 b3 54 29 30 a9 f7 53 96 d1 38 fd 63 23 23 c7 7e de de dd fe b7 ef fd 3e 57 b6 2d 65 39 b2 c5 30 9e d8 55 4a 35 d9 17 2b 3f 1f 78 6d e9 f7 2e 63 e3 07 19 3f 49 27 13 8c 6c 26 da 2d a2 ca 9e 0d fe 61 bc ed 4d e0 62 c1 54 d0 55 5b 51 d5 ef 2c a3 c5 28 d3 4d 16 24 da 77 cb 77 96 db 75 97 4d fe 23 c4 60 30 6f Data Ascii:)DdsN5RMgb@*F'X+][xm[ualQKez7=/S+w6BA #L@_-tS=ne0%jx rT)O8c#~-->W-e90UJ5+?xm.c?l!&-aM bTU[Q.(M\$wvuM#`0o
2021-09-16 04:28:57 UTC	972	IN	Data Raw: 2a a5 9a eb 94 5e 19 6a 36 ce 50 2a c5 ce 46 fb 5f f4 6b 59 de 06 a5 dd 28 f9 1d 4d 8d 51 4c f9 00 15 fc cd 6c 89 9c 10 10 10 58 8a e1 3f 21 5f c8 01 62 31 ed ed 33 24 03 80 7f 43 22 97 4c 45 74 d6 4d 64 02 4d 4f 55 c5 d5 1d 46 50 ca f8 1f ce 64 8c d8 d7 3d f6 de f7 7b a6 40 96 c1 cd d3 76 69 54 d8 16 4d 21 31 66 3e cf fe 89 fc 82 b7 3b 1d d9 d0 a0 ed 4b 2b ab 61 17 e9 27 37 5a 0a 5a ad bf 1f d5 54 5d 7d 8e 51 9a 8d 86 5e 56 f0 7d e3 c0 c2 96 2b f8 1a 5e a9 50 a8 55 d0 42 c1 6b 15 7c a5 50 1e a3 91 18 51 87 30 05 10 5e f2 64 47 28 5d 75 53 af 5e b8 a0 d1 61 37 97 5c 35 31 47 2b e0 7f 19 c9 92 96 1b 5c eb 16 2d 5a b4 eb 08 2a cf 4d 94 3f 5e be 44 dd de 57 1b 23 31 47 26 1d 97 2b ba a1 69 03 8e f1 5e 3b 1c 34 78 fd 15 6b f2 fa dd a7 6e 86 cd 21 af b0 a5 a3 Data Ascii: *^j6P*F_kY(MQLIX?!_b13\$C"LEtMdMOUFPd=([viTM!1f;:K+a^7ZZTj]Q^V)+^PUBk[PQ0^dG(juS^a^7l5lG+!-Z*M?^DW#1G&+i^;4xkn!
2021-09-16 04:28:57 UTC	973	IN	Data Raw: 71 91 fa 0e 29 b0 ff 00 ba cb 5e aa a1 ea 79 65 e6 e4 b5 6d 5b 61 86 6f 63 ac 36 d1 d8 96 31 b6 5e c2 9f 14 d7 a5 05 05 a9 59 a4 dc db 5b 2b 4f af 88 0d 85 c5 e6 ee de a3 10 35 48 0b 67 6a ff 00 24 1e 43 ff 00 a5 1b c1 70 b7 68 db 8a b4 da c2 76 c1 bb 71 dd 67 1d c2 c4 04 a6 8a 9b 8e 93 1c 9c 9f 1d 44 0c 44 61 61 e3 32 66 66 24 0a 32 72 70 c4 73 b2 9b 12 02 f8 b6 3b 98 77 88 fd 60 a1 80 54 d7 49 48 8e dd 36 b1 84 16 11 65 56 45 e7 62 c3 ec be c5 99 b7 f9 6c b2 67 39 b8 a3 1a 90 ac 0e 87 31 97 2d 36 e5 92 63 a5 18 c9 d8 6c 7f 33 5a c1 6d 4b 2b 6a 33 69 51 75 6b 6a ff 00 e4 aa aa c1 96 92 6e 0d 8d 9b 56 76 71 b3 2e 37 0a 94 8a d4 94 58 8b 11 dc e4 e4 f8 8f 03 e4 b0 b1 98 5e 42 46 63 0b 26 32 70 f1 b0 62 d8 bb 3b cb 25 e2 3f 5e e2 51 9a f5 d4 5a c2 45 b9 Data Ascii: q)^yem[aoc61^Y[+O5Hgj\$CphvqgDDaa2ff\$2tps;w`TIH6eVEblg981-6cl3ZmK+j3iQukjinVvq.7X^BFc&2pb;?%? ^QZE

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	974	IN	Data Raw: 5b 5e 69 32 c8 56 65 57 57 6e df 38 dd cd 9d 70 5c 55 0a d3 04 a9 99 9e e6 48 8e 4b 07 17 31 23 3d b3 0b 0f 03 03 26 0f 27 f4 ef b8 21 60 b4 5d 0d 99 21 60 18 c9 21 d5 8d 79 0b 62 6d 26 c2 db 13 8b 9a 67 44 a9 ca c6 70 c2 c4 dc 94 10 8e ba 35 5a a5 43 ef 7e 3e f1 ff 00 0d 0e ab 6e 31 ae 6a f6 25 a3 7e b9 3b 88 5d 27 56 0c 0c af 8a 11 96 cc 09 c5 9c b7 2e ce 10 aa 8f e3 76 dc 1a cc 50 1e 6a 09 6c d9 4e b5 93 16 aa 34 46 cb 18 cc 9c 29 ee 70 a4 b2 72 30 26 08 26 64 e4 b0 a0 70 33 b3 89 8f db b8 28 38 60 b6 18 58 d8 38 56 51 5d 74 42 8d 56 d5 69 4f 54 80 05 51 a3 94 65 78 23 4f 56 ce 09 ff 00 83 5f f9 bd 5e 08 ad 7b ad 83 45 5b 4d dc b6 9d 0d ee d3 4b 5c 55 69 7b 8d 87 13 a9 6c 6d 2f 5d 5f 69 a7 6a 03 2b ca b0 bc 74 dc b4 56 49 93 c1 eb 6a 9b a7 61 4d 68 ab Data Ascii: [^i2VeWWn8pUHK1#=#&!']!^lybm&gDp5ZC~>n1j%-;]'V.vPjIN4F)pr0&&dp3(8'X8VQJtBViOTQex#OV_^([E [MKlUi(lm/)_ij+^Vl]aMh
2021-09-16 04:28:57 UTC	976	IN	Data Raw: 19 b0 1d a2 94 eb 13 39 55 26 84 d5 d8 29 21 ca 73 76 1a c7 3d 7b 3a 7a e3 a2 49 3d 65 a3 f1 12 33 93 0f 8d b8 5d 14 3a 9a 76 cc 9c 45 8f c7 b0 8d 65 71 ac 8a ed 55 36 2a 6c 92 5c c2 92 ee fe b2 ed 1c 29 39 39 89 1c 1f 13 87 9e dd 94 f8 8f e4 79 ec 04 b9 af 00 3d 11 49 4c 8c fb 71 aa 90 64 d3 67 73 93 fa 06 46 08 84 04 6d c3 db 5a 1e b6 59 af b6 49 cd 89 e9 75 bb 4a db 64 71 e1 2a db 0a b6 97 f6 61 eb 2e 57 7c e7 4b 9c 9c b4 3b 64 9c eb 59 b9 3d 95 3a cf a6 5b d7 56 3a aa 1c eb 60 55 b2 18 e3 49 7b f7 da cf 7f ab 68 11 1c 97 80 fd 19 93 9e dd e7 7d ff 00 13 c2 c0 94 cd 68 5c 7a b4 4a 7b 82 12 e2 48 fa 11 fb 44 f6 53 3e 3a 1c 08 08 54 2f 2f 57 d7 e6 aa b4 ae b3 69 8d 07 f1 26 73 4a ba b9 bc 55 34 6c f1 cf a6 9d 0c 2b 15 9a a2 19 91 8c 19 2c 66 5e 4c 84 e5 Data Ascii: 9U&J)sv={zl=e3j:vEeqU6*I\}99y=ILqdgsFmZYluJdq*a.W K;dY=[v:~^UI(h)hZj{HDS>:T/Wi&sJU4h+;f^L
2021-09-16 04:28:57 UTC	977	IN	Data Raw: 93 12 47 26 56 ad 6e ad da 26 67 7f fc 7f e7 9b a1 c3 2f 65 4a 4c 0a d1 91 94 c6 47 8b cf ff 00 54 da e4 fe a3 81 8b ce 24 96 2a 30 5c b7 04 8e 44 40 84 44 f7 bf a9 e0 b0 b0 bc 0f 89 92 ce ff 00 49 c3 92 c8 c1 f1 18 8c 4c 69 d0 95 df 66 b6 02 46 63 23 27 c7 7d cc b4 9e fe 9a 6b f2 bc 29 ff 00 e1 ef b8 9e f3 b6 d2 8a b0 61 2f 2d 61 cf 63 3d 8e af b6 4d 7f a2 50 fd a3 06 53 9c 3f 18 2e 8f 64 31 66 b9 1c 8c 8c 89 cd ea bb ee 72 70 fc 47 89 c9 cf ff c4 00 4a 10 00 01 03 02 03 04 06 07 06 04 04 05 03 04 03 00 01 00 02 11 03 21 04 12 31 10 22 41 51 05 13 20 61 71 81 23 30 32 42 91 a1 b1 14 40 52 62 c1 d1 24 72 e1 f0 06 33 82 92 15 43 53 63 f1 25 50 a2 16 34 c2 d2 44 64 b2 ff da 00 08 01 01 00 03 0f 01 1c d4 9d 56 72 b7 76 40 40 2b a9 ed ef 28 50 7f f6 7c 82 Data Ascii: G&Vn&g/eJLGT\$*0ID@DILlIFc#~}k)}pf/-ac=oPS?.d1fPpGJl1"AQ aq#02B@Rb\$3CSc#P4Dd?Vrv@/@+(P
2021-09-16 04:28:57 UTC	978	IN	Data Raw: 9d 46 9a 6e 83 fe df a2 a1 22 9e 20 77 07 7f 50 b2 3f ad a6 24 71 ef 1c d3 6a 31 98 ac 3b e2 ab 7d 93 fa 1e e5 ff 00 10 c3 f5 ad dd c4 53 d5 bf a2 fb 4d 18 74 67 09 a4 4b 6c a0 47 62 3b 33 d9 d5 58 ad e5 2b 78 f8 27 23 b2 37 87 62 6b 05 60 ac 10 85 21 08 28 00 50 01 6a b5 5e 99 db 08 4e e7 b1 b9 48 da d6 0e f5 79 4d 26 10 30 87 62 0e db 7d dd b8 76 77 9e 0a a6 47 3e af b4 f3 a7 20 ba da bb ce 83 07 31 fc 2d 37 ca 3b cf 14 dc 36 12 28 0c af a9 20 3c f0 68 d5 cb 2b a0 49 7e 51 af 00 7f 52 9c 30 d9 9c 4b 59 1b c4 71 e4 d0 9b 59 ad 67 bc 3d b8 f7 79 30 77 9e 2a 95 1c 34 3c b7 31 9b 4c 00 3b f9 0e 6a 8d 77 97 4c b2 9e f4 9f c5 1a c7 3e 5c 96 14 82 e9 0d 9d 27 55 40 dd a4 b9 38 11 16 44 e1 20 8b c2 ac 33 65 d5 74 85 16 f1 3e 61 67 96 d4 a6 5b de aa e1 cc 8b b4 Data Ascii: Fn" wP"\$qj1;]SMTgKIGb;3X+x#7bk'!(Pj^NHyM&0b)vwG> 1-7;6 (<h+I-QR0KqYqYg=y0w*4<1L;jwL:'\U@8D 3et>ag[
2021-09-16 04:28:57 UTC	980	IN	Data Raw: eb f8 a3 84 e9 41 55 a7 75 ae bf 7b 5c b2 54 6b c7 c5 3a b6 06 8e 26 46 e6 eb ff 00 94 ae a7 12 fa 53 bb 32 3c 0a 2e 19 87 b4 3e 61 35 e2 40 03 33 7e 9c 56 11 b0 33 bd c7 89 88 1f 34 1a 03 9a ec cd 3c 7f 43 d9 23 68 43 b3 64 61 15 32 ae af b4 a2 9c 36 c8 57 ec c1 ec 5f b1 65 74 49 44 90 ac 15 91 84 54 f0 42 74 40 70 51 eb 0c c2 68 7d dd 7e 42 e8 15 a6 c2 55 b7 79 a3 f6 8a 8e 9d 1b 6f 14 e2 e7 99 b8 1b bc 9a 0a 8a f8 70 2c ca 2c 2f 3e 48 d4 73 89 3e c3 6c 3b f8 a2 e7 39 dc 62 07 9a 0d a8 04 d9 a0 35 65 6b 47 13 ff 00 e4 8d 43 4a 9a eb 1f 34 29 e1 98 d1 c1 a0 6c b7 66 ca fd 96 62 f0 75 29 38 4c 85 59 ad 7b f7 e6 53 6d ff 00 d1 74 2b f4 4d 1a a6 e2 00 77 82 93 57 08 e3 67 b6 c9 f4 df 7b 9a 6e ea dc 7b b8 2c d4 a7 8e a2 b3 d6 6c 1c b2 d9 48 22 7e 87 e2 8b 2a Data Ascii: AUu{\Tk&FS2<.>a5@3~V34<C#hCda26W_etiDTBt@pQh)-BUyop.,/>Hs>;/9b5ekGCJ4)lfbu)8LY{Smt+MwWg {n{.;lH"-*
2021-09-16 04:28:57 UTC	981	IN	Data Raw: 9f 92 cb 54 f2 28 96 b3 9c 16 fc 2e 9a c2 01 68 ca e3 20 f1 ba 65 7c 2f 56 41 98 b7 73 86 b8 25 56 06 ce 82 7b 88 e0 9e 69 19 27 da db 75 6d b6 ec 40 f5 16 50 7b 76 d9 07 b1 25 5f 66 9b 2d b2 cb 55 e9 56 8a 8c ee 21 77 ab a6 be ce 24 01 ca e5 08 74 27 8d 0a 98 cc 2e 9d 52 a4 df 28 b9 57 a1 4d be dd 47 5b bb ff 00 01 30 53 cc 2c 58 4f c4 68 9a dc 36 1d d0 6e e2 9c 19 1e cc 92 04 f2 3f ba 3d 7f 84 fc 16 7e a8 77 95 35 ab 1e 60 34 78 04 3a d1 de 42 75 4a 74 2c 60 d2 c8 7b 88 2b 1a 1e 5b 70 66 2d a4 2a 6f c1 6e 03 d6 07 02 fe 26 15 4e b1 a4 54 dd e2 a9 53 e8 a7 9a f4 64 55 76 60 d2 2f 61 aa e9 13 88 2f c1 bf 2e f9 f4 79 49 80 06 b2 a7 04 d7 57 a6 d6 e2 59 a9 6e 85 16 3c 20 69 9f 05 99 ca 96 33 0c ca 2e 8c bd 66 72 0e 84 f0 95 85 c1 41 a7 4c 69 a3 46 50 ba 3e Data Ascii: T(.h e /VAs%V{i'um@P{v%_f-UVlw\$!t.R{WMG[0S,XOh6n?=-w~5'4x:BuJt,{'+{pf-*on&NTSdUv'/a/.yIWYn<i3.frALIFP>
2021-09-16 04:28:57 UTC	982	IN	Data Raw: ce 6a 9d 1a b6 e6 85 2a 72 dd 53 6a ea 53 0e ab 2b e3 61 56 50 c2 87 fc 56 27 dc 9f 9a 2c e9 8a cc e6 ff 00 a5 d0 6f 56 7b cf c0 a6 b6 bc fe 55 15 35 ee 2a 70 ce 66 ad 20 42 2e c0 92 df 74 87 fc 17 a5 a8 d8 f6 5e 7e 08 1f bc 5b 65 95 8a ba 8e d1 08 87 29 01 6e ec b2 9a eb 45 0d ec df b1 07 b3 0c d9 7e c6 1d 8f 65 85 5a 87 87 ba 3f 74 59 97 33 8f 58 f3 99 ce 1a 81 a4 0e a1 18 b7 b7 c1 a3 82 35 2b 3a 9b 4d 81 00 9f c4 e3 a4 05 95 9a 78 0f a2 a9 5b a4 5b 4a 9d a4 ef 7c 11 a5 82 c9 30 65 8d 3d c3 54 e3 88 20 11 97 ec f1 f1 4c 6d 1f f4 47 c5 1e b5 a0 09 7b 8e e8 e5 0b 2d 07 41 11 93 53 fd f1 59 1c 1e 75 37 3e 1c 10 fb 36 7d 0b dd 03 f7 4d 77 45 38 8f 1f 20 50 7b 05 f6 95 99 7d 96 b3 2f 13 37 54 28 54 8a ad a9 1f 89 a2 53 6b 53 9a 75 2d 08 e1 70 bd 69 6b 9e 78 Data Ascii: j*rSJ\$+aVPV',oV{U5*pf B.t^-[e]nE=-eZ?Y3XA5+:Mx{[J]0e=T LmG{-ASYu7>6}MwE8 P{j/7T(TSkSu-piix
2021-09-16 04:28:57 UTC	984	IN	Data Raw: 4a df 3e a0 a2 5c a5 44 28 1b 2c 8a 82 a3 b3 6d 84 2b ec 3c d1 3b 41 78 99 8e e4 05 27 75 54 9a 09 81 98 dc c6 a7 5d 17 57 d2 34 47 b4 ea 74 80 2e fc c7 78 c2 22 90 8d 5c eb fc 53 7a b6 f8 26 31 b4 2f 12 fd 38 de ca 71 ee d0 0e ac f9 0d 10 7f 48 3c 8e 5f 44 2a e3 e9 d2 fc 1b a4 7f 2b 65 64 ac ee 22 7e 48 37 09 4d 9f 8a e4 7d 16 46 1e fb b9 3a a3 bf bf ee eb 0b d0 18 21 50 b5 a7 16 e1 14 db ac 13 c4 aa 95 f1 75 2a 54 71 71 73 ae 4a c9 4e 0a 16 56 08 39 a8 08 2b 03 52 b1 75 6a 2c 7f 79 0b a2 c1 8f b3 d2 89 fc 21 74 49 de ea 69 e9 c1 bc 79 2e 87 14 e4 39 80 c0 b6 4e 6b a2 f0 f5 77 9b 00 c7 b0 00 2b a3 9e 4d 8c 47 10 a8 d2 07 ab 10 0f 24 ea f5 b2 b7 fd 47 92 6e 45 d5 d3 21 58 99 5b d4 c7 7e 62 b3 e0 70 6e fc 54 cf d5 10 c3 e0 17 59 8a a9 c9 bf 52 54 65 3f de Data Ascii: J> D(.m+<;Ax'uTjW4Gt.x"Sz&l/8qH<_D*+ed"--H7M}F:IPu!TqqjsJNV9+Ruj,y!tliy.9Nkw+MG\$GnE X[-bp nTYRTe?
2021-09-16 04:28:57 UTC	985	IN	Data Raw: 59 6d 1e 0a 8a e1 82 c6 9e 12 8d 20 7b de 33 3b e6 f4 2a e2 a8 52 65 9a d1 94 7f 7e 08 43 c0 e2 08 fd 17 53 41 d9 46 fd 47 e4 f2 e2 8d 1c 59 20 fb e2 4f 80 fd 17 5f 42 87 7d 38 fd 53 bf e1 a2 a8 d5 b5 2e 3f 9a d7 42 b6 10 7e 29 12 9c dc 25 4a 64 a1 a7 65 98 47 1d 47 d5 43 cb ae 33 3a f3 c0 f1 09 f4 69 3e 45 89 40 e8 a0 c1 5c b4 fb bc 48 44 76 ae 16 e8 d8 10 85 0a 50 53 b6 ca db 65 49 40 1e c4 e5 1c cc fe 89 81 ed 0d 13 16 09 d5 03 9a 34 80 4f c5 65 a4 18 10 a7 af b6 53 9f 58 84 c7 61 5c 35 7c 99 ee 59 5c 4f c1 46 28 1e e4 d7 74 70 77 e5 9a ea b9 22 25 d0 d1 dd 3c 7c 94 d0 6b 81 39 4b 02 dd 07 e2 8b 30 f4 ea f0 2d de f2 d5 1a 25 f8 72 43 a3 42 dd 0f 10 8d 2a e5 cd f6 4f 0e 4b 87 64 ae 45 62 9a 20 54 7f c5 62 0e af 77 c5 15 7d 96 2b 25 17 be 2f 61 e1 cd Data Ascii: Ym {3;*Re~CSAFGY O_B}8S.?B~)%JdAeGGC3:i>E@ HDvPSel@4OeSXa5 Y O{f(tpw~%<k9K0-% rCB*OKdEb Thw)~% a

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	986	IN	Data Raw: f6 b0 d7 fb 25 83 c8 b7 44 0d 4c 4c 93 3c 8f c1 39 bd 13 40 ff 00 da bf c5 32 9f 4b e2 07 19 06 7c 51 76 3d a5 b7 ce d1 fb 76 2c 14 95 25 00 21 49 d8 46 dc fd 27 4e d3 95 d2 b3 61 2a 31 be ef 59 4f cc a7 1c 76 21 bc a8 37 ff 00 8b 94 56 af 9a 60 12 1d ce 1e d4 4d 1a ed 9b b4 80 86 23 03 9b 93 27 cd a6 e8 e7 65 f5 19 97 5d d1 2d 3f 82 63 c0 ad 41 b8 d0 f7 82 9b 4d b0 4e e4 e4 33 f2 2b 2e 23 ab 74 c8 99 f3 42 b5 33 68 37 ba 69 63 98 e8 2a 93 98 fc 86 38 42 78 dd 2c 36 46 74 4e 17 75 82 93 eb af eb c1 43 6c 22 8c a9 52 8a 3b 63 65 f6 0b 29 1b 79 a0 78 2a ad f6 60 79 2a b9 a5 cf 71 73 b4 0b 12 1f 1d e9 cd c3 b6 91 12 73 48 e6 ba 47 11 8d 0f a9 39 5b 72 38 26 d1 a5 73 19 45 d5 77 b8 52 a2 d2 6a 46 9f 87 c5 54 a3 43 23 de 1d 50 fb 6e 0e 13 f3 bb 29 b7 08 b7 c3 Data Ascii: %DLL<9@2K Qv=v,%!!FNa*1YOv!7V`M#e]-?cAMN3+.#tB3h7ic*8Bx,6FtNuCl"R;ce yx*`y*qssHG9[r8&sEwRjFTC#Pn)
2021-09-16 04:28:57 UTC	988	IN	Data Raw: 2c 0f 7a a1 fd 3f 64 06 1c 41 bb c1 9f 01 fd 4a 14 03 07 0c bf 45 d6 bc ff 00 7a 2c cd 20 ac a4 a7 0f 4a d1 e3 b1 d7 b2 de 2b 75 1c ca cb 7a 11 dd 09 c1 8e 81 77 ee 7c 75 47 ad 73 67 ff 00 e2 cf 81 cf 29 b4 3a 72 bd a0 b9 d9 8f 74 85 d7 61 f0 f5 e3 fe 4b 33 1f 1e 29 df 63 a9 4c f0 87 0f f4 84 06 2d ef fc 6e cd f1 08 b7 e8 42 fb 47 47 10 35 6d c2 fe 20 0f cc 10 20 fe 59 05 39 d5 29 01 c4 4a cd 45 b5 07 e1 84 ee a5 a7 c1 cb 33 2d c5 d1 e1 ee b8 2a 6c 73 b3 6b dc 98 1a d6 f1 8b 14 0f 8f fe c9 07 68 56 41 4f 65 ef a8 d6 31 a4 b9 c6 00 1c 55 3c 05 06 be ab 5a 6b 9b 93 cb b9 35 8d d6 17 04 5d d9 87 78 04 2a 57 11 66 b1 1a b8 9a ce 61 3a e5 11 dd c1 36 85 0a 54 ff 00 0d 21 a7 31 72 a8 33 11 4e 8d e5 9a cb cc 77 fe e5 36 98 65 5a 96 ea d9 f5 10 07 c1 3d ce 7e 3a Data Ascii: .z?dAJEz, J+uzw uGsgj:rtak3)cL-nBGG5m Y9)JE3-*lshkVAOe1U-Zk5jx*Wfa:6T!1r3Nw6eZ=-:
2021-09-16 04:28:57 UTC	989	IN	Data Raw: ac ad 1e 8e 88 39 07 37 c7 e8 aa 62 3a 5a ab e2 72 35 ce f1 33 1f 32 9e d0 c7 87 13 95 99 67 c4 ca a5 d5 51 65 51 ed 36 67 f9 6c 99 83 c2 5a 65 d7 f1 9d 16 5a 3a de 6d fc c5 0f bf 87 47 d0 1c 6a 9a ae f2 b2 34 ba 12 8d 21 ff 00 31 c0 ff 00 b0 66 40 31 ce 8f 7a 0f 87 35 93 2b 85 db 3f 15 d1 f8 8a 70 ea 79 8b 64 8f 34 dc 06 3a a3 cb 6a b7 3b b7 88 d0 f1 5f f1 2e 9d c1 8a c0 0c 0d 30 da 8f 34 a5 c6 27 de 9f 79 57 c4 f4 8f 48 62 98 fa b4 70 ee 73 69 53 96 fb 8d 25 d7 55 19 d2 f8 0c 0b 1b 4f 7d 8f ab 55 d1 71 4c 08 6f bf 8a a7 88 38 a9 b3 69 55 cb 31 36 03 eb 2b 0e ec 4f 50 e0 e6 54 14 7a e2 0f e1 06 16 03 11 87 35 98 e7 1a 63 de 8f 25 d1 fd 4f 5a 6b 34 33 36 49 fc dc 96 11 ae 82 5c 03 98 1d 39 4c 41 d0 ac 5e 33 16 30 b4 69 06 b5 cd cf d6 ba f2 d1 ca 38 ac 0e Data Ascii: 97b:Zr532gQeQ6glZeZ:mGj!1f@1z5+?pyd4:j;_04'yWHbpsS%UO}UqLo8iU16+OPTz5c%OZk436l9LA*30i8
2021-09-16 04:28:57 UTC	990	IN	Data Raw: 75 48 56 d8 5c db a0 dc 45 fc 91 a3 d2 39 4e 8e 29 a7 04 4f 13 4f 4a 4e 0d 2c 3e 3d c0 1d 10 a7 d2 14 27 9f d5 58 c5 a4 40 fd 56 5a 75 23 83 6d ea 13 ea e1 c5 67 88 79 05 a7 c9 38 52 68 3c 6f e4 9c d6 3b be 9b 9a a0 c8 d3 54 73 b4 2d d3 dc 10 ea cf 35 4f ab c8 ba ba b0 74 2b d2 bd 48 d8 cc 5e 19 d4 cf 2b 2a f8 a9 d1 9e 3c 0f aa b7 df 4b 88 08 60 7a 3a 9d 3e 24 66 77 89 d9 de a7 61 ed 5d 18 52 63 82 22 b8 f1 46 a6 09 c7 8e 52 9c f6 35 bf 8d a1 9e 65 ca 05 72 38 0c bf a2 c9 87 a1 3c 29 97 91 e0 13 8b f3 34 5c 5c 2a 75 73 00 22 75 1e 08 16 69 70 65 0e bd ad fc b3 e3 29 b5 ba 46 8d 27 f1 97 0f d9 0c 25 5e 8d c2 30 45 30 d3 9b c6 a1 fe 88 e6 a4 78 81 1f a8 47 17 fe 1f 67 36 12 0a ab 43 14 da ec de 6b bd de f5 45 d5 19 53 5a 15 59 23 ba 78 2c cf 76 1e a4 75 94 Data Ascii: uHVE9N)OON,>="X@VZu#mgY8Rh<o;Ts-5Ot+H^+*J<K'z:>\$fwa RC"FR5er8<4)l\us"uipe)F%"0E0xGg6CkESZY#x,vu
2021-09-16 04:28:57 UTC	992	IN	Data Raw: f6 5c 04 8e 44 2e a3 a4 6a d1 3e c8 05 ed f0 72 fb 53 2b 52 77 f9 8c 76 60 86 27 00 fc fa b2 c5 0c 2b b3 0b 43 a3 cd 67 c7 b1 dc 20 d9 02 fc bf f7 0c 7c 65 0e a5 c8 b6 a3 47 fd 9f d5 69 e2 a5 ca f7 40 84 5a a5 4a 19 f2 f9 a1 4f ac e4 d6 7d 50 fb 4d 16 b7 82 04 d1 9e 0c 4e a5 88 7c d9 b9 ed f5 46 a5 32 e2 dd c9 82 8d 0c 1c 34 c8 0f fa a6 be 63 da 1f 54 cc 41 00 ee bd 57 c2 19 f6 a9 f1 05 35 f4 da e6 bb 74 a2 04 8d 14 04 64 a3 25 7a 4e d4 15 a5 76 8f 1e d5 b6 5f ee 97 42 15 b6 4e dc a6 ad 53 a7 b2 a4 f6 8e d8 33 b6 ca 4a 8d 93 d1 d5 7f 94 ae ab a6 19 53 81 0e 40 e7 1f 8c 8d 7b c2 ce ea cd 8d e1 30 bd 19 a4 f6 c8 d6 56 4a c5 87 d9 76 8a 33 53 3e cd 49 8f d9 32 86 77 34 6f dd 75 18 fa 8c aa 24 00 5a 7c d4 3d b2 77 5d 69 1c 13 8e e5 43 2f 0e 83 df de 9b d6 35 Data Ascii: D;j>rS+Rwv`+Cg eGi@ZJO}PMN F24cTAW5td%zNv_BNS3JS@{0VJv3S@12w4ou\$Z =w jC/5
2021-09-16 04:28:57 UTC	993	IN	Data Raw: 00 c5 54 d9 c3 2b 08 fa ad e1 dc a4 a9 07 c7 65 a5 19 d8 d0 d4 4b 1d dc 9c cc 4d 3a fe e9 d5 07 51 1e 16 54 f1 34 1c c3 ca 55 7c 0e 33 30 1a 1b ac 3b b0 f9 dc f0 1b 12 65 33 a1 9a 5c f6 55 65 52 73 61 c1 68 73 49 1b df 15 89 e9 0c 6b f1 15 8c d5 7b a4 9d 16 6a 8e 3c ca c7 f4 6d 66 ba 85 42 d3 32 e1 c0 f7 2e 8f e9 6c 2f 53 89 6b 5b 57 8b 48 b1 ef 0b 04 ea 19 f0 ba 49 36 7d bc 04 f1 58 8c 2b a2 a3 1e df e6 55 f0 b8 b6 61 aa 3b d1 9d 27 82 b8 95 96 9c fb a9 b5 7d 23 1d aa 73 1d 04 f6 6c ba dc 2b c7 72 ca e2 39 1f bc df 6d 96 67 00 b7 14 05 f6 5e 8a 60 3a bf 78 ad ef 51 37 50 17 57 48 8e f2 13 dd 58 31 dc b5 5a 20 50 a7 84 ab 88 75 a9 52 03 3b f8 0c d6 1f 15 d1 9d 1d 53 13 87 a0 3e d3 57 a9 0d 65 46 ba 29 b2 a3 b5 f1 cb f5 5d 2f d2 a6 88 c4 d7 cc 29 52 ea Data Ascii: T+eKM:QT4U 30:e3 UeRsahsk j<m B2.l Sk WHI6}X+Ua;"}#sl+r9mg!~:xQ7PWHX1Z PuR;S>WeF)J)R
2021-09-16 04:28:57 UTC	994	IN	Data Raw: c6 09 54 f0 5f e2 dc 5d 16 3e a3 9a 32 91 9d c5 c4 03 c2 4f a8 bd 22 d5 f7 0f 5b f9 c2 41 28 46 53 91 8e cd b6 35 f8 59 3d ab f6 7f ff c4 00 28 10 01 00 02 02 01 04 02 02 02 03 01 01 00 00 00 01 01 21 31 41 10 51 61 71 81 91 a1 b1 c1 d1 20 e1 f1 f0 30 ff da 00 08 01 01 00 01 3f 10 90 06 11 4a cc 69 79 2d 25 a4 33 78 0a 11 80 a8 4c 2a 87 4e 20 67 13 63 cc 2a 4a e8 14 66 05 19 84 cb 26 51 23 02 09 51 86 08 20 83 a8 08 20 84 8f ff 00 30 00 c3 0c 24 c5 35 53 1e c9 aa 89 21 42 85 73 5b a9 c5 9f c7 bb 85 58 27 73 5f 72 a7 98 73 76 65 43 2a bc ca ef 32 e3 98 c7 30 f3 99 88 b5 33 29 19 96 04 b3 a0 42 0b 2d 70 73 88 03 08 5c 25 8e 21 c7 43 49 2e 99 a4 4c c9 36 45 8a 2c c5 36 99 3a fe 51 1c c0 79 9e 63 3c c4 a0 c9 a9 61 b2 39 c9 10 66 1e c8 58 cc ad b9 4a 3d Data Ascii: T_]>20%[(FS5Y=(!IAQaq 0?Jiy-%3xL*N gc*Jf&Q#Q 0\$5S B X's_rsvceC*203)B-ps!% Cl.L6E,6:Qy3a9fXJ=-
2021-09-16 04:28:57 UTC	996	IN	Data Raw: 61 e0 c0 d1 07 84 25 e2 05 61 29 3a 81 92 4b 25 44 d4 77 95 af 32 e4 f0 91 00 a1 3c 40 61 69 59 ed 1a db c0 46 20 88 f7 98 cb 3a cb 18 91 11 30 18 83 4c 41 e1 05 e2 50 62 01 52 80 74 87 44 04 96 3d 58 c2 1d 1b 74 10 31 23 1f f1 a5 c1 2d 85 e2 07 ca 74 3f 30 8c 98 c3 a9 a7 b0 19 7b 11 63 09 63 9c 05 c5 b9 70 19 77 11 c4 02 7f 2f e4 aa 60 e2 26 85 d2 d6 57 2d f2 1c bc ad d4 ab 26 02 01 29 8e ce 5f 59 8d 69 c0 fa 33 e0 ef 59 ad b9 88 3f 20 b0 38 09 6f 2b a3 b5 d1 98 e2 91 27 29 57 9a db fc c7 ca bb 0d 05 7a 8e 80 22 38 19 4e f1 1f c4 a7 45 b4 f0 63 31 78 f8 2e ed ca 65 4e 4f c4 4a b4 a3 82 8f 71 b4 dd 94 32 82 06 70 21 07 9 3e 63 2e a5 71 b5 3f 2a 86 a8 eb dc 7c 5b 5f 88 80 2f 1a a6 cd 9f 63 5d e3 00 83 b2 9d 9f 31 b1 5a f2 3e 26 9a 8f 37 2e 97 42 17 05 40 Data Ascii: a%a):K%Dw2<@aiYF :0LAPbRtD=Xt#-t?0(ccpw/'&W&_)Yi3Y? 8o+)'Wz"8NEc1x.eNOJq2p!>c.q?' [_/c]1Z>&7.B@
2021-09-16 04:28:57 UTC	997	IN	Data Raw: bf 4c 5a 82 c4 e9 43 2b c0 80 09 08 0d 87 87 c3 98 df 26 8f 66 d5 d7 83 32 d8 8d 4c e8 8d 09 0d 93 96 95 f1 12 80 2c 6e b0 b4 b4 ea a6 5e 8a 0a b3 63 91 8a 77 1d 4b 97 42 83 c5 c4 b4 80 a1 99 83 73 06 e1 0d c0 47 30 33 05 61 9a e1 29 11 d2 35 30 cb 10 1b c4 a5 62 c2 86 56 91 43 32 82 01 88 24 08 1d b0 29 8b e5 96 4c e3 f0 8c 31 3a bd 2b 92 10 c4 2e 92 b6 e3 10 56 15 39 95 15 32 89 43 48 e5 38 97 59 6c 60 f0 b7 33 20 ed 18 85 e8 9a 47 a1 0e 9d 65 04 a8 c2 fc a3 72 cb 8d cb 39 84 15 37 0f d4 c8 18 3b fa 8f e2 fe b9 87 3b 97 04 ad 28 ca 85 1e e9 cf 6b 8b 50 29 83 74 3b f8 ea ca c3 55 1a fd b3 94 f6 e3 e6 23 c2 83 dc c6 fe 52 ca 80 2b 5a e6 bb fd bf d4 55 2d bb 25 a3 7f c4 34 ea ea e7 85 3c 00 fb 98 ad 55 7b 1f d2 fd c0 e1 40 05 1a 87 15 1e 03 89 41 e2 24 c6 Data Ascii: LZC&f2L,n^cwKBsG03a)50bVC2\$)L1+:.V92CH8YI`3 Ger97;;(kP)T;U#R+ZU-%4<U[@A\$
2021-09-16 04:28:57 UTC	998	IN	Data Raw: e1 79 0c 7b 8c 69 2d ca 1d b7 50 60 68 54 6d ad d1 cc 48 a5 e2 c7 2f 3d a2 6b cd 38 17 5f 2d 62 52 ed 38 16 c6 44 37 33 16 eb d9 fe a7 01 91 bf 1a 63 0e b3 b0 7c bf 71 8c 34 78 05 64 fc 30 b0 88 b8 cd e7 b3 38 97 d0 93 36 30 6d d7 10 ca d0 aa 11 0e 28 3f 2a e6 61 d0 60 42 92 f1 f3 e9 5c 62 18 65 4d b3 6d 1f b4 cf 09 92 94 9a 95 04 23 d0 a7 96 21 52 ba 16 1d 06 92 a4 b8 3c b8 8d 88 01 16 52 87 a5 5b 1c 22 62 2d 18 e9 18 19 ce 2c 7d c3 fa e0 40 68 86 13 11 11 2a 94 7f 83 d4 45 02 15 30 d1 8c 6e 35 63 bc a3 68 65 76 25 b4 60 63 b0 7f ed cb f1 46 7b 07 f2 cb d9 78 0e de a2 62 de 3f 17 b8 ec 85 58 ac ab 01 cb 10 91 2e 2c aa c9 f9 66 df 82 30 20 d4 1c 19 3f a9 9b d5 25 53 b5 57 ea 25 98 dd fd 40 73 04 bf 1d a2 26 d7 dc e4 87 5b 55 3d 06 0d ed 63 89 8d ad Data Ascii: y{i-P`hTmH/=k8_-bR8D73c q4xd0860m(?*a`B beMm#!R<R["b-.)@h*E0n5chev%'cF{xb?X..f0 ?%SW%#@s&[U=c

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	1000	IN	Data Raw: f9 43 55 e9 35 26 b1 8f 47 ab 18 fa 75 91 c1 cc a0 e6 10 73 0c b8 be 91 7b 71 b1 ca 14 f9 80 95 ba 84 f0 62 b4 b3 29 ac 39 a6 5c 38 80 65 db c1 fc ca 0a 45 93 9a 39 6f ba 98 87 5e 5c b9 c0 e0 28 2e 5a 68 94 cb ae 55 e2 d5 ce 7c 41 1b d4 bb 10 29 35 76 9d 19 8e e0 c6 e8 5b 58 ed 83 ca 47 ed 60 4f 08 ec fa dc 26 a6 ad 3e 59 84 f6 b9 13 ce 31 f3 f8 80 23 80 5b c5 f3 12 b9 c0 0b 5b e0 f3 0a 99 f0 1c 1e fb c0 15 6c 9e e6 f7 12 76 0b df 7a 62 98 0b e5 c7 60 55 44 4b 4a dd d8 5f 17 c1 e2 56 a0 aa 6f e3 d4 af 0e 60 46 9f 2f 69 65 d2 a4 4d 4b 03 6c 4b 6b 3d d2 a5 d8 ca db 88 20 97 71 44 4a b0 7f 52 b1 ec 5f 93 af dc 2d 86 53 f3 b8 22 22 fc 79 3c 7e 62 bd 1d 0d 6c 02 44 d6 22 ce 59 ff 00 b9 70 d4 36 97 68 5e be e6 74 02 af 45 11 f9 21 40 aa b7 6c ac c4 97 98 74 5c Data Ascii: CU5&Gus(qb)9l8eE9o^(\.ZhU A)5v[XG`O&>Y1#[[lvzb`UDKJ_Vjo`FieMKIKk= qDJR_~S""y<-bID"Yp6h^tE!@ t\
2021-09-16 04:28:57 UTC	1001	IN	Data Raw: 14 c1 a7 ae 18 14 04 51 5d e1 db 8b 86 9b fb 8a 2b 13 17 92 28 15 0c 9e d5 21 00 62 a7 ec 7e ae 25 2a 34 c7 7c d3 1c 41 e9 03 b0 59 32 45 8a ad 34 17 8f 4c 13 31 96 de 59 82 60 15 07 92 d7 d4 65 c7 32 a7 24 72 b1 10 0c 42 a8 68 86 11 03 2b 12 c7 8c 41 0d 4d e2 62 99 4a 4c 11 a4 a3 0d 4b 59 30 cb 9c 34 b0 ed d2 15 70 82 c5 55 65 c3 a9 f5 0c 1c 2c 5c c8 40 85 5b 80 aa 97 1e e5 04 e0 4a 09 41 28 bc ca 2f 31 4e d1 fb c7 c6 66 89 59 99 e4 9e 58 88 c0 06 12 1d e3 e6 3a a3 79 94 99 c8 44 28 89 57 bf 9e ff 00 1a 83 25 3c cc 0a c1 c1 6a f6 e8 81 bd 07 8d 02 e7 3e 89 b8 85 3b 72 57 c0 6b be e0 2e b4 6e df 01 fd b2 e5 73 57 38 c2 fd a9 e8 86 6c 44 97 86 ff 00 39 0a 94 a2 10 56 f0 90 df 38 b5 8d 0a 44 14 bc 08 1c de e2 2a 24 d9 a7 27 da fc 4b 2d 2e 1c 96 d0 d7 d8 3b Data Ascii: Q + (b~%*4 AY2E4L1Y`e2\$RbH+AMbJLKY04pUe,\@[JA/(1Nfy:yd(W%<~>;rWk.nsW8ID9V8D*\$K-;
2021-09-16 04:28:57 UTC	1002	IN	Data Raw: 11 54 54 27 9a 36 c5 c4 a8 44 51 21 06 02 16 d1 ac 5c b1 cc 31 33 1c 19 81 8c c4 10 69 cc a6 e5 b6 71 1c 6e 5e 66 56 dc 2a 73 0e 39 cc 66 b3 68 4a 46 06 d7 b0 5b 16 11 ec d4 d7 83 6e 68 57 68 d8 04 81 58 37 86 0b 70 06 88 94 9c d0 31 8d 51 e0 d1 1a fa b5 c0 6c 3f f7 10 d4 0a 15 1c d0 84 c1 f5 2b 01 ad 3b 5b b7 fe d4 41 28 94 e7 37 9f f6 54 81 2c 43 b2 74 f2 c0 74 07 88 66 2c f6 e2 35 4a 4f 36 b9 6e bb 95 0a 2c 42 a6 02 d7 c7 77 2f 82 2d 7e 01 da b4 67 12 1d e3 e6 5b 00 e0 d0 7b 79 94 3b 4b ec c2 32 eb 26 65 5b 5e 39 95 1f 11 26 ea 51 b5 7b 07 78 af 49 1a 35 f1 0e 23 e7 ff 00 73 03 bd 6b 80 fe 21 7a 16 83 2c 01 26 74 52 f0 7a 8b 0e 72 ee bf a4 b4 2a 5a 23 ec 92 89 7e 2c c7 97 52 e0 d7 4a 37 d8 cb 4d 95 41 17 09 43 44 53 5a 20 f2 b5 af 41 0a 2c cb d0 75 51 Data Ascii: TT^6DQ!l13iqn^fV*s9fhJF[nhWhX7p1QI?+;[A(7T,Cttf,*5JO6n,Bwl/~~guE{y;K2&e[9&Q{xI5#skIz,&tRzr^Z#~.,RJ7M ACDSZ A,uQ
2021-09-16 04:28:57 UTC	1004	IN	Data Raw: 6f 7a 7f f3 08 b6 16 13 f7 f8 8e d9 47 f7 60 08 c1 30 6c 2c ad 41 6d ab 1d ba d5 c3 2b c9 83 d6 02 08 a6 16 87 03 12 b1 94 56 ee de 7d 13 5c 69 68 f9 9e 70 15 3c da 05 a9 cb 41 00 04 a1 96 78 c4 32 ad fd 62 90 35 39 c8 29 93 24 c3 18 aa e2 0a 8b 25 21 58 a8 65 7c 4a e0 8e 5c 93 29 8b 02 78 95 40 4a c9 ae ff 00 2a 07 75 94 22 98 d7 12 e3 d2 88 e2 48 95 bc 81 f8 98 ee 9a 27 a3 2b ed 8e 5d 39 d5 5a fe f1 88 56 4a 14 c1 dd b0 fc dc 53 03 ed 00 c7 96 db 21 f8 02 ec 68 0f 06 99 86 11 b0 b3 2a a8 26 41 65 ab 3c 2f 31 d1 9b 60 b9 03 9f 88 c9 67 75 3b af 32 eb 46 1d c4 c4 d2 38 47 09 65 4a 48 a9 6c ba 32 1b 6a 38 40 91 54 c3 be 8b 19 7c 41 81 20 b8 e5 93 2d 72 d7 46 87 a1 08 4b 8e 28 b0 83 4c 58 52 b1 99 46 f3 3a d9 8d cc b8 e6 5c b9 82 18 96 3a 11 40 e9 12 6a 12 Data Ascii: ozG`0l,Am+V}ihp<AAx2b59)\$% Xe J)x@J*u"-W'+j9ZVJS!h^&e<~'gu;2F8GeJHl2j8@T A ~rFK(LXRF:\:@j
2021-09-16 04:28:57 UTC	1005	IN	Data Raw: b7 29 6a 7c d4 3b b5 41 6b 2f 4e 6e 5f 44 6e 2f 15 66 3b e4 dc 5a 07 cc 95 5b c5 38 97 42 c4 97 c2 fa 24 cd 17 79 78 c8 21 5a 96 80 f0 31 ef e1 e1 ac 34 97 e2 ed 88 22 1c 2f d2 9f 09 1a d0 fa 44 ff 00 b0 88 11 03 b8 1f c1 30 75 55 0e d7 8b f5 38 6c 9a 74 8f 69 7a 04 7b 4c 06 2f 3b 94 6c d9 f9 22 20 42 d0 c6 c4 df 37 66 66 96 46 59 a9 23 25 39 e8 e2 48 a5 1d 0d 47 14 c2 55 d0 19 44 80 61 33 7e 25 b7 89 bb 11 bc 10 23 99 a6 6a 47 b2 60 89 21 9b 8a 9c 43 2f 13 24 c5 e9 51 33 1c 23 d3 33 16 fa 40 97 51 11 c4 7c e2 24 6b 1c c7 b8 7b bf 88 e4 1a da e0 0f 31 c6 40 0a f2 f6 bc c6 e0 40 46 a3 7a 17 ef 5c 45 2d b1 50 85 76 3d bc c6 17 81 4d 98 71 b0 79 8d 52 dc 50 39 e0 67 82 3d 4c ee 58 5e 68 fe d8 cc 5c e1 a5 7b 78 34 4c c4 29 9e 45 94 be fc 43 e2 e8 9f 3a 1f 70 Data Ascii:))j;Ak/Nn_Dn/f;Z[8B\$yx!Z14"/D0uU8ltiz{L; ;" B7ffY3%9HGUDa3~%#G`I'C Q\$3#3@ Q \$k!1@~@FzIe-P v=MqyRP9g=LX^h\{x4L)EC:p
2021-09-16 04:28:57 UTC	1007	IN	Data Raw: c7 3f 10 98 97 47 68 0d 19 89 5c 13 f9 89 8d 65 c9 60 40 cb a8 96 59 18 af 99 46 b4 94 1f 3b 83 1e 4e 75 fd af 70 db 43 3d ec b0 7d 97 72 b2 cf 1d ea c1 f8 42 06 11 57 38 63 70 0f c4 2f ae ff 00 2a 07 75 94 22 98 d7 12 e3 d2 88 e2 48 b5 59 f8 20 49 4a be a1 fe 18 e0 20 4a 1b 25 6b de a2 83 83 2f 4a 7f 53 b8 72 ae e6 d9 9c 8b 33 dc 75 31 c5 92 ff 00 67 98 71 70 0b d8 7f b4 a0 5f 24 4a dc b9 b9 79 83 a5 59 37 44 ac 16 4c 19 9b ac 04 96 c5 63 d2 61 1e 21 69 69 33 f4 3a 3d 05 85 23 91 fb c7 18 bd e0 09 51 06 98 42 c7 42 1d c0 87 10 c6 a7 15 28 b8 97 a9 b8 96 cd 6a 9c 24 00 82 b2 94 54 42 25 a3 ea ef 6a d0 41 29 32 c5 5b dc c1 33 5d cc 13 fc 4d 11 f5 ff 00 2c a5 1b 7f f0 10 31 29 c8 fc 15 06 cc 55 20 ac 1a 21 17 09 74 77 65 e0 98 03 4e 67 cd 5c 1d e1 f2 ef 96 0a Data Ascii: ?Ghle`@YF;NupC~rBW8cpL/L9#)KY IJ J%k/JSr3u1gqp_.\$jyY7DLcalii3:=#QBB{(\$TB% a)2j3[M,1)U !tweNg\
2021-09-16 04:28:57 UTC	1008	IN	Data Raw: c8 a0 b0 a5 ae c6 9b 5e 0c b1 f3 25 18 2b 6a 83 81 15 2e 6b 3c c6 3b 4f 79 b5 3f 70 89 af 62 d8 5c e1 bf 3d 82 5e 0a b0 78 05 24 fd 4c fc d6 4c 0f 27 8b 7e a0 4b 16 00 c6 0c 1f 2b 6c 40 a4 9e 02 ee 9f 32 db 06 0b f7 05 82 ca 87 66 18 46 5c 43 9b 1c 7b 8c 2b 75 75 28 80 53 73 06 b7 2c ca 31 79 b9 86 8e e0 02 0d a1 0e 33 30 bb d2 16 31 a0 ba 70 a8 1f 64 48 85 24 ee 51 7e c8 d7 ad 85 97 f5 92 e0 19 93 08 8f c4 29 a9 4d e9 b1 59 fb 82 ba 50 be f6 a5 77 6a ff 00 b4 40 b4 51 76 38 bf fb 0a 94 52 df ce e0 a4 39 ef 0a ea 09 16 e8 79 26 12 dc 94 e2 b7 17 76 02 25 25 96 7e 26 0f 05 c9 ee 14 94 5c 3e 1d 89 64 af 8f 89 61 ce aa 53 fe 12 91 18 2f a3 24 49 86 57 12 56 3a 0b 70 8e 81 55 18 6e 5c b9 72 e5 c5 97 08 1d 56 2c cd 63 46 e8 82 41 84 a0 cb 02 e4 30 0b 0c c8 31 Data Ascii: ^%+j,k<;Oy?pb!=^x\$LL'~K+!@J2fIc{+uu(Ss,1y301pdH\$Q~)MYPwj@Qv8R9y&v%&~&~&daS/\$IWV:pUnIrV, cFA01
2021-09-16 04:28:57 UTC	1009	IN	Data Raw: 2b a6 4e d2 90 e9 0d 7d 35 90 3d 2f fc 2e 0c 51 62 26 21 e9 36 cb 02 5a ea 78 61 f6 94 74 8e a5 b2 a2 5c ab 31 e0 36 bc 10 53 05 95 be 65 e5 82 65 ab 55 2c 35 f7 c4 61 cc c0 8a 5a 01 cd cc f1 cc c7 a6 18 3b 21 53 3c 4a c5 2c 1a f8 8b 40 07 d3 42 22 56 3c 2c 03 7f 88 cb 02 3d dc 52 8d fe bd 47 ab d6 b1 d0 6d f7 6e 3c ca b8 52 55 9a 5d cb 01 1b 11 96 c2 96 f0 ac a7 3a 5a e7 06 c5 79 94 44 eb 5e 85 7d ca 00 0a 1a 8b ee af bd b3 b4 26 96 d8 06 3e 75 15 86 21 76 b6 c8 7e 2d ea 68 6a 87 37 85 3c 64 48 c1 25 81 c3 2b 1e 21 3c c6 0d a0 68 fb 26 73 01 bb 21 e3 b4 c5 f8 3b b7 22 4a a1 11 b4 c2 77 25 0c 03 6b c0 a3 7c 12 cf 13 08 79 4a 14 e3 96 35 6f ac 30 02 54 2a c8 08 a1 97 0d 84 1e 0b 76 07 78 ef 27 59 ad ab bb 5b 96 5c 3a 48 2a 0a 63 44 2f 97 b8 22 8f c7 20 08 Data Ascii: +Nj5=/.Qb&!6Zxat!16SeeU,5aZ;!S<J,@B"V<.=RGmn<RUj:TyD^)&>ulv~--hj7<dH%+!<h&!;"Jw%klyJ5oOT *vx`Y[l:~H*cD/"
2021-09-16 04:28:57 UTC	1011	IN	Data Raw: a2 17 45 7c 60 9f c4 b2 05 9e 34 9c 77 bf d4 b4 4b 74 3d db 1f 99 c4 c5 7c 2c 89 e2 15 24 21 3e 49 5c 8d 19 f3 44 c6 f7 11 e6 31 ac 78 cb 7f a9 53 5e 28 84 57 62 9a 2e 0e 66 0d 6a c2 28 a3 99 99 22 06 16 ca 1e 4b 99 dc 0e 1e e4 50 e9 2b b8 d7 06 0b 22 2a 29 19 13 0b 97 b9 99 32 41 a8 e6 0c f4 b9 72 e2 c5 ea c7 1a 4c 29 65 4b 69 98 90 81 05 30 cc b2 99 68 4d c8 af d6 35 f9 95 d2 e5 1a 6f 1b 97 aa 65 85 b3 72 84 00 d7 6e 3f b8 87 33 73 45 73 36 21 84 69 85 89 a0 cf f5 02 ee 58 87 37 ae ee 52 a6 16 b9 03 7d d1 10 0b cc 67 45 35 f0 42 c1 b7 1b 79 ef c6 62 d2 c0 7c 40 54 a1 10 86 b8 c8 a1 ed 32 ae 04 96 c9 c6 62 bd e1 2f b9 af b9 aa 94 56 b5 77 bf cc b9 50 58 cb b0 f3 2f c0 1a b7 64 3f 34 cc db 94 68 dd 28 32 e8 8c a5 f0 8f dc f3 b5 8b e1 d3 11 76 cc 56 39 27 Data Ascii: E `4wkt= ,\$!> D1xS^(\Wb.fj("KP+~")2ArL)eKi0hM5oern?3sEs6!IX7RjgE5Byb @T2b/VwPX/d?4h(2vV9'

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	1012	IN	Data Raw: 38 f7 1d 1c ea 10 eb cb 05 2d 5e 95 a8 3f 07 3e e2 a9 6e fd 1a e6 98 c1 53 8e d5 3b 3d 16 10 1d 37 72 ea 1d de 63 95 88 a6 61 94 ba 56 27 72 12 e5 c5 8f 42 11 62 38 f3 37 9b 11 c1 12 0b 31 18 2c 8e 18 82 dc 21 88 3b 80 be 5d b3 76 3e 22 8a 4c 8b e6 22 b1 30 cc 1c df 30 18 98 16 a5 68 8a 82 e5 84 25 62 92 cb cb c5 ea 3d 5f 30 02 85 a4 7c c1 06 ff 00 00 81 fc 40 89 da 7e 0a 7e 21 e7 56 97 67 b1 14 6c 86 03 5c 23 ee 77 3d af cf 0c 70 6c 1b 71 75 9f e5 09 a3 14 7b a9 83 ea ee 5b 55 a4 ca 38 66 22 ea 80 38 09 8c f3 18 58 15 fc 74 40 41 55 0b e0 4b f4 25 99 56 69 d2 6c 46 80 7b fc 39 48 66 90 10 8c 58 53 5c 6a 01 53 6b 1c 52 69 8e 43 ad 4e 44 bc fb 97 11 68 8d 79 a5 fc b1 8a 97 96 fb 0a 63 d0 b7 93 5f 89 4f c9 07 28 69 a8 6b 69 47 60 89 45 6d f1 1a 00 61 cb b4 Data Ascii: 8-^?>nS;=7rcaVrBb871,!)>v>"L"00h%b=_0 @~~!Vg\#w=plqu{[U8f"8Xt@AUK%ViIF{9HfXSj\$SkRiCNDhyc_O(ikiG'Ema
2021-09-16 04:28:57 UTC	1013	IN	Data Raw: 50 c2 ec b5 2f 15 c9 40 1b f1 4e 4f 31 09 af 4d 5b e0 78 9b ad 8a d3 c9 7f c4 c2 11 e5 e2 30 90 76 ed 88 88 07 d3 0a ae e0 90 18 cd d0 34 7f 94 ba 9b 43 ea 59 36 b9 93 06 66 88 2e 03 31 51 95 64 a9 56 40 63 d6 fa 10 26 91 53 1b 3d 19 21 c2 5f 51 08 e0 a0 72 d4 1e 1c 4b 56 b5 2a 79 ac e7 3a 97 27 bc fd 90 ab 3b a2 aa c4 ab 71 00 ad e2 31 a6 50 b5 6a 11 05 99 c5 c6 07 67 24 71 4b 55 77 24 50 0b 91 99 cb 99 46 4b 21 6a 8b ee b4 41 6c 44 2d 8a bb af 55 86 1b 02 e0 10 6f 0d 97 29 dc cf 1f cc 05 05 54 00 e5 74 4c 04 0a b9 50 1f 9f b8 e4 dc b5 65 1a be 82 a3 6e c3 45 2c 57 a8 d1 65 82 3b b8 f1 01 6c 3b 68 b6 7c 44 d0 af 5a 7f a8 a9 98 2c d4 35 2e ee da a0 79 21 67 7e 77 2a 17 49 99 31 78 d6 30 4a 61 42 51 5a c1 44 a4 63 01 df 15 3e c9 97 5a 2a 1d c2 fe a3 c2 de Data Ascii: P/@NO1M[x0v4CY6f.1QdV@c&S=I_QrKV*y';q1Pjg\$QkUw\$PFKijAID-Uo)TlLPenE,We!;h]DZ,5.ylg-w*11x0JaBQZDc>Z*
2021-09-16 04:28:57 UTC	1015	IN	Data Raw: 3d 28 80 66 fd 2f 40 4e 82 84 0b 06 5c 56 2c 44 8b a1 91 2b 10 61 01 48 08 8d b7 2a 26 29 07 4b 55 26 60 b7 0e f3 62 ee e3 26 e2 c4 d1 d2 18 66 84 5a bd 4c 0b cc 75 50 88 bc 66 2a 16 25 b4 05 06 2e 25 f3 f2 24 d9 8d 41 2f 2c e7 a3 b9 c4 7a 71 d3 8e 86 af fc 2e 5d 41 41 c4 58 94 15 81 09 88 a6 46 a2 29 c3 3c da da bc ac 08 0d 92 fa 9a 0d 47 f4 42 3c 4a 26 87 6b 45 8a 8c 33 7f ba 85 cf 9a 8c be 88 d0 b5 1a 92 fb ca c5 b6 2a 06 b4 9c e2 58 bb c9 b1 66 42 87 13 6f 5b cc 7a 2c cc ec 41 7e 04 05 b5 9a 3f 12 d2 c0 b5 44 31 8c af 72 a0 8e 99 87 10 45 4c 58 b6 c3 c2 8c 7e a5 ae 16 8d eb 38 85 99 6d f5 7f ff c4 00 2c 11 00 02 02 02 02 02 01 04 02 03 00 03 00 00 00 01 02 00 03 04 11 12 21 05 10 13 31 22 14 20 23 32 06 41 15 24 33 30 34 35 ff da 00 08 01 02 01 01 Data Ascii: =(f/@NV,D+aH*&)KU&'b&fZLuP!*%.%\$A/,zq,JAAXF)<GB>J&kE3*jfBojZ,A~?D1rELX-8m,!1" #2A\$3045
2021-09-16 04:28:57 UTC	1016	IN	Data Raw: 84 c3 bf 99 07 f1 ce 3f c5 7f 7f 27 51 9b 53 e5 ed 2c 06 29 dc f8 c9 9f ae 60 29 a8 89 ae af 21 46 43 17 94 2f 2b b3 2c 34 84 0b 65 ac c5 ac b7 5c 54 00 f5 db a0 ce 58 3b 15 b4 66 de 52 b7 63 77 22 05 b7 0d 68 fe a3 1d bf 87 93 72 c1 c9 35 ad b9 ed 2f c9 dc b2 ed c7 b0 92 5c 88 1c 98 bd 8f a2 0f 68 d1 4f 46 24 c4 42 4d 7b e3 ef 07 ab 39 89 9c ff 00 c5 6f f6 62 65 80 c2 0c 52 44 a1 b6 69 ac 18 b5 0d 32 05 f5 94 3f 1c 80 41 f1 e9 ce cf 34 36 84 8a b1 2b d6 c3 96 67 23 4a db 15 b7 57 57 cc 8c 2b 8b 20 54 0e 46 9c 92 cc ba cb a8 e9 7e ac 7b 78 b5 99 1b 02 e2 61 31 f6 21 68 af da 36 e1 1b f4 ad a3 53 ee 13 dd 63 bc 4c 10 aa f5 0e 3e b5 31 9f 8b 7c eb af 21 97 b0 5f 64 0d c6 a7 61 a8 30 d4 41 a0 f1 7c 40 19 78 80 2e 61 35 32 50 15 cb 56 d7 8d 55 59 79 56 cc f2 Data Ascii: ?(QS,)!)FC/+,.4e!TX;fRcw'hr5/hOF\$BM[9obeRDi2?A46+g\$JWW+ TF-[xa!lh6ScL>! !_da0A @x.a52PVUYyV
2021-09-16 04:28:57 UTC	1017	IN	Data Raw: 09 f8 6a bd 2c a7 33 10 e3 d8 a6 0b 3b e5 b0 4c 56 d1 e5 3b 31 07 61 74 7d ee 6e 6c 4b 8e 93 c8 b9 0c 4b 13 de 99 49 3e 3f 1c 28 c8 c9 d0 b6 c2 cc ad 15 a2 5a 67 22 4d 63 83 e3 5b fc 15 10 93 26 e2 e1 34 d7 15 d3 2b b0 99 08 39 62 dc d4 9b 5c b4 5e 2a 6b 0a 86 ef c4 3f 73 22 b6 4a 51 b7 31 cf 07 a4 e9 8f 25 5a 2b 2e 42 20 0a a3 e2 b0 7c d5 3a 32 36 fb 4e c1 4d 42 75 15 b7 13 7b 02 01 ec 98 4c 26 02 66 43 69 33 ec 05 95 77 0a 75 f1 c6 b0 2a 5d 69 62 07 7b dc e4 34 a6 57 32 06 9e 9a fa 2e 0d 96 82 0d 48 1f 22 c6 3c 54 e8 f2 e4 ac 07 c1 8b 7e d1 c1 80 82 2d 5d 8b 3e c0 6b 16 b0 dc f2 b1 ca 5b 5a 29 50 55 9e b6 44 b8 dd 12 c2 67 2d 1b e9 4c ba 38 9e 55 81 1c 0d 11 2b fb e1 00 d4 00 fb 30 9f 42 66 12 2a ce 6f ce 86 0c 38 6c 3f e2 2e b4 eb 73 7e d0 6a 23 09 90 Data Ascii: j,3;LV;1at!n!kK!>?(Zg'Mc[&4+9b!^*k?s"JQ1%Z+.B :26NMBu[&L&cf3wu*]jb[4W2.H~>T~>]>k[Z]PUDg-L8U+0Bf'o8!?.s~j#
2021-09-16 04:28:57 UTC	1019	IN	Data Raw: 08 28 b0 93 12 55 1e e0 16 d3 89 27 99 45 c7 14 d7 e0 4c 22 30 2a 61 52 90 8f 22 df 54 c3 8c 23 4b 22 32 3b 93 2a e8 d5 5d 1a ef 04 35 04 35 94 78 70 0d 2c 88 c1 13 63 84 26 b4 dc 36 10 19 0a a3 cd 77 d5 75 09 a3 f2 cd f7 1f fe 0d 3e a8 72 05 0f dc 13 8e 65 4c a3 0a ea fa ce f8 43 73 9e a2 8e fd 95 b5 12 ba 94 00 b0 bf 54 1f 86 d5 3d 97 c5 36 21 1e 65 06 8c 91 3c f5 5d 16 06 cb 8e 28 68 a2 99 14 74 71 50 26 95 50 a1 46 7a 22 bc c2 1c aa 9c d9 ae d4 a8 9e 24 20 86 f1 47 7e a3 5f 24 49 34 0a 1b 6c d4 0c 1c 13 7f c0 84 5c 70 43 cd 4e 64 eb da 6d d0 74 46 65 46 39 e7 a8 2f c3 f3 63 82 d2 37 2d 27 be a2 46 a8 e2 09 1b d7 5b 23 5d 95 b5 0d 70 35 90 22 a8 09 b8 3f c2 73 5c 3c 30 25 40 b1 28 68 c7 25 0d b9 a0 fe 7b 28 cb 57 84 12 02 f9 1c a2 9d c4 9f 35 f2 1f 35 Data Ascii: (U'EL"0*aR"T#K"2;*)55xp,c&6wu>reLCsT=6!e<](htqP&PFz"\$ \$~_!\$!lpCNdmtFeF9/c7-!-[#]p5"?s)<0%@(h%{(W55
2021-09-16 04:28:57 UTC	1020	IN	Data Raw: 07 c9 1d 23 8d c4 40 52 da 89 12 11 89 a6 05 49 c5 77 47 ae a0 42 1a 56 8a 3a fd 77 a3 80 54 73 d6 07 01 dd 14 73 94 e6 ba ce 04 79 2f 10 99 a1 e4 73 ee 8c 0b 9a a8 b8 4e 20 78 41 01 c3 91 a2 6c dc 78 4f 6c 53 27 1a 15 4b 83 e8 bb eb 98 5a 42 3f 59 44 0b 95 2d ab 0d c6 48 1c 25 48 b7 a8 54 ac 7a 8d 44 eb 2c 3d 91 e2 94 7a a1 a8 ee 93 ac 8c c2 db 6b 4e cc 8a 9a 0a a2 f7 b9 a6 1c 49 d9 ac 0c 48 44 9d a9 a0 bd 0a 35 78 24 5e 71 cd 3b e0 e9 81 92 68 e1 09 ed d2 b0 b4 96 8a dc 1e 52 af 51 00 f5 06 10 27 01 ee 89 fd b5 5d f5 00 6e 9e 41 b0 94 e6 9c d6 c1 30 45 16 cd 64 a3 a4 21 b1 3f 24 c3 88 fb 2d 82 1f b6 0d 5a e7 41 ed 08 bf f0 ae 24 e2 c7 7d 8a 21 c0 b5 c0 c1 07 3d cb a9 c0 d7 58 d5 1c 02 bb a3 16 0b 90 08 ee 04 e7 0c 0a b2 05 ac 86 fe a3 40 a5 e3 6d d1 8d Data Ascii: #@RIwGBV:wTssy/sN xAlxOIS'KZB?YD-H%HTzD,=zkNIHD5x\$*q;hRQj'nAoEd!?\$-Z\$)!=X@m
2021-09-16 04:28:57 UTC	1021	IN	Data Raw: b6 59 c8 37 8a b9 ac ab c5 a5 60 52 56 aa 0f e1 62 ed 72 91 92 ef da 0d 90 bd 59 ad 17 81 a0 33 e4 6a 6e 6f 70 88 0c bb 10 85 6d ab 16 26 09 b9 bd 4e 70 30 32 bf ea 3e da 84 ad 01 17 a0 0b 94 df 95 60 93 8e 84 b5 4a 35 70 d2 32 91 5e 32 f6 e2 57 50 fa 65 a8 69 76 9d 71 ab 2a 39 a1 c9 be af c8 35 80 52 41 7c 85 ee a5 22 d3 f1 e5 93 57 6e 56 67 2e ae 3b 0c 3b 55 3a 02 01 ed 44 65 82 66 20 13 29 40 b3 d6 fa 30 c4 95 7c 08 17 73 81 85 26 bb ac ca 9a 64 da 35 7b 12 d8 b5 ec d5 5a 80 3a 0e fb 23 8b 26 32 f1 42 37 65 15 ee 8c 8a b4 51 5a 56 38 81 c0 65 3a 86 05 40 94 aa 87 c8 ff 00 d1 97 8d c4 0d 79 8f fd 4c 0c 44 0f 1c ec 71 81 67 18 07 a3 17 e7 5b 8c a4 1c d3 32 db 76 fa dc 3f 06 2c ab e1 65 35 72 23 10 ea dc 62 23 a1 04 3e a0 c8 13 26 fd cd ec e2 f7 2b ea 39 Data Ascii: Y7'RVbrY3jnopm&Np02>`J5p2*2WPeivq*95RAI"WnVg,.;:U:Def)@0]s&d5[Z:##&2B7eQZV8e:@yLDqg[2v?,e5r#b#>*&+9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
149	192.168.2.3	49932	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:57 UTC	1032	OUT	GET /style/met-gala-2021-red-carpet-best-dressed HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:28:58 UTC	1033	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 236174 Connection: close Date: Thu, 16 Sep 2021 04:28:58 GMT Cache-Control: max-age=3600 content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Apigw-Requestid: FvQxpi2-oAMEJxg= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 474733f16f494ddb794b4f7dfd7de967.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: xRxt38LQe7hPgWUHM83YxH_46I6JTXtcV4QEaGEV6DelZeEmkKTA==
2021-09-16 04:28:58 UTC	1033	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:28:58 UTC	1037	IN	Data Raw: 31 2f 39 2f 31 33 2f 38 37 30 66 63 32 63 62 2d 66 65 66 32 2d 34 39 33 33 2d 39 38 63 30 2d 61 38 66 33 34 62 64 66 36 38 34 39 2d 6d 65 74 30 30 32 2e 6a 70 65 67 3f 77 3d 31 32 30 30 26 68 3d 36 33 30 26 66 69 74 3d 63 72 6f 70 26 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 66 6d 3d 6a 70 67 26 66 70 2d 78 3d 30 2e 34 38 36 37 26 66 70 2d 79 3d 30 2e 30 32 37 38 22 2c 22 77 69 64 74 68 22 3a 22 31 32 30 30 22 2c 22 68 65 69 67 68 74 22 3a 22 36 33 30 22 7d 2c 22 61 75 74 68 6f 72 22 3a 5b 7b 22 40 74 79 70 65 22 3a 22 50 65 72 73 6f 6e 22 2c 22 6e 61 6d 65 22 3a 22 41 76 65 72 79 20 4d 61 74 65 72 61 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 72 2e 62 75 73 74 6c 65 2e 6 3 6f 6d 2f 70 72 6f 66 69 6c 65 2f 61 76 65 72 79 2d 6d 61 74 65 Data Ascii: 1/9/13/870fc2cb-fef2-4933-98c0-a8f34bdf6849-met002.jpeg?w=1200&h=630&fit=crop&crop=focalpoint&fm=jpg&fp-x=0.4867&fp-y=0.0278", "width": "1200", "height": "630"}, "author": {"@type": "Person", "name": "Avery Matera", "url": "http s://www.bustle.com/profile/avery-mate
2021-09-16 04:28:58 UTC	1047	IN	Data Raw: 76 20 63 6c 61 73 73 3d 22 51 52 5a 20 43 63 48 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 66 65 5f 22 3e 3c 68 32 20 63 6c 61 73 73 3d 22 69 74 57 20 7a 50 6a 22 3e 3c 68 32 3e 41 6d 61 6e 64 61 20 47 6f 72 6d 61 6e 3c 2f 68 32 3e 3c 2f 68 32 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6f 5f 72 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 4d 53 20 63 43 56 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 43 43 22 3e 3c 66 69 67 75 72 65 20 63 6c 61 73 73 3d 22 51 4d 67 20 70 61 43 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 76 78 5a 20 61 70 4b 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 35 30 25 3b 22 3e 3c 6e 6f 73 63 72 69 70 74 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 Data Ascii: v class="QRZ CcH"><div class="fe_"><h2 class="itW zPj"><h2>Amanda Gorman</h2></h2></div><div class ="o_r"><div class="sMS cCV"><div class="sCC"><figure class="QMg paC"><div class="vxZ apK" style="padding-top: 150%;><noscript><div class="cCV"><div class="sCC"><div class="QRZ CcH"><div class="fe_"><h2 class="itW zPj"><h 2>Brooklyn Beckham & Nicola Peltz</h2></h2></div><div class="o_r"><div class="sMS cCV"><div class="sCC"><f igure class="QMg paC"><div class="vxZ apK" styl
2021-09-16 04:28:58 UTC	1063	IN	Data Raw: 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 33 2f 63 36 66 38 62 31 39 35 2d 34 66 63 39 2d 34 37 64 34 2d 62 33 34 61 2d 65 34 33 62 36 62 31 39 38 66 64 61 2d 67 65 74 74 79 2d 31 33 34 30 31 32 39 30 30 35 2e 6a 70 67 3f 77 3d 34 31 34 26 61 6d 70 3b 68 3d 36 32 31 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 22 20 73 72 63 73 65 74 3d 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 33 2f 63 36 66 38 62 31 39 35 2d 34 66 63 39 2d 34 37 64 34 2d 62 33 34 61 2d 65 34 33 62 36 62 31 39 38 66 64 61 2d 67 65 74 Data Ascii: com/uploads/getty/2021/9/13/c6f8b195-4fc9-47d4-b34a-e43b6b198fda-getty-1340129005.jpg?w=414&h=621&fit=crop&crop=faces&auto=format%2Ccompress" srcset="https://imgix.bustle.com/uploads/getty/202 1/9/13/c6f8b195-4fc9-47d4-b34a-e43b6b198fda-get
2021-09-16 04:28:58 UTC	1075	IN	Data Raw: 52 65 6e 74 61 20 64 72 65 73 73 20 74 68 61 74 20 77 61 73 20 61 20 72 65 70 6c 69 63 61 74 69 6f 6e 20 6f 66 20 74 68 65 20 48 61 6c 73 74 6f 6e 20 67 6f 77 6e 20 74 68 61 74 20 42 69 61 6e 63 61 20 4a 61 67 67 65 72 20 77 6f 72 65 20 74 6f 20 74 68 65 20 4d 65 74 20 47 61 6c 61 20 69 6e 20 31 39 38 31 2e 3c 2f 70 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 66 69 67 75 72 65 3e 3c 66 69 67 75 72 65 20 63 6c 61 73 73 3d 22 57 49 4e 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 43 56 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 43 43 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 51 52 5a 20 43 63 48 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 66 65 5f 22 3e 3c 68 32 20 63 6c 61 73 73 3d 22 69 74 57 20 7a 50 Data Ascii: Renta dress that was a replication of the Halston gown that Bianca Jagger wore to the Met Gala in 1981.</p>< /div></div></div></div></div></figure><figure class="WIN"><div class="cCV"><div class="sCC"><div class="QRZ CcH"><div class="fe_"><h2 class="itW zP

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:59 UTC	1284	IN	Data Raw: 65 72 2d 69 6e 73 70 69 72 65 64 20 67 6f 77 6e 20 66 72 6f 6d 20 4a 6f 6e 61 74 68 61 6e 20 53 69 6d 6b 68 61 69 20 66 6f 72 20 74 68 65 20 4d 65 74 20 47 61 6c 61 20 65 76 65 6e 69 6e 67 2e 22 5d 5d 5d 5d 7d 7d 2c 22 69 6d 61 67 65 22 3a 6e 75 6c 6c 2c 22 76 69 64 65 6f 22 3a 6e 75 6c 6c 2c 22 69 74 65 6d 22 3a 7b 22 69 64 22 3a 22 38 34 33 35 36 33 30 35 22 2c 22 63 61 72 64 22 3a 7b 22 69 64 22 3a 22 38 34 33 35 36 33 31 31 22 2c 22 74 79 70 65 22 3a 2 2 6d 65 64 69 61 22 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 74 72 65 61 74 6d 65 6e 74 22 3a 6e 75 6c 6c 2c 22 65 66 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 75 6e 62 6f 75 6e 64 65 64 Data Ascii: er-inspired gown from Jonathan Simkhai for the Met Gala evening.]]]]]],"image":null,"video":null,"item":{"id":"84356305","card":{"id":"84356311","type":"media","settings":{"treatment":null,"effect":null,"palette":null},"palette":null,"variant":"unbounded
2021-09-16 04:28:59 UTC	1300	IN	Data Raw: 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 75 6e 62 6f 75 6e 64 65 64 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 61 6c 74 22 3a 22 4e 45 57 20 59 4f 52 4b 2c 20 4e 45 57 20 59 4f 52 4b 20 2d 20 53 45 50 54 45 4d 42 45 52 20 31 33 3a 20 4c 6f 72 64 65 20 61 74 74 65 6e 64 73 20 54 68 65 20 32 30 32 31 20 4d 65 74 20 47 61 6c 61 20 43 65 6c 65 62 72 61 74 69 6e 67 20 49 6e 20 41 6d 65 72 69 63 61 3a 20 41 20 4c 65 78 69 63 6f 6e 20 4f 66 20 46 61 73 68 69 6f 6e 20 61 74 20 4d 65 74 72 6f 70 6f 6c 69 74 61 6e 20 4d 75 73 65 75 6d 20 6f 66 20 41 72 74 20 6f 6e 20 53 65 70 74 65 6d 62 65 72 20 31 33 2c 20 32 30 32 31 20 69 6e 20 4e 65 77 20 59 6f 72 6b 20 43 69 74 79 2e 20 28 50 68 6f 74 6f 20 62 79 20 54 68 65 6f 20 57 61 72 67 6f 2f 47 65 74 79 20 49 6d 61 67 65 73 29 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 54 68 65 6f 20 57 61 72 67 6f Data Ascii: ",null,"variant":"unbounded","fields":{"alt":"NEW YORK, NEW YORK - SEPTEMBER 13: Lorde attends The 2021 Met Gala Celebrating In America: A Lexicon Of Fashion at Metropolitan Museum of Art on September 13, 2021 in New York City. (Photo by Jeff Kravitz/Film
2021-09-16 04:28:59 UTC	1308	IN	Data Raw: 7b 22 61 6c 74 22 3a 22 4e 45 57 20 59 4f 52 4b 2c 20 4e 45 57 20 59 4f 52 4b 20 2d 20 53 45 50 54 45 4d 42 45 52 20 31 33 3a 20 4d 65 67 61 6e 20 46 6f 78 20 61 74 74 65 6e 64 73 20 54 68 65 20 32 30 32 31 20 4d 65 74 20 47 61 6c 61 20 43 65 6c 65 62 72 61 74 69 6e 67 20 49 6e 20 41 6d 65 72 69 63 61 3a 20 41 20 4c 65 78 69 63 6f 6e 20 4f 66 20 46 61 73 68 69 6f 6e 20 61 74 20 4d 65 74 72 6f 70 6f 6c 69 74 61 6e 20 4d 75 73 65 75 6d 20 6f 66 20 41 72 74 20 6f 6e 20 53 65 70 74 65 6d 62 65 72 20 31 33 2c 20 32 30 32 31 20 69 6e 20 4e 65 77 20 59 6f 72 6b 20 43 69 74 79 2e 20 28 50 68 6f 74 6f 20 62 79 20 54 68 65 6f 20 57 61 72 67 6f 2f 47 65 74 79 20 49 6d 61 67 65 73 29 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 54 68 65 6f 20 57 61 72 67 6f Data Ascii: {"alt":"NEW YORK, NEW YORK - SEPTEMBER 13: Megan Fox attends The 2021 Met Gala Celebrating In America: A Lexicon Of Fashion at Metropolitan Museum of Art on September 13, 2021 in New York City. (Photo by Theo Wargo/Getty Images)","attribution":"Theo Wargo
2021-09-16 04:28:59 UTC	1316	IN	Data Raw: 65 62 72 61 74 69 6e 67 20 49 6e 20 41 6d 65 72 69 63 61 3a 20 41 20 4c 65 78 69 63 6f 6e 20 4f 66 20 46 61 73 68 69 6f 6e 20 61 74 20 4d 65 74 72 6f 70 6f 6c 69 74 61 6e 20 4d 75 73 65 75 6d 20 6f 66 20 41 72 74 20 6f 6e 20 53 65 70 74 65 6d 62 65 72 20 31 33 2c 20 32 30 32 31 20 69 6e 20 4e 65 77 20 59 6f 72 6b 20 43 69 74 79 2e 20 28 50 68 6f 74 6f 20 62 79 20 54 68 65 6f 20 57 61 72 67 6f 2f 47 65 74 79 20 49 6d 61 67 65 73 29 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 54 68 65 6f 20 57 61 72 67 6f 2f 47 65 74 79 20 49 6d 61 67 65 73 20 45 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2f 47 65 74 79 20 49 6d 61 67 65 73 22 7d 2c 22 69 6d 61 67 65 22 3a 7b 22 69 64 22 3a 22 38 34 33 35 37 38 38 32 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f Data Ascii: ebrating In America: A Lexicon Of Fashion at Metropolitan Museum of Art on September 13, 2021 in New York City. (Photo by Theo Wargo/Getty Images)","attribution":"Theo Wargo/Getty Images Entertainment/Getty Images"},"image":{"id":"84357882","url":"https:/
2021-09-16 04:28:59 UTC	1332	IN	Data Raw: 6a 70 67 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 54 68 65 6f 20 57 61 72 67 6f 2f 47 65 74 74 79 20 49 6d 61 67 65 73 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 55 72 6c 22 3a 6e 75 6c 6c 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4e 45 57 20 59 4f 52 4b 2c 20 4e 45 57 20 59 4f 52 4b 20 2d 20 53 45 50 54 45 4d 42 45 52 20 31 33 3a 20 4b 69 6d 20 4b 61 72 64 61 73 68 69 61 6e 20 61 74 74 65 6e 64 73 20 54 68 65 20 32 30 32 31 20 4d 65 74 20 47 61 6c 61 20 43 65 6c 65 62 72 61 74 6 9 6e 67 20 49 6e 20 41 6d 65 72 69 63 61 3a 20 41 20 4c 65 78 69 63 6f 6e 20 4f 66 20 46 61 73 68 69 6f 6e 20 61 74 20 4 d 65 74 72 6f 70 6f 6c 69 74 61 6e 20 4d 75 73 65 75 6d 20 6f 66 Data Ascii: jpg","attribution":"Theo Wargo/Getty Images Entertainment/Getty Images","attributionUrl":null,"description":"NEW YORK, NEW YORK - SEPTEMBER 13: Kim Kardashian attends The 2021 Met Gala Celebrating In America: A Lexicon Of Fashion at Metropolitan Museum of
2021-09-16 04:28:59 UTC	1348	IN	Data Raw: 70 20 61 74 74 65 6e 64 73 20 54 68 65 20 32 30 32 31 20 4d 65 74 20 47 61 6c 61 20 43 65 6c 65 62 72 61 74 69 6e 67 20 49 6e 20 41 6d 65 72 69 63 61 3a 20 41 20 4c 65 78 69 63 6f 6e 20 4f 66 20 46 61 73 68 69 6f 6e 20 61 74 20 4d 65 74 72 6f 70 6f 6c 69 74 61 6e 20 4d 75 73 65 75 6d 20 6f 66 20 41 72 74 20 6f 6e 20 53 65 70 74 65 6d 62 65 72 20 31 33 2c 20 32 30 32 31 20 69 6e 20 4e 65 77 20 59 6f 72 6b 20 43 69 74 79 2e 20 28 50 68 6f 74 6f 20 62 79 20 4d 69 6b 65 20 43 6f 70 70 6f 6c 61 2f 47 65 74 79 20 49 6d 61 67 65 73 29 22 2c 22 77 69 64 74 68 22 3a 32 33 33 36 2c 22 68 65 69 67 68 74 22 3a 33 35 30 35 2c 22 66 6f 63 61 6c 70 6f 69 6e 74 22 3a 6e 75 6c 6c 7d 2c 22 76 69 64 65 6f 22 3a 6e 75 6c 6c 2c 22 6d 65 64 69 61 22 3a 7b 22 5f 5f 74 79 70 Data Ascii: p attends The 2021 Met Gala Celebrating In America: A Lexicon Of Fashion at Metropolitan Museum of Art on September 13, 2021 in New York City. (Photo by Mike Coppola/Getty Images)","width":2336,"height":3505,"focalpoin t":null},"video":null,"media":{"__typ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49772	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	582	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvIWw

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1106	IN	Data Raw: 38 03 43 03 4f 03 5a 03 66 03 72 03 7e 03 8a 03 96 03 a2 03 ae 03 ba 03 c7 03 d3 03 e0 03 ec 03 f9 04 06 04 13 04 20 04 2d 04 3b 04 48 04 55 04 63 04 71 04 7e 04 8c 04 9a 04 a8 04 b6 04 c4 04 d3 04 e1 04 f0 04 fe 05 0d 05 1c 05 2b 05 3a 05 49 05 58 05 67 05 77 05 86 05 96 05 a6 05 b5 05 c5 05 d5 05 e5 05 fe 06 06 06 16 06 27 06 37 06 48 06 59 06 6a 06 7b 06 8c 06 9d 06 af 06 c0 06 d1 06 e3 06 f5 07 07 19 07 2b 07 3d 07 47 07 61 07 74 07 86 07 99 07 ac 07 bf 07 d2 07 e5 07 f8 08 0b 08 1f 08 32 08 46 08 5a 08 6e 08 82 08 96 08 aa 08 be 08 d2 08 e7 08 fb 09 10 09 25 09 3a 09 4f 09 64 09 79 09 8f 09 a4 09 ba 09 cf 09 e5 09 fb 0a 11 0a 27 0a 3d 0a 54 0a 6a 0a 81 0a 98 0a ae 0a c5 0a dc 0a f3 0b 0b 0b 22 0b 39 0b 51 0b 69 0b 80 0b 98 0b b0 0b c8 0b e1 0b f9 Data Ascii: 8COZF~ -;:HUc~+;:lXgw7HYj{+=Oat2FZn%:Ody'=Tj"9Qi
2021-09-16 04:28:58 UTC	1107	IN	Data Raw: 94 8a 94 f4 95 f5 95 c9 96 34 96 9f 97 0a 97 75 97 e0 98 4c 98 b8 99 24 99 90 99 fc 9a 68 9a d5 9b 42 9b af 9c 1c 9c 89 9c f7 9d 64 9d d2 9e 40 9e ae 9f 1d 9f 8b 9f fa a0 69 a0 d8 a1 47 a1 b6 a2 26 a2 96 a3 06 a3 76 a3 e6 a4 56 a4 c7 a5 38 a5 a9 a6 1a a6 8b a6 fd a7 6e a7 e0 a8 52 a8 c4 a9 37 a9 a9 aa 1c aa 8f ab 02 ab 75 ab e9 ac 5c ac d0 ad 44 ad b8 ae 2d ae a1 af 16 af 8b b0 00 b0 75 b0 ea b1 60 b1 d6 b2 4b b2 c2 b3 38 b3 ae b4 25 b4 9c b5 13 b5 8a b6 01 b6 79 b6 f0 b7 68 b7 e0 b8 59 b8 d1 b9 4a b9 c2 ba 3b ba b5 bb 2e bb a7 bc 21 bc 9b bd 15 bd 8f be 0a be 84 be ff bf 7a bf f5 c0 70 c0 ec c1 67 c1 e3 c2 5f c2 db c3 58 c3 d4 c4 51 c4 ce c5 4b c5 c8 c6 46 c6 c3 c7 41 c7 bf c8 3d c8 bc c9 3a c9 b9 ca 38 ca b7 cb 36 cb b6 cc 35 cc b5 cd 35 cd b5 ce 36 ce Data Ascii: _4uL\$hbD@iG&vV8nR7uD-u:K8%yhYJ;.:lzp~_XQKFA=:86556
2021-09-16 04:28:58 UTC	1109	IN	Data Raw: 38 c8 17 5d 22 d8 1e 56 d5 56 34 5c d7 6b 89 2d 7c 54 df ac ea 93 c9 54 54 ca da a3 64 93 04 c8 a4 f5 57 b5 ff 00 04 1a 2d 64 d5 d5 cb 23 3b 1b b8 e3 a1 08 c0 75 46 27 94 a8 b5 24 8b bb c7 5e 3f 7b b5 3b ba 40 36 92 58 1b 09 eb 21 d1 e5 e6 2f a5 16 e9 11 73 de bf c4 b5 5a 46 36 6a a7 91 8c 59 50 1a 8a e3 d1 bb 36 da a1 d3 d1 e2 5a 88 9d 6e a6 ed f2 9e 97 89 00 df ce 87 27 7a 55 79 58 90 46 67 22 ef 67 95 5b 34 59 65 83 bf d1 2e 58 f3 87 f4 be d9 37 45 d5 06 b1 3b 8d b4 d2 b3 19 43 b9 df ca f8 2b 5b c6 05 4e f8 17 cf 7c 3b be d7 0b b4 ea ab 4b c1 a3 46 dd f6 4f 57 1a 73 3c 30 6e 87 ed 3c 5a a2 95 61 11 6b a1 74 26 f0 d3 cc a3 27 1c b6 7d b5 9a ad 45 21 1a 87 c2 6b d6 5d 41 da fe 16 d9 f0 8d d8 df 4f 2e 3a c3 f4 f2 2a c4 d4 55 3b 1e b4 6c dd a3 12 5e 67 ae Data Ascii: 8j"VV4k;-TTTTW-d#:uF\$^?;:@6X!/:sZF6yP6Zn'zUyXFg"q[4Y5%.Xs7E;C+[N];KFOws<0n<Zakt&~}E!k]AO.:*U;:l'g
2021-09-16 04:28:58 UTC	1110	IN	Data Raw: 77 b3 b2 9c b6 bb 64 fe 83 05 a8 bc c4 74 b3 56 52 0a e5 3f 70 5f 37 89 33 6e ef 7b fa f2 89 43 09 3f 61 ae 5c 46 6a 79 c9 2b 0a a0 a9 7d cb 1f 64 3b b6 47 56 a3 be de 70 88 5c 00 8b ad f5 fa 82 0f f2 eb 9b eb 2d 2a 77 55 e6 db 95 2e a8 a3 73 27 f8 cd 24 07 e5 ec af 3d 50 09 aa d5 4c 25 b5 b1 05 c6 56 43 6b ed 8e a1 f5 10 5e f4 7d 26 f0 b6 77 78 45 db 3f a6 39 0c f3 21 c3 6c b1 75 8a 06 e7 35 e1 bf 5b 8e 47 66 3b ac 8b 63 67 5a 83 e6 9e a5 5f 3b a1 e0 a1 5a 4d a3 fe e3 87 eb bb 73 75 b6 a5 fc b1 a7 30 d8 01 cd 83 e8 77 7a a8 2f 9c 20 27 2c 42 c0 f1 a7 6f 07 fb 1b 42 7a 40 09 79 17 ed ba 79 3a a5 a8 ed 11 a8 b6 a3 57 23 ae 04 ed a1 aa 46 ea dc 8e 7a 6b 93 2f db 23 57 ec bd ce 52 fd 8d 72 fe b6 c1 cb 3c 7a e9 61 f1 07 6e b7 2e 99 e7 2f e5 70 4f 02 9d 11 Data Ascii: wdtVR?p_73n{C?alFj+~}d;GVp!~*wU.s\$=PL%VCb~}&wxE?9!u5[Gf;cgZ;_ZMsu0wz/ ',BoBz@yy:W#Fzk/ #WRr<zan./pO
2021-09-16 04:28:58 UTC	1111	IN	Data Raw: 25 ae 03 dc 37 2c 16 0f b0 92 2c 88 6c c6 ee f1 97 38 1b 98 ce a1 6c 7e b1 8e f5 26 c9 db bd cf e5 7e c4 ad a6 3a ed 39 fb 37 b5 45 18 47 17 2d 03 0e 73 fb 90 bc 36 7a 9f d2 1f 45 c6 67 ef e4 d1 71 f8 68 22 48 05 fb d1 8c 2c 8a 94 a3 d1 1e e7 d4 0f a5 6e 1e e9 87 b0 f9 02 75 44 95 b5 96 86 71 12 c4 f1 b2 a3 55 44 9a 09 4a 46 2c 72 cd 9d c8 58 02 b4 6c 79 f1 79 9f 5b f8 a9 af 33 37 12 c4 e3 46 69 db 13 5c e8 46 37 3f 51 f9 eb 74 3b d3 f1 93 4f b0 cb 34 41 65 53 75 f8 30 56 fe f2 1b 87 f9 16 fb 24 9a ab e6 7f 91 f1 c0 e8 c2 05 71 f7 e5 0f 44 f2 b0 6b 96 b6 dd 68 3d 4e 93 7d 3b fc e2 d7 86 f5 ca c8 02 1b 60 b5 de 68 16 55 1e 37 10 b4 92 93 53 45 69 aa 45 e5 cc a9 2b 52 b1 89 2f 28 d8 6b 70 c4 7f ae 7a 9b cf 89 40 82 c3 ce 06 b1 6a 6d 58 ad e6 f1 1b 45 8d Data Ascii: %7,,l8l~&-:~97EG-s6zEgqh"H,nuDqUDJF,rXlyy[37FiF7?Qt;O4AeSu0V\$Qdkh=N);`hU7SEiE+R/(kpz@jmXE
2021-09-16 04:28:58 UTC	1113	IN	Data Raw: d2 47 9c ee e2 51 ea 34 9c f8 b2 8e 81 be f1 29 7c 39 84 82 41 3a 82 ca 69 97 3b db ca a6 73 27 46 5d 4b 4d 49 a4 0f b5 ee bd 32 fe 3a 51 c0 33 6d c7 49 ff 00 45 82 90 7f eb 7f 61 65 f7 0f e8 f8 9a ab 31 89 50 3b 14 d1 e4 90 a4 56 74 38 93 66 99 87 4a 4d 98 c6 f9 80 6b 8c 9e 62 ec 47 c8 7c 3c 8c 0f 2c f7 d3 e8 87 0e 76 f1 7a 2d 52 4d 76 12 23 15 93 42 6e 4a d2 5f 67 d2 40 e5 b2 29 5b 12 84 24 9c fb 30 ea 77 f9 75 e5 a7 cf 5c 00 23 95 04 12 26 b9 e5 63 76 73 aa d2 42 34 1b b9 d3 11 51 63 95 73 ed 96 fa 7d 95 36 64 fe 17 a5 1b c0 96 39 94 5d ca b9 da 09 e2 18 14 a9 b8 f5 52 0d f9 46 6e 8a 98 f9 7f d7 59 85 50 7a b5 fa 29 e8 92 3c 6b e7 4d 69 2a 1b 24 f4 18 85 d3 8b c1 1a ca 6b 79 9a b2 d3 46 f9 4e 73 cc dd b3 67 26 70 63 32 ae ca 34 ba aa 4a fe 9c b0 94 Data Ascii: GQ4)9A;i;s'F]KMI2:Q3mIEae1P;Vt8fJmKbG]<.;vz-RMv#BnJ_g@)j)\$0wu!&#cvsB4Qcs]6d9j)RFnYPZ)<kMI*\$Ax[kyCNsg&p24J
2021-09-16 04:28:58 UTC	1114	IN	Data Raw: d6 66 5d ea f1 9f 04 15 97 14 0b 39 ad 75 f5 ea 95 cb 63 eb c0 64 13 4a a0 49 b0 13 08 d0 d7 fd 5c ee 84 a6 40 ac 77 e7 f7 b7 44 3c 6e 98 e1 04 12 6c 39 ba 2c cb 4e a4 25 b2 5d 2d 44 db 63 8e 07 44 7e 38 ab 3e c9 f7 7c 1f ce 9d 51 57 36 31 0e 68 36 7e 31 70 ce 2e 3b 40 34 5a 5b 11 9c d3 33 a9 4c 06 6d 9c 3c fb 5f 64 72 cf 1e 46 23 c4 c9 3e 3c d0 b2 da db 08 9e 43 f2 43 da dc a4 ee a9 15 22 83 3a 91 04 7f d5 2e f7 3e 7e fc 3f 19 ba de eb 2c 10 19 17 76 05 c9 83 a5 08 a9 ea 8b e7 87 b5 cd 80 bb 86 89 7c 6a d6 9d 04 fa 57 8b f0 4f 50 eb f9 30 c0 4f da 3d 7e b8 19 cd a6 55 9c 72 c5 84 92 84 4a 24 90 b9 76 67 13 89 bd 98 14 c9 ed 72 89 cc 9c 9b c7 f1 8d 63 3b 13 51 a8 50 60 4d cb a0 61 93 14 e9 c4 4c e7 40 3e 8d a4 c6 31 17 44 5a 2f 5a b7 c5 b3 05 de be 7a e5 Data Ascii: fJ9ucdJl\@wD<nl9,N%]-DcD~8>]QW61h6~1p.;@4Z[3Lm<_drf#><CC";.>~?;vJjWOP00=~UrJ\$vgrc;QP'MaL @>1DZ/Zz
2021-09-16 04:28:58 UTC	1116	IN	Data Raw: 2a c0 b5 63 39 06 8a cc e0 69 29 cc 60 c4 69 6d 66 46 0f 8c c2 46 a8 76 6f d8 fe 2f f3 bf 8c 7e a3 d3 c1 69 ad f3 4d 1a 95 aa ae 98 e9 50 77 55 0b 2a 62 65 f4 17 d3 65 86 3a 1b 08 b4 a5 cf 6e 10 f9 6a dc 60 9d 14 fe fe 8a 36 14 3d bc b1 37 1c 50 16 97 da 22 06 74 71 34 35 1e 9b 11 26 fa f3 3b 8d 79 6e e9 b6 15 b6 9a 21 c6 02 c7 03 81 e8 fd 17 d7 a0 cc 03 75 56 d2 62 a8 c9 19 15 8e 8b 40 7c a3 53 a1 01 58 05 9d ce b3 63 7e 99 7c 41 93 b3 9a 43 a8 9d fc a3 67 ed fb cf ec eb bd 2f 62 df 21 0f 60 43 26 6d 7e 58 21 bd 12 cd f6 82 2e 62 18 c8 bc 68 8e 6c ee 41 3c a4 93 a6 dd a0 e6 13 d5 f4 ba 8a 47 93 35 8e 8a 4c d6 6e 9b 50 d9 e6 17 cd ec 75 97 ad 8c 06 d9 57 67 47 9f 73 d3 c2 93 40 8c bd d1 95 af 6e 08 7d dd aa e3 34 c6 0c da eb 0b db 09 c2 f2 fa f0 6c c7 1a d0 Data Ascii: *c9j)`imffFv0/-iMPwU*bee:nj`6=7P"tq45&;yn!uVb@ SXc~ ACg/b!C&m~X!.bhA<G5LnPuWgGs@n]4l
2021-09-16 04:28:58 UTC	1117	IN	Data Raw: 2a c6 95 25 c5 a6 6d 97 a0 60 eb bd ac ea b2 25 bb c4 63 91 56 57 a2 ae 27 36 b0 39 c6 8d 28 0e 23 6c 08 8a ae 8a 0d 5e 70 b6 4c 89 10 95 34 3a 0d 26 df cf fd 06 d9 3b ad bb e7 bb 44 6b 25 7a 4c 8f 3b 81 26 90 0a 5e e1 ab d2 69 17 94 bd 45 a4 81 a7 b3 42 65 23 d2 c7 7b fd 12 e6 44 c6 41 f3 2f 69 c9 f9 9e 99 6a 1f e8 86 5c e5 8f 54 e3 62 dc 1a 99 9c 44 9a ae 59 92 aa e8 ac ef b4 23 2b eb 72 d5 22 e2 48 f4 0d 53 d2 3d 5e 9b c9 9b 7b 2e da 9a e4 91 f2 5b 0a 09 15 98 bb 86 56 8d 4a 93 b9 0d e8 2c f2 f8 f7 da 9b 38 a6 80 2c 9d 58 44 f3 6a 6c b5 f3 55 d0 fc 43 6e 03 42 d1 8f a5 57 d9 8a 75 6e 77 24 d9 6d 29 54 82 3e 93 7c ef 31 cc 6b 76 81 69 07 07 0d 02 2b 10 b3 e3 6d b7 ca ef 38 c1 5c e8 1c eb 87 8a 4f 59 47 35 6e 57 2c d0 1e d1 38 b5 13 36 3a 73 e0 72 64 d3 Data Ascii: *%m"%cVW'69(#{^pL4:&;Dk%zL;~iEBE#{DA/ij}TbDY#~+r"HS=~^[.VJ,8,XD]UCnBWun\$M)T>]kivi+m8lO YG5nW,86:srd

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1118	IN	Data Raw: b0 35 6b 23 2a a6 ae b5 04 6d 1b 86 e1 d9 61 cd ab 35 19 e5 07 ca f3 f1 bb 1c c6 a0 b3 a7 d8 c5 0a 4f c3 b7 dd 8a b6 1f 6e 50 37 d5 8d 5c 2f f9 4b e3 ea 1c 87 d6 f4 3e 97 9e 24 3d 4c 89 2e 22 8d 22 95 24 37 35 65 9d d3 e7 7f 7d 61 71 62 7f 95 52 b7 57 9d 55 ef 59 a3 9a cd 59 36 db 9d 56 d2 33 0d 68 36 70 cb 78 31 8e 6d a8 6d 93 ad 0c 94 63 ae e2 83 91 4b 35 2c a0 d0 35 93 5b ab 34 4d 1a 61 4c 95 67 08 b7 b3 fd cd 7e 4f ab 8b 07 f9 d6 71 74 ad 85 c6 e7 85 4e c9 63 a5 9e 1d d7 36 db ad d9 4a bc 8d 9b 7d 2e 3d 96 9c da 9a a3 3c a1 f9 5e 7e 37 23 74 47 bb ff 00 d7 c9 a0 09 a8 93 ec 37 c8 0a b5 fc 72 8f b9 8a b4 a9 8f df 4f 1c cf d2 3e b3 e3 f7 5f bb 9b b8 60 45 d5 e1 91 af 2e c7 aa 87 57 56 2b 24 33 a9 b9 f4 57 32 6d c5 ac e3 af 2b 9c 6a e1 64 b3 e8 59 ed 9e Data Ascii: 5k#*ma5OnP7VK>\$.L.""\$75e]aqbRWUUY6V3h6px1mmcK5,5[4MaLg~OqtNc6J].=<^~7#G7rO>_`E.WV+\$3W2m+jdY
2021-09-16 04:28:58 UTC	1120	IN	Data Raw: b7 98 60 62 4a 20 e2 04 0b 5a 7a 44 21 41 41 68 25 62 a5 85 5c 6a 3a 30 35 7b 67 24 66 07 14 29 55 66 4d 46 cd a0 a5 a7 fa 62 90 a3 db 4e 19 55 eb 75 1e e2 0b 71 1c dc 8f 20 2a 1d 3d cd 5b 58 bb c9 69 a1 da 46 97 7a 25 bb a4 c8 d1 b0 34 4f 7d 0a d4 c7 05 4e 32 86 10 2a 36 ec 42 d7 51 45 09 05 6a dc 9a 2d 9e db 8a 9c c8 35 48 59 2e 2e 24 7a 55 0f 18 8d 81 db 41 24 7a 8a d6 22 eb 29 cd a8 91 53 51 94 bb f4 0d 7a 73 4f 03 0a 2b 4c 94 d8 dc af 32 3c 1c 45 a7 3b 2c 31 dd 5b c4 66 b5 bb f4 45 c4 96 12 8a e1 cb 56 54 a1 43 f1 f2 8b e2 de 6a 2a 97 cc 66 97 e9 fd f2 15 71 67 7d 3c f7 3a 7e 9f 6f 1d db 1f 5a 6c 2d 99 64 4d bc ad 41 13 5c bb 75 3f b4 71 65 ae ad d6 3b 2d 04 37 a0 8e 85 66 b3 59 a9 40 23 55 b0 49 2d 7f 1b 01 91 13 00 b7 3f 81 69 fe ab 4b 82 8d 1c c0 Data Ascii: `bJ ZzDIAAh%b\j:05(g\$F)UfMFbNUuq *=[XiFz%4O)N2*6BQEjJ-5HY..\$zUASz`)SQzsO+L2<E;.,1[fEVTc)`fqg] <:-oZl-dMAU?qe;-7fY@#UI-?iK
2021-09-16 04:28:58 UTC	1121	IN	Data Raw: b3 92 24 a0 5c 93 bc 8d 56 72 f3 69 71 f4 d7 00 57 ac 20 07 9d aa 32 fb 77 9c b7 54 d2 07 da 2d ce 04 29 52 23 a9 c0 e9 18 24 35 f7 e3 68 64 49 51 a2 a9 32 b4 25 19 9a 5c b5 ca 6e ae 94 31 0b b6 dd 3a 18 45 47 63 a6 5c a4 b6 82 15 93 f0 a5 ed c2 55 b6 b6 ea 2d f5 bb 57 8d 6e a1 63 a8 de ae 5a ed 16 07 d4 4e fd ee 69 19 d6 9a 04 90 49 b6 19 2c 2f 4d 43 2c 91 b5 8f 12 c8 b5 05 cc 33 a5 6b 47 fc 55 7a 56 f7 23 e6 a5 6a 99 bd ce f5 75 f9 ff 00 55 68 eb 97 92 44 9e ca e6 de e6 08 9d 1c 0a 56 a3 47 b9 89 06 c8 fe 54 d8 ab 86 f6 c7 a6 29 91 12 cc 9c 9a b4 9a 35 b8 9a 49 24 ad 23 52 6d 3e f2 5e 3a ba 35 a9 ea d7 7a 84 9c 90 50 61 8b 4b be 85 c4 1c 59 70 f5 3f 14 dc c5 57 77 cf 3c d6 b7 2c cd c8 51 f1 4b e7 86 ec d9 ae 6b 55 bc 54 1b 82 bc 93 f2 58 f7 37 4c Data Ascii: \$!VriqW 2wT-)R#\$5hdIQ2%ln1:EGcU-WncZNil,/MC,3kGUzV#juuHdVGT)y5!\$#Rm~^:5zPaKYp?Ww<,QKkUT X7L
2021-09-16 04:28:58 UTC	1122	IN	Data Raw: d0 35 6b 66 1a 1e 14 d3 c2 eb 15 ae 4e 61 d2 e6 b2 58 d6 33 93 f0 64 96 8b 56 7b dd 42 0c 71 62 94 e4 24 a5 0c 70 47 2c 2f 6c c6 a3 52 8a 43 8a c4 86 84 4e 68 46 f4 62 c5 68 70 03 2e af 0e db 8d 1d c1 17 b1 08 67 9a 74 45 b9 9f dc 1f 06 d6 5b 69 84 92 ec 6e b3 1a ea 62 b7 54 0b 2c 96 92 ea ca d5 2c fb eb 45 b1 b8 96 7b fd 17 d4 55 ce 89 75 05 3e 43 30 34 8e c8 cb ae 6a 29 08 79 e6 7b 5b d3 0a 5b 38 91 52 ee 4b 69 c6 a1 35 c9 bb 99 61 b6 ba d4 65 92 34 f0 d5 fd 47 85 19 7d 3e c9 46 b9 ad d8 4b 0e 9e 48 ad 2b 44 5b a6 3c 3b 6f 09 e3 08 d2 3b cc 7d 22 bf af 0e f1 09 b5 6f 4f 67 32 49 a5 d3 58 5c d2 69 b7 06 a2 d3 e1 15 c4 7a aa d8 db 79 30 b1 07 47 b6 7b e7 36 17 b0 54 97 96 c2 a5 9c 2c 51 ea 17 6a 6e 26 92 59 39 85 a0 8b 5a 4d b2 2d b8 eb d6 a3 73 29 a0 ca Data Ascii: 5kfNaX3dV[Bqb\$PqG,/IRCNhFbhp.gtE[inbT.,E{Uu>C04j)y{[[8RKi5ae4G)>FKH+D[<;o;]"oOg2lXizy0G{ 6T,Qjn&Y9ZM-s)
2021-09-16 04:28:58 UTC	1124	IN	Data Raw: 34 30 5a 34 33 dc 58 41 2a 1b 39 85 5a d9 97 79 f4 18 a4 ab 4b 73 0a 6b d6 eb 1c fc b3 c8 79 a1 cb 81 a2 db a6 6b 58 1a 8e b7 76 2e b5 44 4c 9d 03 58 8c 58 d0 5e c1 85 ae 95 7d a9 5e e9 3c 1f a6 d8 d1 62 d5 b6 b6 f2 ed 57 fa 46 9b 7f 52 70 5e 86 6b 88 f4 03 a6 4f a5 86 17 a7 b9 04 83 ff 00 b4 5e 0d 19 83 13 c0 56 80 df 1e 5b 69 52 b1 f4 62 80 a3 e0 f8 e2 5b d1 65 6c cc 59 aa d0 7d fb 8b 3c 45 0c eb 98 9c d4 6c 71 aa 68 6f 2d 67 97 04 a4 6d af f1 03 95 d2 e7 1d e3 94 b2 cd 20 e9 41 11 e9 fa 31 d3 90 ed 01 81 6f 55 04 4a d7 25 e5 6f 78 07 68 8c ef 0b 27 68 6e 3d b1 26 6e 4f 79 04 fb 67 36 e8 d3 dc ba a4 a2 40 e6 6d d0 23 1c 11 33 01 1b e6 a6 0b be d1 08 48 24 ee ad 48 73 4d 4d da ad e5 31 cb 79 0f aa b4 e2 08 24 ea 9f 0b e5 65 75 6b 2b d8 25 5e a0 4a 92 Data Ascii: 40Z43XA*9ZyKsykXv.DLXX^Y^<bWFRp*kO^V[iRb[elY]<Elqho-gm A1oUJ%oxh'hnn=&N0yg6@m# 3H\$HsMM1y\$euk+%^J
2021-09-16 04:28:58 UTC	1125	IN	Data Raw: 27 6d bf 75 32 b5 b0 bd 6e db 1a 6f 29 10 3d 19 d9 72 f9 a0 b2 6d 4c 6c 72 7a 64 6f 46 b5 56 59 63 d8 33 b0 5b ac 04 c2 8f be 38 a9 17 15 b6 8a 9a e1 e9 7e df 13 20 31 c9 32 28 47 f6 4a ad 45 d6 11 d5 87 11 4e 8c 8c ea f5 69 1e e1 7b 94 33 dc 48 48 ef 5e 92 6d 91 cf 24 6b 16 af 76 82 5d 52 ea 44 d1 ad 62 e8 49 69 21 a9 03 d4 9d 23 d2 d4 a6 96 f0 1e f1 b5 48 3b 21 fa 4d 11 58 a6 f1 c6 f8 f4 dc b8 3e cf af ad 8f ab 35 9a 39 e4 d4 39 b7 8e 26 2e 75 ce 46 53 d3 a3 43 f1 bf c7 97 09 4a 63 e2 1c 77 bc 8c 8d 42 69 03 98 b7 81 3b 7b 9d dd a1 58 cb 54 31 fb 2e 54 98 d6 2f 71 46 a5 8b dd 70 77 9e 8b 3b c9 6c 12 2d a0 4b 25 47 ee a9 72 89 6f 2f 78 9a 15 87 d1 f5 16 e3 4a bb b6 8d 06 e3 24 af 24 8d b4 c8 71 50 48 3a 67 15 2c 60 14 46 67 85 00 a5 14 ab 49 d2 05 da Data Ascii: `mu2No)=rmLlrzdoFVYc3[~ 12(GJENi(3HH^m\$kv)RDbli#-H;IMX>599&.uFSCJcwBi;XT1.T/qFpw;I-K% Gro/xJ\$\$qPH:g.`Fgl
2021-09-16 04:28:58 UTC	1126	IN	Data Raw: 17 4a e1 a9 4c 5a db f7 ae 27 99 62 d1 e4 90 bd 30 c4 66 76 d8 eb ba 3c 7b 6c 1f 65 48 00 2a dd a0 95 43 bb 2f a8 26 90 3b 38 4d d5 1b 60 2e 5d 4e 44 0b 1c 7d 09 db d9 1e 48 31 2c 69 71 53 93 d1 d0 ed 8a c1 21 7a 2e 05 3d ca d7 59 dd a2 da 4a 95 40 30 2b 74 b3 36 c3 1d 44 bb 8a c5 81 23 04 49 a4 dd 1c 4c 52 18 90 2d 4c 7e e4 63 df 39 6d eb 23 6d e9 60 d9 39 59 2e 65 67 30 11 bb 1f 73 2d b6 63 df 66 ea 77 88 ac a3 7a c4 76 bf c9 ba fb 84 d2 86 ae 05 9d 5b 4f 2a b5 d2 5a d8 82 89 5a 7c b0 83 b3 d0 34 bc cf 8e 39 c7 a5 e0 2b d7 5f e9 3c db e6 28 73 35 c7 51 ff 00 8d 06 4c 58 34 df 2c 0a 63 8a 67 ca ab 00 38 4f 4b f5 ba 9b 1c 9e 33 9e 41 6a a4 6c 8d 1a 4a 60 32 a2 3c 4d 84 ab 73 28 a9 58 67 71 df da 82 02 ee 40 68 57 b5 c2 98 8a 63 a4 af b1 52 4e a4 6f 8e Data Ascii: J LZ'b0fv<{leH*C/&;8M`.JND}H1,iqSlz.=YJ@0+t6D#ILR-L~c9m#m`9Y.eg0s-cfwzw[O^ZZJ49+~_(s5QLX 4,cg8OK3AjJ`2<Ms(Xgq@hWcRNo
2021-09-16 04:28:58 UTC	1128	IN	Data Raw: 22 86 de 46 a7 f8 70 91 ff 00 8f e4 28 72 8b ce ea cf fa f1 52 fe 38 24 f6 a1 46 ad 8b 5d 35 a3 15 14 22 b8 c6 21 ea 24 8a 32 91 26 f7 8f 05 a2 56 dc f0 1e ae 9f 6a b6 9a 79 ac 60 6a d7 02 4d 4f 3b aa 68 5b 72 2b ad 44 d8 65 24 cd 2f 98 9f ee 3c a5 a9 51 48 81 0a b5 e2 b3 20 75 7a b9 56 25 41 58 d0 93 22 90 6a 35 72 5c ed 36 3a d4 96 e2 2d 4a 09 6e 75 2d 43 d5 48 b0 8a 58 d6 82 57 b4 50 19 a1 2c 61 f7 82 55 59 ab 69 99 7a 11 ec d9 b2 2d a1 aa 40 72 a7 dd 7a db 62 63 d4 54 e9 ad 29 4e a3 af b5 6d d8 d4 90 22 88 23 6c 41 d0 0a 42 65 89 a5 2a 69 46 79 31 62 02 9d ed 26 5d 58 a8 55 02 b7 82 aa 57 1c 33 1e fd 67 34 03 52 ab 72 66 a9 73 8e 09 98 0b 8d b5 b7 e8 8f e7 fe d7 1b ab 4d f7 da f4 cd 0e a8 a0 d5 da 8d 71 93 91 72 e4 ec 80 90 2d 9a 05 91 a5 89 4f 0a 5b Data Ascii: "Fp(rR8\$F]5`\$2&Vjy`jMO;h[r+De\$<QH uzV%AX")j5r/6;-Jnu-CHXWP,aUYiz~@rzbcT)Nm"#ABE*iFy1b&]XUW3g4RrfsMqr-O[
2021-09-16 04:28:58 UTC	1129	IN	Data Raw: 17 23 25 54 d7 06 40 92 ea 6f 9d ff 00 bd 63 51 5b 1b 1d bb e8 ae 29 20 26 28 3b 1d d8 97 cb f5 00 79 26 c2 21 56 47 14 bd eb 77 74 1e d1 1f bd b7 75 21 8c 28 67 f6 46 42 cb 37 96 fc 88 ed b6 e6 37 8c 47 de 97 f1 c6 cc 56 4f 29 f1 fd 52 50 f9 49 da b7 15 47 f8 4f dd 23 f3 0f 81 f8 e4 f3 16 d2 97 91 2b 06 8c 74 d6 4c 04 05 dd 20 90 2c c7 15 93 94 dc cc e3 0c ea 95 29 2b 43 70 2c d8 55 f0 7e 0b 82 ac 5a bc 1f 14 ad df 81 e6 63 6e af 40 8e 4e 79 49 19 8e f3 4e 18 b0 fa 1b c5 b9 f7 7f ab 3c ef ef 7d 2d 9e 8b 7a d7 7a 66 6b 06 b6 d6 2b 5c ff 00 e4 6e 6c 82 6b 83 9e 43 ae b7 cb c5 71 8b bc b7 71 a6 56 4c 83 1b 75 17 6f 4d 9d 4e ed cd 96 5c 31 09 b5 06 69 d7 07 6e 44 6a 33 08 ef 28 19 b4 8f 73 1f 12 7f d7 fe f3 e3 76 e1 d4 20 8a 93 c2 d0 fc 70 fe 3d ac f2 0f 1f Data Ascii: #%T@ocQJ] (&{y&IVGwtu!(gFB77GVO)RPIGO#+tL ,)+Cp,U~Zcn@NyIN<-;zzfk+nlkCqqVLuoMN1inDj3(sv p=

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1130	IN	Data Raw: 79 70 d2 b3 39 8c 03 4e a3 25 69 d1 b1 0a e0 12 59 c9 f6 06 65 0d 0c 84 8b 6c b1 8c 83 16 2a 31 53 0c 4e 58 86 d0 a4 29 ae 2d 63 96 68 9e f6 f1 6c 93 1c ba 62 ba 42 ba 55 d2 ad 86 b0 d5 de bb d6 0d 74 f3 5e 9a 3a f4 d1 d0 b7 88 50 89 05 7b 69 9f 6d 3d ca c6 f0 dc c5 8e c6 a5 74 ea f2 cf 27 c6 2e 96 45 bb ed bb 81 a2 59 35 8a fd 71 95 b8 5d 4c f6 5f 24 fb 93 e2 95 bb 6e c2 a3 60 ca 43 33 b5 28 d8 2d 97 a8 54 76 b8 56 cc a0 e5 6b cd 0f 9b 21 79 07 e4 34 bb 3a b8 c0 1f 89 2a 4f 8b 8c 73 3f 21 26 22 8f c2 f2 e9 c8 4c 9f 98 86 ca 85 0b 2f e4 fd 8f 80 f8 6c 66 af 0c 32 2b 50 b6 e9 b6 37 13 6c 63 37 1d dc 06 c2 96 2b d5 31 51 dc 2b 75 07 c0 49 90 d3 60 82 cc 02 28 29 6a df 72 e3 dc 58 f6 b7 66 86 ed 0d 67 90 15 8a 1f 9b 3f 4e 2b 06 b0 6b 15 8a db 5b 6b 6d 60 72 Data Ascii: yp9N%Yel*1SNX)-chlBbU!t*P[im=t*.EY5qjLX\$`n`C3(-TvVkl4:*Os?!!&L/lf2+P7lc7+1Q+ul`)jrXfg?N+q[km`r
2021-09-16 04:28:58 UTC	1132	IN	Data Raw: 0e 3c 63 6d b4 42 92 b4 2a 55 d6 aa 46 19 06 b9 42 67 4f 65 ff 00 28 79 57 a2 ff 00 85 bf 03 89 c0 a9 fb bc 38 dd 4c ae 25 66 6e 87 13 1a c2 6d 49 92 ed 7a ab b6 0a 00 6c b3 aa ef 18 2e 35 c0 1a c6 1a 2f d4 ab 6c 16 9c 2d 8d fd 95 36 72 f6 2d e8 83 a2 54 65 c0 97 28 84 51 41 bd 13 07 2f 65 bb e0 87 f6 5e 8b 7a df 81 c4 e0 7e ed 99 e7 fb ac ad 6b ba a9 11 2d 12 24 ab 34 66 2a e0 39 08 f2 17 41 57 9f 45 95 b7 e1 80 9e 28 cb 6e 5b 1a 99 d8 18 5d 1e 09 ad 09 d4 5e e9 81 22 76 1d d7 1b ab 1f 65 4d a4 d8 b8 62 76 f3 6f 59 1c a6 31 98 44 22 55 26 fe 60 9b d3 18 77 89 e4 79 47 ee 89 c9 0e 8d 0e 8a 1a 72 b3 80 28 91 21 d1 ac a1 4f b4 79 4e 8e e1 8f e2 43 cc bd 31 f4 47 13 81 fb a1 13 12 bc 62 5f a4 73 4e 2f 39 ea fc 99 d1 48 68 27 9a ca ed 06 ec 35 bf 15 32 83 0b Data Ascii: <cmB*UFBgOe(YW8L%fnmzl5/l-6r-Te(QA/e^z-k-\$4f*9AWE(nj)*~veMbYoY1D*U&`yWGr(!OyNC1Gb_sN/9Hh'52
2021-09-16 04:28:58 UTC	1133	IN	Data Raw: 2a c2 17 a2 d2 94 62 af d5 66 ae f9 f5 51 51 b0 ef aa a8 3f 39 c0 bc 0b 0d e8 ec 77 ad 80 c9 d4 a7 38 d6 1c 93 98 77 18 d8 2e 7f 9e 9b ed 19 45 ba 92 99 49 ba 34 22 e2 8c 9b ec e6 a4 e2 1c 14 77 85 65 77 99 17 1d 55 c2 b3 57 88 29 01 59 5f 09 4d 91 99 ce dc 14 b2 44 6a 0a cc 8b c8 57 a7 ba 77 e9 85 82 9c 32 86 92 79 2b a6 39 95 40 0c 66 40 1d 6f 36 f5 2f 6d a6 27 8e 0c 1f 97 6e 56 ab c2 6c bc 4a db 72 38 ec 94 55 b5 c2 c8 5c 58 fd 55 ae 18 d3 09 16 44 08 13 c1 58 61 99 aa 58 f2 39 e6 d1 06 c9 a8 3d f8 bf aa 95 50 61 12 75 c2 58 d5 95 e2 0e 0e 67 b9 50 fc f0 ac 39 ce c5 36 f0 6a 65 3a 3e 62 56 ad 5a b5 1a 6f f3 0f 63 53 b4 3b 47 78 5a a5 64 e0 8e c6 88 a8 41 cc 75 d0 cd b5 18 59 52 a9 fe 63 1d 99 a7 82 ef 88 74 9c d6 16 d5 35 a8 39 b4 b2 c6 82 67 ea 83 ea Data Ascii: *-bfQQ?9w8w.El4"wewUW)Y_MDjWw2y+9@f@o6/m'nVlJR8UxUDXaX9=PaulXgP9j6;>bVZocS;GxZdAuYRct59g
2021-09-16 04:28:58 UTC	1134	IN	Data Raw: 02 7f 08 de 55 1a 6d d1 b4 40 db 0b ba ad 7a 47 ff 00 af 3f f8 41 cd 88 37 05 a5 78 2a 7a 38 2d df 15 77 34 2f 14 bb e8 bb aa 70 2a 38 68 3f 08 52 89 4f 65 37 33 33 5b 9a 0d a7 a2 97 d2 74 72 bf d1 44 dd 17 04 48 a8 56 67 99 3b 45 e0 78 9c a1 b6 ea bb b2 8b cf a0 41 c6 f1 78 4e 5d f3 78 dc 2a 2d a5 73 90 17 9e 67 63 2f 04 20 5b ba 74 e0 05 7c ae b9 fe 10 c3 06 7f b6 de a8 e2 d6 e6 f0 95 6d 15 ce d4 46 12 d5 99 e5 06 8c 78 0e 5a a9 8d 57 95 68 14 d4 73 ba 0b 2e eb 2f d9 e5 cb 97 92 ab 40 fe 07 47 a6 ec 18 07 0c 32 11 60 bc 38 dd b2 14 ab a2 1a bc 72 a5 72 da a2 de 35 02 ec e7 8d 17 22 08 55 bb af 26 74 d2 c6 b7 ca 2e aa 56 8b 37 ec d9 fb a3 c9 83 6a 06 39 1f e2 a6 4e 9d 77 84 da 94 dd 2d 3b f1 75 43 77 6e 1c 4a 75 47 99 24 e1 ea a9 f3 6b c7 cb 08 af 41 8f Data Ascii: Um@zG?A7x*z8-w/p*8h?ROe733[trDHVg;ExAxNj)*-sgc/ [t]mFxZWhs./@G2`8rr5"U&t.V7j9Nw;-uCwnJuG\$K&A
2021-09-16 04:28:58 UTC	1136	IN	Data Raw: ee 75 4b 05 df 76 a0 da 95 bf 08 d5 ad ff 00 9f 69 53 b6 37 fc c6 86 3b 75 c6 fc 29 97 34 67 6b 21 ce f7 b0 25 76 6a 5e ed 26 cf 53 7f 6a f7 ef a4 f6 b8 7d 31 1d 53 8f e5 52 9a f7 82 32 6a 11 7d 83 5a 34 09 d5 5e 7a 0e 03 61 99 4d bb b7 e6 e8 9f 25 c0 48 d3 f7 59 81 45 66 01 09 50 ac 2e a4 e0 0a 8c 01 29 90 80 5d 14 e8 9d 95 4a a8 f5 d6 34 5e 13 be e3 48 e8 87 4c 45 d0 5a 61 7b b4 ec e4 45 bc 53 b8 ce 10 98 70 82 a4 61 97 6f 45 76 94 2a 3c c7 24 47 7e 47 4b 2f 0d 49 50 75 5d 98 3b de 91 ed 5b 1e f9 fa 6c 50 a3 ef 54 13 d3 7f b6 ed 83 fd a9 f8 5f 63 36 15 6a 1a 90 c0 04 8e 2b 2b 64 52 1a 0d 9f f1 35 1b f6 b5 b4 9d cd ff 00 94 ca 40 91 9d c6 79 c6 10 88 1a 29 53 2a 53 b3 2b 63 2e 0a c3 c2 9a ed ca 79 2f 55 33 08 84 4a 2f 8b 1b 23 ae 69 b2 cc db c5 b6 bc bf Data Ascii: uKviS7;u)4gk!%vj^&Sj}1SR2j}Z4*zaM%HYEfP.))D4*HLEZa[ESpaoEv*~\$G-GK/!Pu;[!PT_c6j++dR5@y)S*S+c;y/U3J/#i
2021-09-16 04:28:58 UTC	1137	IN	Data Raw: e2 15 5b 1f 1d 92 3d 87 67 ea ed d8 56 ed 07 4a 6c ca 3a bb da 0d aa b4 f8 54 77 d5 02 00 cd cb 61 bd 31 63 78 b8 05 4e 83 34 60 84 f7 9f c2 d9 b2 73 c9 bb 9c 4f c5 4a 9d cb 33 54 ac ca c7 0e 89 cd 10 c8 b2 ef 43 36 f5 91 66 e0 b3 71 4d 20 21 95 5d 02 4a a5 06 ed b1 1c 93 8b 1c e6 07 0c ae cb 69 1c 14 37 4d 7e 0a 32 95 2f f8 28 16 1b 50 15 f1 94 48 3d 56 b8 e8 a1 65 52 50 ca 11 72 95 09 b0 2e a0 e3 e5 5e 0a 69 d5 6a b2 1a 30 a6 7f 0d 3f b4 77 a6 9b 23 d8 76 7e ae c2 94 8f 15 4f b4 3e ba 7b 41 b5 da 39 bf 37 c5 3e 9b a2 37 20 78 a8 5e 20 9a d4 41 00 10 86 51 ba eb b3 78 67 ed 06 15 7b b9 9b 69 c2 70 01 65 c0 27 01 e5 c0 c2 95 00 e1 cd 35 48 45 05 dd ad 50 43 a2 39 5c 21 0d 17 74 d1 ba 7a 2e 7c 76 6c a6 44 2e 29 e5 da 8c c3 63 2a 27 72 ca d5 08 85 75 9d fa Data Ascii: [=gVJl:TwalcxN4`sOJ3TC6fqM !Ji7M~-2/(PH=VerPr.^ij0?w#v~O>[A97>7 x^ AQxg[ipe5HEPC9!tz.(jD.)c*`ru
2021-09-16 04:28:58 UTC	1138	IN	Data Raw: 13 62 80 95 aa 32 70 cc 55 e3 97 34 d1 a1 08 1d 25 12 6d 09 d8 15 d9 af ab 8f d3 68 a7 b7 dd ac ef 9e d1 f6 ce e8 50 da a6 e8 f3 53 8f 81 40 b5 dd 51 f1 18 84 42 81 a2 f0 b7 cc 15 0a 2b 5a 81 53 38 42 8e 38 07 2b 71 5e b2 a0 a8 e0 30 ca 54 23 09 87 82 ba 0d 42 11 94 57 42 88 98 e2 16 46 10 f1 ee 92 6d d1 3a a7 6a 6f 81 9e 4a 42 f9 8f 3e 8b 25 30 45 30 bf 12 fe 1f c5 6e 0a ca d7 42 5d 69 fc 37 5b cf c9 70 4e cd 16 11 e1 11 a2 a6 63 7a 80 7f 12 ea d4 1d 0a 78 dd 67 f4 c1 a1 11 2a 14 ca b9 44 c5 91 15 25 78 46 06 54 28 40 73 57 40 0f c2 9c 66 e5 75 46 c8 2e ce 7d dc ce f8 0d a3 d1 76 aa 33 ac 3f f6 da 3e d8 b7 88 84 d2 78 6d 51 68 1a 53 2e f9 ad 37 a3 98 1d 17 8e 61 1c ba 05 49 d5 34 a6 0b c0 e9 84 aa f5 38 33 eb 6c 04 21 28 80 af 84 ec 6a b2 ea 15 94 a8 Data Ascii: b2pU4%mhPS@QBl#O(To)0T#BWBfM:joJB=%0E0nBj7[pNcxg*D%xFT(=@sW@fuF.jv3?>xmQhS.7al483l!(j
2021-09-16 04:28:58 UTC	1140	IN	Data Raw: 64 14 e2 41 c7 9e 10 9b 4c 40 be a7 f7 44 20 d5 d2 49 e8 bc 60 96 8d c2 c8 7a af e9 4d 55 35 9c e8 f4 08 7e a4 50 d9 2d 07 c2 75 08 af 44 c4 e0 82 9e 48 f3 0a 53 87 aa 93 a1 ba e4 8a 2b ea 81 53 38 42 8e 38 07 2b 71 5e b2 a0 a8 27 44 ee 5b 1d aa 9e fc cd 77 ed b2 51 6f e7 21 76 71 37 6b 32 1f 4f 6d a8 52 01 2b 40 d5 79 77 5d 8a cc 1f 89 ad 7f ed b3 54 7f b6 ef a6 04 2e d2 37 9a 63 eb 8f 68 ee cc de fd 57 31 80 8c 63 09 d8 0a cb c7 3c e1 1c 02 1d 53 bd 13 7d 54 9d d1 3e 2b 91 c9 37 ba 15 35 fc 45 3f f5 04 e4 3d 51 c0 e2 51 45 7a 2c d2 2c 7e a8 ff 00 dd 50 41 37 ae 03 e0 8f 23 f5 5e 2c 01 de a1 42 20 a3 b1 7d c3 0b 22 31 94 d9 5d a3 f9 43 eb b5 da 5b 58 f8 18 f7 3b 2f bd e2 fa 26 86 34 34 37 40 2d 18 68 b4 38 ea a0 5f 1d 7e 4b 52 b5 72 d0 ad 16 bb 4d 3f 84 Data Ascii: dAL@D l`zMU5~P-uDHS+S8B8+q^D[lwQo!vq7k2OmR+@yw]T.7chW1c<S)T>+75E?=QQEz.,~PA7#^,Bj`1]C[X;/&447~-h8_-KRm?
2021-09-16 04:28:58 UTC	1141	IN	Data Raw: 4d 36 4e 5e 27 16 d8 ee 99 28 af 44 36 3a 85 77 5e 2c 23 54 fb 0b b7 f6 43 e4 83 46 a5 d8 14 51 f4 2b e7 83 9b 94 ce e3 28 28 45 a7 42 b2 29 5c b1 b2 37 be a1 66 9b ab e0 42 70 3a 6e 56 e1 85 95 31 ee 3d ed f9 cf dd 35 d9 77 44 eb c7 44 4f 1d aa 7d a3 fd 56 5f f5 35 02 17 68 a9 c2 90 11 d4 e1 4f b3 cf 93 c4 7a 95 6f 64 0f 21 8b b5 f1 36 11 ca 09 81 36 c3 55 1c f0 cd bb 36 5c 07 e9 5e 89 a8 f5 c0 af 18 89 00 8e 87 65 a8 7a a0 9c 2e 0e 87 a1 47 a4 a1 d5 34 a0 a3 a8 43 e0 87 45 29 c3 d5 75 c3 f3 0d 17 77 51 a5 ae 80 63 aa 84 70 24 05 e8 70 77 5c 0f 4c 0f 45 ea 8a ab fc f3 f4 1f 7a 3e 9f 5d 86 e3 d9 ff 00 9a ef a6 1d ab f9 6d fa af ea 5d af f9 88 ed 9c 0a 6f e9 18 fa aa 9f c8 a9 f4 5e 98 0c 4f 52 87 45 fd 29 bd 17 a9 c5 9f a1 bb 05 7a af 52 87 aa 7f ea 08 fe Data Ascii: M6N^"(D6:w^.#TCFQ+((EB)\7fBp:nV1=5wDDO}V_5hOzod!66U6!^ez.G4CE)uwQcp\$pwULeZ>[m]o^ORE)zR
2021-09-16 04:28:58 UTC	1142	IN	Data Raw: 07 10 83 79 fd cb 39 6e 02 56 b1 11 f8 3c b1 93 92 09 05 09 b0 ca 8c 67 73 1b 97 82 58 89 f8 37 0c 89 81 bf 39 ef 07 4d 2e ca 3f ed 1b 56 f9 21 18 9e c7 31 dc bf 49 84 f8 66 26 52 b1 d2 db 8a 20 b5 01 71 1f 00 7e f1 4b 04 87 48 5c ea c6 2a 51 2c 22 7a 6f cb 14 d6 36 e3 36 86 a0 e3 f3 3e 63 2c 37 2e 3e 1d 17 ad 99 5d 18 12 b4 71 2f 81 18 ae 5a 82 30 0c 25 f6 f6 8b ae d0 57 92 ce 61 70 00 a9 e0 39 62 d0 46 1a 35 a5 f9 66 26 60 60 d0 2d cd 82 2d ed dc 78 cd 1a 9b 98 1c 34 3d 8e 23 e9 5d 5e 2a ab c3 d6 e0 c1 96 fb 11 ab 12 53 63 08 56 35 5f 70 94 46 75 34 90 89 9c 21 fe e6 01 17 e3 13 2d 6f a3 8a b6 4b 2d 3f 73 15 d2 d2 1a 8f 9f 02 3d 2c 5a 85 b2 52 cf 2e d2 9e c5 51 ed 96 43 2b 71 c0 fa db c9 e0 c4 e5 46 a6 75 52 dd 84 4c db 03 be e3 6d dc b2 c6 e5 bb 5e a5 Data Ascii: y9nV<gsX79M.?V!l!f&R q-KH!Q,"zo66>c,7.>]q/Z0%Wap9bF5f&``-x4=#j**ScV5_pFu4l-oK-?s=,ZR.QC+qFuRLm^

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1144	IN	Data Raw: 5e e0 78 08 72 6b 8f 11 e6 99 b1 55 e0 39 30 55 dc 24 38 55 72 af 10 a5 fe 10 de bf 6e fd 8f 73 89 a7 79 5e 82 ec ae 0a 99 c7 4f ed c6 1b 20 74 82 a1 af 9f 3f ac 45 3c b7 36 e9 16 71 7d 46 66 08 c9 1e 3a 3d 4c e1 99 67 c2 4c 3e 14 8a 92 e6 34 69 3e d9 77 7e d4 55 69 e3 33 26 e5 43 20 cc b4 e9 6e 4a 33 c6 60 5d 3d 91 0c 99 65 15 a1 e6 06 f2 ed 2e a1 1d 92 62 ba 73 7f f7 37 e2 ed 84 06 9b 96 b7 28 e8 cd 4b 2c 5a a2 14 d2 8c 15 51 cc 4a 03 6c e2 a3 e2 6a aa 04 cf a5 49 dd 96 47 f8 f6 f6 0e 62 c1 76 2f 30 d0 60 8b 1d 45 84 b9 ae e0 96 67 7f 36 0c 8b 88 49 77 d3 7d 3d 86 2a 15 7a cf dc ec d2 7c 09 50 e5 8f 1c af b9 9c 59 5e a1 bc ca 80 52 76 0c 83 81 16 a6 6f 12 e1 c4 7c f0 26 fd ae a5 c3 0a 8e f1 0f 8e 60 93 24 2c 1b 3b 16 e0 98 68 a6 2c 23 d4 2e 13 25 c1 99 Data Ascii: ^xrkU90U\$8Urnsy^O t?E<6q]Ff:=LgL>4i>w~Ui3&C nJ3"]=e.bs7(K,TQJlJGbvO' Egl6W]=*z[PY^Rvo[&\$,h,%,#
2021-09-16 04:28:58 UTC	1145	IN	Data Raw: 07 13 11 6e 12 39 4a 86 ee 25 85 72 8d 6c 97 82 f1 3b dd 0c 0c 4f 40 ec c0 7e 8f ed 3d a8 33 08 f1 38 6c 41 43 31 79 58 12 c6 fe 31 18 93 a0 dc 2a fd c0 95 0d 2f d4 be f1 51 0c 76 2f e6 08 f1 2b 21 20 90 dd ba 99 18 6b db 17 1a ab c5 83 f0 25 44 c7 88 68 34 b3 44 b7 13 40 d8 33 e4 cf 31 38 a2 fe 12 ba 9b ff 00 cb 8b 12 94 4d 70 c6 b0 a8 ee 2e 71 39 47 14 33 37 55 7c c1 8b e0 36 21 5a 9f a2 12 39 5f 50 44 c6 6f 2e 5f 98 ed 29 49 ea 73 d6 d3 b1 c1 1e f5 03 e5 72 c3 17 30 f1 2a 95 88 8a 14 f4 b8 63 94 0b 67 39 cc 46 0d 84 1d 6e 65 46 53 51 96 61 98 3a 02 e5 c0 02 e5 49 e4 9b 63 96 cc 4a 38 bb b2 8c af 83 f5 07 25 b2 fa 20 22 7c 5f 02 18 2e 4b 40 ad 29 e2 2d c5 c6 60 f2 70 9f 55 0b be dc 39 a6 7b ab 92 39 05 b9 f9 96 5b a4 5b 5c ff 00 b8 34 a5 5f fb cc 7d b5 Data Ascii: n9J%r!;O@~==38lAC1yX1*/Qv/+! k% Dh4D@318Mp.q9G37Uj6Iz9_PDo..]sr0*c9FneFSQa:lc8% "[_K@)-`pU9{9[[_4_]`
2021-09-16 04:28:58 UTC	1146	IN	Data Raw: 10 f5 a1 04 22 f3 2f a3 a8 b0 cb fa a5 ba 5e af 2a db eb de 28 92 1c 18 47 92 b1 2a ca 7c 8f c9 2c 60 7e 8f f3 10 28 bd df ea 53 dd 7b 6a 05 b6 0d 83 ca 1e 65 a8 fd cb 63 59 09 4b 26 b1 82 e9 f8 4b ea 7f 22 bf b4 53 31 db 51 de cd 62 05 ad ab 13 27 b8 f5 a6 5c e7 a0 b0 42 57 a0 8c 38 04 2e 29 46 5a 9b c8 8d 7f 34 6a 10 ed 6a 10 e3 11 ed 63 69 2c 9a d1 1d 89 9d df a6 14 63 0c c5 2f 00 c1 e9 2a 99 0b e0 d6 e6 f9 87 50 8d 6c 36 bf 94 c5 bc c4 64 5c 5c 21 0a c2 65 1d e3 95 a3 67 10 ab cc a4 b3 10 71 de 2a 54 06 41 ce 09 6b 0c 32 83 58 2e 66 32 e6 c2 12 a7 15 52 e3 f1 51 af c4 8e 96 b1 f7 cc 2b 37 83 19 f1 0b 80 ce a5 20 5b 32 fc 12 cd 5c 95 80 16 17 bb 99 84 fc 11 42 a3 c7 6f 98 3a 91 f8 57 2a 66 05 50 f7 d9 7c 90 52 77 61 83 58 4b 3c 54 23 c0 73 2e 40 18 18 Data Ascii: "/^*(G*],~(SjiecYK&K"S1Qb\BW8,)FZ4jjci,c/*Pl6d\legq*TAk2X.f2RQ+7 [2lBo:*W*fP RwaXK<T#s.@
2021-09-16 04:28:58 UTC	1148	IN	Data Raw: 73 17 1f 45 f4 31 32 89 a8 cb 6b 06 e6 24 95 d9 16 e1 98 c1 f1 de 64 0c 8b ca 77 9c 26 73 d6 d2 e2 cb a8 9f d5 30 09 72 29 05 ed 9c b2 f2 0e e0 62 54 41 a0 1d 90 e1 cc 0d 53 ae 4e 3d cb b7 0d a4 d7 7c 10 6a 83 34 33 f8 e5 ed 95 c6 86 82 0a 69 11 20 c3 a8 0a 84 80 7c 90 37 d8 23 fb b9 c4 93 3d 87 6a a5 24 78 ea ef 2c a9 bb 6e 1a 40 9a 49 8a 1b 4f cc 3e 2f b4 aa 60 ec 60 8e 73 8b ed ff 00 44 58 c4 4c c2 fd 1a ca 89 2a 12 24 fc d8 83 49 b7 c5 bd bb 88 05 ab 6f 4b 33 b7 1e c7 e6 64 94 75 6c 47 65 39 4c fd 5c ce 65 ae 04 a8 2d 90 ab 06 9f 12 e0 6f 73 c7 32 83 86 98 51 b4 cb 2c 6a a4 b0 5c 65 3b 58 0a 3c 4d 15 b6 66 18 b9 7c 34 1c 45 73 97 bb 43 5d 12 1f 69 50 ca ab 75 2d db ee 81 ac 50 25 d0 5e 29 40 5a 5c ce d4 12 be 31 58 8d 89 85 d7 cc 5b 4e 26 38 e2 Data Ascii: sE12k\$dW&s0r)bTASN=]j43i [7#-=j\$X,n@lO>/^`sDXL*\$loK3dulGe9L\le-os2Q,j!e;<X<Mfj4EsCj!iP-Pu~^`) @Zl1X[N&8
2021-09-16 04:28:58 UTC	1149	IN	Data Raw: f1 37 05 fe 66 a9 c4 5a 01 2c f2 ef 53 be 3a 97 ed 97 32 e3 d8 94 51 4d 72 ea 02 ee 30 f7 f1 52 ad 9c cb 2e 95 11 24 21 15 3c 36 e1 4d a0 85 5b 8e 50 b4 ad 37 2d ef 15 89 a1 ba 20 6c de 0a 14 0b ed ce 6a 19 ad cd ae 1f 0f e6 39 f6 82 16 dc c2 32 9c 29 bc 1d e5 13 f1 fb 8b 76 8a 19 ee 95 58 a1 d4 bb 12 8f 58 81 f7 17 15 77 b2 5c b4 ad 39 25 da 11 07 48 6f 12 56 77 89 83 ac 9f 3c c6 6b be 25 a5 da 6c 7b c7 5e 55 e6 38 fb c8 ab 94 d4 47 10 2a 05 57 3b 96 2b 06 ba 74 aa e5 54 1a da e4 ca 61 b1 76 12 d8 33 fc 25 7a a6 64 99 87 8a a6 60 5c 1c 04 41 8f 68 29 e5 f5 15 84 95 d0 5d 91 ff 00 0c 91 3a 3c e7 6f f7 bf e3 a5 c1 1b ef 05 50 1c fa a0 d4 0f f1 61 d6 c8 98 3d 6a 3d ba ef ba f4 e6 50 78 3b 94 c7 88 aa de af e6 12 d9 e6 5f 40 26 5a b6 2b 23 ea 2d b5 ed 1c a1 Data Ascii: 7fZ,S:2QM0R\$.!<6M[P7- lj92)vXXw9%HoVw<k%[(^U8G*W;+tTav3%zd\Ahj]]:@&Z+#+-
2021-09-16 04:28:58 UTC	1150	IN	Data Raw: 4b 7a c2 d6 4e e4 8b 03 6e dc 4a 09 74 5c 58 f7 e6 5a 8b 61 ba 9d f1 ad 65 43 bb 50 d5 9b 8c 3d a2 ca 60 83 2d 22 f0 da 31 12 ca 3e 25 65 77 9b 9a 66 60 1b 72 6a 54 c6 33 ac 1f cc 40 11 f5 2a 58 72 bf 68 0d c7 00 aa 3b bc 20 d5 47 a2 42 3a ff 00 20 0b 69 30 e3 ba ff 00 33 b7 3c 74 a8 5f d0 ff 00 07 ff 00 07 a3 d0 d0 3d ca 20 bc 60 56 54 8d 67 5b e9 4d 3d 42 f9 04 63 d0 44 ee 25 4b da 38 b8 17 b1 d7 77 6a 5d a5 51 e7 bf dc 17 94 67 4b 71 da 66 1d 6d f9 42 83 7c ca d6 42 0f 33 30 2b c4 00 59 2f 30 4b 89 35 00 10 84 6a ee 92 c6 30 8e 20 ba 9c 16 1b 94 83 2a 70 a6 e3 80 31 c2 3a b5 1c 22 29 57 30 01 92 c0 54 87 69 ce 03 89 97 72 a6 ce 18 7c 79 ef 1b 17 41 66 ed 56 c9 6e c1 53 8e 78 57 9c ea 21 ad 1d 8e 63 03 a7 86 ff 00 e4 a7 a7 8a 50 83 c4 ee c1 45 26 d2 Data Ascii: KzNnJt\XZaeCP=-:"1">%ewf`rjT3@*Xrh; GB: i03<t_ = `VTg[M=BcD%K8w]]QgKqfmBjB30+Y/0K5J0 *p1:"jW0TirjyAfVnSxW\cPE&
2021-09-16 04:28:58 UTC	1152	IN	Data Raw: 48 47 c2 c0 fd 44 2c 72 65 7f 83 69 bd a7 33 08 c2 02 00 b6 34 3d 43 6e 90 08 68 75 32 70 98 1b 32 9a 54 fa 87 18 09 c8 9e d1 54 42 66 bc cc 90 c2 f6 9e a9 07 32 ba 03 b0 43 d3 c8 ed 11 2b 19 2e f0 ac c4 47 e2 25 b6 0c 1e ea 0b 86 55 17 d0 3d 2b e9 08 5f 41 c4 73 24 d2 0c d6 27 6e 0d f1 09 8a 2f a8 51 d4 3a 31 7d 58 c6 29 cd e1 81 8e 97 a0 a2 77 f1 9f 41 fa 88 54 3b d7 78 b5 52 90 1e 51 bc f6 82 82 fc d4 c3 a3 02 e2 5d 14 a4 f4 b9 94 00 0e 02 14 02 e2 62 13 09 d9 6b 44 b3 58 0a e7 32 66 25 65 66 a2 77 94 51 0a 21 16 a2 a2 48 9d 0b d3 38 3c e2 2c 36 60 49 66 a6 a0 41 d9 17 f8 85 dd cc 56 e5 f1 1b 18 41 7c cd a9 40 ec fe 49 54 ad c0 0f 91 fe 25 01 e1 11 4e 7e be d0 12 b5 7d c5 b5 c7 69 b6 5d f3 27 3e af 43 32 e2 ee 4c 4c b0 b3 f1 7b 9b d4 ab f8 13 2c 99 Data Ascii: HGD,rei34=Cnhu2p2TTBf2C+,.G%U=+_As\$`n/Q:1j)X)wAT;xRQj]bkDX2f%efwQ!IH8<,6`IfAVA[@IT%N~j)]>C2LL{,jW0TirjyAfVnSxW\cPE&
2021-09-16 04:28:58 UTC	1153	IN	Data Raw: 0e d9 cb 3e 40 92 e6 09 e6 06 b2 7c 51 ed 9f 3a 89 ff 00 80 97 2e 52 fe 43 d7 98 a4 0f 25 20 06 72 6b 1c 4b e1 2e 1d 1d 8d 77 c4 70 8e 3b 7b f7 85 d6 00 2c 34 ff 00 e2 4b b4 e3 9b cc cb 0c 6f c5 e6 05 b8 13 f8 b1 b1 ad 32 8f 43 2b 87 6c c5 55 66 17 13 35 81 98 99 b6 56 de d9 79 15 68 99 ac 17 1a ad d8 1a 9d d9 84 ed a8 ea b9 09 59 aa a3 2b 9b 52 e4 f8 41 21 31 57 72 01 7b 11 ff 00 65 27 05 5c cf 35 cd fc cf 67 0f 92 5d 8a e3 a4 aa 20 84 69 bc a7 02 c0 f8 6d 11 51 80 cc a8 31 7d 1d 2f fc 9f f0 21 29 f7 0f b1 50 bb b5 07 d9 86 57 a8 e2 29 9c 41 8d 21 c1 44 33 9c d3 f8 8a 74 bb 8f 33 92 c0 12 21 a8 a3 9e cc 30 22 56 57 31 92 c5 ee 1c 08 c4 60 bf 15 4f 35 e1 5d e0 26 5a 84 46 15 36 a1 16 a3 71 51 4d c1 98 85 48 bd 2a 32 8a e6 6b b7 51 26 a2 a1 96 40 16 00 Data Ascii: >@ Q:.R.C% rKk.wp;{,4Ko2C+Uf5VyhY+RA!1Wr[e\5g] imQ1j)!PW)A!D3t3l0"VW1" O5jZF6qQMH*2kQ&@
2021-09-16 04:28:58 UTC	1154	IN	Data Raw: da db 2f 4c 54 2b 29 f5 05 ae c0 73 2b 5c c6 d2 e6 4c cc b5 59 83 f9 44 2a 5d 9d cd 4a c7 10 bd 17 9c f7 05 b8 6d a6 37 0d 28 30 f6 16 6a 2a de 12 aa 07 77 08 25 b3 08 32 62 d3 d5 bd 29 7c 07 4a fe e3 6a c2 ad 5a c5 5f 67 31 33 ca 83 4f 4a 98 69 bf 71 3d fd 59 53 82 7b e5 2a b8 55 14 70 7c 18 af 6f cc 7b a7 d3 19 17 ff 00 10 47 fd 82 22 e4 f7 70 79 00 f5 32 8a a8 1e 2f dc c4 cc 1f 2c 7b 13 22 be d6 04 04 98 ba 14 f2 32 3e e5 c0 32 23 e9 94 4e 22 a8 04 dd e8 65 37 60 d8 7e 61 53 5d c3 2b 3d f2 44 28 a8 02 3c ce 67 62 5d 69 35 c3 e9 19 02 35 1e 08 02 c8 4e ad 29 bb a8 30 61 75 fc ab 1d a3 b5 6a ec e0 ad cd c7 79 bb 4b 57 a2 50 64 bd a6 be 22 95 9c 65 3d b2 ee 45 f2 5f a9 8b fa ca e2 d5 a1 bf 27 ea e8 c5 e0 0a 73 57 b6 67 58 53 7c 4f d0 99 08 ed 97 Data Ascii: }6&o8jV[wJ>3_4j8@^rY6T*yq^ma!,Doj`]Ct8igs6U_];rh6K"57;]6iC@7zLe/0e[]\8A-QJc9U672vHzSq"1L/c(5(4
2021-09-16 04:28:58 UTC	1156	IN	Data Raw: ad db 2f 4c 54 2b 29 f5 05 ae c0 73 2b 5c c6 d2 e6 4c cc b5 59 83 f9 44 2a 5d 9d cd 4a c7 10 bd 17 9c f7 05 b8 6d a6 37 0d 28 30 f6 16 6a 2a de 12 aa 07 77 08 25 b3 08 32 62 d3 d5 bd 29 7c 07 4a fe e3 6a c2 ad 5a c5 5f 67 31 33 ca 83 4f 4a 98 69 bf 71 3d fd 59 53 82 7b e5 2a b8 55 14 70 7c 18 af 6f cc 7b a7 d3 19 17 ff 00 10 47 fd 82 22 e4 f7 70 79 00 f5 32 8a a8 1e 2f dc c4 cc 1f 2c 7b 13 22 be d6 04 04 98 ba 14 f2 32 3e e5 c0 32 23 e9 94 4e 22 a8 04 dd e8 65 37 60 d8 7e 61 53 5d c3 2b 3d f2 44 28 a8 02 3c ce 67 62 5d 69 35 c3 e9 19 02 35 1e 08 02 c8 4e ad 29 bb a8 30 61 75 fc ab 1d a3 b5 6a ec e0 ad cd c7 79 bb 4b 57 a2 50 64 bd a6 be 22 95 9c 65 3d b2 ee 45 f2 5f a9 8b fa ca e2 d5 a1 bf 27 ea e8 c5 e0 0a 73 57 b6 67 58 53 7c 4f d0 99 08 ed 97 Data Ascii: /LT+)+s+LYD+Jm7(0j*w%02b))DjZ_g13OJlq=YS(*UplO[G"py2/,{["2>2#N"e7~aS]+=D(<gbj)55J)0ujyKW Pd"e=E_sWgXSjO

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1157	IN	Data Raw: c1 2c 44 0b d2 51 ba 58 61 42 b3 7c 33 1b 3a 96 ed b7 29 10 95 dd 46 d5 ad 6a e5 90 b6 8c 38 24 0d dc d9 0f 86 67 04 ad 4e 24 fd 3c 04 23 2c 18 99 81 79 fd 21 dd 12 04 b9 89 ed d2 10 4b 76 96 ed 3d 21 d4 f0 76 97 ed 10 d1 1d ee 80 08 0b 4f 40 2e fd f8 b9 9a 29 39 ad 3f 7b 99 52 be 58 0a 4c df ea 5e 06 51 95 10 83 48 25 5c 79 9b cc f1 00 50 87 97 73 2f 91 35 ae ee 39 56 a2 47 eb 13 15 47 b9 82 20 3e 0b de 1c 40 09 78 25 9c 25 8f 92 82 89 5c e6 50 80 b9 4a 07 2a a2 68 10 7d bc bd 28 45 ba 57 04 03 a7 81 1e 05 eb 98 2c 0b 3e 96 51 9d 42 d8 91 cb 93 9b 63 94 22 15 f0 89 5d 16 99 77 ae 80 d9 f9 25 59 49 80 5d 0b 78 87 28 d1 5a 52 ce 31 00 7e 0f c4 03 70 d0 45 f8 47 70 a4 05 88 f1 67 04 ab f0 cc b9 a7 cc 74 38 75 fb 97 b1 ea 0b 6f 64 58 f6 07 f8 98 b3 bd 9f 73 Data Ascii: ,DQXaBj3:)Fj8\$gN\$<#,y!Kv=lvO@.)9?{RXL^QH%lyPs/59VGG>@%x%lPJ*h){EW,>QBC"}w%Yl)x(ZR1~pEGp gt8uodXs
2021-09-16 04:28:58 UTC	1158	IN	Data Raw: 92 39 d1 35 43 71 e4 f7 36 7d 4a 05 d9 83 f1 26 95 ed 5f 4f fd 81 ec 55 27 c1 08 be a8 b9 31 7c 15 f5 15 27 89 b1 ff 00 d2 5c 5b ca 97 28 8a 03 b3 7e b9 9c 6a c7 da 10 f1 80 64 66 8f 4d ff 00 a4 a9 14 85 d8 59 a8 8b c0 88 04 c4 a2 d2 cb a4 ae f3 5f f5 c4 dd ff 00 0a 73 9f b9 f9 4f f1 21 51 a9 cf 43 d0 db a0 e0 6a 29 65 06 2f ba c3 52 f0 a8 31 a3 af 98 ed ea 7e 2f ee 9a fd bd 6f c2 e8 74 f4 17 57 d7 43 9f d9 3f 39 d2 d7 ee 6c 74 f0 9a 26 ee 83 77 a9 fb 13 fb 0e dd Od b3 47 41 5a 91 b3 e2 7e 67 4b 97 40 1f 91 1d 7d 3a c6 72 f5 36 fb 9f df f6 9a bd cd 9e e7 7f 71 dc 68 f6 9a e5 fd ef 53 fb ae f3 fb 7d 4d 3e b3 f1 3 73 6f 4f e2 1f df d4 fe 8f b9 fd f7 69 cf db f5 3f af e2 6b ec f4 7f b4 fe ff 00 84 dd ea 68 74 0f d9 3f ff c4 00 3a 11 00 01 03 02 04 04 04 03 07 04 02 Data Ascii: 95Cq6)J&_OU'1'\[(-jdfMY_sOIQCgz3~--otWC?9lt&wGAZ~gK@):r6qh3)M>soOI?kht?:
2021-09-16 04:28:58 UTC	1160	IN	Data Raw: 32 ba ac a5 bd c2 f1 1b 99 c0 5c 80 8c e6 26 15 3a 2e 2a 95 18 3a 22 16 cb 38 1f e9 39 e1 8f 00 ea 53 65 d7 52 62 16 58 07 d4 22 21 16 95 fa 23 7e 6d a6 1e 9f 49 d4 e0 6a 13 69 3d fa 59 3d 81 ae 81 cc 81 09 f8 30 7c a5 3b 0f 55 9b 2a 78 7a ae d9 53 a2 29 fb aa d4 dc 5b 21 1a 75 22 e0 a7 e1 2a 62 29 65 06 2f ba c3 52 f0 a8 31 a3 af 98 ed ea 7e 2f ee d6 54 c9 2d 12 a4 2c ad 7b 4f a2 6b 40 10 ab 12 05 95 37 66 6c aa 51 05 6c 83 84 2a 8e a6 19 d4 75 4f 08 38 66 88 4c ac fd 18 6f ba 35 2a 46 ab 33 bb 94 ca 8c 6d 76 97 13 0b ed 14 c6 23 33 66 13 18 2a 3e d6 09 ac Od 16 4e 78 02 e8 7f f4 4d 92 13 58 d6 e8 9f 56 6a 4c 2a 75 b6 3c 83 5a 9e c7 4c 27 b5 ed 16 54 a8 c0 97 6b ce 90 e8 3e e1 62 Od 80 42 0b 42 ab f9 8e e7 b7 2b 39 79 7d f9 c4 a1 4d a3 40 a1 42 2a 0b 9e b3 Data Ascii: 2l&.:*:"89SeRbX"l#~-mlji=Y=0j;U*xzSj)[lu"*b)e/R1(UT_-{Ok@7fllQ!uO8fLo5*F3mv#3f~>NxMXVlj_u<ZLTk>bBB+9y)M@B*
2021-09-16 04:28:58 UTC	1161	IN	Data Raw: f1 47 ee a9 38 8e fb 7e eb 07 f0 89 91 e3 d6 00 9b c3 6f fc ac 3f 05 c2 e1 ae da 54 de 46 ee 26 57 1c e1 18 9a 0f 75 70 26 9b 9d b6 de eb 45 57 a8 20 00 b0 d1 06 4a 77 9a 49 f6 4d 07 36 a9 ef 4c 66 77 ca 71 8d 53 4c b0 a2 01 b2 a5 95 8e 6c 23 97 b2 be c1 54 17 09 a6 0a 1f 83 fa b9 e2 db 25 01 70 ac a0 2a 6d 86 ac 51 9a 87 d1 31 dd 4b 43 25 41 71 94 22 53 b4 40 3b 54 75 47 cf 1e ab 82 51 f1 b8 b5 06 c4 8f 14 12 3d ae b8 fc ff 00 e3 9d fd c1 63 7c a3 dd 53 6b 88 b2 e1 5c 5b 11 81 ad 95 c4 9a 67 51 fe d6 1b 19 4e a4 65 20 93 eb b2 dc 1d d5 66 32 a1 2c 74 65 2c ba e2 f8 73 84 c5 d5 a2 7f 49 b7 b1 d1 03 99 96 54 b3 04 f7 38 26 b7 54 04 19 4e f2 a0 5c 1c aa 12 74 4c 16 2b 27 55 8a 6c 8f 8d 4d d1 13 29 cc e9 51 64 d3 f8 3b a1 cb 19 e5 09 83 ab 5d 15 49 d7 64 cd Data Ascii: G8~o?TF&Wup&EW JwIM6LfwwSLl#T%*mQ1KC%Aq"S@;TuGQ=cjSk[gQNe f2,te,siT8&TNlL+UIM)Qd;]ld
2021-09-16 04:28:58 UTC	1162	IN	Data Raw: b8 07 7f aa f1 61 d3 dd cb 12 db d3 8f ea 0b 10 f9 0d fe ef f0 53 69 7d e6 6c ce f6 9b 2a 36 ae ef aa aa 7e e1 9f 44 1c 3c 47 0f 42 a8 fe 5a d0 05 98 8f d9 66 3e 21 f7 47 43 ef cb e2 0c 2f 8f c3 6b 32 2e 5b 6f 7d f7 f2 bc c6 ea 9e 97 4e 79 54 fb b9 3e 33 59 03 d4 7b 26 f9 48 47 64 5a a8 c0 6c 73 a6 d6 81 6e ea 4a 9e 4e 12 85 36 a8 68 52 14 f3 71 e7 7c c5 53 f2 ac 54 f8 7f 54 d6 b6 10 1e aa 64 d9 1b 5c a1 aa f8 73 87 37 1b 8f cb 50 4d 36 75 1f 5f 45 89 7c 55 22 c2 22 13 ff 00 42 27 ef 3e ab 14 01 0c fe e5 4e e0 7b 21 6a 2f ff 00 f4 aa 30 3d 94 da 74 50 45 57 fb 15 90 1a 59 48 d8 27 6a 81 ea 0a e5 c4 fa 04 d9 ca 27 58 e5 59 b9 98 42 e2 b8 73 87 e2 35 a9 01 a3 cc 7b 1b 85 94 e5 94 1b 65 b4 04 41 26 53 1a 0b e4 94 43 22 c5 4e 52 9e e9 2d 3e 8a 81 e9 e6 09 0b Data Ascii: aSij)*6~D<GBZf>IGC/k2.[o]GnYT>3Y{&HGdZlsnJN6hRqjSTTdls7PM6u_EUj""B">N{ij/0=IPEWYH"}XYBs 5[eA&SC""NR->
2021-09-16 04:28:58 UTC	1164	IN	Data Raw: ca e9 09 18 fa da eb 5b b4 76 30 f0 69 5e c3 96 9e 19 46 1a a4 4a 24 61 0a 55 1b 4b 93 c5 a6 cf 16 16 e4 95 6b c7 64 25 2d 4a e6 cd 5c 7a 9f 29 91 49 98 88 ad 23 45 17 49 46 5a 9e e5 59 c1 a4 96 48 79 2e 4e d9 c7 92 34 de 93 c2 76 2a 2b 48 70 65 08 4a 4a c5 1a 4e 17 b8 ef a7 6d 99 0b af 55 99 6f 72 16 73 f4 ba 57 5e 4f d9 2d ba 16 54 64 a1 24 df 63 fd e3 ff 00 61 4a a2 9c 14 bd fa 31 15 7c 3a 2e 5d fb 0e 5b dd 8a a5 e0 8d b9 24 d3 83 b9 86 ab 5a 2e fb b8 92 9c 5c 8f 2f b0 94 6d c1 aa 7a 36 43 f1 5d bd ca 6a ab 8f 98 9b ac ed a3 61 5e de 6b 5c d2 a4 ec cc 55 1d 11 4f 2e e2 11 62 c5 90 85 35 96 1a 9a bc 64 5a e7 11 31 90 57 72 f9 23 26 8a 55 a3 1d 32 ef 72 56 7b ae e5 85 11 ee 6e 4e 9b 99 5e da 88 bb 31 f3 9a 1c b2 c2 62 63 18 a8 3e 8f a8 d5 bd 45 0e cb ff Data Ascii: [v0i^FJ\$aUKkd%-Jz)l#EIFZYHy.N4v*+HpeJJNmUorsW^O-Td\$caJ1:].[J\$.Vmz6Cj)a^kIUO.b5dZ1Wr#&U2rv[nN^1bc>E
2021-09-16 04:28:58 UTC	1165	IN	Data Raw: b9 16 9c ac 71 c0 db 16 e8 97 d9 43 e3 3e e6 a6 5d e5 1e 09 72 37 b0 86 77 3b 16 dc 7c e6 9d e6 91 42 82 ab 3d 2f 8e e4 61 08 2b 25 64 55 c4 d0 a7 ea 92 2a fd 53 fc 11 bf e4 a9 8b ab 3e 64 d7 e0 fa 7d 6a 6d 69 be e4 9a 2b 4b 5d 4b 93 56 17 19 76 ca d9 b2 3c 9b 9b 7b 91 1f da ed 9b e7 a1 70 3e 46 2b 74 6f 7d 8b 16 27 e9 65 f1 5f 80 f5 49 fc 15 1c 78 31 18 58 55 85 e1 6b a2 71 68 64 24 e3 ba f7 2a 62 75 50 8d b9 92 dc ce 37 73 b0 fd 39 5b 3b 0e c4 3d 48 65 ac 26 5c 7f 6f 62 5d 2c 7d 1b 24 2d 84 f2 ab 2d ec 50 a1 52 da da b2 30 90 d1 07 26 62 31 12 a9 51 be c5 2c 4c e9 ca e8 af 88 95 57 77 64 77 2e 52 a9 b8 8f ef 25 93 cb b6 71 e4 97 22 e5 0e f9 ae 32 68 7d 0e d9 a3 93 49 21 e4 96 52 e7 a6 f9 27 61 b3 cd 27 c6 e6 1a 8c d5 2f e5 7f 3f 84 62 71 b2 9b d2 bd 25 Data Ascii: qC>]r7w; B=/a+%dU*S>d]jmi+KjKVv<[p>F+toj'eQlx1XUkqhd%*buP7s9j;=He&lobj.}\$\$--PR0&b1Q.LWwdw .R%q"2h)!!R'a'/?bq%
2021-09-16 04:28:58 UTC	1166	IN	Data Raw: 83 60 3e 4d c2 b0 07 5a 67 16 3d 43 bb f1 0e ff 00 8f f2 1a 6b ea 13 a6 6e 81 e5 01 61 9e 0e e1 9c e5 ad df f7 8c f8 01 cd 66 b5 3c c0 2f c7 f0 a0 c1 48 39 94 26 3e e2 9f 28 31 ef 94 14 22 69 0a d6 9f 30 63 58 c7 88 52 b0 cd 78 95 2a Od 6b 99 76 c9 34 c4 7e 89 69 36 55 f1 97 29 6e 8f e8 a9 50 62 62 0a f9 cb 5d 02 bd 19 62 ba c3 8c e2 16 cc ab e1 19 c7 ef a8 c3 13 ec b2 b6 71 6a 90 ee fc 7d 46 a0 37 f5 3f 6e 20 84 8f bf a8 52 37 6e 00 b5 fa cb 74 ed c4 b4 9a 74 20 ad 7d e0 ad fb f7 2a 2c 39 cb 2c 6f 12 95 37 9a 33 48 ae 19 22 a8 ce 14 c8 9c eb 51 82 11 04 bb 86 d4 b9 08 81 50 4b 1a ab ac c2 ec e0 43 c1 2c ac 5a 86 06 d9 75 78 5b ec c3 b1 49 d2 48 6c f8 Od cb 23 21 Od 16 f1 7b f4 97 0e 4a 14 41 7b 5e 91 3e e5 f4 1c 59 6e 51 e9 cb 99 96 55 06 40 04 bb cd 3a Data Ascii: `>MZg=Cknaf</H9&>(1^iOcXRx*kv4-i6U)nPbb]bqj)F7?n R7ntt`*,9o73H"QPKC,Zux[Hl#;{JA{^>YnQU@:
2021-09-16 04:28:58 UTC	1168	IN	Data Raw: 18 71 9c c4 21 41 93 00 40 26 e4 0d b4 1e 73 2f 84 2a cc 7d 6c 83 39 c3 7a 71 d5 6d 81 0b 06 f9 fc 4b 0b 7a 36 0f fb 17 ad 80 8e 7e 4f ea 3f c6 5b 13 9c 88 60 75 c4 36 15 68 ec 3b ff 00 66 a0 02 9d 39 5d d7 18 88 fa 4c 62 ef b2 51 81 b3 45 e7 b3 cc 54 5b 04 2e f7 05 19 b9 79 8e 1d 68 30 7b 19 2c 87 89 97 46 0f fd c6 90 d4 89 17 72 f6 9e 65 cd 4b 4c ee 67 88 71 12 39 43 99 01 84 c9 0b c4 49 c3 06 84 0e 47 4c ab 9b 48 74 10 af fe c7 63 27 32 a9 a5 b0 b2 da 8b f8 26 42 15 5f 89 82 aa 00 af 8c b1 82 4c 08 b5 96 a0 d9 7b 95 6d dc 54 b1 b5 47 42 2b cf 50 9b 2d 04 91 2a 1b 5c b3 3b ab 13 75 cf e9 96 0b 38 a8 38 dc b0 32 d5 44 b6 8b 68 26 0c ce 22 c9 57 01 4d 6c b9 4d f9 3a 2f 69 ce b1 c1 6f 11 7a c8 b4 87 d3 fd 44 73 81 68 55 2c 16 8a e6 2d e2 34 a0 b0 6a 0c 28 Data Ascii: qlA@&s*)9zqmKz6~O?['u6h;f9]LbQET[,yhQf,FrEklgq9CIGLHtc'2&B_L[mTGB+P-^;u882Dh&"WMIM4i ozshU,-4j(

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:58 UTC	1169	IN	Data Raw: a9 ca 15 3e a5 75 42 cb 25 c4 ab b2 1b d7 3f 67 e2 25 86 2d 82 61 b2 58 e0 00 e6 bb 54 6a c5 fb 88 34 00 e6 bb f1 19 85 b3 8a 8a c7 42 cb 3c 1b 31 58 02 ed 74 79 2c 20 00 14 6c 0f 30 03 b4 e3 3b 82 a2 c5 c0 c4 4d aa 00 ef 88 07 45 c6 61 5a 15 f5 59 88 18 d8 de 2a 63 c9 b4 38 50 bb 50 cf 4d 3a 3c 4b 91 2a 70 08 90 5b aa e6 85 7a 47 e5 60 ed b9 8a 15 f5 82 1c 2b ae eb 51 94 33 c1 fb 60 b2 99 35 19 67 9f 55 31 03 b2 5e cf 68 d9 73 4a 44 46 dd aa ca c2 61 83 b6 1d 7f 4e 1a 74 17 a4 5a ba 98 ae de 0a a9 29 ca 66 1b 42 79 5a 9a 6a 94 bf 49 65 97 99 2a 9e 47 d4 b5 3f a8 6a 22 4a 0e 30 22 1a fd a3 e5 4f cc 7e 2f 71 4f 72 08 73 f4 97 2c 8e 3a 8d 8d 77 c1 2e 91 70 77 09 1f db 2e cc 78 26 6a 67 1c d9 f3 36 16 18 5e e5 eb f8 38 67 43 1d f7 73 1f 12 d5 65 59 38 cd d9 Data Ascii: >uB%?g%-aXTj4B<1Xty, l0;MEaZY*c8PPM:<K*p[zG`+Q3'5gU1^hsJDFaNtZ)fByZjle*G*?]J0"O~/qOrs,;w .pw.x&jg6^8gCseY8
2021-09-16 04:28:58 UTC	1188	IN	Data Raw: a0 57 58 2b 81 e2 f9 66 8a c2 25 a5 51 65 71 ea 56 24 d4 5a 7f 77 ea 05 25 d6 82 c7 1b d1 30 c6 c1 59 3e aa c2 58 91 90 bc c2 ab 54 d4 ba 05 22 8a 0a d3 f4 cb 94 0b 07 03 87 92 05 95 db ab 73 f1 2b 98 00 91 38 25 a9 e2 1e 11 1c 9f ec 0a 21 8f 92 50 80 61 83 98 82 9f 89 69 15 26 1c 66 21 31 b6 2e 61 c4 84 30 5c ad a8 af 9a 79 87 b7 0d 31 05 4d 17 01 b8 1c a0 51 d2 64 5a aa c0 e9 2e 6a c1 1c a3 6b 78 f5 29 b0 5f 90 9d cb a7 47 a0 ad b1 c8 c8 0b ab a6 5d 7a a5 97 ee 13 04 cf f8 94 3c 0c 5b a7 e9 86 9b ea 09 05 9d 04 11 aa 80 9a 94 05 db fb d0 54 87 87 00 09 43 0c 46 a6 54 ec 80 d4 04 20 b1 b1 8c 15 99 78 df ff 00 c4 ac 65 91 a4 62 2e 62 fc ca a9 94 6b fd 91 0b b2 51 29 0d 78 31 88 2c 11 7b 4c 9c 75 0c 25 4c 59 66 a7 9a 8a 89 35 0a 43 16 f3 2c da 8b 28 3e 2b Data Ascii: WX+f%QeqV\$MZW%0Y>XT"s+8%lPai&f1.a0ly1MQdZ.jkx)_G]>[TCFT xeb.bkQ)x1,{Lu%LYf5C,(+>
2021-09-16 04:28:58 UTC	1204	IN	Data Raw: a6 0d b1 e4 26 90 86 e0 e1 2c 15 1d 16 e2 f5 1a 86 ea 51 b5 b0 cb 00 e4 e4 8a de f3 78 26 a1 60 b6 5c 65 25 5c a0 05 fc cd 93 31 e0 61 d3 32 d9 14 6c b8 80 2b 44 79 7c c5 98 8e d7 16 47 8b 25 d9 79 21 b6 0c 1e 8b 9d c9 19 ea 84 14 4c 91 64 64 ec e2 09 b6 bb 0f f3 2d 72 f4 b6 30 13 64 d3 bb b9 0a 1c 7d 93 be 3d 46 eb 43 89 ad 34 d8 b2 be cf a4 88 0d 2e d7 e2 51 49 83 a5 80 24 ec 35 b8 12 14 f2 ab 7a 25 00 54 73 9b 18 8b 82 a5 8f eb 74 a8 7b c4 b8 f5 12 d8 6e a1 b8 86 c5 06 77 0c 08 11 cf 6c 4a 0a 7c 9e d0 1d 16 d6 d9 8c 0b 5b 9b 0a 39 a6 01 33 c4 84 36 82 0f 98 9d 33 fa 8f 51 58 d2 c4 7d 5c ae 52 9d a2 0f d4 62 07 58 65 6e ec 26 1e 9d b9 95 03 3a 85 f4 34 ef 18 30 0b cb 8c 4c b6 80 f9 74 23 bf 88 10 29 7c 43 47 4a 65 23 99 70 51 4f ae 9c 23 43 e6 36 28 a1 Data Ascii: &,Qx&`le%l1a2l+Dy[G%y!Ldd-r0d]=FC4.Ql\$5z%Tst{nwJl[9363QX)]RbXen&:40L#})CGJe#pQO#C6(

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
151	192.168.2.3	49941	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:02 UTC	1364	OUT	GET /entertainment/justin-bieber-net-worth-hailey-baldwin-earnings-money HTTP/1.1 Accept: text/html,application/xhtml+xml,image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:29:02 UTC	1364	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 67320 Connection: close Date: Thu, 16 Sep 2021 04:29:02 GMT Cache-Control: max-age=3600 content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Apigw-Requestid: FvQyQikNoAMEMJA= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 474733f16f494ddb794b4f7dfd7de967.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: w8WotJn9V-pfsSYCbGXMMBwJB87hFD2ZBrAd5nT2ed29gRASrrJWw==
2021-09-16 04:29:02 UTC	1364	IN	Data Raw: 3c 21 64 ff 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 70 7a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/hs#""><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:29:02 UTC	1380	IN	Data Raw: 74 72 65 61 6d 20 61 6e 64 20 62 65 63 61 6d 65 20 74 68 65 20 68 6f 74 74 65 73 74 20 6e 65 77 20 74 68 69 6e 67 20 69 6e 20 6d 75 73 69 63 2c 20 3c 65 6d 3e 46 6f 72 62 65 73 3c 2f 65 6d 3e 20 70 6c 61 63 65 64 20 68 69 6d 20 6e 69 6e 74 68 20 6f 6e 20 74 68 65 20 70 75 62 6c 69 63 61 74 69 6f 6e e2 80 99 73 20 6c 69 73 74 20 6f 66 20 74 68 65 20 68 69 67 68 65 73 74 2d 70 61 69 64 20 6d 75 73 69 63 69 61 6e 73 20 69 6e 20 74 68 65 20 77 6f 72 6c 64 2c 20 61 73 20 68 65 20 68 61 64 20 72 61 6b 65 64 20 69 6e 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 66 6f 72 62 65 73 2e 63 6f 6d 2f 70 69 63 74 75 72 65 73 2f 65 65 67 69 34 35 6c 66 6b 6b 2f 39 2d 6a 75 73 74 69 6e 2d 62 69 65 62 65 72 2d 35 33 2d 6d 69 6c 6c 69 6f 6e 2f 3f 73 68 Data Ascii: tream and became the hottest new thing in music, Forbes placed him ninth on the publications list o f the highest-paid musicians in the world, as he had raked in <a href="https://www.forbes.com/pictures/eeegi45lkk/9-justin-bieber-53-million/?sh
2021-09-16 04:29:02 UTC	1386	IN	Data Raw: 79 20 72 69 63 68 20 6d 61 6e 2c 20 61 6e 64 20 68 65 20 6c 69 6b 65 6c 79 20 70 75 6c 6c 73 20 69 6e 20 6d 69 6c 6c 69 6f 6e 73 20 69 6e 20 72 6f 79 61 6c 74 69 65 73 20 70 65 72 20 79 65 61 72 2e 3c 2f 70 3e 3c 68 33 3e 33 2e 20 45 6e 64 6f 72 73 65 6d 65 6e 74 73 3c 2f 68 33 3e 3c 70 3e 54 68 72 6f 75 67 68 6f 75 74 20 74 68 65 20 64 65 63 61 64 65 20 68 65 e2 80 99 73 20 62 65 65 6e 20 61 20 67 6c 6f 62 61 6c 20 73 75 70 65 72 73 74 61 72 2c 20 42 69 65 62 65 72 20 68 61 73 20 74 65 61 6d 65 64 20 75 70 20 77 69 74 68 20 61 20 6e 75 6d 62 65 72 20 6f 66 20 62 72 61 6e 64 73 20 66 6f 72 20 68 69 67 68 2d 70 72 6f 66 69 6c 65 20 63 61 6d 70 61 69 67 6e 73 2c 20 61 6e 64 20 61 6c 6c 20 6f 66 20 74 68 65 6d 20 68 61 76 65 20 70 61 69 64 20 68 69 6d 20 77 Data Ascii: y rich man, and he likely pulls in millions in royalties per year. 3. Endorsements Throughout the decade hes been a global superstar, Bieber has teamed up with a number of brands for high-profile campaigns, and all of them have paid him w

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:03 UTC	1434	IN	Data Raw: 94 8a 94 f4 95 5f 95 c9 96 34 96 9f 97 0a 97 75 97 e0 98 4c 98 b8 99 24 99 90 99 fc 9a 68 9a d5 9b 42 9b af 9c 1c 9c 89 9c f7 9d 64 9d d2 9e 40 9e ae 9f 1d 9f 8b 9f fa a0 69 a0 d8 a1 47 a1 b6 a2 26 a2 96 a3 06 a3 76 a3 e6 a4 56 a4 c7 a5 38 a5 a9 a6 1a a6 8b a6 fd a7 6e a7 e0 a8 52 a8 c4 a9 37 a9 a9 aa 1c aa 8f ab 02 ab 75 ab e9 ac 5c ac d0 ad 44 ad b8 ae 2d ae a1 af 16 af 8b b0 00 b0 75 b0 ea b1 60 b1 d6 b2 4b b2 c2 b3 38 b3 ae b4 25 b4 9c b5 13 b5 8a b6 01 b6 79 b6 f0 b7 68 b7 e0 b8 59 b8 d1 b9 4a b9 c2 ba 3b ba b5 bb 2e bb a7 bc 21 bc 9b bd 15 bd 8f be 0a be 84 be ff bf 7a bf f5 c0 70 c0 ec c1 67 c1 e3 c2 5f c2 db c3 58 c3 d4 c4 51 c4 ce c5 4b c5 c8 c6 46 c6 c3 c7 41 c7 bf c8 3d c8 bc c9 3a c9 b9 ca 38 ca b7 cb 36 cb b6 cc 35 cc b5 cd 35 cd b5 ce 36 ce Data Ascii: _4uL\$hbD@iG&vV8nR7uID-u`K8%yHYJ;.:lzp_g_XQKFA=:86556
2021-09-16 04:29:03 UTC	1435	IN	Data Raw: fd 63 bc 79 06 2f f1 26 c8 f3 ef 7f 74 d8 0f 4f 07 a0 00 17 0c a1 6d b6 49 bd 5d d8 6d 18 02 5e 0d 4a c3 2e 97 8b 96 27 ce 52 e3 9b ec e8 bc 8a 38 a3 7b f2 d3 94 6f 7b 3f 7a ef 2a 6d ad 55 a8 79 1a 92 8a 2b 6d be c5 91 e6 5b e3 e8 9e 7f c3 9c db a9 71 98 25 6f 7c a6 5d 6f 47 7d 46 8f e7 d5 8b 43 52 f5 07 42 4d b0 da b4 85 be 8b 96 68 f6 fe c8 de 7a 4b b2 fa 27 df 3d 9b 79 95 6e b5 53 64 17 78 2d 96 4a 30 3c c1 ad e8 28 ad 37 ba fe 67 b1 cc 8e 62 64 5e c7 ec 71 c5 ae be 2e d5 e5 fd 1f d1 3b 8e f7 93 4f 99 ce 7c b9 89 c8 b7 61 92 b0 cd bb 75 fa 19 f4 ab 85 3e 43 4d 97 22 92 44 11 5d be 81 fd 66 d0 3c 05 91 65 f3 36 66 c9 a6 c5 75 dd 26 ac c5 34 4e b2 e8 1b 8d ea ed 7b fa cb 93 c3 1a 65 e6 4e 3d 45 23 22 bd 4c c5 6c e0 63 b8 f5 24 35 76 c8 e6 69 bd 75 ec 73 Data Ascii: cy/&toM]m^J.'R8{o{?z*mUy+m[q%o]oG]FCRBMhzK'=ynSdx-J0<(7gbd^q.;O]au>CM'DJ]f<e6fu&4N{eN=E #~"Llc\$5vius
2021-09-16 04:29:03 UTC	1437	IN	Data Raw: 6a 7e bf fa 1d ae b4 5e 91 c0 37 95 36 df c7 fe d4 65 64 51 79 07 be fb 43 4e 00 30 6e 49 8a 38 a3 23 8a 6c 51 f9 1c 52 76 27 1c 5c 36 c6 da cc fd a3 a4 91 62 c6 f2 dc 7b 91 a8 e8 39 c3 6f f4 bf 38 f4 56 f8 e9 2d 83 c7 3f 0a 63 82 65 b2 1e b9 fb 9d 60 e5 0b 8e 9b b4 56 6d 9d e3 5b a4 36 de 1d 85 e2 19 0e 65 6d d5 1a 0b 05 c3 23 db b9 4e 17 f5 fd 60 bc f5 ec 3e f8 a4 90 00 30 6e 49 8e 3f 51 7b ec c4 c8 bd 9b ec 1b 2b 9b f1 3d a3 b6 72 2b a5 ce 55 2e 11 8f 67 5a c7 51 e5 d7 7c 5f 10 d8 5c 71 db 99 a7 47 ec 4f 9d bf 1f 10 2d 91 fd 18 fa e3 84 e8 1b c6 5d 53 5b 93 e1 18 8e 1d b9 73 18 a5 5b b0 9d 79 a4 b4 26 2d 41 99 fa e7 2f 66 bf 4d 36 b4 5e f9 ef 8f 5e 51 c9 00 18 3f 24 45 33 d1 ec df 66 26 cc 27 6a 3b 4e 7f b3 33 7b cc d9 9a e3 5f e7 99 b6 94 c1 77 3d e6 Data Ascii: j~^76edQyCN0nI8#lQRv^6b{9o8V~?ce`Vm[6em#N`>0nI?Q{+=r+U.GzQJ_!qGO-J]s[ysj&-A/fm6^~Q?}E3f& `j;N3[_w=
2021-09-16 04:29:03 UTC	1438	IN	Data Raw: e7 80 03 06 e4 00 3d 8b c8 62 f2 4c 32 e0 b4 dc 2d 5b 7a c5 86 6b 7c 93 6a 5b f5 a6 a9 a6 dc 7b 62 64 53 63 99 51 17 bb bf 8d 7e 51 c3 ef 9f 48 3e ab 5b 39 e3 56 6f ea 9d 2b a4 75 0e 8f cc 3a 77 42 61 18 ed 46 c4 bf 64 97 5c 4b 51 d3 77 55 1e 69 a2 77 76 f9 c8 36 c5 77 af 22 f1 ef 80 01 82 f2 08 0f 7c f7 df 69 a9 ed 75 99 df 1f 6c 2e a7 b3 c7 3f 16 d7 58 9d 92 8b 01 e9 8c fa 3f 62 a8 9f 37 df 77 3f cd ce 05 f3 d8 7e bf f7 7e a5 e7 1c e7 6f e3 9a bd 9e 74 be 19 7d fa 73 cd ba b6 d5 26 e5 7c ca 68 75 ce 2f 74 be 1a 5c 3f 51 6f 4d fd 2b a3 be a6 21 f5 e8 00 17 3d 20 00 f3 b6 5d b7 74 96 21 74 9d 89 fb d1 98 d5 e7 ca bb 7e 23 82 eb bc 6f 0e cb f4 4f d0 84 c9 f3 66 ce cb b4 27 c9 19 31 cd fb 77 b5 34 3f b9 b6 7b aa b9 de fd cc 56 fc 87 e9 94 bd 63 6a 9b 1d 65 Data Ascii: =bL2-[zkj][f{bdScQ-QH>[9Vo+u:wBAFdKQwUjwv6w"jiul.?X?b7w?~--ot)s&[hu/t?QoM+!7]tlt~#oOf1w4?{Vcje
2021-09-16 04:29:03 UTC	1439	IN	Data Raw: cb e5 2e a9 e0 ba 6c 27 22 ab bb ed 4e d6 fc d4 69 6a 7e e9 f9 c3 5b 8e 6a 69 37 b8 ea eb a4 de f6 c5 7c ca e9 d5 d5 72 52 64 c7 70 95 22 4d 3f 22 5f e7 75 a6 e8 c8 2b 26 63 b8 0e b3 c2 ac df 71 fb c0 00 62 5c 87 a9 f7 2d 9f e9 3e 03 af a8 b1 cc 87 7a fc f4 a1 8c ab ab e9 9e a9 aa 53 2a 79 bb 95 a8 2e 16 6b b4 8c df 7c d7 eb bd 45 6c f3 a5 f3 6f cb cc 99 77 7d 3d 7d d7 1a ca e9 91 d4 d4 cd ac cd 72 bb 9d 5c d9 71 c7 22 93 d9 b5 95 33 7c 87 1c e6 fb 57 58 ec ad a1 7a a9 9f 4d 8c eb fd 7b 8b 7d b2 ee 80 01 84 f2 4f 35 76 07 bd ff 00 7c c0 f4 b7 4a 50 d2 fc d6 b5 5c a3 82 e7 e7 4f f5 34 f9 f2 24 d5 73 6f 31 da ae b8 bd 75 c2 0f a5 b3 60 a5 a8 8f 1e d1 9f 9a 58 a3 d6 16 0a ac 03 d9 57 9a 9a c8 ef 19 45 ee eb 5b 49 e5 2d be 64 d9 b5 d5 d7 19 f2 65 f1 d5 76 5d Data Ascii: !."Nij~[ji7]rRdp"M?"_u+&cqb!->zS^y.kj Elow)=}r!q"3jWXzMj O5vjJP\O4\$so1u`XWE[!-dev]
2021-09-16 04:29:03 UTC	1441	IN	Data Raw: b9 5e 57 98 d0 c8 d7 58 dd b3 a4 f4 dc cc e3 00 a5 8a f5 6c b9 5a f0 e9 15 5b 6f 6f 7d c8 ed a0 00 00 00 00 03 df 00 bd ea bf cd 27 31 ef 5d a7 c3 fd e5 c3 b5 39 8d ae 87 24 ea 7a b9 5a 97 9c 29 ee 19 8e b8 ce b6 de 45 5b 16 bb b2 6c 6d 5b aa ee 36 fd 95 af e9 af 17 cf 70 3a d8 21 a3 ca ef bf a1 1e f0 00 00 00 00 00 00 02 e f8 9f e5 db 9d 7b 5b 4f d8 36 77 2c d9 32 2c cb 1d a6 df 5b 6a 77 27 60 b6 cc 87 28 aa da 19 86 43 75 c6 2e dc ff 00 ad af 38 a6 bf 83 2a 97 15 fe e5 32 c5 6f f2 82 b7 f4 d1 c8 9d 05 f4 24 00 00 00 00 00 bc e1 7f 97 4e 6b eb 3d 2f d3 da 5b 7c 73 95 eb 12 bf 68 bd d7 d1 b2 b8 97 18 95 b2 f6 2e c5 da d7 2a 3b 74 58 17 3d e9 f8 6e 98 8e c7 c3 e6 d1 55 e5 54 f4 d2 2c b2 7f 42 9d ff 00 e6 41 94 00 00 00 00 00 00 27 5e 39 c7 f3 b1 ce f9 fe Data Ascii: ^WXIZ[oo`]1)9\$zZ)E[!m[6p:!.{[O6w,2,[jw" (Cu.8*2o\$Nk=~/]sh.*:tX=nUT,BA^9
2021-09-16 04:29:03 UTC	1442	IN	Data Raw: 4c ae bb 84 e7 7e c9 ea 90 34 1e 63 a0 c8 d5 ed ad 87 8b 75 1f 07 5d dd 51 5a 6d b2 07 37 f9 ef 45 2d 5b 93 d6 bd 92 cc b6 59 7e 2c 90 fc 4b a2 fb 0f a4 b6 0f 37 e5 9a 89 51 75 1b 1d 8c 68 db 9d 1e 8d 11 0d 3d b0 fa 82 e7 d8 fb 68 af 61 f4 7c 1c db 68 78 2d ac 6f 97 7d 07 ed be 9b 1e bf 93 f3 0d 66 0a c2 cf 9a 97 6d 29 64 df 4d aa ea 6d b2 07 37 f9 ee 28 a5 fd af d0 da fc fb 3a e0 d7 60 e1 bc 27 a1 fd 14 df db a9 e5 3c c7 57 1a 46 58 f5 d7 ca e9 b6 dc 8c ef 52 ad 6e a6 e3 20 73 9f 9e f5 a2 95 66 f4 7f 6f 85 59 f3 21 6a f5 bf 32 e0 99 fa 53 d2 62 d1 f3 3e 53 4d 7e ff 00 61 ae d5 ea 64 77 56 f2 b2 fd 43 2d 69 6e ef 30 73 9f 9f 75 aa 97 52 ef 6d f5 2c 18 ee c3 1a cf 13 f3 7a 65 fd 1d ee a3 73 9c ff 00 8d ae 74 d9 65 44 87 9a 67 4b 67 3f 6f a9 cb ad 8d e6 Data Ascii: L~4cu]QZm7E-[Y~..K7Quhh9Qha[hx~o]fm)dMm7(:`<WFXRn sfoYlj2Sb>SM~adwVC-in0suRm,zesteDgKg?o
2021-09-16 04:29:03 UTC	1443	IN	Data Raw: 5e 94 a4 0f 09 bb b1 5c 8d c3 cc cc f5 1d ac f3 38 5b 92 78 b7 7f 5f 9d f7 67 2f 33 0e 17 43 f7 15 ab 52 b5 a9 1f 8e db b7 5c 7f a5 95 ad 3c d2 e6 99 c6 e7 64 6d c6 62 dc 93 cf b1 c7 e0 2f 48 59 8d 1d 9d 11 0d 3d b0 fa 82 e7 d8 f9 7a 07 8a ab 56 3c 79 b7 62 fd 9d e7 da dd 1e 39 9e 8d 35 89 8f ea 95 94 ce c0 9f f9 d7 51 bf 21 5e 87 d7 f1 75 a8 f9 f9 c9 4b 1c d6 06 53 56 89 a2 95 ac 57 81 3b f6 9f af 1e 4a 45 72 5c 7f 76 22 e4 33 6d 5f cc c2 ea 5f 27 e9 de e4 32 77 de 9b 91 15 e2 72 d6 66 5e 97 a3 4d 40 6b 9e 55 b7 85 8c 13 9f 69 f9 14 6b bc da d5 6d e1 49 dd c0 88 ce d8 b6 ff 00 96 35 5a e7 c9 74 2d d6 ce c9 8d 27 a3 cd 4b c1 46 6f 5c 67 4f a9 48 9b 61 39 f6 a5 29 ef c3 cc 47 23 f5 72 9e 72 ae 47 62 e7 6c 7e be 6c d7 12 12 dd 1b a0 de 8f 96 87 cc ca bf Data Ascii: ^!8[xw_g/3CR!<dmb/HY=zV<yb95Q!^uKSVW;JErV`3m`_2wrf`M@kUiKml5Zt~KfKfoHA9)G#rrGbl~l
2021-09-16 04:29:03 UTC	1445	IN	Data Raw: 00 01 04 01 03 02 03 05 08 02 02 03 01 01 01 00 02 00 01 03 04 05 06 11 12 13 21 07 10 14 15 20 22 30 31 16 17 23 32 33 35 40 41 24 50 34 60 18 25 42 36 90 a0 ff da 00 08 01 01 00 05 01 01 ff 00 fa 62 f2 0b 17 fd 8a 49 38 a2 d9 d0 1b 3b 7f d8 24 36 01 df 77 03 7e a6 e8 67 34 12 89 ff 00 d7 8c d8 06 69 4f 93 90 f0 8d b6 67 e2 eb 75 03 4b d5 ff 00 ae 11 33 34 86 46 5d c5 e4 89 a2 8c 44 48 37 ef cf 65 11 3b c9 ff 00 5b 77 d9 4b 2b 93 ef b2 73 77 56 76 6a fb 6c c9 c5 d0 bf 12 17 dd bf ea b6 ac c7 5a bf da 7c 72 fb 4f 8e 5f 69 f1 c8 35 15 13 32 9d cd dc 96 ec b6 57 5d fd 3f 7d 99 33 6c 32 e5 69 43 2f da 2a 0b ed 15 05 f6 8a 8a fb 43 45 7d a0 a2 be d0 51 5e df a2 bd bf 45 7b 7e 92 f6 fd 15 ed fa 4b db d4 97 b7 a9 2f 6f 52 5e de a4 bd bb 49 7b 76 92 f6 ed 25 ed Data Ascii: ! "01#235@A\$P4`%B6b!8;\$6w~g4iOguK34F]DH7e;[wk+swVvjJz[R0_!52Wj?}3!2iC^CE]Q^E{~K~oR^!f%v
2021-09-16 04:29:03 UTC	1446	IN	Data Raw: 35 c6 40 76 d9 dc cd a3 8a dd 92 b1 2f cb db cb 35 68 ab e3 ec 11 c9 36 cc cd 5c 1f 6c 74 02 a1 87 75 0d 46 e9 c5 4a 28 d0 c5 de 57 e2 c1 51 8a 1c ae 10 1d 59 c5 b0 26 a6 4c ba 4f b4 83 19 c7 3f e5 38 1f 72 87 79 ea b9 91 3f 69 b4 d6 60 f2 34 2a 6c d5 bc 61 80 5f 16 b6 f2 75 ba dd 3a 6f a8 af 0d eb f2 9d be 9a ab 24 50 52 d8 9a 3a b8 fd 98 5a b0 3b 1f c7 52 7a 22 9a ce 3c 98 ee e2 d9 a4 2c 4c ed 2d 6a 42 a2 e4 cf 74 ea c3 24 d8 40 b4 36 31 e7 1c 9c 0e 39 87 51 8c d1 7c 15 ce b6 52 7c 6c f9 5a e4 47 4b 29 f8 d8 eb d0 5d a7 ee 33 93 21 26 26 24 4d df 74 04 ec e1 20 a6 5d 9d 58 07 62 f7 e4 97 72 77 4e ee e9 9f bf 14 4e 4c 88 4c 93 48 2c b2 b7 7a c7 ee b7 c9 d7 53 38 63 0d f6 2a b5 d5 58 9c cb 1d 08 ed 5e 2f 86 1e cc c8 41 d0 06 c9 9b 76 9e ab 3a 9b 0a 0e d7 Data Ascii: 5@v/5h6!tuFJ(WQY&LO?8ry?i`4*_la_u:o\$PR:Z;Rz"<~.L-jBt@<619Q[R JZGK)]3!&~\$Mt]xbrwNLLH,zS8c^X^/Av:

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:03 UTC	1447	IN	Data Raw: 9a 94 8f da 18 71 da bc 63 da 36 40 ca 31 42 db 33 a7 64 62 a4 65 2b ec a5 26 46 cd b5 ae ca cf d7 25 5f 92 b1 54 99 4b 11 83 9c a0 04 d6 22 e3 84 22 25 24 af 1a d0 66 d0 e6 fe 54 67 b7 95 aa d0 ca 1f 2f 33 fb 67 cf b9 fa 35 61 70 93 58 c5 1c 98 ed 3b 4b ab 72 b8 6c c3 17 26 3a 71 72 3c 7d 23 7b 5a 4b 1d 33 db d1 b9 38 da 0a ca 53 92 96 ab c8 42 78 4d 4a f6 e2 8e 56 71 17 74 ce 89 fb 49 23 32 e6 26 d2 ab 44 ac 1f 7c e8 fe 3e 87 a7 b4 51 49 c0 eb bf 28 a3 6e 6f a8 31 a7 8e cd 79 3b 27 f2 16 5e 1c 55 e9 e3 3f ad 75 1b c5 96 c5 c8 0d 01 6a 3c 4c 6a 9e 7b 1f 30 c1 6e 22 78 a5 15 d4 65 d4 47 64 44 6c e7 eb c6 57 b5 93 b1 da d5 37 64 29 33 5a 81 e4 6d 59 98 ae 71 ea 5a 96 c6 53 ea 45 ee ae 56 67 52 cf 24 25 62 a0 c9 1c 83 c0 b4 eb bb 59 36 63 a5 a6 26 68 f3 1f Data Ascii: qc6@1B3dbe+&F%_TK""%\$fTg/3g5apX;Krl&:qr<}#{ZK38@SBxMJVqtl#2&D]>Ql(no1y;^U?<Uj<lj{0n"xGd DIW7d)3ZmYqZSVgR\$%bY6c&h
2021-09-16 04:29:03 UTC	1449	IN	Data Raw: ef e4 eb 2e ed c6 01 6d a1 dd 41 f5 6f a6 fb 29 25 74 11 91 36 48 18 26 6e 9b 04 52 c6 4f 14 61 c3 39 0f 13 c5 6c 36 ca 3e cd 59 94 9f 43 16 63 be 6c c3 a7 e9 b7 53 cb 1c c2 d5 3e 8b c5 3c 84 56 f5 4b ad bc cd 90 b7 7d 07 5b a5 89 59 1f cb 5c 5b d5 d7 50 32 0d 91 48 2c ac cb ba 8b b0 5f 2e 4a 29 9a 32 a9 2c 64 a2 2e cc 4c eb e1 53 ed b5 b7 6d ee ca ca 79 b7 52 3e ee 6c a9 18 b1 63 31 57 a4 28 8d a5 3d 39 13 49 9b c3 f3 92 7d 3a 5b 07 ca 2f af cc cc 7e db f3 7f 5b ac b3 be f5 d4 22 5b 81 20 dd 30 ee 3d 36 5c 99 96 4e 2e b4 76 28 5c 98 28 d7 ca 52 78 f3 3d 38 a5 cc c3 78 b1 c0 5e aa 37 ec 6c c8 c5 58 2e f7 46 49 e4 a3 1f 08 bc b1 72 73 aa e2 cb c5 f1 e3 a8 7d c2 6e f5 c3 94 fa 76 1e 9e 3d 64 ff 00 24 4f b5 d8 1f 62 88 97 51 1c cc a4 7d cc 63 ab d1 b4 3f 14 Data Ascii: .mAo)%t6H&nROa9l6<YCclS><VK}[Y[P2H,_J)]-[~["0=6m.v\(\Rx=8x^7IX.Flrs)nv=d\$O bQ]c?
2021-09-16 04:29:03 UTC	1450	IN	Data Raw: 8d d8 98 e3 89 d7 26 03 b0 60 2d 6a 6d d8 65 f8 26 b1 b0 e3 2b bf ba de 5b ac 3c dd 4a 3e 23 53 2a fa c1 6e bf b5 8d 8b ab 90 c4 c7 c2 92 27 d9 b2 b2 f2 96 57 71 8c 1b 8d 3c f4 01 24 99 28 c1 8f 1b 7e 2b 31 c3 dc 58 05 74 05 3d 71 47 10 a7 16 52 1b 32 cb 64 18 23 8a 5d ca f6 51 84 66 b5 3d 83 f4 e3 18 d8 8f e2 9c 38 5d d3 15 f9 43 95 c8 58 98 f1 d1 30 63 25 d8 b2 f8 9e f6 23 2d ac 40 5d f7 fe 36 67 f6 cf 9a fe 73 f2 79 e6 e9 81 3c 06 27 28 4c 12 10 ec c3 27 e1 d5 95 cd aa ef b6 c9 99 4c 0d b4 d2 18 bc b2 84 91 14 8c a3 73 50 d2 79 4d be 9e e3 79 9d 07 37 0f 18 f1 47 c5 fd cd 25 5f ad 3c 3c 61 56 4d 82 1b 04 f2 4e f1 94 91 48 db 45 a9 eb 89 e5 f3 1c 46 a5 6b c5 8b c8 d1 9c 64 08 d0 0e ec f1 8e d3 c6 cc ac 4a c2 af de 60 0c 86 43 ab 35 9c a0 44 03 5e cd Data Ascii: &~jme&+ [<J>#S^nWq<\$(-+1Xt=qGR2d#]Qf=8]CX0c%#-@]6gsy<('LsPyMy7G6%_<aVMNHEFkdJ`C5D^
2021-09-16 04:29:03 UTC	1451	IN	Data Raw: de 18 4e 2b 4c 4b 14 f3 70 92 a3 bc 83 cb 6f e1 e6 7f 6c f3 39 23 8c 71 af ed 0b 95 69 14 50 8d 54 10 b3 26 15 dd 32 b5 76 ad 61 cc ea 39 67 8e 29 0b 78 a4 19 04 81 f7 8f e8 ed b8 c7 0e ea 0c 0d 41 97 6e c2 c9 93 fd 0d 91 32 e3 dc d9 13 8a 90 f7 58 1c 68 df 91 85 33 22 fa 7a 57 37 96 b0 b2 07 21 6b 14 29 59 56 b0 56 e2 4e 2e ca 96 fe ae 1d b9 6a 4a a5 57 3f e5 a0 eb f5 32 f1 b6 c1 e7 e3 35 cd aa ff 00 74 83 f1 a6 7d a3 74 ea 77 ed e1 ad 2e 9e 1b 1e 7f 8c 1f 4f 26 fa 3a 94 94 84 8c 57 15 13 32 96 3e 32 a2 88 49 5b a2 06 da 97 39 5a 84 9c 5c 8d c8 b2 d4 31 98 fb b5 69 61 1a 25 1c 42 0d fc 5c cf ed 8a 6b 50 44 a6 ca 4a e8 86 49 1f 42 46 23 64 09 93 38 ae 4c b9 b2 29 10 c8 cb 2f 8f 1b d5 0c 5d 10 9d 94 53 90 3c 72 0c 82 28 83 90 d4 de 42 04 c2 b8 a1 dd 3a 36 Data Ascii: N+LKpol9#qIPT&2va9g)xAn2Xh3^zW7Ik)YVVN.iJW?25t]tw.O&:W2>2l[9Zl1a%BlkPDJIBF#d8L)/J\$<r(B:6
2021-09-16 04:29:03 UTC	1453	IN	Data Raw: be c9 89 6e ad dc 0a c2 19 6a 24 82 d5 63 5d 48 d3 d8 ae 28 b2 54 19 49 98 a4 2d 0e 3e 96 4a c4 18 bc 7c 09 dd 77 f2 db b2 d6 03 f8 12 83 3b 48 1c 0c 5b 76 88 f8 a8 a4 62 46 1b 2d 25 3b 49 52 76 7e 5c 2c e4 2d af a5 ff 00 a7 5a 2e bf 57 33 03 71 8b 3d a9 71 18 4a da b7 5f e5 f3 65 75 dd dd ca 30 68 67 9d e5 fa 33 ba 10 dd ba 4b 6d 97 d5 eb 55 32 43 1e c8 3e 8f bb a1 85 dd 04 0c 22 6e 89 74 d4 50 82 18 c1 85 99 99 6f b2 37 dd 1e cc 9e 44 f2 2c f5 b3 92 4a e2 14 ea 51 80 a6 96 b5 6d 9a 38 10 c4 e9 e2 52 47 da c0 a3 dd 93 c8 fb 6f 0f 12 32 58 43 a9 66 0b 35 be 64 1f ab fd 44 b6 5f d6 a1 36 f6 b5 4a fb 26 37 96 6e 6d ca 52 e4 ac 4e 46 5c 1f 96 12 26 8f 16 e8 5b c9 d3 79 6a e2 ff 00 12 2b 56 22 32 b7 2f 06 c8 4d bc d9 09 d3 5d b6 4f 27 4b 8e 91 6f f1 97 75 b2 Data Ascii: nj\$cl)H(TI->Jlwr;H[vbF-%3lRvw^,"Z.W3q=qJ_eu0hg3KmU2C">ntPo7D,JQm8RGi2XCf5dD_6J&7nmRNF&[yj +v^2/M]O^Kou
2021-09-16 04:29:03 UTC	1454	IN	Data Raw: 8e bc 24 36 69 b4 fc 86 de 73 30 ac dd 20 ac ec fc b6 5f fc f1 dd 08 ec 9d 97 17 5a 49 b6 91 bc ff 00 b7 f2 d5 3f ae 89 96 cf b9 b7 6b 07 c1 42 ef b5 7b c4 23 25 38 7a 82 50 93 51 8e 1a f3 75 a3 e3 aa 4a 6e 51 50 96 25 10 18 87 8d 5f b7 79 69 98 f6 8f fa c3 11 84 b6 6c 4a 0a 5b 96 ec 08 36 cc 99 33 26 64 2c 85 90 8a 11 46 db 79 6c b9 2e 6b 74 dd d0 b2 00 42 c9 99 90 ed e5 a9 2f ec 34 61 8c 8e 8d 72 9a 6a 35 ba 51 ef df 74 2e 88 97 2e ec e9 dd 31 28 cd 6e 8d 48 1d bc 39 6d b4 f7 cc 96 b8 58 8e 68 88 22 9c b8 97 d2 ae 3c b1 ce 17 6a 3e 32 2b 16 8a 22 74 58 fb 11 57 c8 df 9a 58 24 b4 47 03 e2 67 b1 42 33 ea 46 cc b8 f6 61 ee c2 b8 ae 2b 4a b7 e2 f9 97 d5 fc b5 37 fc 9d 91 32 d9 71 59 29 3a 74 bf fb 05 62 af c7 c8 39 b7 17 8e d4 b3 04 58 ec 85 7c 92 3a Data Ascii: \$6is0_ _ZI?kB(##68zPQuJnQP%_yilJ[63&d,Fyl.ktB/4arj5Qt..1(nH9mXh"<j>2""""zXWX\$GgB3Fa+J72qY):tb9X]:
2021-09-16 04:29:03 UTC	1455	IN	Data Raw: cf 3d 99 e1 c5 db da 68 24 86 42 72 01 17 27 37 fa 9c 82 51 fa 4b 5d 3e 5b c5 5e 73 ad 28 68 69 00 a4 4f 2a 79 94 93 29 a6 dd 39 b8 a8 6e 86 f1 3c 12 b5 80 78 89 a7 ef 04 aa 29 37 60 25 e1 9f ff 00 9b f9 95 ff 00 5a cb 76 6f cb 24 0e f8 d9 2f ce 44 56 9e a6 27 9d 85 8a a8 15 6a 6a 4c 3c f0 48 13 d0 27 c8 c4 45 4f 00 2f 66 cf bf a8 3f e0 4a cb fb 83 e9 95 1f 87 1c ff 00 01 fd 74 ff 00 ed de f3 e1 eb 95 cc 97 fc f5 3d 88 a2 6b 74 46 e9 54 af 4a b1 61 31 a0 39 3d f7 6b 4d fe 4d d2 21 af 23 ee d4 e2 9e 45 96 ab 15 19 22 99 a3 9e 6c c5 61 80 89 dd 04 09 45 4b 47 bf 4a 4a 93 e3 6d a2 c2 1f ac ef b3 58 7f 88 cd a3 0e a8 48 4d 13 6f b8 83 ef dc 49 d8 a2 c9 80 57 b7 69 e7 28 e2 92 54 ce 21 66 d1 46 f6 28 cd 5a bc b8 dc ee 3e 4e ba af 00 f5 a4 3d b8 63 a6 Data Ascii: =h\$Br7QK]>[^(s(iO^y)9n<x)7^%Zvo\$<DV^jjL<H^EO/f?Jt=ktFTJa19=kmm!#E"laEGJJmoXHMolWi(T!fF(Z>=c
2021-09-16 04:29:03 UTC	1457	IN	Data Raw: a4 03 d8 3a 64 8b 6d b7 4e 5d ab c4 12 2b 02 ec f8 be 4f 3d 4e 9d 29 be 56 b5 1b c4 58 fb 10 8b d7 8a 9d 7c 95 e9 87 24 f6 61 9b d7 d7 36 9a 08 32 36 b3 16 8a a1 de a0 d1 21 76 de 1e 9b 2b 12 bb 22 db 8e 3e 07 e1 6e af 4d 7f 6e 04 0a 62 8d c9 77 f2 df 65 e1 06 8d 8a c9 7b b5 7f 4b fd 8e db a6 dc 46 0d fa 9e 29 58 08 74 5f d5 68 5a dd 2c 67 88 9a 26 ae 5e 88 f5 21 92 49 e3 96 94 52 14 67 57 50 7a 9a 59 5c a6 d1 39 1c 92 bf 4c 54 31 31 1d e8 f6 67 fa f2 07 21 2d 91 39 13 e3 5c fd 44 78 f9 1d 8e f4 b5 ec 54 0e 4f 0f a7 c8 90 d8 b1 1d 1c 4d 89 a1 13 40 19 ed 0b 82 c 10 5c bb 35 ca f7 0d 89 33 3a 19 cd 9b 96 ea 28 00 86 33 18 e2 b5 33 99 3e ec 9c 8d db cf 75 a7 30 d3 e5 f3 34 69 55 a5 53 dd ab fa 5f ec 59 f6 77 ea 37 6e 7e 2f c2 e7 a4 a0 0e 52 e9 b8 7a 74 17 Data Ascii: :dmNj+O=N)VX[Sa626lv+^>nMnbwe{[KF)Xl_hZ,g&^!IRgWPzYl9LT11gl-9)XdTOM, 53:(33>u04iUS_Yw7n~R/zl
2021-09-16 04:29:03 UTC	1458	IN	Data Raw: 09 a7 48 72 6a 14 71 51 e9 9d 9c 7a 92 33 f4 2e 25 49 58 68 95 0d cd 5e 79 13 1b 93 9c 8b 8e df 3c 69 51 fa ca d8 e1 b0 73 4e 7d 6a ae 7b 8e fd 89 a5 d9 2e 12 84 ec 51 b1 4d d2 79 05 f5 8c 3c e4 1f 92 c2 5b df 28 b1 ee 96 ec 3b 94 3e eb a9 9e 32 8b e9 9e e3 b5 11 ed 6f 5b c0 c6 76 85 aa e2 e6 3b 36 9c 8a 65 7a 2e 04 1c c6 e3 b8 f5 6a d9 ea 76 5e d8 e5 c5 54 a3 50 43 98 e2 d3 d5 ac f6 cd e7 5a df 7f b8 08 4e 9d 81 49 f4 c0 76 8c 8e 8c 34 c8 cf d0 25 4c e2 b1 f1 d1 9a ba cf 15 27 35 8a 86 f6 47 9e 34 e9 b8 74 ce a3 d9 2e 71 24 1f 8c 2e ce aa 1c 13 40 19 ed 0b 82 c 10 5c bb 35 ca f7 0d 89 33 3a 19 cd 9b 96 ea 28 00 86 33 18 e2 b5 33 99 3e ec 9c 8d db cf 75 a7 30 d3 e5 f3 34 69 55 a5 53 dd ab fa 5f ec 59 f6 77 ea 37 6e 7e 2f c2 e7 a4 a0 0e 52 e9 b8 7a 74 17 Data Ascii: HwkqZz3.%lXh^y<lQsN]j{.QMyc<[(>2o[v;6ez.jv^TPCZNlv4%L5G4t.q\$.@NAaaFY[.##NYLDSaZ0`JR
2021-09-16 04:29:03 UTC	1459	IN	Data Raw: 7b ee bb 34 ca 8d da d0 51 69 18 38 7c d5 a2 94 01 72 b3 db e0 7c cd 3e 4a a1 19 91 03 db 7b ca 5c 78 f2 46 85 8d ae 71 da ee e5 e2 af 39 a1 bc a4 fc d6 32 54 19 0b 5f 10 b5 9a 0a 90 11 20 09 48 a8 06 27 72 99 24 6f 58 82 8c a3 19 ac 57 47 53 1d cf fd 57 44 f7 76 7e 45 3e cf 51 a4 c3 3f 88 6d 18 fc 10 b2 3d df 52 fd 6a 2e f7 76 77 84 ca 9b c6 3c fa f0 74 48 d1 c5 0d e1 65 8a 8d 8b 87 56 14 39 6b 0c 37 2e c3 3c 14 0d 19 ab 8d c5 e7 e1 e8 34 69 8d 8d 47 7c 42 68 39 e6 b8 9c d4 37 2d e8 2e 1e 68 e8 27 40 d9 0e 05 11 c7 f9 ab 3b ff 00 c1 6c a6 f7 2f 28 36 23 fa 55 4c 3b fc c3 46 f2 15 31 c0 2a 54 bf 79 5f 72 34 28 12 db 38 31 51 e3 37 f0 1c 10 8a 61 60 b2 58 85 97 54 98 51 0b 10 88 28 8c 25 5e 66 0a 1f 96 f4 1c 35 99 97 71 4c b5 01 79 d4 f7 66 5b fc 93 1a Data Ascii: {4Qi8[r]>J[xFq92T_ _Xr\$xoXWGSWDv-E>Q?m=Rj.vw<tHeV9k7.<4iG Bh97-.h'@:/l(6#UL;F1^Ty_r4(81Q 7a`XTQ(%^5qlYf[

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:03 UTC	1461	IN	Data Raw: 82 bc 02 3a 0a cc 2a 6c 00 e2 53 3a 71 4d d5 1c 3d 7c 4a 35 ac d0 1b b5 83 f2 5e 4b 8c 61 b0 a8 f7 94 df 97 a4 56 e4 3e 7e 81 8e 4e 05 aa a3 de 0c 63 ac 31 56 78 32 1c e9 94 38 0e ae 18 2d 57 0e f5 8c 21 34 da f8 da 46 4b 8c 2c d1 4f 97 43 42 fa 55 d7 ba 98 23 37 46 7b a1 7d 60 a8 cc 27 55 f7 cf 82 06 a0 a5 52 70 98 c7 bc 2e 96 8c b4 1f 64 e0 51 b9 54 9e 79 a7 07 64 d0 55 4b 53 86 b5 7a a4 8e 43 45 47 ee 81 a3 ca 55 58 35 9b 41 d1 df 87 5e 80 f7 a5 30 70 55 0f ba 55 40 79 aa d5 6c 90 e8 99 69 c3 2d c8 b7 eb 31 3d 95 4e db 52 d0 e6 5e 21 91 4b 63 4e f5 f6 a7 e4 eb 75 b5 c6 47 48 cb 4b 04 03 18 90 41 22 0f 8a a7 52 db 67 d5 7f f6 b4 76 73 09 b0 fb cc 70 05 a7 78 2a 51 68 46 ab fb 23 60 cd c4 ec 4d 16 e2 ea 76 41 8f 46 cd bc ba b1 d4 f2 38 6d 1a ac 26 75 60 Data Ascii: :*!S:qM= J5^KaV>~Nc1Vx28-W!4FK,OCBU#7F{}`URp.dQTydUKSzcEGUX5A*0pUU@yili-1=NR^! KcNnguGHKA#RgvspX*QhF#`MvAF8m&u`
2021-09-16 04:29:03 UTC	1462	IN	Data Raw: 5d 2d 12 5f 67 8c 69 ed ee 57 99 57 9c e6 14 5e 0b 12 ef e3 50 03 16 6d 0a 45 55 71 ac 71 91 39 20 ce 85 c1 80 49 72 85 08 0d 2d 67 fc ba 4e 79 f9 2a 0e b7 0f ab 74 83 9c 49 18 64 a2 9f 45 0d 11 14 c5 d8 e0 ef 7b 7a a4 48 c1 82 47 31 80 4f 8d 94 fe 65 33 fc d3 ff 00 68 84 ef bc ef 48 ad c8 7c fd a0 a7 00 17 05 12 b8 a0 36 c2 89 44 ac 42 de 37 28 7d 35 17 58 ee 68 74 35 de df 76 64 2d 56 07 1f 74 c2 fa ca 30 5d bc a0 c1 b4 e3 c1 5d 50 dc 4b 8e 09 94 c6 c1 8f 3e ab 2e e7 78 29 e2 aa c4 63 42 91 c3 97 58 bf 7b b4 98 3b 15 dc e1 a4 fe 4a 89 fb bf 24 e1 c7 41 e1 8a ab 69 bb 2c a9 4a e3 99 9e 46 41 0a a1 65 2a 4f c2 09 03 7e e4 40 b3 d3 06 33 0a 3e 8b 4b b3 99 18 a7 4d 16 60 d2 49 8c 55 2f a3 b1 b5 a0 b7 56 9c 13 de 81 ec 8b b7 78 a0 da 6c 00 23 a4 a2 4e c5 68 Data Ascii:]-_giWW^PmEUqq9 lr-gNy*tlde[ZhG1Oe3hH 6DB7({5Xht5vd-Vt0 }PK>.x)cBX{;J\$Ai,JFAe*O~@3>KM^IU /Xl#Nn
2021-09-16 04:29:03 UTC	1463	IN	Data Raw: 11 e8 d5 b9 0f 9f 9d 98 d1 8a e0 a9 d4 02 45 f8 70 e0 54 b4 cb 1c df 81 4e a4 6a b8 06 cb 63 3c 7b d7 d2 28 bc d4 8d db b9 26 bc 7a cd 05 15 96 8d 66 84 5c d2 e6 fc 51 1d 31 c8 e2 42 97 b9 ce 38 e7 86 6a 95 2a 63 07 67 1b 78 20 f7 9d 6d db 02 a3 c4 13 e3 e6 aa 37 7b 77 26 5a 08 fa ba d4 40 69 e2 cc 0f 55 ae df 8e 89 77 d9 b7 e2 ba 16 60 3d 72 36 0d ca eb 46 c0 02 91 94 40 5c 49 c5 36 f3 85 4a 97 de e1 78 63 48 0f 65 5f 76 d1 80 4f 3e c8 55 27 37 7e 6a 40 3b c8 f0 d0 5c d1 aa 4a c9 65 d4 cb 4e 4b 25 66 1b 43 69 b7 fe e2 15 77 53 79 69 25 b3 b4 1d 99 2b 54 fb 04 2e 21 df 35 3b 9f 3e 28 b4 ec 91 dc 53 2a fb 26 1d c9 02 3d 1a b7 21 f3 f3 81 8d cb d6 3b 82 b2 b2 86 ab 4d e0 a0 d3 63 ce f7 35 12 73 d0 43 7b 42 1c 38 c2 af 66 77 a8 64 03 b0 3b 62 b5 55 38 dd Data Ascii: EpTNjc{({&zfiQ1B8j*cgx m7{w&Z@iUw~r6F@\\i6JxcHe_vO>U'7-j@\\JeNk%fcIwSyi%+T.i5;>{S^&!;Mc5 sC{B8fwd;bU8
2021-09-16 04:29:03 UTC	1465	IN	Data Raw: 7a 8e 3c 15 5f 74 47 5a cb d3 64 2a 18 e6 32 d1 48 f1 43 cc cd 7a f4 e9 8f 79 c0 27 32 c4 df a4 54 df d9 67 f3 4e 16 ca 95 69 ce 22 90 d5 00 1e 0a 62 39 a9 76 27 aa da 4e fe 91 66 ff 00 96 e3 8b 7e e9 d8 83 e8 5a a9 b5 bd 69 d4 70 6b c1 e4 7d 15 d4 6a b6 f3 1d 98 e5 8a e8 fe 8b 46 ef dd 52 2c cd ef 24 a8 36 5a 5f c2 a7 e8 f1 c9 c5 35 96 5a 40 b6 a0 bc e0 e2 76 6e 5f 5b 46 a3 79 41 5f 6c 5b f7 9a 57 f5 80 79 02 a2 85 27 bc ef 76 a8 53 d3 16 0d cc c1 0b c4 55 6e d0 ef d5 31 9d 03 83 9c 43 73 18 4a 37 c3 aa 49 93 78 ab f4 c1 e8 9d f0 e1 a4 4e 69 c5 8d 0e 0d ee 45 af 61 63 a4 e0 44 29 1d 6d 67 00 8f 46 de f7 60 a5 ee be 7e 1e 0b 1d 02 9d 31 89 f0 08 9a 77 2a 3b da 98 8e 48 53 be de 91 a0 07 32 71 07 a9 7a a3 da d1 c5 45 e7 3b 93 50 6b 2a 43 bd 97 08 2a d2 3f Data Ascii: z<_tGZd*2HCzy2TgNi"b9vNf-Zipk)jFR,\$6Z_5Z@vn_[FyA_[WvyvSun1CsJ7lxNiEacD)mngF~-1w*;HS2qz E;Pk*C*?
2021-09-16 04:29:03 UTC	1466	IN	Data Raw: 57 79 1f da bb e6 ae b5 4e d2 a7 69 58 22 a1 8c 73 b9 09 4c 63 2a 30 dd 68 18 1d ca 5c 40 1c 54 1b 43 3b b1 5f d6 69 af b6 0e fb b8 af b3 ab 1d cb 2a 83 b9 32 9d 95 e0 96 3a 5d 7b 08 0b fa c1 bd 1e ce 0a e9 7d 3b bb d7 db 99 fb ab eb 6b 39 dc 84 2f a9 a8 e6 bb de c4 20 d9 a7 1b e5 5d ad ad 7c c8 b9 c1 6a d0 7c 73 58 8a 8d 3c a5 45 f7 0e 25 ab 52 b5 33 fb cb 35 98 55 f8 41 f8 e9 c7 a8 c1 12 d1 89 ee 43 9a f2 85 4a a6 5d d3 b9 bd cd c0 69 b5 79 46 a8 9b bd 91 ed 3b 20 15 5b 5d a5 f7 aa d4 74 93 f9 0d 0e 3c 13 49 06 f6 25 c8 90 00 1b 80 8f fe 7d 1f 14 6e f2 09 b4 c7 6d f9 ab e7 bb cd 9f f5 75 3f 2f 3b 55 f4 dc 5a e0 04 11 cd 7d 65 57 bb 99 54 3b c7 8a 95 17 9d e2 a9 82 07 60 7c 95 eb 97 1d bd 98 29 7d 5a a7 80 80 a1 95 1e df 88 5f 6f 4e 39 15 f5 b5 dc ee 0d Data Ascii: WyNiX"sLc*Ohl@TC;_i*2:;};k9/ }jIsX<E%R35UACJjYf; [jt<1% nmu?;/UZ;eWT;)}Z_on9
2021-09-16 04:29:03 UTC	1467	IN	Data Raw: e5 43 75 fb 8d 51 31 bf 66 0b a3 73 9c ed a4 f4 b9 6e cd 34 d3 bc ea 81 b8 d3 0e 8b d1 b6 46 70 ba 17 07 b2 a4 4b 09 ca 4e e2 7e 4b a6 b3 cb cb 2b 07 11 1b 66 08 99 03 04 1e 0f 69 79 31 98 f6 6a 3b 4f 95 eb 7f f1 9e 34 3a e9 21 c3 6e 04 46 d4 48 71 92 23 0e 3b 0f 9a c3 ce 97 3b 20 24 a9 b8 e0 f2 75 a4 f8 40 d8 85 36 e4 30 40 91 e7 8f fa 87 fe 5e 74 2a c3 7c 14 e6 fb e1 35 db 84 af a4 54 07 a0 7b b1 d6 37 43 b7 38 7c 8a 7d 2a 66 a6 34 f6 d2 58 f9 c0 60 e9 fd 13 05 4a 95 0b 8e 26 7e 01 46 b0 99 8c 36 27 53 e9 5d 72 a0 ba eb ae 21 5d 00 c0 c5 ee 7e 57 63 21 bd 3a a7 42 da d0 67 17 66 ef bb 04 20 c7 de 61 e8 71 6b b1 6b 78 08 40 0a ed 81 ee af b7 ff 00 b5 7d bb bc 17 db bb f8 57 db 9f e1 5f 6c ef 05 f6 ee f0 57 e9 9b e6 a1 bb ad 84 42 c5 94 d7 d6 52 70 e5 8a cd Data Ascii: CuQ1fsn4FPkn-K+fiy1j;O4:InFHq#;;\$u@60@^*t* 5T{7C8 }*f4X`J&-F6\$S rl~-Wcl:Bgf aqkxkx@ W_IWBRp
2021-09-16 04:29:03 UTC	1469	IN	Data Raw: 4f 17 02 e1 7c ef 81 99 42 ca 6c 94 2e b4 cb 5e 1b 75 e1 e3 d6 95 63 36 d7 3e a1 e9 24 6c bb bb 2d 9c 14 6d 55 ea 53 6c 53 a5 f5 2d de 6e 6d d0 e7 bf 69 d5 fd 53 18 4d da 6c e0 9c 1b 8b 5b 80 76 fe 25 06 8c ca bb d2 3a 0c 18 4f 6c ea 83 b7 34 c7 d3 71 88 90 54 de 32 ae 55 f1 f3 17 9c 61 5d 10 d1 39 8c d6 d2 a5 a4 82 af 3c cb 8a 80 1b 2e cb 1c fb d4 39 a4 1d c8 c4 63 e2 af 19 cd 4a c7 b5 7b 3d aa ff 00 44 fb 9b e1 5d 28 3d bd fc 50 70 da 3a d2 85 e6 b8 7c 50 ba e0 54 8c ba a7 fd 4d 4f cb ce b5 77 8d 15 a9 b7 3a 35 ea 40 ef 9f cd 3e a5 56 3c 3d e7 09 69 f8 f0 4e 74 74 8f ad 54 33 1d cd 13 97 7a 06 a7 46 c9 f5 5a d1 25 52 e9 1b f5 8f ba 0f 0e 0b e9 14 58 2a 52 da d2 26 ef f2 50 fa 24 71 69 56 2e 80 91 f5 78 4e 18 5e 51 5b 5a eb 26 37 9e 3e 63 f7 c7 54 72 d0 Data Ascii: O B ^uc6>\$l-mUSIS-nmiSMI[v%:O!4qT2Ua]9<.9cJ[=D]=[Pp; PTMOW:5@>V<=Intt3ZFzF%RX*R&P\$qiV.x N^Q Z&7>cTr
2021-09-16 04:29:03 UTC	1470	IN	Data Raw: 24 3e b6 95 31 44 74 6e b5 98 69 a8 f1 bb 15 67 ad e5 06 ba f5 30 48 ad 4e 4b 61 7d 3e ad 5e 8d ef c2 90 dc d1 84 1e 29 ad b3 5a 09 ac f9 bc 66 e8 6b 77 13 b6 51 77 48 1a de 8e e1 a4 60 8b c3 70 4d 35 5d 8b 1b 72 00 dd a2 42 87 0e f5 87 56 e8 18 f5 29 59 6c ec 2f ab 51 d7 5a d0 99 66 64 3a ab b5 ab 54 f6 9d fa 0d 89 f6 ff 00 25 b4 36 be 75 28 8c 9f c5 bc 53 da f6 96 b9 b6 da a0 83 98 cb fb d1 9c d7 94 aa 52 70 0f 16 67 c1 4e 68 cc b6 15 46 b9 b0 4b 10 d7 21 8e 6b 9e e8 f7 77 73 55 6b ba 99 bd 5e a4 cc 6c 0a a3 d8 69 41 a8 71 78 24 88 e4 aa d2 16 8a 4c 0f 74 dc 22 0d 42 0c 5d 64 4a a9 65 a5 4d a2 a5 2a 41 cf 27 0c b6 0e 2a a3 6a 64 ea 51 07 6f 08 4d aa dc 29 d4 98 1e ce d8 4f 96 de 05 b8 0d c5 1a b6 5b a5 ad a7 2e 03 fd ee 44 4e 05 34 38 43 a3 44 94 e7 b5 Data Ascii: \$>1Dtnig0HNKa)>^*)ZfkWQwH`pM5]rBV)Y /QZfd:T%6u(SRpgNhFk!kwsUk^!Aqx\$LT`B]dJemA*jdQoM)O[.DN48CD
2021-09-16 04:29:03 UTC	1471	IN	Data Raw: 4a 9d 17 44 71 e8 a8 f1 e6 9f 64 f2 77 4b 57 a4 60 75 5a 2a ea b1 a7 d9 3b 09 54 4d 92 a8 a0 28 0f ad a4 f2 5b 0c 03 1d 42 31 e6 a9 db 6a da 3e 8a f7 7f 56 22 1b 7a 36 99 cd 55 65 aa 8d 33 5e b3 6e 8a f4 fb 35 36 6b 6e e2 ae 3a 97 d5 53 83 d2 ce 77 bf f4 a5 4e 72 37 94 63 e4 82 07 1c 37 7c 06 1b d3 8b 1e 2e e5 86 ed cb 14 6f 34 ee c7 04 2e 82 30 19 9d bd 53 e5 8b 5b 25 ac 7d db 3b 4e 45 c3 37 f7 6c eb 77 ff 00 7a 0e 2a d4 1d 1f 58 f6 31 be 3a 29 f2 4f b4 d2 61 fa 5d 36 38 b6 3d 6e 05 1c c6 c2 ab ba 03 5e 60 11 13 3c b7 20 e6 e6 13 69 01 76 b9 d5 bc 0c 61 bd 36 8b 5e e7 16 ed 06 04 22 e3 89 26 53 23 d3 a8 4b 80 6c e6 9b d8 e6 34 60 08 1e 29 d0 63 02 b1 41 8c 21 af 2d 20 13 bc ca 14 1c ee 86 93 29 f4 c5 ef 21 c4 17 64 30 cb 24 2d 4e 6b 8d b9 ec e8 e9 dd c6 Data Ascii: JDqdwKW`uZ\$;TM([B1]>v"z6Ue3^n56kn:SwNr7c7 .o4.0S[%];NE7lwz*X1.)Oa]68=n^`< iva6^*`&#=-Kl4`)cAl-)ld0\$-Nk

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:03 UTC	1473	IN	Data Raw: 26 32 36 e0 6d e0 b5 8d 73 9d cc ab 55 a5 d3 bf f2 8d 07 a0 0d 25 53 77 c9 cb 6f 47 39 81 c7 aa fd 3c 77 58 3d 31 75 3d 1e d0 2d f3 29 81 34 c4 c7 34 78 90 a0 86 28 59 84 7c 54 83 47 71 1f b8 5d 2b 38 95 2d b1 ad fe 8a 6b 4c 92 e4 74 54 dd 6b 1c e7 00 01 25 58 f6 0c af a1 98 e1 1c b8 a6 6c 7d 9f 11 1d 4a 9f cd 9a 65 96 16 92 28 07 82 36 4b 39 04 61 07 b9 3f 63 58 64 1d 9a 1e e5 69 d8 76 88 eb d1 f5 c7 ee 88 20 d0 dd 1b dc c7 07 0d 41 a8 56 0b 53 6d 36 56 48 38 8c fc 77 1b a7 a6 71 cd 03 44 0d 7d 03 de d6 34 b9 c7 20 ad 76 c7 4f 27 e5 1a 05 54 e2 49 a3 7e 6a d1 23 20 8e ba b8 e9 54 49 26 bb d0 c3 24 b2 06 34 66 56 cf d9 f0 d9 9a 28 2a ee 24 a7 be 87 24 5e 4a c4 4a aa a9 58 8a da 5b 36 3b 40 c4 da 09 3e a9 ec 73 1c 5a e1 42 10 5e 4e 5b 3a 3b 41 85 c7 aa fd Data Ascii: &26msU%Swog9<wX=1u=-)44x(Y TGq +8-kLtTk%X)Je(6K9a?<cXdiv AVSm6VH8wqD)4 vOTI~j# TI&\$4fV(*\$\$^JJX[6;@>sZB^N[;:A
2021-09-16 04:29:03 UTC	1474	IN	Data Raw: 42 32 02 34 55 09 c6 aa 69 1b 0c 2e 79 e0 13 9e 5c e2 4e a6 e8 bd 6b 33 a7 58 2b 30 eb fc 2f 9b b2 6e b6 7a e7 20 d2 e1 97 00 86 aa 39 a9 da 15 5d 23 7f 94 a7 48 de 48 bc 95 aa 60 a2 80 51 8e 3d c9 f9 d9 c8 e4 6a b4 51 f6 82 6e 83 75 bd 91 bd b4 3d 82 d1 ee 5f f4 dd a6 e6 c7 88 f4 2e 77 37 7d 16 1c 96 15 85 51 1b b0 ad ab 6a e9 24 e8 da 7a ad fa de d3 47 03 c8 ad 99 37 4b 13 1f fc cc 05 1b ad 07 21 74 ce c5 29 3d ea 30 6a 7c 16 aa ab 13 b9 a2 56 a8 37 34 00 0a 07 70 ee 59 60 78 b9 a7 31 e2 a3 3d 51 ba de c8 de da 1e c1 68 f7 4f fa 7a 1d 9d 11 6d 99 83 f2 d5 55 57 34 45 c5 06 ad a7 6e 74 64 c4 cd 78 9d df 27 09 f3 08 33 e7 f5 47 4b ad 07 ac ad 0f c1 11 4d cd c5 34 54 3b c1 07 0c 4a 9c 55 5a 9d 42 9a d2 aa 06 8a b9 a6 1a 39 30 b7 1b ab c9 03 92 1a 28 4e 43 Data Ascii: B24Ui.y Nk3X+0/nz 9 #HH^j=Qnu=_w7j)Qj\$zG7K t)=0j V74pY^x1=QhOzmUW4Entdx'3GKM4T;JUzB90(NC
2021-09-16 04:29:03 UTC	1475	IN	Data Raw: cb e4 a0 f5 41 5a 3b 20 77 de f7 a2 e5 54 53 50 09 ce 45 c8 02 e3 92 e8 a4 fe 52 a2 80 83 52 a7 76 16 a3 78 0a 88 dd 07 a9 6f 86 ff 00 e2 09 c4 37 54 f8 4c 93 38 34 57 0b 9c ea f7 23 b0 a5 d3 18 c5 88 0f 98 c5 5f 04 e6 be cc fa fc 88 d0 a8 a6 2e c9 d9 3a 95 f8 6e 0b 8e 9b 92 4d d7 96 93 5c 91 12 9b 43 4e 32 de b3 ec a9 b6 1c 9b 2d b0 5a 98 1e d7 66 cf c3 4e 14 72 fe c7 7d 8d 8e 6c d0 48 5c 0e 6e 1a 0f 05 65 9a 19 6b 85 b4 75 06 25 17 ab 6f 82 99 d5 75 c7 45 20 70 28 95 55 5c d3 53 8a 20 a8 e1 7b d3 18 18 da 04 05 d6 91 d5 0a 8a 8b 09 29 b1 73 44 22 d4 54 1e a5 be 1b e7 82 da 0e 22 42 08 a8 34 c2 16 c7 b2 be 38 1a fc 27 13 bb 2e 0f a7 fe b4 35 56 2f 3d 75 aa 92 3d 98 5d 51 82 99 0e 40 2d b1 67 7b a3 18 db 3e 30 72 c6 1b 86 9d d8 55 8a ce f8 c5 5f af Data Ascii: AZ; wTSPERRvx07TL84W#_-:nD CN23B)ZfNrj H Hneku%ouE p(U S j)sD"t"B48'.5V =u=j Q@-g >0rU_
2021-09-16 04:29:03 UTC	1477	IN	Data Raw: 85 00 b4 5b 52 61 25 1c 19 e7 72 a6 1d 2e 61 51 75 02 a7 8f 0c 63 bd 58 a3 1b 8a 10 bd 18 9c 17 26 ee c5 1b 0d d4 8d b1 46 d6 56 cb 35 23 30 3e cd f7 37 7c 18 39 41 89 0b f9 2b 8e c4 5d dc 15 05 2e 2f b4 7e 9c 07 b8 ac 75 a9 dc 8e a9 a1 33 44 53 8a ba 63 bb 55 9a b9 30 9e cb 0b aa ab 98 07 73 be aa 7d 06 e1 b8 a8 19 77 28 e2 2e c8 21 13 5a b2 b6 e0 02 0d 08 b7 35 30 4f c8 a0 eb 85 3b 7a 3e e1 cd b6 f8 6a c0 0d 69 1e 68 a1 23 79 78 98 73 c4 f6 8f 99 56 b0 f7 1b 48 da 0f 34 dc ca 6b 2c 82 71 08 ee 09 a8 29 ba 88 b0 be 8e 6b 70 b1 f9 29 87 43 73 77 71 54 63 ed 7c 93 32 68 4e 29 ef 5c ab ae a3 79 58 b2 56 ba 98 59 4c 13 74 44 5c 22 2c 6d cf 7e 9c c6 56 d8 59 cd 54 af 2f af 84 9f f3 5b f5 f7 0e 75 85 d5 74 f8 e2 b5 b8 a8 85 dc 89 5c aa e5 39 8d 41 4c 7a 2a Data Ascii: [Ra9r.aQucX&FV5=0>7 9A+]./~u3DScU0s)w4(.!Z50O<z:jih#xysVH4k,q)kp)CswqTc 2hN)yXVYlTlD ,m ~VYT/[ut9ALz*
2021-09-16 04:29:03 UTC	1478	IN	Data Raw: 02 a8 da 35 53 75 a4 36 ec 19 0d ce 73 5a 2e e2 00 51 7a 47 4b 15 73 63 d5 87 22 e5 88 11 b8 b5 c6 d6 df 74 11 b2 ab 9e fd 01 e7 ba 9e a2 5a 73 78 dd 87 c1 53 6d ee 13 37 cd aa 1a 88 26 6d e3 78 2b 6f 7d ec 7f ca 55 b3 4d 1d 21 bc bd d8 b5 4e 9e 46 3a e1 c5 49 33 e5 37 71 ba d9 4c bd 53 7b 81 28 ef 68 40 a0 73 44 34 ea a6 c1 13 31 17 59 7a ec 64 f6 29 6a 01 ea a2 f7 11 9f 31 dd 63 ce a7 91 91 d4 46 f7 1b 35 af 04 f8 05 b5 3d 3c 82 2e 8d 34 78 9d f9 9c b6 87 a4 1b 46 b5 d7 92 43 6e ce 0b 63 ff 00 0f 8c 9e 37 fa ef 92 26 cb 1b 98 ed 08 b2 a8 8e d2 38 76 15 b0 fd 20 e4 9a 21 a8 3d 1f c2 ee c4 c7 b5 cd b8 37 09 ba 2e 3b 82 27 25 b6 7d 24 8a 16 18 a0 21 d2 76 f0 0b 64 ed 36 cb 4f 69 5d 63 6f 13 c4 2b ef db 95 13 c2 d8 5f 13 dc c7 07 6a d3 65 b2 b6 b5 75 7c 07 Data Ascii: 5Su6sZ.QzGKsc"tZsxSm7&mx+o)UM NF: 37qLS{(h@sd41Yzd)j1cF5=-<.4xCfnc7&8v !=7.;%)\$ vd6O jo+ _jeu
2021-09-16 04:29:03 UTC	1479	IN	Data Raw: 52 fa e7 16 46 48 c4 73 e1 9a d8 11 cd 4d 16 09 0b 59 d2 b8 b9 c9 d7 1a 7f 45 11 07 a4 d2 0d fb 17 a8 4e 61 2f 73 7a 37 b0 07 52 7b 96 d4 a7 da d0 41 8e 2a 37 3f b6 e4 00 07 9a bf b4 62 06 a1 80 61 71 01 ad c8 0f 92 1b 2a 80 7f 75 fd 4a f6 5d 07 f9 43 fa af 65 d0 7f 94 15 7d 44 d4 b3 18 e1 71 6b 00 16 0a 2d b9 59 6c f0 9f 24 76 dd 6b e4 75 9c 1b 87 80 0a 8e b2 4a f7 72 53 01 86 d7 cb 2d 17 b2 28 3f 21 f9 95 ec 7a 0f c8 7e 69 fb 3e 0e 47 06 27 61 03 4b a7 45 ea 30 f2 91 34 92 72 70 3c 15 06 d8 e5 da d0 e8 9c 0e 98 80 c9 1b 29 78 29 fe f4 aa 61 d2 3b 86 a9 8d 41 a8 37 71 28 94 d6 a0 d4 48 68 cc ae 5e 1b f5 82 9e a8 10 43 55 33 31 3f b8 20 37 12 89 58 90 3b aa be 21 fe 3c e3 a2 a0 74 c6 99 c2 43 77 b5 e4 12 b6 b4 72 49 47 85 8d 2e 71 70 c8 2f 46 23 a7 a6 a2 Data Ascii: RFHsMYENa/sz7R A*7?baq*uJ Ce Dqk-Y \$vkuJrS-(? z-i>G'aKE04rp<x)a;A7q (Hh^CU31? 7X; <tCwrlG.qp F#
2021-09-16 04:29:03 UTC	1481	IN	Data Raw: 70 29 f3 0b 0a 74 52 42 2f 8d d4 05 42 e5 95 d3 bc a2 81 c0 88 79 b4 cc ff 00 03 1f e0 63 fc 4c 0f f8 31 fe 6f f3 0f f8 7f cc ff 00 2f f9 9f e5 ff 00 33 fc df e6 7f 87 fc cf f1 ff 00 99 fe f7 f3 cf 3c f6 62 0a c8 0f 92 1b 2a 80 7f 75 e6 7f 85 fc cf f0 bf 99 fe 77 f3 3f ce fe 67 f8 5f cc ff 00 0f f9 9f e1 7f 33 fc bf e6 68 5c 02 92 98 7f 4e 1d 28 74 c9 4a 24 92 6a 86 04 d5 61 40 a7 8c c5 86 c7 72 29 c2 1c e1 7a 44 43 a7 ff 00 4b fb fe 98 10 dc 28 e5 28 0e 65 63 47 97 6f 61 0e c2 e7 1d e2 20 05 31 2d 15 8d 91 3b 4e 16 d9 d9 59 8c 2a c3 1b 80 0b 09 8c 26 a2 a1 8a e9 08 8a 55 ca b0 df a0 5c 15 02 1e 87 a6 61 29 83 2a 10 f5 af 56 26 22 7a 71 93 54 68 fd c2 23 cc 07 a4 48 87 58 25 31 c1 02 97 6c 63 4d 29 bd 61 94 2d 1c 9b 94 1b c2 fc fb 46 92 Data Ascii: p tRB Bycl1o 3?g3w?g_3h N(tJ\$ja@r)zDCK((ecGga 1-;NY*&U a)*V&?zqTh#HX%1lcM)a-F
2021-09-16 04:29:03 UTC	1482	IN	Data Raw: 0e 07 7c 9e 66 20 77 c3 c3 32 5c 0e 11 f8 7f df dd 70 f8 3e b2 c5 27 a3 b7 49 a8 45 d3 93 05 df 86 85 43 71 c3 79 4f 19 46 ae 5b 0c ad dc 49 e3 72 f7 ac 83 a3 a7 bf a5 4b 81 02 cf d0 c4 86 52 ee 2b 0c f6 fe 4b 98 20 ba ec 11 f0 80 3f 2c 73 0d 6c 2b 18 80 91 91 81 f3 ec 40 a9 a1 aa 67 f0 9b 00 b1 7f 7a eb 0a 09 0d 64 aa 0f cc 5d bb 00 08 81 cb 05 03 eb 0c 0d 7b cc 50 74 be 79 3d e1 88 30 f9 d0 eb 6e 49 96 fd e7 8d f6 85 c1 a8 ce 88 e6 bc 3f 78 41 c9 58 f6 e8 c1 22 d0 94 0e 8c dc 44 a5 85 18 5e 2f bc e1 52 29 f5 71 e0 fa 4c ad 50 1d 57 4d 74 43 fc ee 50 fe 18 11 0a 9a 86 71 7e fd 5c 0f 0c a9 63 8e e3 bf 78 37 c7 13 a4 42 a1 95 40 0f 52 cb e4 88 54 57 37 d6 61 da b3 5f 48 e8 85 84 a6 8e ad f2 ce 7e a0 ac c3 b4 5b 8f 54 dd 18 86 d7 72 ff 00 d9 7b 52 da d1 5c c2 Data Ascii: f w2 p>^IECqyOF IrKL@R+vK ?,sl+@gzd {Pty=0nl?xAX"D^R)qLPWMtCPq~lcx7B@RTW%dyY,'O*xlf7?yP
2021-09-16 04:29:03 UTC	1483	IN	Data Raw: 15 18 69 7e cc cc 1c 2c 08 8f a4 e6 60 83 56 7b 0b bb e7 2d 0b d4 47 f1 2d bc 5e 2b 8f 55 93 bc 0c ee d8 ae 0b 8c 65 13 0d 83 25 00 ca 1d 59 d1 31 da 5d 59 d5 8c 8e fd e6 9c 9d a7 c6 74 c2 f2 12 9c 03 a5 37 de b6 99 51 41 a8 d8 3b 9a 7a 30 ce 76 c8 95 74 4d 78 f6 b8 79 29 41 90 bd 07 47 50 02 c1 6c 0e 1b 30 1b 3f 40 c1 0d 8d 24 01 d1 e4 fc 41 71 ef 33 ad 4c b4 ea 66 b8 ff 00 21 ab 3a 3e 49 a0 5c 93 18 f3 c2 64 65 86 42 c3 da 2b 66 57 3f aa b2 ad 29 97 a4 b4 64 ad 19 8b a8 a7 72 cf 30 e1 4b 18 2e e7 b2 41 74 c3 07 81 28 5d 14 ba a0 4a 4e 80 3a fa 47 5a 17 17 17 c1 de 66 54 a2 e5 32 a0 27 a5 4a 9c cc ac 2e fd 0b 81 0d 4d 14 d1 95 fc 4c 6a 00 60 8c 21 a0 61 da b3 5f 48 e8 85 84 a6 8e ad f2 ce 7e a0 ac c3 b4 5b 8f 54 dd 18 86 d7 72 ff 00 d9 7b 52 da d1 5c c2 Data Ascii: i-;V{-G+&Ue%Y Y 7tQA;z0vtMxy)AGPI0?@\$Aq3Lf!:> deB+fw?)drOk.At(JN4GZfT'J.MlJ^ _a_H- Tr R\
2021-09-16 04:29:03 UTC	1485	IN	Data Raw: af f3 16 80 99 ba 3f cb cb 66 58 c1 b7 66 0a 65 cb 21 5e a4 20 1c 3a 65 13 49 ae 8f 33 4c 50 d4 4b e0 b8 0e 58 b8 c3 ca 5e 4d 58 fc 69 ef 15 dc c6 d6 b1 7d 71 7f 89 5f d6 0c 19 18 b1 8b 56 ac 37 c2 fe 8d 94 a0 c7 43 a4 fe f7 a6 fe 7f a6 fe 81 e8 93 37 ea 6e 01 02 5a 03 72 88 4a 21 a2 76 5e 7e 21 b8 96 bc e9 a4 56 0c 52 bc 60 a4 4e 2c 0f 0c 34 15 53 79 10 fe d1 32 53 50 e9 05 c9 8e 3b c0 e2 f3 0b 9c d9 88 57 82 06 ea a5 b5 50 be f7 eb 2d 70 0a c3 b4 34 2f 0b 07 7b 23 53 c2 45 66 dc 40 08 1e f0 6f 32 26 54 25 4a 1d dc 54 10 09 b9 d8 04 c0 03 7b 6c 8a eb 9a 4c 57 3b 81 13 bb 85 f1 36 8b b9 9c 46 52 91 68 f0 07 d6 00 1e 25 c2 d6 b7 6b 02 54 94 69 73 0f 33 1e 22 15 35 40 ca a2 2a 23 d3 2e ba dc ae e6 e9 40 c4 a6 2d 4f 3d f1 04 ae 9b b4 66 77 23 48 3b 3b c5 09 6a f0 Data Ascii: ?fXfe!^ :el3LPKX^MXi q_v7C7nZrJ v^~ VRN,4Sy2SP;WP-p4 {#SEf @o2&T%JT(LW;6FRh%kTis'3"5@*#. @-O=fw##H;;j

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:03 UTC	1486	IN	Data Raw: e2 5e fb 00 23 1f 56 1a c5 54 03 54 bd 7c cc 56 31 ca 14 11 8d 0d a0 ff 00 34 07 18 a0 b8 2f cd 46 85 4d 58 dc 0e 86 7a 47 48 73 ad 80 cb 45 6d 98 73 66 fe 87 30 70 fb 9f 44 dc bf 07 74 8f 27 5c 25 13 09 f3 32 e1 f9 8d 21 7e aa e1 9c 8b 87 09 2e b4 a7 2d 5c 25 44 cf 89 aa 13 ba d1 cb 4c 34 2d e0 09 7e 78 94 83 ae e6 0b c5 db 89 bd 09 93 de cc 7d 62 21 db f6 5f a4 23 70 6f f4 7d 9f dd fe 97 a6 1f a1 f5 21 bf 43 7f a3 88 75 60 01 e8 a4 5d 22 80 28 5e 99 8b 25 03 36 8d b0 19 b0 03 ae e0 67 4e e3 00 33 58 3b f7 88 62 fd a7 12 c7 2c ce dd 75 20 8b e7 02 1b 6c d7 42 15 97 4b ca f6 3c 43 35 05 00 03 1f 58 20 28 cb 67 82 3c 75 25 2e 7a 07 2c c3 62 1c b6 d4 53 48 6c cd ae 00 39 05 ec ae 60 d9 32 00 1f 2e 7e 21 4e 55 2f 07 a5 dd 47 4a e7 87 c3 61 11 44 c9 55 7c 4a Data Ascii: ^#VTT[V14/FMXzGHsEmsf0Pt%\%2!~.-\%DL4~x)b!_#po)!Cu"](^%6gN3X;b,u IBK<C5X (g<u%z,bSHI 9'2.-INU/GJaDU J
2021-09-16 04:29:03 UTC	1487	IN	Data Raw: 65 1a 7c d0 9c b7 19 d5 e9 28 1d 45 b6 17 6f 88 8b ca 57 b4 78 76 81 dd de de 2a fb 15 35 00 d5 f3 63 fc a2 5d e8 9f 70 fe ab f4 3d 2f f7 8f ef 7a 61 41 38 9b 83 99 79 87 ad cb c7 a1 06 a5 92 e5 a3 15 52 c5 be 08 00 25 eb 30 55 aa 72 f8 86 56 42 8f 79 50 16 47 fe 44 1a 96 b1 33 82 ae ac 96 2d 94 59 7e 4f 13 8b fe 92 2f 5a 84 8b a6 af 80 17 ef 2e 11 aa bc ba f9 8a d6 61 41 d7 11 0a c5 06 be da 98 76 ba af 78 21 ed 30 22 5e 20 09 c2 b5 da 55 8c b6 e8 3b 80 27 d0 21 e8 6e 2b 8b ed 4a 01 6a a2 0b bc 16 bd fb 4c 49 dd 50 15 56 5c b1 cc bc d4 b8 67 10 f4 8c 37 1b e5 87 59 c1 f0 7a 3f 08 cd 83 9f 9b 61 2a e1 a8 20 37 3b d9 af cc 6b ca 14 26 d4 3e c8 5b b1 18 6c c3 02 e3 13 82 0d d7 a9 44 52 95 dc 55 c0 0c a5 94 26 53 c4 65 72 a2 be 08 c4 f9 83 c1 38 9b 10 12 d3 Data Ascii: e j(EoWxv*5c)p=-zaA8yR%0UrVByPGD3-Y~O/Z.aAvx!0"*^ U;"In+jLIPVlg7Yz?a* 7;k;>[IDRU&Ser8
2021-09-16 04:29:03 UTC	1489	IN	Data Raw: 72 d9 1d 4c 59 7c 4d f6 3c 6c e0 8a b2 d5 45 a0 ad a3 b4 2e 04 c0 7b e1 ab ba dc 3d 79 47 7d 4a bf 76 11 5d 75 f0 37 38 22 c3 ad ad cf 1a b7 3d d6 5c ba 87 f5 62 a7 10 f4 df f7 7f a5 e9 f4 c1 84 70 4c 3e 84 cc 23 1e 97 e9 71 17 34 99 c4 3f 64 6f a6 3f 88 db e5 a8 f5 b8 25 05 38 15 2f fc 82 72 d5 aa a5 d4 d4 9d d8 5b 1b be b2 10 5a 33 52 ca 38 e3 71 0d 80 aa bd ce a8 de 10 cf cc ab 11 e2 53 03 81 25 0f 77 89 cd 5b a2 2d 01 2c b1 42 73 6b fc 4c 2b 70 f7 3f c4 25 fa 13 69 92 94 c4 e7 3a 85 5f 91 f9 98 50 05 bb 30 2a f7 23 62 c6 e6 10 2a 45 78 cd 8f 78 4b 98 bf 82 ed 97 76 4b a7 b7 13 8a d3 f8 63 60 db 92 b0 42 a8 f3 a6 28 5b 86 3e 54 89 01 f6 96 df 53 fe 4b 76 5d d1 62 f5 94 00 8c 10 2b c7 30 be 2d 2c e0 f3 14 48 76 aa 73 8b 51 09 e5 f0 2b ed 01 92 66 f8 0e Data Ascii: rLY M< E.{=yG}Jv u78"= bpL#q4?do?%8/rM[Z3R8qS%w f_.BskL+p?%i:_P0*#b*ExxKvKc'B([=TSKv b)+- ,HvsQ+~f
2021-09-16 04:29:03 UTC	1490	IN	Data Raw: 13 fe 91 2c f2 80 3c 12 bb c4 81 2a a8 55 1d 17 c6 a6 64 50 35 d8 5f de 63 b2 59 f1 59 97 69 45 2b 09 d4 fd 98 1d 18 3d 99 69 41 ef 0a da d7 99 62 83 e6 62 c7 58 a9 66 28 b6 34 3c 37 04 2e 63 39 9f 63 82 53 c6 65 c3 51 97 89 6e 41 6e e5 be 46 eb 1d 62 86 2d 71 d0 0f a5 42 7d 06 2b 9c c9 0e 12 e1 bd bf 8e a5 be f1 d0 5a 72 77 b9 8e 19 85 d9 e5 97 1d 7f 2b 09 2b 37 86 be 21 0b eb 9b 83 e9 7e 97 17 f7 7f a5 e9 fd 8e 63 62 0e 5e 83 51 59 2e 2d cb fa 5d 41 41 b0 c2 b5 45 7d 65 32 ed 9a 4a bf 05 e6 16 a1 53 47 27 2c f7 eb 10 30 e5 b4 81 be bb d1 29 81 ae 0e 92 bb c8 c2 b6 5a 6c 92 85 1e 84 37 47 35 9c ce bd 10 f0 74 ad f8 95 d5 99 c7 3a 6a 50 35 2d a5 ee b5 ed 12 90 ba 9d 15 c4 4a 10 85 6e 81 62 5f de 61 d0 39 ed 58 53 f3 29 49 c9 5d 43 3f 56 1c c1 b8 30 7d 0d Data Ascii: ,<*UdP5_cYYIE+=iAbbXf(4<7.c9cSeQnAnFb-qB +Zrw++7!~cb*QY.-JAAE e2JSG; 0)Zl7G5t; P5-Jnb_a9XS) C? V0}
2021-09-16 04:29:03 UTC	1491	IN	Data Raw: 5a 1c 25 38 2f a7 66 76 98 9a ce 5f 68 b0 c2 ba 94 f5 0d 30 00 38 59 cf c4 f9 00 75 82 25 9f a8 d7 ee ff 00 4b d3 19 70 7d 33 50 13 9f 0a fc f4 89 a3 df ed f0 46 8a 09 fc 97 42 10 0e 0d 18 4d a9 6e f0 8e 05 40 90 16 39 2b 3e 25 3e 91 91 43 9f 86 a2 2a 51 ae b2 f7 aa c5 21 86 33 55 46 77 1b 5f 31 94 d7 10 36 5a c1 58 0f ac 23 10 2d ed 5e 58 05 c4 e2 6e 3c c5 4c ab 26 55 12 dc 60 90 83 65 8f 10 e1 2b e6 b2 56 92 24 1b 58 1a 6b af 99 54 f2 b6 82 c9 7d f6 67 82 50 e4 52 c4 1d 37 cc bd be aa 9a cb 60 d2 3d e2 e5 7a 5b 3d b6 42 55 87 70 f7 22 23 2f d2 8d d7 80 b5 a6 26 15 89 0d ac f0 1c bd 08 d4 88 8c 44 a4 ce 93 ac a2 d6 13 1c d8 5b e2 63 ae 1e a9 95 83 41 88 d9 83 f9 e8 ad c5 00 f0 e7 31 6c 5e c8 53 d4 e9 55 44 63 92 59 33 92 8f f3 17 db 5a 5d b5 47 11 19 Data Ascii: Z%8/fv_h08Yu%Kp)3PFBMn@9+>=%>C*Q!3UFw_16ZX#~^Xn<L&U`e+V\$XkT gPR7`=z[=BUp`#/&D[c A1^SUDcY3Z]G
2021-09-16 04:29:03 UTC	1493	IN	Data Raw: d4 35 92 5a df 72 e0 3a bd a3 22 9b b1 8d d0 b9 be fc 47 8e 0e 4a c6 44 9b 63 99 8c 5a 62 77 32 0c 23 e1 dd dc 7c b5 2d ae a5 5a bc 5e 18 42 f7 98 7b b7 29 36 d7 ae d1 f1 14 08 15 91 f7 99 17 a0 b7 9e 85 f0 31 05 46 53 bc d2 b6 1f 98 44 8c f3 4e 73 25 83 c6 10 dc 0b d8 c4 43 08 f8 60 16 a0 77 8b c0 3b 62 7a 01 36 06 c8 ba 00 2f 60 6c 7f 89 aa 36 16 32 fd a5 bb 71 1a b6 34 85 8d e6 05 a0 17 03 7a bb 11 19 c1 34 5e 3a 09 cc 0f 1b 04 eb 4b 11 49 8c de 55 e8 fe d9 21 cd 92 ed 5c 86 f4 f4 4d 45 05 0e fa b2 c6 15 72 e8 e0 e9 28 20 25 20 06 b4 6e 65 c4 31 a3 9b a1 1f 00 56 03 f8 11 a9 d8 d4 1a 53 05 95 55 23 51 d4 26 84 4a 67 2a 0c ba 11 59 a6 22 d6 db a8 fe 88 05 1d 7a a2 0d c3 bd 51 53 c3 68 27 6a 65 ed ac cb 1f c2 72 31 66 26 bf ba 2c fc fd a2 65 c2 36 25 c0 Data Ascii: 5Zr:"GJDCzbw2# -Z^B }61FSDNs%C`w;bz6/'l62q4z4^:KIUI!MEr(% ne1VSU#Q&Jg^Y"zQShjer1f&,e6%
2021-09-16 04:29:03 UTC	1494	IN	Data Raw: 09 57 a6 1a 96 ab 6b cf f1 00 2b 74 57 f4 96 2c 7c cd 0f 8b 10 ae 07 68 d9 7c e2 1d 03 93 e5 0c bb 78 39 25 5f 20 54 b3 0e e2 a2 14 02 1e f6 47 72 b1 e3 e8 73 15 3a da ef 1d 06 80 e0 25 5b 31 12 c6 ca 19 6f 1e d0 bc 74 56 37 6f 12 a1 c8 9b 58 ce b5 2c 65 63 d2 96 40 11 40 39 80 23 88 ee 94 07 88 49 41 63 2b d2 62 7b 4b b0 4d 4a 18 65 36 18 87 43 02 a5 f7 49 1d ae 65 8e a3 3a 1a c3 f7 f6 8f b3 7b 3a ac a1 14 45 ba 58 59 ca de ba 12 a7 59 2a 08 d0 c1 84 70 41 6f da 00 84 88 b0 c5 4a bc a1 86 a3 75 a3 da 67 00 9d 2e c5 17 a2 dd 7e ef d5 bf 68 16 20 3a ad 12 8f c3 b0 56 67 56 81 48 7a 5b bf 44 02 08 89 d6 e2 ac a7 2a 63 dd 18 33 ae 31 09 95 40 aa f3 92 2d 2d 6e 18 4e 51 77 1b 21 13 72 af 68 a4 0a 80 a8 8a 70 47 c1 45 aa 00 f7 63 54 93 bb ea 06 68 43 ca 9f 72 Data Ascii: Wk+WV, h x9%_ TGrS:%[!otV7oX,ec@.@9# Ac+b KMJe6ClE; :EXYYpAoJug.-h :VgVHz[D*c31@~-nnQwlr hpGEcThCr
2021-09-16 04:29:03 UTC	1496	IN	Data Raw: 43 0f f6 af dd 24 5f eb 58 b2 d0 ca 16 ee fb c4 a2 f3 5a f8 82 b1 a4 3d ff 00 e5 01 44 a5 af b2 66 1b 5a c2 fb a2 2b 21 0a e2 ec b4 d7 1b e6 34 87 bc 34 94 d8 0b af 78 68 3d 18 24 02 58 6e de 60 39 97 3a ff 00 a4 6c a7 93 03 1a e0 ba 71 02 cf 18 81 c7 77 98 87 b2 37 6f 99 ad ed 7b b0 62 05 4e 20 30 1b 21 a9 74 fb ff 00 52 02 39 6e 67 ef 2f 22 bf bd 65 d1 27 bf 7d 43 b5 d5 63 4a b9 10 1e f7 4c 17 aa 26 d6 1b 4c 2f 9a 97 0c 5c d0 46 92 94 c7 28 1e 85 09 0b 22 d5 b7 66 b3 44 a9 50 1a b4 fa f0 35 6e 17 30 ea 38 16 bb 0b 93 aa e2 2f d3 6b 95 bc 16 2a f7 e3 71 5b 66 6e 04 a6 b5 b9 75 8e 92 b6 c3 2b 00 b1 54 58 cb b0 7a 6e 72 31 f1 05 ca 42 69 9a 57 dc 67 fb 7a 37 0a 9e 7e 03 cc 4a b1 36 46 15 2a 83 69 9e 84 37 48 04 1e 96 60 de 42 e2 90 1c 4e 98 60 02 e0 2a 3a Data Ascii: C\$ _XZ=DfZ+l44xh=\$Xn'9:lqw7o{bN 0!tR9ng/"e"}CcJL&L&F("fDP5n08/k*Q fnu+TXznr1BiWgz7-J6F~i7H'BN*~:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
153	192.168.2.3	49942	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:04 UTC	1509	OUT	GET /entertainment/is-justin-biebers-ghost-about-selena-gomez HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:29:05 UTC	1510	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 43191 Connection: close Date: Thu, 16 Sep 2021 04:29:05 GMT Cache-Control: max-age=86400 content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Apigw-Requestid: FvQysgbVIAMEPyg= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 d9523e44e96d2539081596bb1d268d44.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: 63LKMPIE3CcoaUO_NsKQqzqZB8kWwGsbJtCK2ct0cuy3THrfZYRMj3A==
2021-09-16 04:29:05 UTC	1510	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:29:05 UTC	1518	IN	Data Raw: 64 63 31 66 30 33 61 63 37 2d 67 65 74 74 79 2d 31 33 39 33 34 30 38 37 38 2e 6a 70 67 3f 77 3d 38 30 30 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 31 36 30 30 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 33 2f 31 39 2f 31 64 35 63 38 66 62 34 2d 39 31 62 35 2d 34 37 30 65 2d 61 36 62 34 2d 39 37 62 64 63 31 66 30 33 61 63 37 2d 67 65 74 74 79 2d 31 33 39 33 34 30 38 37 38 2e 6a 70 67 3f 77 3d 36 31 34 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 Data Ascii: dc1f03ac7-getty-139340878.jpg?w=800&fit=crop&crop=faces&auto=format%2Ccompress&q=50&dpr=2 1600w, https://imgix.bustle.com/uploads/getty/2021/3/19/1d5c8fb4-91b5-470e-a6b4-97bdc1f03ac7-getty-139340878.jpg?w=614&fit=crop&crop=face
2021-09-16 04:29:05 UTC	1534	IN	Data Raw: 6d 65 7a 2e 22 2c 22 73 69 74 65 22 3a 7b 22 6e 61 6d 65 22 3a 22 42 55 53 54 4c 45 22 7d 2c 22 68 65 61 64 65 72 22 3a 7b 22 69 64 22 3a 22 36 37 30 30 30 34 37 36 22 2c 22 74 79 70 65 22 3a 22 68 65 61 64 6c 69 6e 65 22 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 74 72 65 61 74 6d 65 6e 74 22 3a 6e 75 6c 6c 2c 22 65 66 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 7 5 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 69 6d 70 6c 65 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d Data Ascii: mez:","site":{"name":"BUSTLE"},"header":{"id":"67000475"},"card":{"id":"67000476","type":"headline"},"settings":{"treatment":null,"effect":null,"palette":null},"palette":null,"variant":{"simple"},"fields":{"headline":{"version":"0.3.2"},"markups":{"atoms":[]
2021-09-16 04:29:05 UTC	1545	IN	Data Raw: 73 65 6c 65 6e 61 20 77 68 65 6e 20 69 74 27 73 20 61 20 73 70 65 63 69 61 6c 20 73 6f 6e 67 20 66 6f 72 20 61 6c 6c 20 74 68 65 20 70 65 6f 70 6c 65 20 77 68 6f 20 73 61 64 6c 79 20 6c 6f 73 74 20 73 6f 6d 65 6f 6e 65 20 64 75 72 69 6e 67 20 74 68 69 73 20 70 61 6e 64 65 6d 69 63 2e 20 70 65 6f 70 6c 65 20 68 61 76 65 20 6e 6f 20 72 65 73 70 65 63 74 20 65 76 65 6e 20 69 6e 20 73 75 63 68 20 73 69 74 75 61 74 69 6f 6e 73 2e 22 2c 22 70 72 6f 76 69 64 65 72 4e 61 6d 65 22 3a 22 54 77 69 74 74 65 72 22 2c 22 77 69 64 74 68 22 3a 35 35 30 2c 22 68 65 69 67 68 74 22 3a 6e 75 6c 6c 2c 22 74 79 70 65 22 3a 22 52 49 43 48 22 7d 7d 7d 5d 2c 22 65 79 65 62 72 6f 77 22 3a 7b 22 70 61 74 68 22 3a 22 2 f 65 6e 74 65 72 74 61 69 6e 6d 65 6e 74 22 2c 22 74 65 78 74 22 Data Ascii: selena when it's a special song for all the people who sadly lost someone during this pandemic. people have no respect even in such situations.,"providerName":"Twitter","width":550,"height":null,"type":"RICH"}]],"eyebrow":{"path":"","entertainment"},"text"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
154	192.168.2.3	49944	151.101.14.208	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:05 UTC	1552	OUT	GET /uploads/getty/2021/3/19/1d5c8fb4-91b5-470e-a6b4-97bdc1f03ac7-getty-139340878.jpg?w=800&fit=crop&crop=face s&auto=format%2Ccompress HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://www.bustle.com/entertainment/is-justin-biebers-ghost-about-selena-gomez Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: imgix.bustle.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:06 UTC	1564	IN	Data Raw: ab d3 68 b8 a8 fc cd 9a 53 0f 74 59 df 10 36 08 b5 7d 6b c5 a9 26 9b 47 a9 f3 2d 68 7d 00 a7 be 5f e7 5d 32 fd 39 7c 39 9a 56 55 5e 62 45 4f bc 55 c9 83 51 09 8b 54 23 3e 9f 11 3f 8b 84 b0 2e aa 51 8c 58 20 65 c6 79 19 e7 7a 1f 75 ac 1b 99 b4 16 32 ab 46 25 dd c9 ad 18 da 52 74 47 e8 15 eb 63 d8 65 32 f2 d3 d2 ce 57 63 1d 19 19 84 40 bd 17 1f b1 15 ec 3c e9 f0 d0 8d 8f 17 2e 9a 6d 24 bf 7a 41 77 2b 8b 73 36 a1 91 51 f6 55 c4 8f d5 57 d4 45 5f 11 fe 58 99 f0 ec 2d 95 d8 24 09 bc cb 4a e2 ee 21 ac 11 82 07 0c b9 4f e1 db bb d0 fa 9a dc cf 94 e5 11 18 15 1e 41 2b 35 db 07 1f bd 86 de f7 f5 a0 7e 51 33 35 31 2c a2 89 c7 30 83 f9 f5 03 cb 51 19 13 56 cd c4 6d 48 b8 48 73 8f 1a 70 a4 74 f2 5d cf be 1f c6 5a 39 e2 8f 73 9f cf 45 a6 5f 2c 8c 20 bd 8d c2 f3 24 f1 Data Ascii: hStY6}k&G-h}_J29]9VU^bEOUQT#>?.QX eyzu2F%RtGce2Wc@<.m\$zAw+s6QUWE_X-\$JIOA+5-Q35 1,QQVmHHspt]Z9sE_,\$
2021-09-16 04:29:06 UTC	1565	IN	Data Raw: ae c9 d5 fa 55 ba 5f 43 75 8f 89 6c 36 f2 3c e2 01 7a 43 c0 36 6c 6e 89 03 38 a6 a2 07 49 74 69 2d 20 f0 c0 3c fd ac 10 69 b3 f5 36 59 89 de 96 da db 78 c4 b4 f3 99 36 d3 71 86 92 cd 3b b2 8b ab d3 c2 97 5d 45 50 a9 56 7b 05 81 25 ec 76 25 eb 61 1a 9e 5e f6 e2 75 3d 21 cc 69 3a 08 11 07 2f 18 f7 42 97 21 ef 13 d9 2b 61 32 3c 6c 38 08 68 0e b1 41 ab 5a 5c f6 8b 1e 2b 1a 09 e0 f4 e8 de 8e c0 f9 e1 e4 5a 5c 51 54 ec f3 99 ea b6 cc 90 66 85 0e 1d 26 ae 16 5b 0d 79 3c 50 47 65 d2 8e d8 34 f5 b6 6c a5 bb b4 a7 b0 9a ff 00 57 08 bc e9 27 4d d1 25 26 81 fe 4a 10 4a 21 44 f8 d2 47 a2 91 57 98 9a 1d bd 0d 78 a7 d8 49 96 da ac 53 aa 75 71 2e f4 59 ed 64 78 5e 93 11 99 ba 6b 48 fa 53 54 5a e2 bc b7 4a d9 46 e0 58 1e a4 3e 83 15 b9 8d 7e 6b 4d 4f 50 d9 06 59 2c 14 cf Data Ascii: U_Cul6<zC6ln8lti- <i6Yx6q;]EPV{%v%a^u=li:/B!+a2<l8hAZ!+ZlQTf&[y<PGe4IW%M%&JJ!DGWx!Suq.Yd x^kHSTZJFX>-kMOPY,
2021-09-16 04:29:06 UTC	1567	IN	Data Raw: 50 c0 59 0d 0c 9b 2b 1b 5b ec ae 35 91 9f 51 cc 35 72 4c a5 b3 15 62 59 47 34 98 52 04 4b 59 f1 63 21 da a8 f9 56 3b 54 bc d3 20 00 cc 1c bb cb 7b e9 30 61 84 b3 97 39 86 be 17 c7 b1 65 36 6c 94 51 54 f6 75 d2 af 89 0e 24 96 1d f3 ad ec 2d 98 b6 46 e7 da f9 d8 2b fb 4d a2 50 e1 09 ed c8 52 79 e6 a7 61 0d 96 75 e2 6c 92 41 73 ac 47 24 e7 40 8a 48 f2 e7 78 90 e7 14 87 d2 35 54 59 16 f7 76 e8 2a 99 93 54 35 f2 f4 0d 4e 4c 31 da c1 97 01 67 41 21 24 6c f1 59 32 06 e9 59 aa 3f 66 db a7 84 68 43 17 52 d5 a3 97 a1 57 92 e9 ee d7 a7 5a 46 af 98 ce 73 da 80 32 e3 3e 39 c1 34 8d 8d 22 e2 c6 4a 42 ee 7a c7 3b 87 d1 ed 05 91 14 c6 4d 62 82 09 37 bb 8a 2d 92 1e 0d 87 78 da de 33 5a b0 a5 3c 25 91 12 43 87 86 9b b0 dd 45 af e9 72 6b 6a 36 34 89 27 57 76 d7 0f 55 d6 2e Data Ascii: PY+[5Q5rLbYG4RKYc!V;T {0a9e6lQTu\$-F+MPRyaulAsG\$@Hx5TYv*T5NL1gA!\$IY2Y?fhCRWZFs2 >94"JBz;Mb7-x3Z<%CERk]64WVU.
2021-09-16 04:29:06 UTC	1568	IN	Data Raw: c6 98 7d 45 85 57 59 6a e5 6d 5f 92 19 22 31 c9 d8 71 65 e0 ba c4 64 69 00 ca d2 7f db db 77 18 f5 d3 29 58 e0 ac c2 d4 70 a0 29 ea 15 fb 8d d0 82 ae c4 cf 1e 92 cd 50 45 b1 d8 46 f6 ac 5c 12 e4 c2 58 e6 16 4b 65 be 3c c3 07 78 b3 36 c4 bb ec 14 f3 44 ba cc 87 b1 6f bf d8 ac 52 1d 65 f0 d5 b7 4c c5 cb 82 17 f2 df 85 1c 34 4c 78 0c 31 bd 19 5d 3b 15 b9 3a cf f7 6b ff 00 d0 3f cd b1 b0 fc 0f 80 7d e0 ce 3e 3d 61 c1 f0 7d 61 f8 23 e5 46 05 f8 1f e6 70 e7 1f e6 3e 39 f8 38 73 9c 66 cd 82 ab e5 88 ca e4 b6 e4 52 6e b1 87 45 b6 48 d7 74 51 9e 19 83 1b 70 08 d2 17 ee 92 78 cf 0a ec 93 4f 7e 56 68 a2 21 5a 79 17 0d 97 73 18 0c 9e 3e d1 67 c9 ce aa 42 a3 eb 7b 9e 69 89 7d 25 72 5a da fa 96 c2 85 8e 54 68 4c cc 26 b0 ca 85 d7 cd 94 28 7b 96 2e e4 ba e7 be bd 31 2d Data Ascii: }EWYjm_ "1qediw)Xp)PEFXKe<x6DoReL4Lx1];:k?}>=a}aFp>98sRnEHTQpXo-VhlZys>gBf{}}%rZThL&{({.1-
2021-09-16 04:29:06 UTC	1569	IN	Data Raw: 62 25 c1 7e a0 c1 b1 a2 c4 32 90 0e 73 f0 4e 77 0c e7 0e 1f 81 83 06 5a b7 1c 11 ef fa b2 49 0c 92 bc 8d f3 5d d1 5e 8f 50 eb 21 1a bd ef 4d 99 7a 93 6d a4 69 89 ac 5d 65 85 62 96 cf 91 bd 96 91 a5 4c 79 24 2b 14 6e d9 02 c3 1e 1d 83 9c ad 2c fd d1 c7 2b 09 e7 ed 64 96 79 02 25 33 93 52 ee 74 d2 2f 32 eb 12 38 cd 4b 7c bf 9a 30 96 e2 0c ca 92 30 a7 14 b9 6b 59 28 c9 2a 71 28 72 32 f4 65 24 8f f5 27 b9 aa 1f 47 af d7 cc 5a cd 79 94 eb 74 b0 cf 34 9d 3b 40 c1 b8 ac f5 2c 41 e4 95 ac 50 6e 29 d2 59 5b 5e 9e 2b 81 64 33 4c 88 96 ae b8 92 79 22 55 9e fd ae 46 b1 47 0b 23 a1 86 75 5a ba 25 47 9b a9 48 fa 44 43 de 1c 2a ab 7d e2 4e 4c 3c 01 66 46 c1 3f 02 42 4b 44 84 e3 c2 32 1a 4e 72 44 31 e6 97 dc f5 47 e9 7f 89 18 f8 dc e3 13 85 f8 16 ba 87 5b 01 b3 d6 30 64 Data Ascii: b%-2sNwZl]*P!Mzm]ebLy\$+n,+dy%3Ru/28K]00kY(*q(r2e\$GZyt4;@,APn)Y{^+d3Ly"UFG#uZ%GHDC*)NL<F? BKD2NrD1G]0d
2021-09-16 04:29:06 UTC	1571	IN	Data Raw: f8 aa 43 21 02 28 fb eb 4c bc 9f 19 03 c7 81 7b 71 00 26 6b 9c c4 bc 12 88 a3 1e 27 0c 92 7a 8e 4a c4 c6 8a cb 2d 79 bc 8f 59 c6 56 93 bb 24 e1 13 59 b6 92 26 9b 46 93 47 e0 ec b1 3d 39 23 96 bc ae b1 47 e2 63 67 5e 9e 4b d4 d5 31 1f ee a9 af 32 99 eb a0 6f ed 82 28 20 b6 ef b0 dd 54 89 e9 80 cb 91 b1 ef d7 5b 6a d9 5a bf 7d 78 d3 ba e4 11 57 8a 3b e6 ac cb ad a8 b2 d9 bb aa f1 96 aa 79 62 c3 21 86 42 6a c0 62 cb c7 b6 3d 37 29 76 ec 62 74 b7 0f 80 56 a4 64 ce d5 18 d8 d1 8c ae bc 22 48 04 f5 af 46 63 b2 11 8c eb 90 51 91 ce aa a3 47 2d 53 fa 7f 2c 78 ce a1 da c7 52 a7 99 e5 91 11 a5 c4 86 34 52 30 7e 78 e3 3b d3 95 f6 d0 2f 76 32 af 74 81 57 25 8c bb 4b 02 01 dd da 74 bb 2b 0e 36 fd 38 e8 4f 74 6d 13 86 c8 9d 8e 17 90 22 b4 72 99 15 e3 3f dd ac 0a 72 7b Data Ascii: C!(L{q&k'zJ-yYV\$Y&FG=9#Gcg*K12o(T]jZ)xW;yb!Bjb=7)vtVd"HfCQG-S,xR4R0-x;lv2tW%Kt+68Otm'r{r{
2021-09-16 04:29:06 UTC	1572	IN	Data Raw: 0f 19 d5 84 89 c8 c3 e8 c2 d9 23 fe a7 f3 da 8c 88 bc 04 5e 63 29 f6 1f 59 5e 2e f5 fa 20 f0 0d 6a 84 1a b0 cf af 80 85 93 55 dc 25 d5 96 1f db a5 46 8e b8 ca 94 96 22 d5 4f 16 3b f1 27 95 72 ae d2 68 65 b3 e2 99 36 68 e9 26 ae f4 87 36 5c c5 b0 d4 ec c4 c7 a9 ec 44 c2 39 d9 5a 98 31 d0 f6 e2 e4 9e 2a f2 92 57 5d dc 32 a5 33 6a cd 7e 8f 6c 9b 4a f0 59 ab 0a 44 6f 59 42 93 7b 69 2a 71 9a 87 70 2b 59 ef 9e d5 52 d3 df ac 04 50 c4 59 b4 d5 4b e5 fd 3a d6 b4 ee 8d 35 1f 01 17 5d a2 89 c2 f6 a3 f6 bd 86 53 17 67 ba f1 e4 76 bb 21 b6 cc e7 b7 dc 6b ef a6 b9 e6 2f db 9b bb 9f 4b 42 dc ed 3d a5 93 b7 04 bc 02 e7 9e f5 18 cf c9 50 49 50 30 37 a9 2c fa 03 03 1c ef f6 ae 79 8b 96 c8 c3 02 a1 d8 46 dc 61 59 08 00 09 74 bb 10 6a ef b5 94 64 13 c4 a2 4f 34 a8 63 b7 60 Data Ascii: #^c)Y^ .jU%F"O; rhe6h&6lD9Z1*W]2j]-lJyDoYB{!qp+YRPYK:5]Sgvk/KB=PIP07,yFAytjdO4c`
2021-09-16 04:29:06 UTC	1573	IN	Data Raw: 1e 5f b1 e4 a5 60 76 b5 5b 2d 5a ce be d2 cd 03 0e 70 c7 c6 75 a5 3f 15 87 38 a7 9c 58 b9 3a ba 65 a3 8a 35 0a 59 83 42 ab 2c 70 d4 6e 12 a1 06 bf dc b0 28 e6 18 65 39 5a 1e dc 41 8b 8a fe fb f0 3e 77 e7 76 73 85 b3 91 8c 57 25 ed 39 d5 b1 8e f8 58 fd 2c 28 60 9a f7 7d 88 ef eb 95 87 d0 76 db 96 26 10 bc 3c 3c f5 0a 65 76 44 96 93 a7 d7 5d 81 7b f6 34 3b 23 57 f6 23 92 77 8f 67 2a 57 5b 28 61 9a c2 3e 24 31 ac 34 9b ef bb 3b a4 08 86 5d 78 78 4e 6a bc 72 d3 dd 52 11 37 4e ea 1a c4 97 b4 9f 4b 91 42 c1 97 bc 61 f6 25 6f be 23 c6 39 0d 0f 8f b5 a4 94 86 82 3f 3a 51 b0 b5 f2 4b 2b 2b 77 7d 83 f7 49 9c 60 18 33 9e 3e 3f 39 14 5f 6b cf db 85 d8 98 7b 32 28 a3 38 89 08 ca 9a d8 9d e9 e8 94 14 e9 c8 1f 22 e9 bd 70 c8 b4 f0 a6 51 a0 90 08 87 b8 ff 00 03 8c 67 c9 Data Ascii: _\[-Zpu?8X:e5YB,pn(e9ZA>wvsW%9X,(')v&<<evD]{4;#W#wg*W[(a>\$14;]xxNjr7NKBa%o#9?:QK+ww)! '3>? 9_k[2(8"pQg

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:06 UTC	1575	IN	Data Raw: ca 75 75 7e 2d 42 df 7c eb eb 9e e5 71 9d 05 71 a6 d4 8f 8b 90 79 25 34 cf d4 59 af 24 59 32 73 1e b6 c3 c3 26 b5 81 c8 5b 8c 87 ee c4 ad ea 4a 64 e3 d6 65 4b fa 9b d7 6c 6a 74 95 2b c3 3f 4b 99 62 d3 6a 65 a5 35 9d 1a 4d 27 d0 c7 e0 8e 2f 1c 94 df 24 f6 bc 92 a5 25 07 f5 f1 62 90 e0 4e d1 6b dc 73 bc e2 e7 d4 da 8d ed a5 bb 28 7c 91 49 4e b1 99 f7 50 af 87 5f d3 e1 a3 da ea 8c 2f 20 66 3b 16 ee 97 a3 e5 ec b5 b8 8d 66 a7 3d 5e d7 d6 ca 63 9e dd d1 f4 d5 ec d9 82 4a db ab 7c 4b 19 63 42 e1 af 3d 81 5e c4 29 d3 f1 4a b6 28 35 49 28 f8 de a5 ab 0e 6c 57 97 b2 b4 fd f6 59 1f 81 2c fc e3 0e 56 c2 f6 e4 2c 5b 0c a1 d2 64 96 26 ef f2 61 8d 8e 78 3d aa 15 c9 23 63 8d 2a 3c 2c 99 a2 a8 bf 8d 2b 6b 2a f9 37 5d 3a b2 26 cf 58 5a 27 ac fc b8 3d 9d cd 95 e3 f7 d3 da Data Ascii: uu~B qqy%4Y\$Y2s&[JdeKljt+?Kbje5M/!\$%bNks([NP_/ f;f=^cJ KcB=^)J(5l([WY.V.[Ad&ax=#c*<,+k*7):&XZ'=
2021-09-16 04:29:06 UTC	1576	IN	Data Raw: 32 cc 4a 82 db f3 35 69 3f 4e dc 95 e1 86 3b 1f 53 3b c4 8c d6 e9 81 4a 96 b6 82 eb 52 a5 68 e3 ea 1b 3e 31 fd 34 df c1 7a 88 86 5a e7 e9 16 5c db 57 b7 52 cd ba 0a f5 64 ae c8 6a 0e 0e b1 7b 44 67 d2 9c 8f 23 38 b8 54 1c 96 bf 39 77 5b 1b 64 da a5 02 5d 2d 26 8f 5f a3 ac 0c 31 85 8e 48 86 55 5c b8 9f a7 3c 1d f1 6e fa 30 ac b7 68 4b 13 3f 1d e1 ca 3b 76 94 56 e1 a4 4f 6a 59 0e 87 7e 2e 53 99 52 4b 33 6c e0 84 6a f6 eb 3d 9a c9 ca 5b a8 19 b6 f0 78 2d 23 fd cb ef 2a 37 02 bc 99 59 b2 23 91 b6 09 3d 4d 2e 4e 79 4f ab 6a d7 e3 b5 13 c5 6a f4 10 8a 5b e5 e4 ed e3 11 d4 b1 35 b9 1a 2e 62 8c f6 ba bf ab 4f c2 5a a2 7c fb 2b ab 62 6d d2 25 61 29 56 1a 0b 7c c4 48 2b d8 67 1b 68 3c 52 ea b7 4f 0d b7 bf 5e e5 5d 1a c9 03 d9 af 5f b3 6b 6e 51 9d 31 b0 9e 3c 5a 88 Data Ascii: 2J5i?N;S,JRh>14zZ\WRdj[Dg#8T9w[d]_&_1HU<n0hK?;vVOjY~.SRK3lj=[x-#*7Y#=#M.NyOj][5.bOZ]+bm%a)V H+gh<RO^)_knQ1<Z
2021-09-16 04:29:06 UTC	1577	IN	Data Raw: 86 dd 15 e6 c4 36 23 31 5f b7 4c 8d 9c 17 b5 ab 21 59 ac 72 ef 76 13 14 88 8c f2 6a a3 92 39 36 37 18 8e e7 39 4d c7 32 ba a6 41 b7 95 63 15 fb f3 6f 29 5a af 9f ca 89 cc 9d 07 55 46 a3 43 4e 26 ea 8f eb 09 e0 25 a8 7c 2d 39 f3 79 47 69 fe de 5c f2 32 bf 90 b2 4b 17 ab 0d da 3b 8f 70 9d 86 2c 80 e5 71 c9 3f a7 af 5f 52 18 47 33 c4 23 c4 f4 11 4f ed 11 2a fd 34 8b e2 bb 5d 9f c8 1f d4 4f 91 71 8a b8 41 c0 71 1c e0 7c 32 67 93 21 5c db c1 3f 60 dd c7 0a 7f cc 6b 65 6d d8 9f 2b ec 4b 29 b3 e5 91 a4 e3 37 9b 38 e9 eb cc cd 66 5d 72 f8 9a 7b 31 b2 cd da 4c 75 c7 6e a2 28 d6 de ce 4b 35 e3 bd 76 69 06 b7 67 ce 6a 6c 24 3a cd e6 c5 ac 85 f3 19 e7 88 19 b5 0f f6 c0 dd af 09 c8 1f 23 7c 89 b3 5b 33 1c 63 c1 91 b9 16 22 e1 d6 dc 8b 95 b6 56 13 2b df bb d8 6e db Data Ascii: 6#1_L Yrvj9679M2Aco)ZUFcN&-% 9yGiL2K;p,q?_RG3rO0*4)OqAqJ2g!/?~kem+K)78f[r]1Lun(K5vigjl]#:[3c"V+n
2021-09-16 04:29:06 UTC	1579	IN	Data Raw: ae 84 fd 0b 86 89 95 69 ca 22 fa 74 55 a5 5e 7c 9f 5e 18 6c 2a 78 5c 48 09 a2 d1 f6 cc 89 28 64 74 31 d8 78 8a c9 e4 cb 0e 4c b5 a0 9e 7b 54 8f da b9 24 2a c3 b6 58 b2 ad fc ab 75 0e 47 38 38 93 64 52 64 2f 91 b6 23 ae 72 b8 72 43 9d 61 7d 60 a1 b5 45 fe e1 5a 4e 64 76 bb 4d a1 ea 89 fc 3a ba 24 cd 7b be ce 55 8c c5 27 d5 04 5a fa da ef 08 49 44 40 d2 11 43 66 b4 8b 9a 7b 12 45 b0 d6 b8 7a 9b bd 42 d8 b5 26 b5 62 a9 52 89 b3 35 ad 3c d1 e5 66 60 fb 3d 9b 08 63 12 5c ab 26 ae e3 4d b1 d4 de a8 9f 1a 4f fe fe 90 62 29 d9 63 db fd 44 20 ee 21 ee 67 91 bb 22 40 4b 38 55 46 7f bd 47 d9 67 bb c9 5d fb 72 16 69 0a 1f 11 d5 c3 e4 8a 3a 88 d9 5e 9a c5 25 c4 12 45 b0 a6 66 b4 34 e8 89 46 e4 b4 a7 d2 19 20 8d 36 11 c0 a9 6e cc b5 ad 19 99 ac 06 71 62 1e d2 dc 83 04 Data Ascii: i"iU^ *^x H(dt1xL{T\$*XuG88dRd/#rrCa}'EZNdvm:\${'U'ZD@Cf{EzB&R5<f=c\&MOB)cD g"@K8UFGGjr i:~%Ef4F 6nqb
2021-09-16 04:29:06 UTC	1580	IN	Data Raw: 71 83 70 a3 13 77 17 16 ba 86 04 89 b6 27 7d 9b ad 79 a7 74 60 0a 73 b4 03 5d a2 88 ac e5 56 69 e5 b5 2d 4a 88 86 0a d0 97 d9 5a ae 8d 66 5e f2 65 e0 12 e7 0f c7 38 b9 27 b4 5c d0 44 cd d2 b5 31 17 17 38 e7 24 af 8c 9e d6 3e 4d 6a e3 2b 41 ea 25 e7 22 4c 5e 00 c3 9b a9 38 83 61 60 24 73 8e 05 c3 da f1 9e f8 67 5c 91 3e e4 1c 60 1c 1f 40 86 1f 1c e1 ce 7e 3d 67 68 c3 10 c3 12 e1 84 61 85 30 d5 8c e4 95 fb 03 44 93 20 85 95 f4 76 2e d7 c5 ea 4d ac 6b b4 ea 8b b2 45 7b 69 66 65 e0 13 e2 1d 92 46 a8 1e 5e 5a 45 39 12 e3 1e d9 00 e4 fb 03 5d 0f 96 5d 18 48 a1 88 49 66 58 2b 81 8b 16 2a 7a 48 c6 04 19 22 67 60 ea a6 71 f0 cb 93 af db 66 20 0d 85 cb 2d db 91 27 ad 5d ea 73 d7 c9 6c c3 10 86 64 9d 3c 31 64 d2 d6 47 ea 1b 70 2e a3 a1 ed c2 f5 3a d0 44 2f f1 c9 87 Data Ascii: qpw jyt's Vi-JZf'e8\DI8\$>Mj+A%~L^8a '\$sg > @~-=gha0D v.MkE{ifeF^ZE9J}HifX+*zH"q qf -]jsld<1dGp:~D/
2021-09-16 04:29:06 UTC	1581	IN	Data Raw: 3c 70 ee 3a 83 6b 04 f6 6c 6f 64 88 39 96 57 58 b9 c4 83 12 2c 09 eb b7 08 38 71 94 f1 c6 4b 17 38 60 71 84 38 c8 3e e9 00 50 38 f4 a3 2d 27 a1 e8 ae 43 39 19 d3 7d 79 b0 d7 e6 a3 b9 e4 bd 89 b5 34 23 af 15 78 31 13 15 31 57 33 71 96 66 01 7a b3 a9 9a c4 8c df 1d 9c 00 a0 e6 c7 5e 86 9e e9 0a 5c 81 f1 4e 0c 3f 2f 83 f1 c1 ce 30 7c 13 87 9c e7 09 3f 1c e4 df ea a9 fe 9a bc 73 5e 6f 15 ab 97 21 58 a9 54 a7 62 9d bd 64 3e 15 e7 19 4e 20 20 cd c9 55 ee c5 8c e7 47 69 0a 0a 90 80 23 e0 62 1c 41 8b 80 e7 7e 06 e7 e3 9f 93 9c 0c 31 e1 41 85 72 d4 67 8a 84 76 4c a1 90 d7 fb 65 ae 06 58 a8 ac b7 68 f9 63 bf ad 31 dc d7 5b 73 89 f6 45 04 02 3b 3b 8b 89 35 b5 87 12 01 8b 10 c5 5c e3 00 c3 9e b0 8c ed f4 cb c6 11 87 04 7d f9 14 29 1e 0c e3 14 64 cb f6 cc bc 3a 9c Data Ascii: <p:klod9WX,8qK8"q8>P8->C9 y4TxxW13qfz^ N?> O]?s^o XTbd>N UG b#a~1ArgvLeXhc s[E;5])d:
2021-09-16 04:29:06 UTC	1583	IN	Data Raw: c9 60 da f6 1a b6 58 c7 ab ea 74 dd 50 6e 59 61 c6 c3 13 21 3e ff 00 81 f2 47 b3 cf c1 fc 36 7e 73 b4 67 19 c7 c4 7f 9b a7 9b 35 c7 da aa 73 db 48 8d c6 69 da 27 ab b8 95 3b bf 03 b8 7f 6b ea bd 89 b5 34 23 af 15 78 31 13 15 31 57 15 70 26 78 f1 93 1e 3c 20 8c ea 2d 1a 6c aa eb ed 5a a5 69 9b bd 8f 76 43 63 83 47 7d 7a b6 51 ea 3a 56 33 b8 10 c7 da b1 c3 ec 29 cf 5c 11 84 63 8c 6f c3 0c 4c e3 19 73 a8 f4 c2 dc 23 90 63 90 10 ca 41 dd 6a 96 e5 73 dc ac 0e 73 f3 ce 73 9c e7 ec 97 d3 27 c0 f8 43 ec 7b 17 6b 77 a9 04 10 78 cd 4d f0 99 3d b4 ec 7b fc 64 96 99 f2 8c 4b 36 47 5a 04 5e 62 e4 ac 27 2c d3 8f 87 56 86 4a 73 43 62 2b 92 03 84 0c 77 e2 3e 9b 8f ec b6 73 60 3f 4e 16 e5 62 fc 82 38 38 3f bc b7 c1 c3 f9 44 f5 fc f1 84 7c 45 92 1e fb 10 0e 14 92 12 2f 41 Data Ascii: `XtPnYal>G6~sg5sHf;k4#x11Wp&x<- ZivCcG)zQ:V3)coLs#aJss\$C{kwX=[dK6GZ^b'.VJsCb+w>s'? Nb89D E A
2021-09-16 04:29:06 UTC	1584	IN	Data Raw: 13 8e fc 91 20 18 5c 91 ff 00 ae d2 44 a1 c0 e9 c5 ee b5 cf bd 9b 7e b4 9f 8b 63 ee 84 fa 87 f0 4f c7 f2 79 c6 f5 8d 91 7e 17 f6 ff 00 3f c0 c8 35 d6 ac 61 e9 7d bb 47 2d 3b 15 a4 5c 6c 3c e2 8f 6a 3d 49 9d 23 b2 92 96 8e 8c 5d f3 d7 4e d5 a8 b9 0a 64 39 10 f5 17 e1 32 3e 3e 0e 1c 6c 61 84 60 cd ac 5e 4d 7c 3f eb 89 bc 77 a4 3c 63 8e 0c f0 87 58 25 6a 73 1e 19 54 e4 b1 23 ab 43 3d 47 ab 6e 39 97 81 f1 f8 c5 90 1c a1 b3 9e a1 d7 de 82 cc 69 ec 71 9c 67 18 57 19 46 75 4e ad 2e eb 75 b2 b5 7d 82 fb 04 66 f7 57 f5 30 fc 0c e3 e6 5e 54 a3 72 38 f9 fe 62 c6 19 ac 98 36 e4 c9 66 d2 39 51 22 d9 b6 3d a6 39 19 44 9e 57 e4 85 cf 18 ce dc 68 c7 2b ef 1a a0 29 d3 f1 aa 05 03 2e bf 36 5f f1 70 65 7f db 07 e0 fe 0e 7e 30 1f 6f 84 fb 1e a3 ff 00 c8 19 0c 52 4d 24 1a 85 Data Ascii: \D~cOy~?5a G-; l<j= # Nd92>> a^~M ?w<cX%jsT#C=Gn9iqgWfU.N.u)fw0^Tr8b6Jf9Q'=9DWh+).6_pe~0oRM\$
2021-09-16 04:29:06 UTC	1586	IN	Data Raw: 7a b7 21 b3 5b a9 6d f8 35 77 f9 48 5c f1 6a 1f 4c ff 00 95 18 3f 1d 6b 1f 6d f0 73 9c 1f 07 24 5c e7 b1 d0 f7 0f e7 14 f0 62 6f 4c 38 67 5e d6 ad 27 6b bf dd 11 8b b8 58 81 a2 92 bb 73 10 5c fe 19 98 65 89 1b b3 5a 93 2c 41 ce 77 73 f0 c7 2c e2 fe fa d8 7f 04 e7 38 33 a4 e3 ef be d2 24 6b 52 06 95 f6 c4 d9 96 3d 71 79 a5 d8 9a 74 6e ef e5 b1 27 dc 49 75 67 18 31 06 36 36 76 fb 03 dd 76 55 96 a9 f1 ec 28 9c af 90 64 58 a7 d8 c5 c5 38 30 1c e7 e1 8e 1c 90 fa de bb 36 c6 3e 79 61 c9 94 60 3d 8f 0b 06 04 71 f1 61 4a 9a b3 87 47 5c 9a 15 91 6b 9a f6 62 c6 19 ac 98 36 f1 7d f0 4c 30 e7 11 fb 4d 8c 82 1e b2 19 38 cd 26 d4 d4 9f a9 ed 89 73 6e 0f 74 bf ed 4c 7c 4f 8e ba 8f fe a0 7c 07 e3 9f 86 c9 93 2a c9 84 7c 03 90 e4 bf 89 87 2a 1b 83 4a c8 cb 50 84 cd 84 22 58 a9 af Data Ascii: z [m5wHjL?kms\$ bol8g^kXsleZ,Aws,83\$R=qytn!ug166vvU(dx8062ya~=qaJkIkJ#q08&sntL O]*JP"X
2021-09-16 04:29:06 UTC	1587	IN	Data Raw: 70 67 3d c9 28 08 e9 17 09 cf 8f 21 df bf 9c 93 1b f1 26 4d 83 f7 41 8b fb 5d 07 38 a4 9c e7 8c fc 71 9c 2b 0b 55 94 09 61 ed 8d 06 40 4f 30 f0 42 0c fe 3d 71 ce 16 03 16 50 4f ff c4 00 43 10 00 01 03 02 04 03 06 03 06 f4 04 05 05 01 01 00 01 00 02 11 03 21 10 12 31 41 20 51 61 04 13 22 30 32 71 81 91 a1 23 42 52 62 b1 d1 33 40 72 c1 05 14 43 e1 50 82 92 f0 f1 24 34 53 73 a2 63 c2 ff da 00 08 01 01 00 06 3f 01 e0 ba 9c 27 00 9b ff 00 18 32 6e 89 5a a9 2b 36 46 c8 82 14 a0 10 8c 02 0b 2b 9e ca 20 62 11 6a 73 5c 6e 8c 68 a9 b5 aa 93 86 ca 5c 8c 72 45 e5 a5 64 50 84 09 41 66 dd 09 d5 4f 15 d5 b1 09 bf f1 83 cd 68 a1 0d ca 2c 70 2b 3b 10 05 66 51 80 51 b2 ce ac 55 f0 9c 25 6a a1 66 28 1c 0c ab 68 8b 91 4e 94 00 4c 62 9e 88 b3 97 10 c4 e0 13 7f e2 57 Data Ascii: pg=(!&MA]-8q+Ua@O0B=qPOC!1A Qa"02q#BRb3@rCP\$4Ssc?2nZ+;F+ bjs nhvEdPaFOh,p+;fQQU%jif(hNL bW

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:06 UTC	1588	IN	Data Raw: 4a 4f 0e 07 81 b4 c7 3e 01 08 1a 80 2b 30 2b 01 86 51 ea 76 89 c4 9d d0 27 6c 0b 8e 80 29 2a 70 8c 21 ad 32 77 59 03 e6 39 2b 05 76 8b ab 1b f5 59 9c e0 3d d4 53 76 67 6e e3 fd 94 b4 66 f6 52 69 b8 0e 70 84 93 a7 cd 0a 8d 96 b8 58 a2 43 83 2b 72 d3 32 ca f4 d7 08 75 3e 63 56 a2 0e 8e 68 42 f6 28 92 11 70 51 d7 10 d1 cd 00 9b 25 16 3a 34 45 8d e6 af ac 2f 05 90 24 dd 4b 8a f0 a2 d2 ae 8e 5d 0a b2 90 99 3c d4 35 5a ea e1 41 40 88 f2 87 ba 1c 44 93 64 ea 3d 9c 9e ae 53 84 0c 2c b4 94 60 21 c9 4e 66 fb 2b 08 51 29 b9 ae 34 52 4c 28 28 68 8c 2f 49 5d e5 07 91 fd fd d3 69 55 67 77 57 e8 70 25 38 72 e0 1c 05 dc 93 aa 38 f4 6a 32 6c 13 9c a6 2c b2 6d c1 65 de 3c db 90 5d dd 1b 0d cf 3c 2c 3e aa c0 05 6b 2f 11 27 0b 98 f6 42 2b 1f 65 e2 0c 75 f9 42 90 dd 51 76 8a Data Ascii: JO>+0+QvI)*pl2wY9+vY=SvgfnRipXC+r2u>cVhB(pQ%:4E/\$K)<5ZA@Dd=S, 'lNf+Q)4RL((h/l!)iUgwWp%8r8 j2l,me<->,>k"/B+euBQv
2021-09-16 04:29:06 UTC	1590	IN	Data Raw: 1d 56 43 1f 15 98 18 1c 96 5b 5f 92 0b 22 30 b3 15 64 43 96 6d 96 6c 00 5d ec ea a7 40 86 5b 9e 0f 86 01 65 0a 4e 23 1a 95 3e 01 3e a3 b5 2e 94 4a 3c ce 12 56 b8 5d 5f 45 95 bf 15 3c 1f db 0d d6 bf 04 2c ad f3 4c a4 09 d3 74 fa ae 7b 9c ef ca 8e 59 5e 10 b6 50 f0 14 31 d7 8d 0a cb 7f 9a 1f 44 d2 06 a9 be d8 f7 bf 89 c0 20 8e 07 01 d5 41 44 27 8e a8 ca 93 b2 f6 84 6c a7 a2 82 2c 50 11 a5 94 c2 82 15 c5 f9 ab 68 b9 a3 36 ea b2 b8 12 36 3c d5 8d c0 91 fb 2a bd 96 a5 aa b0 48 ea 16 57 8b c4 1f 82 77 56 aa 75 00 f7 41 c4 a8 05 35 36 89 dd 52 0d b4 a6 b4 26 82 83 93 32 1b 82 80 9d 93 20 b6 66 16 60 11 0b 3b 94 2c c5 03 ce c9 a4 72 45 ab e2 9a 4a 0d 62 76 6d 61 44 9c a0 e8 83 1b e9 57 53 88 c6 d8 37 0b 26 51 1a ea 42 9e 19 c2 54 05 27 80 05 37 c3 55 ec bc 26 c8 Data Ascii: VC[_"0dCmlj]@[eN#>>.J<vJ_<L{Y^*P1D AD'l,Ph66<*HwwVuA56R&2 f,;rEJbvmaDWS7&QBT'7U&
2021-09-16 04:29:06 UTC	1591	IN	Data Raw: 02 b3 b7 9d c2 6d 41 b9 1c 39 1b 77 20 64 0e 85 40 ca 89 0e 07 dd 78 da 14 17 47 c5 7a 90 0e 3b f0 19 51 95 ce 24 c0 0c b0 9e a5 06 0a 3d 88 d4 fb d4 c5 52 ea 8c e8 e0 98 6a d0 75 30 4c 67 61 b4 8e 61 00 4c bb 98 d1 54 fe 94 d9 1f e9 b5 66 6b 49 1c 91 9a 6e d1 13 52 99 d5 36 98 01 1f e9 55 1c 39 50 44 04 fa f8 9a 25 aa 0e 04 d6 65 f4 ee c9 c4 1d 93 5c 74 05 08 03 e0 b4 b0 28 30 c4 f2 42 a3 54 82 a3 6d 16 61 aa 99 57 5a 6c 8e 11 cd 65 0d 22 a8 77 c0 b5 11 a1 08 08 52 ba a8 b4 ac c3 6d 11 20 10 50 8f 64 47 25 64 32 d0 71 9d 26 cb ff 00 51 d9 aa 30 73 22 df 3e 2b 05 04 c3 79 94 4b 5b 9f 94 22 de ee a0 f8 20 4d 23 1c dc 84 dc f9 65 39 06 a2 10 8f 6c 1a e1 b1 95 46 a8 fb cc 07 12 47 e1 95 95 13 ba f7 51 37 03 86 72 85 a2 ca dd be 01 19 aa 5e 47 dd a4 27 ea 9f dd Data Ascii: mA9w d@xGz;Q\$=Rju0LgaaLTfklR6U9Dg%uclt(OBTmaWZle"wRM PdG%d2q&Q0s">+yK[" M#e9lFGQ7r"G'
2021-09-16 04:29:06 UTC	1592	IN	Data Raw: c3 20 85 39 a4 ac ae d5 0e d2 c4 5e ed 95 3a 60 78 37 2a 6d 30 bc 26 61 16 b4 15 e2 08 2b 29 01 33 bc b3 73 5d 34 b5 d9 ba b1 92 87 86 af c1 a1 4f 8d 3a 59 56 c1 55 7f 67 6c 53 9b 66 0b ed cb 01 3b 65 e1 ba 95 65 33 c8 28 1e a7 01 a6 d2 8b 5b 62 0a 69 d5 c3 7e 8a 9c 7e 2b af 1c 49 16 4f a9 92 c0 42 68 df ba 1f 54 f0 0f de d0 65 f4 ee c9 c4 3e 1f ec b2 4e 7a 67 49 d9 16 e8 57 da 37 7b 3b 62 99 58 4d d4 ce 03 c8 bb 6f cc 2b 2e ec d3 4d fb 06 96 c2 8d b1 3e c9 cc af 5a ab a6 d6 74 0f 90 4e 7f 66 75 8e c4 a2 2a 5d d1 80 23 55 9c 69 ba e8 57 ba cc 2c 5a 53 0d 48 cf 1e 2f 82 37 b0 ba 80 55 26 93 be 06 53 87 94 53 9a f3 62 6c b5 0b d6 3e 68 02 54 ca ce d1 e1 ea a1 46 04 a3 54 ba d9 a5 36 98 16 09 a5 a7 55 98 ea 80 2e d2 ca 51 9b 85 e1 36 43 f0 22 01 06 c9 cc fb Data Ascii: 9^:~x7*m0&a+)3s}4O:YVUglSf;ee3([bi-~~+IOBhTe?NzglW7{;bXMo+.M>ZtNfu"#{UwI,WZSH/7U&SSb>hTF T6U.Q6C"
2021-09-16 04:29:06 UTC	1594	IN	Data Raw: f7 55 33 44 e5 47 94 a6 1e ab bb 00 e8 bb c3 a2 d3 02 39 84 1d c2 14 e3 a2 f0 c8 40 12 a4 2b 02 a4 e1 55 cc f5 e5 f0 fb a7 97 ba 64 cb a5 02 05 d3 6e 13 5c cd 37 44 75 50 42 96 88 08 35 b6 41 81 5d 08 20 2c f3 a2 f1 94 5f aa 25 d0 b2 32 f7 d5 4a 36 e3 67 ba 6c 72 45 19 db 8c 15 07 da 56 b8 ce 59 5a 29 3b d9 59 6a a9 76 60 6c 4e 67 13 b3 46 aa 8b e9 35 f4 69 34 78 46 58 04 6d 98 ef ee 9b 4b bc 2e a6 69 8a 80 fe 2c c9 ec 78 27 29 80 e3 f8 4e ca ad 17 b1 8d 69 13 4e 0c 96 8e 6d e9 cd 3e 83 c4 39 86 3c 82 50 ef 73 df 7c b6 42 2a b7 e6 bd 6d f9 af 50 5e a0 ac 42 b8 08 c2 b0 b4 aa 95 aa 18 6b 1a 49 55 ab d4 3e 27 92 7f d9 04 10 a9 d9 eb 35 b5 7f 01 df f6 45 95 1a e6 3d a6 e0 a1 28 65 0b 24 d8 ad 30 c8 61 77 4d c3 39 72 6e 19 4f 95 e9 0b d2 16 98 ff 00 95 a6 d0 Data Ascii: U3Dg9@+UdnI7DuPB5A] ,_%2J6glrEVYZ);Yjv'INgF5i4xFXmK.i,x')NiNm>9<Ps B*m^BklU>5E=(e\$0awM 9rnO
2021-09-16 04:29:06 UTC	1595	IN	Data Raw: 35 c0 e8 8b 9c 70 ed 35 7a 42 27 10 15 3a b4 ea 41 91 b2 80 f2 e2 36 1a 23 9c 41 e0 3c 30 b3 94 00 c4 51 66 de a4 14 10 ad a2 d1 4c 20 e2 db a0 ac a4 6a ba e2 03 a4 b3 ea 10 20 ca d7 82 f8 95 4b b2 31 de 1a 22 5f fd 4e e0 60 9f 4a 34 f9 00 51 3f 32 9c ec c6 2e 02 86 d4 70 f8 ab bc 9f 75 0a 35 53 a2 89 50 eb f2 59 89 c3 e1 85 20 3d 2e a6 d7 8f f9 86 37 e1 87 68 bc 03 2f b2 8d 7a af 13 27 e2 54 9a 14 e7 a8 95 e0 63 5b ec 23 07 7b 2e df 40 fa 5c 1b 50 7b b4 a0 88 fc 4a 11 c2 eb a2 b6 1a 70 c3 6a 54 03 a3 96 53 55 c4 75 c2 4a 18 3e 3e f3 9d 86 5a 62 4a c9 51 b0 56 6a 54 cb 96 42 c7 36 13 b3 d3 71 74 6e 13 8c 46 3a e1 3c 20 2c d9 ac a5 58 4b 8d 80 52 6e e3 72 50 c3 45 75 61 c1 23 55 2a 46 39 e9 1f 76 9d 0a 25 b3 e1 f5 0e 5c 75 6b bc fa 5a 60 73 3c 95 5a f5 0c Data Ascii: 5p5zB":A6#A<OQfL j K1"_'J4Q?2.pu5SPY =.7h/z'Tc{#{. @lP{JpjTSUuJ>>ZbJQVjTB6qtnF:< ,XKRnrP EuafU*F9v%lukZ`s<z
2021-09-16 04:29:06 UTC	1596	IN	Data Raw: c2 76 54 ea 72 10 87 f2 4e f6 43 db 1c ef 99 2c 04 7c 51 a6 2a 9c bc 95 f1 11 8f 7b 52 3b a6 6a 4e 8b bb ec d4 bb d2 37 f4 b5 48 34 99 d0 36 7f 55 6a ed ff 00 a0 2f 1b 3b 3b c7 56 c7 e8 87 f9 9e c4 47 5a 6f fe c5 01 fe 6b ba 77 2a ad 2d fa ac f4 6a b2 a3 79 b0 82 3e 9e 6f 4e 2c d4 fd 6d b8 ea 89 a7 57 bb 34 e6 69 bc 6e 36 40 ae 85 77 d4 80 15 37 1f 8b fd d4 11 fc 9e 6e 3f fd 3d 5a 94 9c 7f 03 8b 53 5a 5e de d2 0d 83 6a b6 4f c5 5d 07 bf b0 76 5e c5 e1 93 53 b6 57 80 3a 86 0b ac fd bf fc 63 b4 ff 00 88 3c 5c 76 7e cc de ea 89 3c 8f 44 dc d9 69 f6 76 7a 3b 3d 3b 31 bf b9 ea b5 56 c2 dc 0e 6f c7 f9 37 62 17 66 a8 3f f8 9b 28 82 ac a7 85 bd 9f b3 b1 c5 8d d8 58 7b 94 3f cd 76 b6 87 7e 0a 63 31 5e 11 5b dd cf fe c1 5e 96 6f ea ba ff 00 db 52 ff 00 a5 5f b3 81 Data Ascii: vTrNC. Q{R; N7H46Uj/;;VGZokw*-jy>oN,mW4in6@w7n?=-ZSZ*J0)v^SW:c w-~Divz;=:1Vo7bf?{X}{?v~c 1^f^oR_
2021-09-16 04:29:06 UTC	1598	IN	Data Raw: be 60 e1 3e de 45 37 16 cd 90 f7 53 d7 11 e6 31 df 94 84 d7 0d ae 81 e8 a0 e8 56 76 7c 42 0f 6e aa 0a cc db 39 77 75 be 7c 1d 39 21 94 e6 67 e1 3f d9 78 0c 3b 76 9d 7c 97 08 f1 6c 53 bb 2f 68 b5 46 98 07 9e 3d eb 47 81 ff 00 43 c7 98 6d e4 66 1a a0 1b f1 40 8d 0a 03 16 7b 46 16 56 52 54 ce 19 82 60 ea 8f 24 cf 62 70 07 cf 77 90 1c 7e eb dc 13 53 3c f9 e4 54 7c 13 99 f8 4e 17 d5 66 03 c2 75 08 39 a5 5d 5e c7 9a ca f0 4b 10 73 4c 8e 00 e6 92 08 d2 10 67 68 ff 00 af f7 5d 38 ca 67 6b 60 b1 30 e4 27 d4 2c 70 75 27 ee 9d 4d e2 e0 f1 91 c7 05 5b 75 12 ad b2 d0 a3 aa 2c 3a 87 79 05 d1 a2 30 a3 93 71 1e 44 a3 c1 f6 6c 25 78 69 87 74 05 65 ab 4c b5 dd 47 1f 68 8b e5 a8 2d ee 9e 7f 08 4d 1c b8 07 97 54 7e 59 4f 1c 9e 57 43 84 e1 07 f8 67 e8 a4 2b a8 70 90 b3 53 bb Data Ascii: `>E7S1Vv Bn9wu 9lg?x;v S/hF=GCmf@{FVRT}\$bpw~S<T Nfu 9^KsLgh 8gk'0',pu'M[u,;y0QDl%xiteLGH-MT~YOWCg+pS
2021-09-16 04:29:06 UTC	1599	IN	Data Raw: c6 e3 db 80 bc e8 d0 b3 35 d2 4e a9 8c f8 f0 1c 07 0d 6a 75 23 25 46 6f d1 54 a8 d7 06 53 7b c9 93 6b 20 58 de f1 8c d9 b6 04 f5 2a bd 59 20 d5 f5 01 cb 96 24 53 f9 a3 51 de 91 7f 75 af 0c 2b e1 4f a2 85 4f fa 47 9c 55 43 f9 ca 83 cc 18 ca 83 a8 d7 10 e6 d9 e3 42 a1 d6 70 d4 71 77 67 d2 6e df db 08 50 83 db aa 2e 1b a1 ef 28 70 51 64 fa aa 4f cb c9 20 f1 4f 3c 3a 14 32 28 fb ed d3 83 c5 f7 8c a1 93 44 e3 ca dc 43 db 86 59 62 86 77 13 ee 70 2a 05 ca f1 f1 82 cc f1 03 97 34 40 d0 0e 29 c7 e1 83 7a 59 0e 51 e6 95 53 fa ce 17 c2 f8 ce 22 a3 74 dd 02 31 15 69 fa 86 a3 98 40 85 3c 16 f5 36 e1 5f 5d d4 e2 e0 11 79 df 4e 00 bb 3d 3d 83 09 f2 67 88 f3 c7 aa 17 37 39 c6 f8 47 58 4d 01 93 08 bb 48 1c 6d e2 b9 56 0b c4 65 78 5b 6e 6a 5d 77 61 1e 49 38 39 bf 14 3c d2 Data Ascii: 5Nju#%FoTS{k X*Y \$SQu+OOGUCBpqwgnP.(pQdO O<:2(DCYbwp*4@)zYQS't1i@<6_jyN==g7YGX MHmVex[nj]wal89<

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:06 UTC	1600	IN	Data Raw: 4e 55 e6 63 32 11 c9 46 a5 cb b1 37 c9 72 63 64 89 4a d1 67 56 69 1e 33 74 6a a3 51 19 6c 64 93 94 12 14 9c 71 7f 44 32 6c d1 0c 8d 63 af a2 33 6f 1c b5 33 12 52 c9 d4 c7 18 be a6 28 b9 e5 6f b1 08 29 64 91 87 15 c9 fc 23 3b dc 84 da 1f 87 39 5a 25 37 a9 0d ed b1 54 c6 b6 12 e5 15 b0 90 ca e7 66 a3 5a 27 3d 89 49 9a 99 0c f2 8b 23 92 32 56 84 f7 26 bb f2 8f 29 12 64 99 23 b8 ab 9b 48 f0 d5 da 63 c7 df 96 57 49 33 84 ce e7 3a 7d 0e 27 06 97 b1 0c 4b 6f c1 2e 0f 13 8d 36 7f c4 58 f2 6d 2b 20 a4 d3 22 f4 7f a3 87 86 ed fd 0b 32 c7 69 f7 25 18 35 a8 84 75 90 c7 a2 44 97 ab 61 26 5b d4 4b d4 28 b1 27 5b 9d fc ad 12 64 b2 a3 c7 44 b2 b9 08 63 a3 14 dc 64 45 ee 76 e4 b9 64 90 c9 32 5d 0a 6c 8c 46 6e 58 d8 93 f8 1a 33 b9 6a a3 03 9a 7b 12 ca de 92 13 96 a4 4a 36 Data Ascii: NUc2F7rcdJgVf3tjQldqD2lc3o3R(o)d#;9Z%7TfZ'=l#2V&)d#HcWl3;}'Ko.6Xm+ "2i%5uDa&[K('[dDodEvd 2])FnX3j(J6
2021-09-16 04:29:06 UTC	1602	IN	Data Raw: 42 fd 3a 70 d5 ad ed d8 5c 2c 3f 97 71 e1 84 9f a9 10 f0 e2 9a a2 49 4b 0b 49 22 e3 14 9b 3c 47 38 3f 82 29 25 e9 30 46 73 8e e4 55 72 7d 79 4e 71 ba 64 9e a9 24 8c bb 52 2d 69 48 94 25 ae bb 0a 27 42 59 2e 47 11 89 c9 a9 2f ec 7c 56 88 fa a3 3b fa db a9 8e 0d b5 37 f1 c9 96 22 f9 52 38 7e 1b c4 77 fe 23 c5 1d 35 5b 13 5a 66 6a 8a 3c 78 78 94 d1 8f 2a 46 69 ea 66 0b 76 88 46 91 c6 2d 97 3a 3a b1 3e 56 70 b2 fd de 4e 31 92 dc ff 00 8b 87 e0 9f 03 06 b6 6c ff 00 c7 c9 5e e9 9e 16 68 2f e2 4f 86 72 6f 6a f8 23 8e 74 ff 00 26 0e 1e 5a 77 31 46 a3 42 8d bb e5 2e a4 7a 99 71 ce 59 0c 38 fd 44 a1 63 82 33 5a e8 42 56 8c f9 69 51 7b 97 21 ee 56 dc 98 e2 2d 84 cb 3a b3 0e 3d 38 d2 e5 c4 6c ce 1e 12 73 b7 d0 f0 b1 fd 1e 1c 09 61 8b 31 61 8c 2f e5 9b 1c 54 6f 18 f9 Data Ascii: B:p\,?qIK!"<G8?)%0FsUrjyNqd\$R-iH%"BY.G/[V;7"R8--w#5[Zfj<xx"FifVf.-4>vPn1!^h/Oroj#&Zw1FB. zqY8Dc3ZBViQ{!V.-:=8lsa1a/To
2021-09-16 04:29:06 UTC	1603	IN	Data Raw: 21 35 cd 8d b9 23 81 46 2f 0b 96 dd 2c 8c 44 ce a5 45 09 11 ef fc 03 74 39 3f 24 63 6c 74 bb 0e 42 e4 8c 92 ed dc 5e ec bf 61 b9 31 ae 7b 12 51 63 c4 fd 09 2a 67 4b 4c ca fe 62 3c 4f 82 5c b2 9d 6c 97 53 1c 7a 62 fe e3 e5 8e 4b e0 a4 64 8a f8 51 64 bf 44 45 f3 3e 4a 1a e0 f4 17 62 1d fc ce 65 bd a8 b6 29 09 ad df 62 f7 e9 62 80 aa 87 bc 4a 62 7f 52 32 3a c7 4c 46 68 2b 25 27 d4 7c 2b 56 74 f2 51 c6 d8 d7 28 cd 2b 65 56 cd b6 89 37 48 45 8e 43 da 1e 46 77 f2 ae 46 91 42 96 d3 ed b4 55 b1 22 86 8f 42 c4 8a 38 42 68 7d 25 89 7d 46 9f b1 19 f2 4d 26 8c 9c 48 9f b1 20 d7 52 26 e3 d4 e8 a3 d4 6d 08 6b 92 c6 4a 56 57 05 6f 44 7b ee f6 ae 3c ce 3c 5a dd 32 6e f6 8f 7d fd cd b6 48 7d 88 a3 a5 a2 2f 9e 4e 91 5d 18 fd 99 f0 88 a3 53 1f da 70 37 f2 d1 4c 71 76 26 Data Ascii: !5#F/,DEI9?<\$cltB^a1{Qc*gKLb<O\ISzbKdQdDE>Jbe)bbJbR2:Lfh+)% +VtQ(+eV7HECFwFBU"B8Bh)%}FM&H R&mkJVWoD[<<Z2n)H)/N]SpTlqv&
2021-09-16 04:29:06 UTC	1604	IN	Data Raw: d9 5e 1a f6 67 74 49 13 5b 43 2b 47 c4 8f fe d2 79 1b 5e ce 6c 7c 9d 18 db 22 ad d9 55 32 75 d4 36 7a 59 c5 11 8d c6 c8 c3 d4 ea 1f 95 31 96 46 42 a6 28 fd 46 7c 36 c9 63 7f 0e 3c f6 44 25 2e 2d 98 26 b8 ee 38 af 42 51 28 91 83 51 3c 33 bf 43 0e b2 39 57 cb d3 7e cc c7 92 32 4d 3c 6f fb 1e 27 91 62 c0 94 61 15 d5 c1 ab d4 74 7c ab bb 2a 32 82 fb 11 85 7a 99 31 dc 59 35 52 29 4b ee 31 7e 83 c2 bf 99 09 8e 9a 27 16 35 b5 b2 cd 67 e9 5f 71 10 12 72 54 c5 d5 d4 3e 87 1b 31 63 ea 8b 6f b2 3e 51 f0 b8 30 5f 4c af d8 4a f8 42 f2 aa 48 ef b4 b4 76 26 13 36 34 a2 77 8d 0f 4b 26 f8 46 3e 0c 72 e0 71 4c 94 68 63 22 da ec 61 f1 6d 66 38 d5 a7 f7 3c 47 c5 32 e4 9d cd cd bd 17 b0 e4 e5 2b 66 29 7e cc 93 74 4b 54 fb 22 72 b7 6c f8 b5 21 b5 25 68 4b 83 c3 9f cc c4 26 5a Data Ascii: ^gtl[C+Gy*)"U2u6zY1Fb(F)6c<D%-.&8BQ(Q<3C9W~2M<o'bat}*2z1Y5R)K1~5g_qpGrT>1co>Q0_LJBHKv&# 4wK&F>rqLhc"amf8<G2+f)-tKT"!r!%hK&Z
2021-09-16 04:29:06 UTC	1606	IN	Data Raw: ed 10 b6 ef b5 8d 6d af d0 63 cf 8f bf ff 00 86 a7 06 4c 19 3a 64 27 c9 e1 5c ea bf f8 b3 13 bc 68 c9 8e 33 84 a3 25 69 aa 67 89 68 e5 a5 d5 cf 1b f4 7c 7d bf 21 ed 5e 7a 30 e2 9e 5c b1 84 55 c9 ba 46 0f c2 7a a9 24 e5 92 0b ec 47 4f f0 a1 8f 1e 35 51 89 08 d9 93 8b 67 8f f8 8a d5 ea ea 0f e4 87 0b 79 2b 42 63 f1 9b c0 b1 bf 8b 39 7d 28 5e 4e fb 76 1e de 25 e1 f0 cf 8f fe cf d8 c9 8a 78 b2 38 49 53 47 80 e3 ea d4 c9 fb 44 c3 fa 7f ae df 8b 74 c9 e2 c7 9b d5 3e 97 fd 7f 2a fc cb 6f 05 57 e2 9a 7f f9 ec df cd 74 df d8 8e a2 fb 44 fc 4d e3 3f 0f 1b d3 c2 ba e4 be 6a f4 5e 58 2e 5a fa 8c 7e 54 78 5e 15 8f 4d 1f af 25 fe 4f 73 c5 fc 3f ae 3d 71 5f 34 7f ca 3c 07 15 61 9c bd d9 8b b3 db f1 0e 2e bf 0a cd f4 a9 7f 6f 22 dd ec fc e8 47 e1 e8 f5 78 b6 1f bb ff 00 Data Ascii: mcL:d\h3%igh)!^zo\UFz\$GO5Qgy+Bc9j){^Nv%6x8lSGDt>*oWtDM?j^X.Z-Tx~M%Os?=&q_4<a.o"Gx
2021-09-16 04:29:06 UTC	1607	IN	Data Raw: a4 51 2d 80 87 0b 03 6a 59 01 25 e0 66 1c 69 65 bc ea 39 8b 1c e0 14 d9 56 a1 a9 ad ef 59 83 a8 88 bb 60 9b b8 39 86 58 d5 cd 34 fc 4a c0 65 b3 53 4b a1 63 a9 a0 65 90 ba 9c 33 62 de 51 b9 11 60 88 d8 8e 91 ae 6a 5e 50 e5 3c 71 00 a0 47 1c 71 0c 26 1e 21 00 dd 04 a0 ad 67 b8 2b 01 c4 4c 22 f3 12 85 cc be 3d ca 7c 10 10 15 28 bf 52 ba 8c d1 1b b9 64 4c d9 70 85 2f 30 0a 9e 8b 8f ae 7a 80 6e 28 a1 88 0d c6 b0 3b ea 06 60 5a c7 28 57 f1 32 39 41 31 50 33 ea 64 62 61 1c 4b 25 7a 8d 1f c6 a1 98 ef f6 29 bb 20 9c ee 0a dc 71 0a 58 0b b8 36 17 b4 94 45 79 0c fc 7b 8e 85 a6 35 fc 84 d0 05 e4 72 c4 d2 cc 0b 6d 98 a5 55 84 d7 b8 9c 2d 66 f1 01 0b 58 af 10 38 45 75 6d 10 30 a1 a4 56 fe 2e 18 ee de 1e a6 65 2e dd 75 2e fb 44 4d 00 40 f2 57 b8 1d 2f 86 26 0a e6 6d 01 Data Ascii: Q-jY%fie9VY^9X4JeSKce3bQ^nP<qGq&lg+L"= (RdLp/0zn; Z(W29A1P3dbaK%z) qX6Ey{5rmU-fX8Eum0V. e.u.DM@W/&m
2021-09-16 04:29:06 UTC	1608	IN	Data Raw: 5c dc 48 2f e2 50 d3 c4 62 ce a1 0d 4a bd ff 00 3b 26 13 a6 72 28 8e c8 01 b6 ea 2c a4 0d 82 df 88 e0 2d d4 03 e3 99 62 9b 7d 14 1e 82 39 6e 3c 5b c7 75 32 c2 3c c0 18 10 e5 2d 3f 10 71 0d e5 46 34 81 c2 8a 23 17 2a ca 11 4b f4 9a 61 55 1a 54 b1 f1 ba 87 de c3 60 ef 57 5a 94 4a 0c 28 d7 d4 69 3f 81 4b 8c 7c dc 31 01 0a 88 74 7f 51 af 2c 31 50 33 ea 64 8e 25 2a 98 e5 ea 16 0b bd 90 82 48 bf 94 a1 c9 c9 a6 b9 8c 2d d6 ef c1 32 15 83 57 51 1b 45 f0 46 31 2b d9 17 da d7 1e 61 69 4c 79 60 05 37 90 8e 80 09 5b 2a 76 f8 94 4a 06 6b 57 05 0a 5a b5 6f c9 32 84 0e 2f 5e 89 48 05 9e 31 1a 0f 6d d2 67 2e d9 72 a9 9f 70 b2 58 73 98 ac 29 41 f7 0e cb a8 7e 61 bf bb 2d 7e 2b 8f 73 31 d0 f6 a6 82 0c ab e1 59 d3 e9 8a cd ce 79 b9 7f 75 04 bc ed 09 b9 85 b5 33 2c 79 43 b9 4e Data Ascii: \H/PbJ;&r(,-)9n<[u2<~?qF4##KaUT^WZJ(f?K[1tQ,%*H-2WQE1+aiLyJ?^jvkWZo2^H1mg.rpXs)A~a~+s1Yyu3,yCN
2021-09-16 04:29:06 UTC	1610	IN	Data Raw: 0d 5c 34 4a cf b9 60 07 2c 57 09 2f ed 34 5e 5f 70 97 68 b1 ed 09 fa 62 dc c2 f6 87 0a f5 01 ac 1b 47 15 b9 72 73 c5 ca 0d 62 e3 ba d2 08 c7 ab 63 46 95 2e 66 c1 7d 63 c1 94 e0 9d c0 a6 50 66 49 53 f3 19 ed 8d ab b8 30 d1 a6 d8 e8 dc 31 19 0e 31 2a 96 f8 81 74 72 c7 52 45 ac 6f 15 0e a5 7c 4d d5 89 a5 08 42 de e3 ca 10 73 16 69 12 29 85 59 c4 0b 78 b6 e6 de 1d 29 28 e3 68 36 ba 8e a9 ea 5c 12 fd 40 a5 cc a0 7e 88 c4 18 b9 9a 88 c4 48 17 2f 50 b9 99 4a 4c 91 a8 00 dc 6a c2 bc 5c bc 78 8d 1d 57 2c c6 76 92 d4 57 3e 25 6d 65 4a 26 24 21 5b ae 26 09 45 ae 75 72 ec e4 5d b9 fd 4a 20 32 e2 b9 86 da 74 3f b6 6d b1 a5 71 f5 cc 4e 60 d1 75 69 7d 70 45 7d 94 b0 8c 21 d5 12 ea c2 d0 d7 6e a2 0b 03 d0 b1 2b 77 02 80 77 a6 25 a8 aa bd 62 3a 62 5a cf 11 d2 3e 45 66 59 Data Ascii: \4J^,W/4^_phbGrscBF.f)cPfiS011^trREo[MBsi)Yx)(h6\@~H/PJLjxW,vW>%meJ&\${&EurJ 2t?mqN^ui }pE]In+ww%b:zbZ>Efy
2021-09-16 04:29:06 UTC	1611	IN	Data Raw: 52 39 a2 e0 60 9e e1 96 ab ad 42 5e 70 d7 2e 20 62 b6 c1 ee 2f a6 5f 99 38 3c 40 44 55 fc 67 71 03 22 da 3b 98 39 63 16 c0 2b 5b 77 8a 26 68 e7 af 33 3f 88 56 5e 0f 11 6d 70 2a a3 66 b4 71 8d c0 9c 43 43 18 36 15 71 c1 1b 59 5d d1 a8 1c 0f 9e ff 00 b6 2d ad 9e 6d fa a9 74 18 2c be 21 cc 34 16 65 1d 79 86 49 38 e7 5c 57 73 08 65 5a 5e 75 28 c1 0f 70 c1 64 d0 47 13 d0 34 3f 73 10 c2 a6 2a 84 07 46 61 36 f9 39 8a a9 0b 93 5e 44 0b ba 32 42 08 44 46 09 3f 5f 33 de 33 34 f1 0d 67 64 ce 29 6b ca e3 e0 82 f1 6a a3 c7 3c cb d2 f2 ca 59 ca a3 f1 a9 7b 37 ff 00 b7 1b bb df 1b bb df 73 38 fc 92 f9 59 54 ea 23 be ae 11 6c 17 b6 5d 78 60 37 89 66 3a d7 b8 fe a6 54 fc c1 09 aa fa 8c 43 b7 72 85 13 34 0b 32 6a 06 c0 01 2b 34 46 9e 84 50 e0 42 a0 64 5b 17 a9 32 02 Data Ascii: R9^B^p. b/_8<@DUgq;9c+{w&h3?V^mp^fqCC6qY]-mt,4eyl8lWseZ^u(pdG4?s^Fa69^D2BDF?_334gd)kj<YY={7s8YT#} x 7f:TCr42j+4FPBdJ2

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:06 UTC	1612	IN	Data Raw: 00 20 84 c0 1a 77 1f 27 cc b7 3b c4 e3 dd 3c 4a 31 e1 f3 08 38 ac 8b d3 12 bd 4a 1c b4 49 e4 89 c5 29 0f 96 a1 f8 84 da c8 1f 31 ac 34 35 e6 28 a5 5f e9 18 5c 4d 06 bc c5 57 e0 43 c1 56 e2 94 1f 51 4c bd 01 06 62 ed ae a6 03 86 35 9f a8 3f b3 14 ef 88 15 67 49 8f fa 96 c6 61 de 9c fb 75 2e 49 95 7d 5a ec 98 2e 09 8e f4 60 71 20 2a e2 cf b4 50 03 57 44 b9 24 f3 04 13 37 8a 82 05 08 b8 7e 16 e7 e2 08 db a3 35 0c f6 d9 8c 55 26 4f 32 8d 4d 88 e4 c4 cb cb 1b 51 4e 0e 73 14 55 ee 1a 95 73 be e2 71 b5 ee 30 07 13 b5 04 13 ee b8 22 c3 c5 5a 96 eb 6a 54 44 e6 e3 17 ea 6c e3 4a 70 46 6a 22 ca ee 06 16 1b b6 12 0d 14 2a fc b1 c0 b4 e3 75 2e 65 f3 07 4c ca 4a ab 13 10 80 f9 df 32 d0 5c c7 43 88 65 56 c8 55 8b 20 cf 52 c8 22 56 08 95 82 61 21 cc be 68 82 b1 1f c9 04 Data Ascii: w';<J18Jl)145(_lMWCvQLb5?glau.}JZ.`qp*PWD\$~5U&O2MQNsUsq0"ZjTDlJpFj"*u.eLJ2lCeVu R"Valh
2021-09-16 04:29:06 UTC	1614	IN	Data Raw: 44 56 db 4f 88 2a 2b 31 1e 7e a5 63 c3 33 2a b1 da ae 63 23 82 e7 80 44 51 72 bf d9 70 28 17 80 b1 a2 e9 6d d4 79 25 6b 82 68 05 0e 13 64 62 2b 2a b6 f7 c3 71 b1 ed 83 8c 97 00 dc 31 c7 d4 15 db 35 cb 34 81 b8 f7 44 01 97 e6 3a 8b 66 32 af 15 2e 05 60 aa 7f 71 05 6b 1a c5 e3 e6 2a 9f b0 61 37 61 e6 8b fb 8c 00 b6 80 bd 78 26 4e 65 b4 35 50 cd 08 b6 dc 1f 3d 41 14 6e 70 f4 46 05 e1 ce 03 e0 83 8b f0 a8 9c 14 42 55 92 f4 a3 b3 c4 ac 1b a4 ba c8 c7 a2 ad 37 5d 47 ef 65 2b ac 72 40 12 ec c0 74 1c 22 2f 38 15 d3 d4 ce d7 e5 51 35 73 c6 12 cd 40 0e 06 20 6c 3c 6e 28 e1 84 a1 c2 67 b1 fe e1 bf 26 2f b3 30 66 e9 7a 65 3c e2 af 98 0d cc ac f1 53 19 e4 d7 96 50 9b 2d 69 81 da 71 9b a9 81 db 45 e4 94 14 3e a5 40 61 03 25 b7 bf e0 4f 51 41 8b 26 97 00 65 9e 61 2e 33 Data Ascii: DVO*+1~c3*c#DQrp(my%khdB+*q154D:f2.`qk*a7ax&Ne5P=AnpFBU7JGe+r@t"/8Q5s@<Ikn(g&/0fze<SP-iq E>@a%QQA&ea.3
2021-09-16 04:29:06 UTC	1615	IN	Data Raw: 47 58 6b 10 f1 b2 d5 f3 16 66 d8 8a 89 0c 45 63 54 0f 22 56 6f 10 7e e5 bc 1a e7 10 cf 95 a9 59 fb 17 aa 8d 57 ab 7a b0 d6 f6 43 c4 47 06 8a d8 cc 30 0d dc aa 64 ab c7 0c 69 6c 9b 46 97 4d 10 e4 62 64 2e a3 51 6a 33 29 80 e4 d4 41 2f 2c 78 9b e6 6e ea 87 2e 18 61 54 cb 95 70 f9 18 b2 83 5b 0c 52 64 d8 b5 d4 12 5b 2b f5 0a b4 ba c8 c7 a2 ad 37 5d 47 ef 10 55 0d d4 1c bc 22 33 03 e5 c8 7c c7 e0 30 21 90 36 f0 66 25 6c 16 11 63 c5 a4 00 68 d8 5d bd 0b 21 81 e3 89 71 2e 75 33 db 32 55 5f c4 eb 37 72 9c 14 c5 95 f1 04 26 0d ae 66 5d 0e ac d2 fd c0 3e b6 57 2f a2 3d 10 2b 15 41 02 18 35 d4 08 4c cb 08 04 95 b2 65 63 17 53 26 a5 97 05 48 c1 d4 62 ce 2f ee 23 c4 71 05 be 56 bc c4 8c 63 e1 48 fd 33 1b eb d0 f7 59 85 b9 94 27 36 47 4d 37 52 f2 0a a5 c4 40 4c 29 8a b8 Data Ascii: GXkEcT"Vo~YWzCG0dIlFMbd.Qj3)A/,xn.aTp[Rd[+U"3l0!6f%lch]!q.u32U_7r&fj>W/=+A5LecS&Hb/#qVc H3Y'6GM7R@L)
2021-09-16 04:29:06 UTC	1616	IN	Data Raw: 5a ea 55 7e e1 bd 71 ab 8c e0 d6 18 b0 1e 98 e6 22 26 78 72 27 cf 12 a1 33 18 55 a6 c0 7c 4b 41 a3 fa 62 5a 10 0c 76 44 58 b0 1e 21 3a b6 15 ea 59 1c dc 5c 6f 10 0c 99 b8 63 9d 42 8a 93 92 13 94 13 4b 06 30 46 62 a4 2a db 32 c1 2f 8e 59 54 29 72 c6 4d 4a f8 87 14 a3 e6 2f 8d 88 d3 41 9e 66 88 19 36 e9 e0 83 42 40 7e 62 fd 57 74 4b 1a de 0a 85 35 0b e7 72 d5 96 53 75 2b c3 46 80 98 aa a5 ea 0d 95 c0 34 3a ea 13 d3 4d bb 26 2f c0 b9 65 c0 ea e2 a2 6e ea 21 60 4b 4b 1c 12 9a c3 6c ec 8a 3a 2b 38 a7 71 4b 3c a3 50 6b a6 bf 50 b0 70 bd c7 a8 38 1c 8e c8 ac 2a 19 45 72 86 91 60 0d af 30 22 70 06 61 6d 58 59 e8 90 9c b8 88 6a ab 86 96 1f 22 e2 54 80 d3 4f f2 10 4e 40 bd 6e 51 a2 00 3a e1 f6 4d dd c2 56 f3 dc a9 99 a4 6a f5 8f 84 cc a4 80 05 ae 8a e0 9a 8d 54 71 Data Ascii: ZU~q'&xr3UJKAbZvDX!:YocBK0Fb*2/YT)rMJ/Af6B@~bWtK5rSu+F4:M&en!'KKl!+8qK<PkPp8*Er'0"pam XYj"TON@nQ:VJjTq
2021-09-16 04:29:06 UTC	1618	IN	Data Raw: 51 7d d3 fb 82 96 b7 d9 2f 88 d5 6d 4c cb 33 57 0f 28 b6 51 5f 50 3c ad 91 1a ed 6e 31 ec a8 03 0c d4 44 65 f6 90 97 ce d8 ef 7c 17 ee 6d 20 d9 08 fd c5 67 bd 46 b5 32 05 f6 c5 3b 48 05 d8 e4 58 e1 42 8d 2e 06 f7 98 4c 93 b8 60 9c 0d 03 ab 77 2f 85 0b ed 5a 81 0c 83 8b 1d 8f b8 63 8a 59 d8 ec 7f a8 79 61 66 98 8f 71 a3 64 a6 b2 d5 a0 f1 15 02 05 7e 50 46 8d 1c f9 98 52 aa 65 f6 7f 08 b1 2a 0f e0 ab 13 2c 2c 97 b5 62 45 1f a8 3e 8c 42 e8 25 88 03 2c d7 64 e6 41 9c cc f8 8d d6 25 d4 6d 2b 57 29 9c a0 9f 32 82 8e e5 08 89 80 eb e6 5c 02 8d d7 e9 29 de 2b 3f c9 85 3c a5 3e c8 ea 3c 0f 98 01 b9 78 ff 00 63 b5 33 e5 89 88 64 f7 2d 00 02 c1 63 1e a2 99 0b 5f 50 c9 d0 1c 7f b8 7f 79 74 a0 39 81 64 d1 0d 0f 53 09 99 5e d2 f1 bc 10 5a 11 83 36 c7 9b 88 61 4d 16 be Data Ascii: Qj/mL3W(Q_P<n1DeJm gF2:HXB.L'wZcYyafqd~PFR*.,bE>B%,dA%~m+W)2l)+?<><xcd~c_Py9dS^Z6aM
2021-09-16 04:29:06 UTC	1634	IN	Data Raw: df 11 01 6b bd cb dc 0b b1 43 87 b8 65 fd d1 81 1b a3 65 b9 ce cc 57 06 7a 5f b0 d0 ee 05 65 dc 13 d0 78 62 a2 fa a8 e3 0b 16 13 01 5d 3d 40 46 28 64 aa 24 5d 6c d7 62 54 60 7b f0 1a 3e 47 fc 63 b3 2d 46 0a c6 4f d5 47 71 88 bd 3c 5d 73 15 d2 ea 51 e6 4d 17 a8 6c a2 e6 be 25 c0 9c c2 a6 fa 8e 80 29 29 a2 50 23 f1 58 58 c7 f4 17 1b 02 9d 4c 55 af 52 b4 b3 7b 29 72 ca d6 6b ce cc 99 a1 42 c8 7b 86 ec b8 45 64 78 ee 66 1b 6f 1d 24 28 49 eb ec 1b 80 62 51 b7 0e 65 f2 99 0d 0c c8 73 f5 16 b5 b2 a5 a8 3c 12 c3 33 71 bb b8 dc 31 cf d8 0b dc 12 d1 5f 72 02 06 75 05 ba 4a 58 8c d9 8d bd 46 18 95 05 c1 02 a9 44 54 a4 1b 80 04 d0 38 8a 8b 1d 0c e5 17 29 a2 a0 13 94 5f 5e 0f 22 6c 13 07 9e e3 3e 5d ac c4 68 86 5a 15 b0 9d 0d bd 8c 37 a5 32 22 1b 86 5a 81 d6 40 b7 d2 Data Ascii: kCeeWz_~exb]=@F(d\$)lbT'{}>Gc~FOGq<jsQMl%)P#XXLURj)rkB(Edxf0\$(lbQes<3q1_ruJXFDT8)_~^!>]hZ72"Z@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
155	192.168.2.3	49945	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:07 UTC	1640	OUT	GET /entertainment/justin-bieber-hailey-baldwins-relationship-timeline-shows-how-this-couple-went-from-pda-to-rumored-engagement-so-fast-9692470 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, /* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:29:08 UTC	1641	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 129639 Connection: close Date: Thu, 16 Sep 2021 04:29:08 GMT Cache-Control: max-age=86400 content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Apigw-Requestid: FvQzKgMMoAMEJqg= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 740769d10d5ef217a54d33b1ec64faf4.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: rbn4xVVuEWXq_slzquA5_MP9Yfl2HHqfO_Hpjg0GD55sZRbsj00eZw==

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1641	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 64 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:29:08 UTC	1645	IN	Data Raw: 6c 76 65 73 20 54 77 6f 20 57 65 64 64 69 6e 67 73 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4d 75 73 69 63 69 61 6e 20 4a 75 73 74 69 6e 20 42 69 65 62 65 72 20 61 6e 64 20 6d 6f 64 65 6c 20 48 61 69 6c 65 79 20 42 61 6c 64 77 69 6e 27 73 20 77 68 69 72 6c 77 69 6e 64 20 72 6f 6d 61 6e 63 65 20 63 75 6c 6d 69 6e 61 74 65 64 20 69 6e 20 74 68 65 20 63 6f 75 70 6c 65 20 67 65 74 74 69 6e 67 20 6d 61 72 72 69 65 64 20 69 6e 20 32 30 31 38 2e 20 54 6 8 65 6e 20 61 67 61 69 6e 20 69 6e 20 32 30 31 39 2e 20 48 65 72 65 72 73 20 65 76 65 72 79 74 68 69 6e 67 20 77 65 20 6b 6e 6f 77 2e 22 2c 22 64 61 74 65 50 75 62 6c 69 73 68 65 64 22 3a 22 32 30 31 38 2d 30 37 2d 30 38 54 31 37 3a 31 36 3a 31 30 2e 30 38 38 5a 22 2c 22 64 61 74 65 4d 6f 64 69 66 69 65 Data Ascii: lves Two Weddings", "description": "Musician Justin Bieber and model Hailey Baldwin's whirlwind romance culminated in the couple getting married in 2018. Then again in 2019. Here's everything we know.", "datePublished": "2018-07-08T17:16:10.088Z", "dateModifie
2021-09-16 04:29:08 UTC	1662	IN	Data Raw: 61 73 73 3d 22 69 6e 73 74 61 67 72 61 6d 2d 6d 65 64 69 61 20 55 65 6c 22 20 64 61 74 61 2d 69 6e 73 74 67 72 6d 2d 70 65 72 6d 61 6c 69 6e 6b 3d 22 68 74 74 70 73 3a 2f 2f 77 77 2e 69 6e 73 74 61 67 72 61 6d 2e 63 6f 6d 2f 70 2f 42 41 47 4c 6b 74 6f 67 76 6a 32 2f 22 20 64 61 74 61 2d 73 68 6f 72 74 63 6f 64 65 3d 22 42 41 47 4c 6b 74 6f 67 76 6a 32 22 20 64 61 74 61 2d 69 6e 73 74 67 72 6d 2d 63 61 70 74 69 6f 6e 65 64 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 2e 69 6e 73 74 61 67 72 61 6d 2e 63 6f 6d 2f 70 2f 42 41 47 4c 6b 74 6f 67 76 6a 32 2f 22 3e 3c 2f 61 3e 3c 2f 62 6c 6f 63 6b 71 75 6f 74 65 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 70 3e 49 6e 20 32 30 31 36 2c 20 74 68 65 20 63 6f 75 Data Ascii: ass="instagram-media Uel" data-instgrm-permalink="https://www.instagram.com/p/BAGLktogvj2/" data-s hortcode="BAGLktogvj2" data-instgrm-captioned">a href="https://www.instagram.com/p/BAGLktogvj2/"></blockqu ote></div></div></div></div><p>In 2016, the cou
2021-09-16 04:29:08 UTC	1670	IN	Data Raw: 63 68 75 72 63 68 2c e2 80 9d 20 42 61 6c 64 77 69 6e 20 74 6f 6c 64 20 3c 65 6d 3e 56 6f 67 75 65 3c 2f 65 6d 3e 2e 20 e2 80 9c 42 79 20 74 68 65 6e 20 77 65 20 77 65 72 65 20 70 61 73 74 20 74 68 65 20 64 72 61 6d 61 2e 20 49 20 6a 75 73 74 20 67 61 76 65 20 68 69 6d 20 61 20 68 75 67 2e 20 42 79 20 74 68 65 20 65 6e 64 20 6f 66 20 74 68 65 20 63 6f 6e 66 65 72 65 6e 63 65 2c 20 68 65 20 77 61 73 20 6c 69 6b 65 2c 20 e2 80 98 57 65 e2 80 99 72 65 20 6e 6f 74 20 67 6f 69 6e 67 20 74 6f 20 62 65 20 66 72 69 65 6e 64 73 2e e2 80 99 20 49 20 77 61 73 20 6c 69 6b 65 2c 20 e2 8 0 98 57 65 e2 80 99 72 65 20 6e 6f 74 3f e2 80 99 e2 80 9d 3c 2f 70 3e 3c 70 3e 49 74 20 73 65 65 6d 73 20 4a 75 73 74 6 9 6e 20 77 61 73 20 63 6f 72 72 65 63 74 2c 20 62 65 63 61 75 73 Data Ascii: church, Baldwin told Vogue. By then we were past the drama. I just gave him a hug. By the end of the conference, he was like, Were not going to be friends. I was like, Were not?</p><p>It seems Justin was correct, becaus
2021-09-16 04:29:08 UTC	1678	IN	Data Raw: 20 73 65 6e 74 65 6e 63 65 3a 20 e2 80 9c 4d 79 20 77 69 66 65 20 69 73 20 61 77 65 73 6f 6d 65 2e e2 80 9d 3c 2f 70 3e 3c 68 32 3e 4d 61 72 63 68 20 32 30 31 39 3a 20 42 69 65 62 65 72 20 50 75 74 73 20 4d 75 73 69 63 20 4f 6e 20 48 6f 6c 64 2e 3c 2f 68 32 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 43 43 20 69 47 52 20 76 59 65 22 20 73 74 79 6c 65 3d 22 6d 61 78 2d 77 69 64 74 68 3a 20 36 35 38 70 78 3b 22 3e 3c 64 69 76 20 63 6c 61 73 73 3e 3c 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 42 4e 6f 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 41 69 69 22 20 73 74 79 6c 65 3 d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 37 34 2e 36 30 33 31 37 34 36 30 33 31 37 34 36 31 25 3b 22 3e 3c 2f 64 69 76 3e 3c 62 6c 6f 63 6b 71 75 6f 74 65 20 63 6c 61 73 73 3d 22 69 Data Ascii: sentence: My wife is awesome.</p><h2>March 2019: Bieber Puts Music On Hold.</h2><div class="sCC iGR vYe" style="max-width: 658px;"><div class=><div class="BNo"><div class="Aii" style="padding-top: 74.603 17460317461%;"></div><blockquote class="i
2021-09-16 04:29:08 UTC	1689	IN	Data Raw: 20 64 6f 6d 69 6e 61 74 65 20 74 68 65 20 63 6f 6e 76 65 72 73 61 74 69 6f 6e 20 61 72 6f 75 6e 64 20 42 69 65 62 65 72 20 61 6e 64 20 42 61 6c 64 77 69 6e e2 80 99 73 20 72 65 6c 61 74 69 6f 6e 73 68 69 70 2c 20 62 75 74 20 68 65 20 74 6f 6c 64 20 5a 61 6e 65 20 4c 6f 77 65 20 6c 61 74 65 72 20 74 68 61 74 20 6d 6f 6e 74 68 20 64 75 72 69 6e 67 20 61 6e 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 77 61 74 63 68 3f 76 3d 54 5f 66 77 33 71 4e 78 31 4f 4d 26 61 6d 70 3b 61 62 5f 63 68 61 6e 6e 65 6c 3d 4a 75 73 74 69 6e 42 69 65 62 65 72 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 72 65 6c 3d 22 6e 6f 72 65 66 65 72 72 65 72 22 3e 41 70 70 6c 65 20 4d 75 73 69 63 20 69 6e 74 65 72 76 69 65 Data Ascii: dominate the conversation around Bieber and Baldwins relationship, but he told Zane Lowe later that month d uring an Apple Music intervie
2021-09-16 04:29:08 UTC	1704	IN	Data Raw: 61 73 73 3d 22 6b 63 55 20 65 79 4e 22 3e 3c 2f 69 3e 3c 2f 61 3e 3c 61 20 63 6c 61 73 73 3d 22 61 58 49 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 2e 79 6f 75 74 75 62 65 2e 63 6f 6d 2f 62 75 73 74 6c 65 22 74 69 74 6c 65 3d 22 59 6f 75 74 75 62 65 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 72 65 6c 3d 22 6e 6f 72 65 66 65 72 72 65 72 22 3e 3c 69 20 63 6c 61 73 73 3d 22 6b 63 55 20 62 46 4c 22 3e 3c 2f 69 3e 3c 2f 61 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 4c 6f 77 58 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 73 65 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 2e 62 64 67 2e 63 6f 6d 22 20 63 6c 61 73 73 3d 22 66 78 71 22 20 74 61 72 67 65 74 3d 22 5f 62 6c 61 6e 6b 22 20 Data Ascii: ass="kcU eyN"></i><i class="kcU bFL"></i></div></div><div class="LgX"><div class="ise"><a href="https://www. bdg.com" class="fxq" target="_ blank"
2021-09-16 04:29:08 UTC	1720	IN	Data Raw: 74 6f 20 6f 76 65 72 63 6f 6d 65 20 73 6f 6d 65 20 6f 66 20 74 68 65 20 e2 80 9c 6e 65 67 61 74 69 76 65 20 74 68 69 6e 67 73 e2 80 9d 20 74 68 61 74 20 6f 63 63 75 72 72 65 64 20 64 75 72 69 6e 67 20 74 68 65 20 74 69 6d 65 20 70 65 72 69 6f 64 2e 20 e2 80 9c 46 69 7a 7a 6c 65 64 20 77 6f 75 6c 64 20 6e 6f 74 20 62 65 20 74 68 65 20 72 69 67 68 74 20 77 6f 72 64 e2 80 94 69 74 20 77 61 73 20 6d 6f 72 65 20 6c 69 6b 65 20 61 74 76 65 72 79 20 64 72 61 6d 61 74 69 63 20 65 78 63 6f 6d 6d 75 6e 69 63 61 74 69 6f 6e 2c e2 80 9d 20 42 61 6c 64 77 69 6e 20 74 65 76 65 61 6c 65 64 2e 20 e2 80 9c 54 68 65 72 65 20 77 61 73 20 61 20 70 65 72 69 6f 64 20 77 68 65 72 65 20 69 66 20 49 20 77 61 6c 6b 65 64 20 69 6e 74 6f 20 61 20 72 6f 6f 6d 2c 20 68 65 20 77 6f 75 Data Ascii: to overcome some of the negative things that occurred during the time period. Fizzled would not be the right wordit was more like a very dramatic excommunication, Baldwin revealed. There was a period where if I walked into a roo m, he wou

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1755	IN	Data Raw: 38 03 43 03 4f 03 5a 03 66 03 72 03 7e 03 8a 03 96 03 a2 03 ae 03 ba 03 c7 03 d3 03 e0 03 ec 03 f9 04 06 04 13 04 20 04 2d 04 3b 04 48 04 55 04 63 04 71 04 7e 04 8c 04 9a 04 a8 04 b6 04 c4 04 d3 04 e1 04 f0 04 fe 05 0d 05 1c 05 2b 05 3a 05 49 05 58 05 67 05 77 05 86 05 96 05 a6 05 b5 05 c5 05 d5 05 e5 05 f6 06 06 06 16 06 27 06 37 06 48 06 59 06 6a 06 7b 06 8c 06 9d 06 a6 06 c0 06 d1 06 e3 06 f5 07 07 07 19 07 2b 07 3d 07 4f 07 61 07 74 07 86 07 99 07 ac 07 bf 07 d2 07 e5 07 f8 08 0b 08 1f 08 32 08 46 08 5a 08 6e 08 82 08 96 08 aa 08 be 08 d2 08 e7 08 fb 09 10 09 25 09 3a 09 4f 09 64 09 79 09 8f 09 a4 09 ba 09 cf 09 e5 09 fb 0a 11 0a 27 0a 3d 0a 54 0a 6a 0a 81 0a 98 0a ae 0a c5 0a dc 0a f3 0b 0b 0b 22 0b 39 0b 51 0b 69 0b 80 0b 98 0b b0 0b c8 0b e1 0b f9 Data Ascii: 8COZF~ -;lHUc~+!XgW7HYj[+~Oat2FZn%:Ody'=Tj"9Qi
2021-09-16 04:29:08 UTC	1757	IN	Data Raw: 94 8a 94 f4 95 5f 95 c9 96 34 96 9f 97 0a 97 75 97 e0 98 4c 98 b8 99 24 99 90 99 fc 9a 68 9a d5 9b 42 9b af 9c 1c 9c 89 9c f7 9d 64 9d d2 9e 40 9e ae 9f 1d 9f 8b 9f fa a0 69 a0 d8 a1 47 a1 b6 a2 26 a2 96 a3 06 a3 76 a3 e6 a4 56 a4 c7 a5 38 a5 a9 a6 1a a6 8b a6 fd a7 6e a7 e0 a8 52 a8 c4 a9 37 a9 a9 aa 1c aa 8f ab 02 ab 75 ab e9 ac 5c ac d0 ad 44 ad b8 ae 2d ae a1 af 16 af 8b b0 00 b0 75 b0 ea b1 60 b1 d6 b2 4b b2 c2 b3 38 b3 ae b4 25 b4 9c b5 13 b5 8a b6 01 b6 79 b6 f0 b7 68 b7 e0 b8 59 b8 d1 b9 4a b9 c2 ba 3b ba b5 bb 2e bb a7 bc 21 bc 9b bd 15 bd 8f be 0a be 84 be ff bf 7a bf f5 c0 70 c0 ec c1 67 c1 e3 c2 5f c2 db c3 58 c3 d4 c4 51 c4 ce c5 4b c5 c8 c6 46 c6 c3 c7 41 c7 bf c8 3d c8 bc c9 3a c9 b9 ca 38 ca b7 cb 36 cb b6 cc 35 cc b5 cd 35 cd b5 ce 36 ce Data Ascii: _4uL\$hbD@iG&vV8nrUD-u`K8%yHYJ;.:lzp~_XQKFA=:86556
2021-09-16 04:29:08 UTC	1758	IN	Data Raw: ac cd 53 69 ad d3 4b 4e a8 3e ae d5 85 f5 97 9e de 53 45 22 4b 0c 11 2f 6c 2a 98 30 46 0c 02 c8 24 c5 4f f1 d4 7b 52 f7 b4 dc 75 23 90 08 0c 63 7e 1b 0f bd fb 06 cc 90 6e ed 2a 00 00 02 00 bc 76 9e 59 6d 65 88 3d cf a0 ff 00 54 a8 68 85 47 1b dd 9d bc 3a 69 d7 8c 7a fa b1 c4 f7 6c 44 23 52 2b b6 4f 0e 6c b6 ac 4a 2a 57 4a 7c 23 4d 22 4b 0c 13 c7 db 2a 80 c0 00 c1 80 64 84 4e 88 e7 57 79 3b c3 1e ee 6d cc 5b 9b 10 ca 85 9a cd ea ab 36 6d 21 c2 58 64 08 f1 c8 b7 19 8e c0 33 5b 3c 40 57 ef 7d 99 c9 3a 7b 32 c9 7c 9d 92 07 5f d7 12 f7 d8 f2 69 ec b2 ac eb 5f 59 36 c3 14 b9 8b a7 eb ec ae 3f 31 d5 a2 58 60 8e 29 e5 ed 91 52 30 60 c1 91 81 8a 70 8a c3 8c f7 6c 8a 97 9f a5 13 eb f6 12 ba 50 c6 b6 44 7b b2 eb dc 79 dc db c1 4c 81 80 0c 87 8e 82 33 5f 2c 71 29 8f Data Ascii: SiKN>SE"K/I*0F\$O{Ru#~n*vYme=ThG:izID#R+OIJ*WJ#M"K*dNWm;[6m!Xdd3<[O@];{2!_Y6?1X`)R0`plPD[yL3_q)
2021-09-16 04:29:08 UTC	1759	IN	Data Raw: 1a 80 c8 64 01 91 73 77 cb 1a 2f e8 04 d2 84 b4 ed 19 4b fc 91 d3 7b 6b 57 51 b9 92 37 1d 87 44 a9 7e 52 af a7 df 5f 7a ad c7 3d 9c 8f 67 70 c0 f1 9b 8e 06 ae 0d ce 6b f4 97 d7 69 dc b3 95 f9 41 b6 b6 ae 9f a8 be c6 fb 19 64 55 9c 4d f3 f2 ae b9 9f 2c e9 2c 72 e7 e8 eb 61 c3 8e 39 3f 56 f9 ce ac f9 86 30 4d 24 93 f3 6c 6a 18 33 23 2c 78 ff 00 e4 5d 87 d9 d4 04 d6 ef 90 c8 1f df a4 8e 3b 1a e9 b3 30 c7 23 b1 c8 5d 69 cb 15 24 9b ea 87 5b c8 76 56 30 be ae 66 5e 33 b1 25 93 41 bf 04 ee af ae 9d 21 6b c1 e0 dc b7 ce 55 92 dd 39 d8 3d 4e 55 ad 57 4f 72 0c 09 de 7b 73 dc b2 b6 4a 42 cf c6 5c aa f7 d1 70 fa 9b e6 60 c5 24 93 4c 7b 65 50 c0 00 c8 c2 7c ff 00 f1 06 c3 ec 3a 1b a0 a6 12 b7 f7 a7 c9 13 be 78 1b 24 6d 8d 99 8e 1f 02 a0 f9 52 cd fa 29 d7 b2 bd bc Data Ascii: dsw/K{kWQ7D~R_z=gpkAdUM,,ra9?V0M\$!j3##,x];0#]j\$[vVOF^3%A!kU9=NUWOr{skJBj`\$L{eP;:x\$mR)
2021-09-16 04:29:08 UTC	1761	IN	Data Raw: 43 5d 14 90 47 0e b7 fb ca 95 61 59 d8 d2 7d e6 b8 ee 2c a1 77 f7 a8 c4 15 d1 7d e7 97 2e 53 f8 9f a4 6b e1 91 6a e2 0c 60 7e e2 55 00 10 4d 9e 25 2c 89 73 5b dc a6 aa d7 7d 95 4b 66 2f 44 d9 51 44 e7 b1 78 1d 8b 64 6f b7 c4 e0 70 58 ad e2 e5 b9 63 4a 1f 9c 06 40 10 f1 9f 84 86 73 4d 27 ae 82 68 a0 93 e7 a5 6d 86 f8 7c e2 41 0a e6 7a 25 b7 62 df b9 a7 fb 1a f1 c8 ee 4e af 19 fc 9d e1 63 0b 98 c5 02 00 b1 3f 71 6a 99 19 1a 6c 4b 2d 4f d1 b4 36 77 a3 33 ec a2 61 2f 7c 0d f4 26 95 a7 5e d5 f6 fd 93 b8 c9 10 81 43 78 be fd ec f4 ec 29 63 c6 f1 80 00 f1 9c 90 d9 d0 c1 04 75 90 41 34 fe d6 75 42 ac 72 09 3c 1e 83 a2 a3 4e b6 3d ff 00 36 69 db d1 8c a0 86 c3 87 c0 98 60 cb 25 49 32 18 10 c7 3f 71 ca 00 61 34 59 9d 20 cd 3f 3f 6a 7e 84 b2 1b 37 e4 f2 e9 53 d6 d6 Data Ascii: CjGaY},w}.Skj`~UM%,s]KfjDQDxdopXc.J@sM'hm Az%bNc?qjIK-O6w3a /&^Cx)cuA4uBr<N=6i"6!2?qaY4 ??j~7S
2021-09-16 04:29:08 UTC	1762	IN	Data Raw: 6f 8a 6c 9d 28 cb 13 53 43 7a 92 db 3a d1 97 bd 3d 47 7e 61 f0 67 db 7f 8a 96 05 d7 36 63 da b1 b1 a8 e9 9a a5 85 0f 6a 6a 18 32 30 0c 01 58 f1 24 89 f7 72 44 fa f1 b4 82 43 4d a3 43 46 37 59 b3 f3 7f 5d f7 8c 9c 81 a5 82 c6 01 01 99 f8 d1 eb 8a 5e 14 c8 de d3 ae 34 d4 70 d0 66 91 3a f4 9f da fe 2a d2 9f a3 ac d4 ce 88 77 b2 ac b7 f7 7d da df e5 44 93 eb 27 9c c5 d1 d4 8c 38 df fd 7f 32 42 2f 42 d7 be b8 d4 30 01 80 0c 51 dc 8e ac b1 f1 17 89 2b d6 ee 0a 1e b2 7a 2d 50 8a 83 49 eb bb 66 8b 82 09 a6 b1 80 00 31 e5 77 0a ca ab ac d7 d9 24 54 4d 57 66 e6 c7 5d d9 4f c3 68 25 bb 37 71 d3 d4 3c 77 a7 52 a7 39 06 c5 17 c1 ff 00 62 1b 3c d0 c3 9a 5e ad cb ce d8 5e 09 57 6c fe 52 be 87 0c c0 30 0c 40 b9 72 0c 83 ac a1 d5 0d a9 13 fe fe 66 96 01 b9 8a b6 a9 9d b4 Data Ascii: ol(SCz:~G~ag6cj20X\$RDCMCF7Y)^4pf:*w)D'82B/B0Q+z-P!f1w\$TMWfjOh%7q~cWR9b<^^WIR0@rf
2021-09-16 04:29:08 UTC	1763	IN	Data Raw: 8d 68 e7 95 e9 bd 89 14 a4 ec d9 32 6c ac 51 60 92 c4 a3 5c 4d a9 67 b2 b4 cd 05 c3 4a cd 44 20 13 7a b6 3d ba 1b ef 8f 5e d4 44 2b a4 29 fa e6 49 2c 6c fe 74 36 6e 98 75 6a 84 9d 17 53 61 34 17 2f 60 0f 5b ab 58 b7 2a 0e 22 96 42 ab 91 d3 14 96 3a 94 92 7c dc 4e 60 d6 2e 9d aa 55 ae 3d ee c8 e9 46 3c 3c dd de b1 ae 8f 37 58 59 ad 78 82 a4 0c 4d eb e5 31 ba 44 9d 2c de 63 30 b6 4e 66 15 57 15 ee ca c2 49 70 64 9b ce a0 a5 51 1e 25 a3 6a c8 85 55 6a 9c e5 9f 42 93 b5 7e 6e 85 79 d8 ac a7 5e 71 35 ee 8b 45 dd 97 0a 49 ca 50 a3 4c 1a 70 84 c4 03 3c e8 df d7 91 4b 2d f6 4a 39 dc 9c 20 ac d3 a9 78 1a 36 f2 ee 74 1a f2 74 dc 3c dc 92 1d 0a 55 74 6c 46 35 04 c4 b3 a4 62 12 73 9e da 4d 1a 5e 89 2b 88 85 8c 0b 3a 66 bf b5 ad 27 4b 86 94 e6 49 67 65 d3 e9 87 06 Data Ascii: h2lQ`lMgJD z~^D+)l,l6nujSa4)EX""B: N`.U=F<<7XYxM1D,c0NfWlpdq%UjB~ny^q5EIPLp<K-J9 x6tt<UtlF5bsM!+:f'KIge
2021-09-16 04:29:08 UTC	1765	IN	Data Raw: c2 cd 38 9b ad 02 db cf cb f2 48 84 55 75 c0 2d 57 ec b6 ef 47 9e cd 76 a5 5b 16 70 b0 30 60 44 33 45 51 dd a7 75 a4 de 92 f6 16 62 c7 57 95 f3 96 a2 aa 97 50 59 63 e8 7b 45 b1 90 dd 87 b6 b5 98 a1 e2 b0 50 43 30 72 8b ad ea f7 d1 ab 23 a2 6c 1e 71 cb a0 2a 96 d4 15 7b 6c de a2 f4 75 74 90 82 6c 6c ec fe 68 50 ca 7a 82 af a1 f4 b2 4f 76 a2 c0 fa 9e 77 80 88 2a a5 c0 09 37 f3 7b ab 73 45 b0 c2 82 73 79 f1 73 4a a1 96 3c 51 7a 4e f6 cd a5 32 e0 92 f7 9a 61 b1 51 50 b8 a2 2a 77 b7 e2 bb 63 d5 bd 7e 19 be 66 e5 b3 24 e2 a9 b9 14 cc 51 c8 ab d1 7a ae 46 3c 04 fb 92 49 e6 b8 6d 04 52 d2 a2 80 be 9b a1 13 ba cd 6e 77 9b e6 f9 7a 4f 8d c0 67 0a f1 ef b9 ec d2 d7 ce af 72 cc 4d f2 24 85 14 12 c0 02 ad cf 4b 96 c5 58 db 67 07 90 ad 59 11 c8 19 b2 dc b0 84 79 fe 89 Data Ascii: 8HUu-WGv[p0'D3EQubWPYc{EPC0r#lq*{lutilhPzOvw*7{sEsYsJ<QzN2aQP*wc~f\$QzF<ImRnwzOgrM\$KXgYy
2021-09-16 04:29:08 UTC	1766	IN	Data Raw: 2b ec d3 2b cf dc 3f eb 22 16 33 40 63 c5 8d 9b 1d 5d 0f a9 3d 1d d1 f7 76 d2 fd b0 d4 e9 34 3d 38 fe 6a 5e d7 6a d7 61 d7 3d 45 72 6a 57 37 36 1e 1d 87 59 45 94 ba 83 73 23 a3 cf 3a 4d a9 6a eb db 65 44 bb 0f ed 07 55 50 56 b3 43 47 75 ed 54 bb 4e 49 9a 09 a0 ab 7f b0 c3 e4 38 88 c7 5a 7f bf 9a a6 1a 37 20 cb 0e 24 cd 26 c4 8b 16 2e 72 bd 75 d0 15 9a 91 39 22 95 38 7f 05 e3 b5 c0 2a 7c 07 c9 7e 3e ef f9 6c b6 83 9d 74 1c d8 bf 4c 79 77 64 ee 99 62 0d 38 93 98 e3 50 0d c9 fd 0a df 96 5a 51 47 15 6d 81 69 2e 50 af 52 a9 d9 8b 96 2c 25 68 82 f9 f1 44 2c ee 67 98 e9 63 b4 5e a4 42 28 17 07 1e 1c ff 00 d5 a8 c1 66 bd 2a b2 64 0d 45 a2 e8 de 88 fe 66 da 52 ab 01 da 08 a7 99 ed ec 27 c8 f5 f4 66 78 fa 73 55 6a a7 d8 68 a3 8a c5 3d 4b d8 8e d5 7f 2c d9 a6 90 eb Data Ascii: ++?'3@c]=v4=8j^ja=ErjW76YEs#:MjeDUPVCGuTNI8Z7 \$&.ru9*8!->ltLywdb8PZQGmi.PR,%hD.gc^B(f^dEfr'xsUjh=K,

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1767	IN	Data Raw: a3 c6 ac c0 af 72 60 59 9c b5 7b 08 0d 99 41 84 79 86 be ae 77 cb 5d 21 2c aa 35 d7 7c ae 24 85 98 52 71 3b 43 4f 34 7b 59 06 43 5f ed ef 30 f2 a6 b5 61 9a bf d5 d9 23 79 ff 00 35 f9 2f c7 dd 63 96 6d f1 9b 5d 92 ae 6c f6 4e 61 ad 65 63 c9 6c f2 bf 79 1f 7b d8 69 e4 96 52 f6 a7 d8 91 52 0e e8 b2 49 46 75 03 49 e4 54 be fd 9a 2b 56 fb 56 c0 ef 46 8f 99 eb c4 42 bc 45 29 db ec 34 36 31 9c 49 d4 e2 bf 39 cf 87 38 3c 4e 0f 6b 9c e7 f0 fa 7a aa 76 fb 59 63 8e 0b 32 77 65 15 01 e9 b8 09 ce 34 98 59 c9 e2 4e e7 ed e1 bf ae 4b 39 07 e4 5d 18 81 54 72 d4 03 60 d3 a3 14 d1 42 b9 1e a9 17 16 a2 8c 5a a9 ca eb ea 86 86 18 d4 32 ff 00 69 eb a1 6b b5 a2 0f 3d 28 ce 59 41 25 6d 7c b2 54 b9 5a 62 95 76 dd 88 d4 a4 ff 00 f1 fd 53 59 fc e9 63 64 7f c8 7c 97 e3 ee d9 7e d8 Data Ascii: r`Y{Ayw}l,5}\$Rq;CO4{YC_0a#y5/cm}JlNaecly{iRRIFuIT+VVFBE}461I98<NkzvYc2we4YNK9J}Tr`BZ2ik=(Y A%m}TzbvSYcd ~
2021-09-16 04:29:08 UTC	1769	IN	Data Raw: de c4 ce d0 c8 72 1a 51 ca 62 d7 3f 78 4e 65 6a c0 63 c0 cb 91 d5 ef 4a f4 9b 25 d4 06 c1 ab f4 b7 a8 0f 8f 5f c1 36 69 a9 46 3c 32 c9 cb a9 5e 2b dd ed b5 a4 b7 e6 d4 82 53 89 21 38 bf 80 c1 ed 71 e3 5d 43 4f a9 db 88 ad cf 30 39 d3 12 7f dc 89 12 24 ea 3e a0 6c b7 bc 62 f6 6e cf 74 db 0b 12 c8 b2 cf 26 41 6e e2 65 2d ac d9 4b 62 cc b4 67 25 64 99 d7 2e 5b 70 bb 3b b2 65 87 91 83 41 29 3e 43 0c 8a 09 89 a7 0d c3 95 e9 48 17 57 5f 8c d6 c2 ea f5 f5 84 91 00 92 d0 fe bb 0f fe 42 b8 f2 e5 95 a4 b1 04 d4 1c d7 67 e7 5f 35 9e 59 98 9f 1a 56 4d 6b 77 ce fd cd cf 01 fb 5f 8f b7 d4 7c b5 7d c3 f9 92 45 28 b8 53 70 cb 6a e6 9f 47 1c 70 ec 55 a3 82 6a c8 b8 35 56 e4 31 ea 6e 26 43 ae e5 a3 d7 93 89 ad 2d 83 59 e9 63 52 dd 90 eb 86 47 af 41 23 57 5c f2 57 25 ac 9c Data Ascii: rQb?xNejcJ%_6iF<2^+S!8q]CO09\$>lbont&Ane-Kbg%d.[p.eA)>CHW__BMg_5YVMkw_]jE(Sp[GpUj5V1n&C-Y cRGA#WWW%
2021-09-16 04:29:08 UTC	1770	IN	Data Raw: fe 03 e4 bf 1f 68 e5 d1 dd 1d d8 bc cc d6 20 fb bb a3 be f4 11 2a 88 c7 a2 64 63 00 c4 18 06 28 1c 71 9e 9e 07 1c 63 8c 23 12 c4 9f a0 ca 0c e3 d2 df a6 6e 13 fb e8 2b 17 cd 79 ee 14 f9 ed e2 65 2d ac d9 4b 62 cc b4 67 25 64 99 d7 44 f4 3d 51 5a 30 fc 62 4d e8 92 f3 8d 27 18 f3 e4 d7 11 17 77 b9 3c 74 be b2 4b 0b 5f b5 52 4b 08 17 cf 53 8c 50 8b 95 bb b3 7d ad 26 be 9b 6c ca 68 5f ef 1e 72 9c 07 03 67 c7 19 88 c7 94 71 f1 7d 72 da a9 4d e4 b1 a6 50 ad db 9d 4b 45 66 4a 1c c5 7a a4 7d da ff 00 a9 f3 ac dd 43 e1 cf e2 bf 25 f8 fb 52 1f 4d 93 76 c3 61 24 41 5c 18 72 b1 32 4b 5f d5 23 19 03 16 cc 23 23 9e 23 88 c8 71 08 c5 fd 72 33 fc 83 8c 70 f1 8e 47 32 cf 12 e5 fe a7 a9 13 5d eb 4b ad 20 ea 8d 9b e6 b7 ab e1 97 2c 48 92 47 be 1d a9 d2 d1 73 95 23 f2 e4 Data Ascii: h *dc(qc&dn+y^s9??TD=QZ0bM'w<tK_RKSP)&lh_rgqrMPKEfJzjC)%RMva\$A!r2K_#9####qr3pG2j]K ,HG#s#
2021-09-16 04:29:08 UTC	1771	IN	Data Raw: d6 1b 3b 9f f9 10 dd 86 9d 5f e7 64 b8 f6 76 54 23 57 dc c4 c5 b6 81 8d 7b 94 9b 05 8a 84 43 b7 15 d9 6d d4 b7 03 4c 61 c7 d9 c4 63 bc a6 29 b4 96 8c d0 a1 21 98 71 88 ca 44 63 d1 70 5f d5 bf 02 dd dd d8 15 52 d7 9a ff 00 75 ee 6b ff 00 26 1e 17 ad a5 6a f5 a8 cc e5 04 70 c7 b9 64 49 da b5 78 8c d1 8f bb e3 d6 3f da 62 ae 34 0a d8 fa a8 58 ae a4 0c 4d 5c 79 04 4a 82 73 c8 7f dc 72 90 2d 1e 4d 73 e8 bc 15 78 94 e1 ab 11 cf b6 5c f2 f1 d7 8c 97 19 d2 31 55 4c ba cd 3b f3 0c 3f ba e7 98 81 ff 00 74 7e fd c3 f9 fd 16 94 c9 a6 9b d3 17 bb b7 63 28 48 ba 83 65 6d d0 dc f2 ad 6e ba 90 4a 95 6f 5c 9e 0f e1 76 52 d4 87 a2 e5 f2 6b 74 9e d0 db 93 a4 2f 28 8e 8d c3 97 b1 b0 8d 86 f5 eb c9 fe ac 0f 1a bd 9b 4c d1 cf 1d 7e 9d 8b 85 e4 2b 95 52 b1 a8 e6 17 e4 12 Data Ascii: _dvT#W{CmLac}lqDc`yemKuk&jpdx?b4XMyJsr-Msx1UL;?t~c(HemnJolvRkt/{L~+R
2021-09-16 04:29:08 UTC	1773	IN	Data Raw: 89 79 72 4b 68 c6 39 e3 0c 76 41 b2 d6 d4 98 e1 d8 64 b3 97 79 ec 13 24 76 3d 27 98 64 d6 33 57 46 49 e4 8a 30 ab f5 10 81 d2 27 8f 02 3d c1 f2 5f 8f e6 d8 17 17 36 30 79 f4 5e 7b 55 2f c1 70 5f d5 bf 02 dd dd d8 15 52 d7 9a ff 00 e3 f5 8a 70 1f 45 ce f0 32 5b 00 64 bb 9a 11 64 1d 41 ae 79 3f 92 8f 2c 6f 69 c6 a9 d4 1a f7 c8 ae a3 81 3f a4 d2 67 19 29 c3 9d 43 3b 25 6b a8 7e 9e 5f cb 87 a5 a0 6d c6 dd 4f 2d 5e 31 de 9f af fa 27 c0 f8 a7 77 3a 1a f0 5b e9 6d 95 4b 14 9a 2d b7 95 1a 6f 71 37 06 44 9b 6a 18 3e c9 c8 5d 91 e2 5d b9 65 7d 9c a2 33 7c f1 fc 8b 21 9b 65 e5 a8 bc 16 71 67 b3 24 b4 4b d0 a4 67 6a b1 ac 6a 83 d7 ea 58 ce e9 2f 13 fb ce 33 8c e3 38 fc 87 c9 7e 3f 99 c0 3c 7a e3 a4 5c 4e 5d 9e 97 aa ed e9 ec b6 f2 84 ae 77 32 8c d7 79 d1 98 9b 95 39 13 Data Ascii: yrKh9vAdy\$v='d3WFI0'=_60y^{U/p_mRpE2{ddAy?,oi?g)C;%k~_mo-^1'w:[mK-oq7D]>]}e3jleqqg\$KgjX/38-? <z^Mw2y9
2021-09-16 04:29:08 UTC	1774	IN	Data Raw: a7 6f d3 25 48 f0 e3 08 c2 30 8c e3 00 f5 5f 8f b4 46 4f 07 70 b9 46 75 3e 5d cd 0c 59 d3 f6 98 98 30 1c bd 42 bd b8 76 7a 2b fa f7 ad d6 52 d5 6a 5d 4d ad b2 8d b7 af c4 9d 41 42 3c 7e a7 d6 8c bd d6 fa 98 86 c7 ad 2e d9 3a 1d 74 f6 65 de d5 0b ad d8 bf 75 78 39 33 69 74 82 e5 fa fd 1b ad 28 7a 23 54 72 b7 4d eb eb e4 70 2a 02 30 7b 90 c3 2c b2 53 e9 78 91 3e f2 ad 48 ed dd 0e 64 5e 44 b1 49 dc 64 95 0d 6d 94 f0 b7 dd 79 90 f9 fc e0 67 e6 1d a9 89 ba 27 ea 46 a3 65 05 8f ef 26 c6 9c 57 6a 1b 52 43 6d fb 78 70 70 91 cc 9c 72 c3 24 4c 92 3c f2 ce 2a 3e 56 24 65 6e 78 ad fa 56 c4 1c 62 37 a4 ed c2 f5 b5 af f8 7a 0f ff 00 6b 6e b1 b1 d1 91 70 82 23 ca d2 96 54 c4 f3 1b 22 6f 4d 8f 4e 6b ed e5 fe 93 d8 57 12 45 24 6d c6 11 84 61 18 3e 4b f1 f7 0a 29 ce a3 bb Data Ascii: o%H0_FOPfu>]Y0Bvz+Rj]MAB<~.teux93it(z#TrMp*O{,Sx>Hd^Dldmyg'Fe&WjRCmxppr\$L<^>V\$enxVb7zkn p#T"oMnkWE\$ma>K)
2021-09-16 04:29:08 UTC	1775	IN	Data Raw: 47 30 7a e4 11 71 83 09 52 65 97 83 35 8e 32 59 bc c6 aa 38 15 54 ae 3b 67 98 7b a3 94 86 1f a2 40 c9 b6 7a f8 b2 6e a7 d7 ae 58 ea 8b af 93 4f 6e cb 2c 18 b1 e0 51 9d b8 c3 1b d7 15 39 31 c7 c0 60 31 46 2e 28 e7 0a e7 19 1e 0c e3 c0 0c e3 1b 25 cb 07 24 18 07 ae 15 ee 5e 78 30 9e 71 a1 07 00 92 29 29 75 2b 2e 57 b3 5e 74 fc c0 fc 22 da 4d 03 56 d9 c6 ca 48 ed 92 30 04 a8 cd a4 cc b9 5e cb a6 19 a0 b2 0f 9d 52 41 66 39 12 c0 0a 56 f2 b6 cd 43 c9 c1 26 79 b9 df 8a fc 61 2a c1 d1 90 83 9d 3d bc b1 a5 dd 52 b1 5a e5 47 8b 91 b8 e9 28 e4 26 46 af 63 9e 70 9c ee c1 20 c4 61 cd 9b 51 c5 1f 55 6f a4 bf 6b a4 2a 7d b7 4b 81 80 60 19 d6 e0 ff 00 a3 e3 8b d6 24 0a 10 ff 00 53 31 c9 66 51 93 5c ed 12 d8 77 35 a3 c8 10 71 03 1f 09 0f ac 6f e8 76 7b 36 0c f3 c9 9d Data Ascii: G0zqRe52Y8T;g{ @znXOn,Q91`1F.(%\$^x0q))u+.W~"t"MVH0^RAf9VRC&ya*=RZG(&Fcp aQUok*)K`\$S1fQlw5q ov[6
2021-09-16 04:29:08 UTC	1777	IN	Data Raw: e9 e9 18 84 16 ba 99 d5 c4 d3 bb 30 b1 36 9f 75 d0 e6 c0 73 5c 11 c0 40 76 12 2e 22 51 7b e9 35 b8 6e e2 d8 88 df 64 fa 85 b0 e1 6f 15 52 9d 3c 9b 18 9c 72 58 29 4b 88 cd dd 3e ad 84 8d ae c8 0f 15 83 1b 1d 1b 5b 97 64 39 a1 cb d8 4b 9c 61 a3 35 d6 d7 b3 7d d6 14 d6 b7 3f ee 16 bb ac 0f 35 84 00 1b b2 62 e7 8a c2 c1 ac 73 a8 7e c1 10 6a b4 38 0f 88 12 9d 48 39 b9 e6 59 3f 30 89 c7 b0 de c4 23 81 c2 cb 03 cd 8d 9c 3e e9 95 1b 7c 72 df 14 1e 04 96 8b 1f 1d 89 a5 ac bf 24 c7 44 75 95 a3 c0 a9 9f e1 03 32 b6 31 bf 35 c7 79 f6 ed 5c 2e e4 e0 54 8a 75 07 82 c3 83 5b 86 d4 cd 2b 49 71 69 d8 d6 b7 11 8e 28 b7 46 a8 c6 b7 6c 0b 8f 35 5d a5 f5 0b eb 90 f7 16 e7 23 9a 3d 73 b4 d7 4d e1 d0 ef a2 02 b5 57 b0 1c 83 eb 61 93 e0 89 d1 aa 32 a3 8d a0 55 15 3c 2e 50 71 d0 Data Ascii: 06us}@v."Q{5ndoR<rX)K>[d9Ka5]?5bs~j8H9Y?0#> r\$Du215y}.Tu+ iqi(Fi5)}=sMWa2U<.Pq
2021-09-16 04:29:08 UTC	1778	IN	Data Raw: d3 5d d6 d6 b9 db 7a ac 20 ff 00 a6 55 b4 6a 35 44 83 2d 23 f5 05 5f 41 7d 33 f1 62 bf 9c a6 8d 27 1b 67 27 3c 5b c1 ed 5d 75 0a 9d 5d 43 ef 35 d8 49 f1 c9 de 2b 1e 37 9f ce c1 0e fe 66 5c 11 c9 3b 48 c0 da 8d 6e 6e 66 61 63 a7 53 f6 86 81 ac c9 97 b0 78 dc 84 1f a2 16 d4 a2 e3 25 92 75 5c 73 0d dd c8 e6 9f 45 b8 c3 6a 9b b3 71 d8 e1 cb de 1b 91 6d 46 75 9a 33 dd 82 a5 37 5d b3 f9 4e c3 c1 7e d3 f8 63 8d 6d 17 e0 77 7e 9f e4 70 dc bf 69 a2 f7 32 e3 11 39 b0 8d 8e 8d 9b 8e c4 f2 e6 45 59 1d 73 79 f7 6a b7 81 c8 a1 50 33 11 8d 78 17 73 79 6d 8d a1 3b f1 8f c1 c3 7a a8 9a d4 1b 93 7f 33 38 70 e8 8e c8 73 43 97 b0 56 27 fc a5 a4 b4 8e e6 14 40 50 dd f7 58 c9 16 10 10 73 45 85 4b ff 00 30 52 e2 27 6a c3 41 b1 6b 94 44 18 1b 7d d5 05 ba d8 47 c9 56 a6 e7 4b 44 Data Ascii: jz Uj5D-#_A)3b'g<[u]C5l+7f{;HnnfacSx%u\$sEjqmFu37jN~cmw~pi29EYsyjP3xsym;z38psCV'@PXS EK0 R'jAkDjGVKd

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1779	IN	Data Raw: 8f dc 27 63 c6 ef cc 11 a3 a5 3f 15 3a 8e 81 51 d9 b5 db 9e 78 ef 44 38 6a 92 80 92 74 7b c6 d3 4c 93 ff 00 69 dc ba e0 2d 38 5e d1 7b 1d bf a2 ab a0 e9 04 f5 55 0b 9a 0f 3b ff 00 50 aa 53 0f 1f b4 50 76 3a 64 fb af c8 b4 f0 72 66 97 4d b1 ad ae c3 ee bb 22 a2 3d 5b 87 5a df e1 98 23 9b 4a 75 0a b0 ec 4c db b7 8a ad a1 d6 a3 ea 41 d5 1b b8 b7 b1 1c d0 e5 ec 24 2c 12 46 1b 2d 47 9b 1c bf 42 9a 23 6e 4e 00 a9 14 98 d3 bc a9 aa 4b b7 0d 83 c1 6a 00 a4 99 28 fd 02 80 10 26 0c ec 5b 6e 8c b7 c1 5e fb 80 57 99 dd c1 10 a1 5f da 5b 0c c5 7e ee 4f 34 cd 2c 8a 9f b3 dd b4 87 71 91 90 4d a9 58 df 33 cc a3 48 b9 c4 6b 17 09 de 66 db 91 13 84 03 2e 39 94 1b 42 28 33 dd 6b 6e ee 6e 27 7a 86 e9 15 63 99 57 d2 2a 9f 12 81 66 91 54 8d ce 74 a9 2f a9 c4 12 08 f2 21 45 66 Data Ascii: 'c?:QxD8j{Li-8^{\U;PSPv:drfM"=[Z#JuLa\$,F-GB#nNKj{&[n^W_[-4,qMX3Hkf.9B(3knn'zcW*FTt)!Ef
2021-09-16 04:29:08 UTC	1781	IN	Data Raw: 0d 3d de ad b7 f8 77 15 0e f4 c7 34 39 76 c7 e6 9d 87 34 6f 65 85 a4 9c 33 92 04 95 6c c0 d8 85 fb c6 39 2c 4e e4 8b b6 e0 4c 6b bb a2 1c e5 6b 34 2e 4a 06 ff 00 94 5d 56 6c 58 9c 2b ab 39 8b 2c 33 9a 34 5d 20 82 20 ef 05 75 6f cb 61 50 63 3c d4 85 7d 8b ba 1e 37 ed 57 69 6b b7 6c f6 7d 08 49 8e b9 ae 8d 84 85 1c 65 17 6c c1 ff 00 6a c5 b2 14 f4 59 77 56 49 ad 6b 0d f6 ee e8 ee 88 1e 6b 25 9f 44 ac d6 4a d7 f4 33 51 b3 a2 08 46 d5 bc 4c 27 36 d2 77 11 e0 9a e6 d9 ec 70 77 95 96 10 75 ba d6 bc 71 8f fc a1 17 11 1e 68 33 73 96 87 50 dd 8e a2 69 d4 1c 11 a5 36 ce 99 fb 28 3e 90 e6 87 2e da 07 34 77 c1 95 84 1b a7 5e 09 4e 6c c9 84 09 ce 53 40 c9 46 c9 08 f1 1f 75 1f 1d 48 f2 4f 7e c1 f4 09 ce df 56 dc 80 55 1d b1 35 c0 77 9d 74 36 03 b9 37 74 c2 c5 ef 34 44 Data Ascii: =w49v4oe3l9,NLkk4.J[VIX+9,34] uoaPc<}7Wikl}leljYwVlkk%DJ3QHL6pwuqh3sPi6(>.4w^NIS@FuHo~VU5wt67t4D
2021-09-16 04:29:08 UTC	1782	IN	Data Raw: c9 5a 84 80 af d3 4a b0 f7 1d 2a ad 68 8c 6e 9e 91 cd 0e 5d a3 58 3d e7 b1 be 65 57 74 58 97 f9 01 0a 67 58 56 93 c6 2c 9d 86 fa d8 53 29 96 cc 9c 4e fc c7 f4 0b 0b 77 45 94 ba 5c ed c1 03 84 37 9a b9 b7 9a 69 75 8e f6 ab 5f 8a 9d ab 9a 91 98 41 f1 cc 23 6b 74 f8 2c b3 4e 0b 7a d9 75 86 62 51 87 34 1e 08 09 06 44 ac ca cd 77 be 4b 62 e3 ec 12 99 86 f7 58 be 36 36 3c 93 ad 90 cd 3d b1 c9 5d a6 66 e8 ea a1 24 4a 2f 6d 27 96 83 9c 23 ea 5c ae d2 14 82 80 1d 19 42 36 57 45 61 63 64 af 70 73 2b 54 d0 71 fe 25 35 34 67 46 f6 6b 2d 52 27 e6 10 ba 00 20 a5 3a d1 64 7c 50 33 90 03 c9 54 3f 11 fa a6 bb 61 05 ab 49 c3 9e 0f 92 82 08 ec 07 34 39 76 98 cf bb 75 a4 c1 bb 9a e8 f3 28 34 df 5b e6 42 a7 5a a7 1f 3d a7 c1 75 ae 66 bb 84 06 ee 1b 02 c3 9b f6 ee 6a 3b 5c bb Data Ascii: ZJ*hnjX=eWtXgXV,S)NwEl7iu_A#kt,NzubQ4DwKbX66<=f]\$J/m#B6WEacdps+Tq%54gFk-R':d]p3T?al49vu(4[BZ=ufj;\
2021-09-16 04:29:08 UTC	1783	IN	Data Raw: 46 d1 ec 95 28 0d 66 0a d7 6e ec 48 75 34 83 49 26 4e de 8c fa 78 a8 94 ca ad 12 5b 3f 31 09 cd c3 7c a1 7a ca 27 0f e5 29 af 63 e5 a5 12 5d c5 7a aa 46 06 d7 20 1d 47 c8 a1 72 39 a1 54 7c 29 f7 f7 6c b3 43 a2 65 49 2b c5 47 40 29 d4 eb 6f b2 f5 70 98 d6 7b c5 54 a4 d7 61 a9 52 ca 4f 60 39 a1 cb b2 32 e0 14 49 00 05 0d 09 d5 1d 93 41 71 f0 55 73 c5 56 b7 f5 29 a3 a0 0f 70 21 8d ad 28 0c 21 41 68 44 34 2c 6d 2a c0 ef 95 85 db 3d 03 75 65 2e 0b f7 6e b7 05 76 3c 2c fa 69 9d c5 55 69 f7 8c 8f 14 c3 b9 31 c3 6e 48 54 16 20 e1 70 f6 4a f4 24 e2 ef 11 c1 5f 78 64 0a 95 31 cb a1 c 7 30 a2 16 4a 5c d1 8b 2c 4a ed 0e 84 43 62 11 0b 09 00 ec 52 c8 4d 2f 75 b7 20 0c c2 52 54 1e 8b 80 b8 74 70 41 14 4e 2b 0b f9 a1 50 6e 95 28 d4 a8 44 35 39 ac 71 ea a9 d8 76 23 9a 1c Data Ascii: F(fnHu4l&Nx{?1 z'}c]zF Gr9Tj))Cei+G@)op{TaRO`92lAqUsV)p!(AhD4,m*=ue.nv<,iUi1nHT pJ\$_xF1OJ\JCbRM/u "TtpAN+Pn(D59qv#
2021-09-16 04:29:08 UTC	1785	IN	Data Raw: 49 42 f3 0e cf 9a 7d 58 83 3a dc db 65 e6 87 3e d2 14 f6 3a 29 71 81 56 68 9f e7 de 8a 2a b3 f1 1f 59 1e 11 6b 74 64 9a ec 37 59 0b 5d 41 43 08 68 5d d6 9d ab 26 c6 68 c5 d5 c9 cd 07 66 88 c9 4a 9e 8b 29 9e 83 25 60 16 25 98 bc 49 80 8b ce 64 c9 ed 47 34 39 76 05 bb 62 13 df f9 a0 78 74 1e 81 7b df fa 05 e0 a3 d3 cf d2 8e c3 a9 2f 68 73 68 8b 13 b5 d7 55 a9 65 2d 16 e4 a7 e3 69 07 98 b2 07 82 6e fe d0 4a 74 76 34 6a 8b 16 54 6b bc 8c aa 75 98 75 5e d0 ef 35 e0 89 26 c8 11 e2 a6 2d 08 2b 1d 88 90 24 4a 23 01 59 1e 3e 2a d4 dd ba ea 09 8c ac 10 db 2b 82 92 8a 27 a0 f4 f3 5d 4c d9 b1 db 0e 68 72 ec 1c e1 9e ce 27 62 c0 3d de 83 08 92 8b 34 52 1f 87 bc e1 78 3c 91 a6 e7 08 19 da 11 1b ef d8 b8 20 a6 3a 01 43 d2 85 a6 54 27 3d 23 08 f0 b0 fa 26 32 b3 9e f0 1d Data Ascii: lBjX:e->]qVh*Yktd7YjAChj&hfj)%%&l dG49vbxt{hshUe-inJtv4jTkuu^5&+-\$jY#>+*]Lhrb=4Rx< :CT'=##&2
2021-09-16 04:29:08 UTC	1786	IN	Data Raw: 2a 73 89 17 50 2c 44 85 c4 ac f6 28 9e 09 97 33 89 c3 e4 16 01 94 41 5c 31 28 8c c8 4d 11 c9 5d a8 15 3d 3a 54 ee ed c7 34 39 0e d6 4a c9 64 8f e5 00 2c 54 ed 55 b9 14 58 f1 86 a3 6c e0 a7 d0 32 16 2a 32 c7 70 56 66 3e 4b ff 00 6c e5 1d 4c 73 53 59 f0 37 05 aa 2f bf d0 2e 68 97 e4 06 e9 da 56 27 b8 97 3c e2 29 c5 00 9c 7c 02 20 84 df 0f 6a d0 89 ff 00 2a 3c 41 45 14 58 46 a9 32 b5 27 79 84 d2 27 c8 9d d0 bd 66 cd 99 ca 81 e0 a3 0c 8d a9 cd 0d 00 46 63 7c ed 5a d9 0c 94 c2 d5 6a 12 82 0a dd 35 e8 53 cc c1 f2 58 4d 6a 85 c3 34 6a 51 3d 65 3f 9f 6a 39 a1 cb b7 24 a7 3b 79 9e 4e ba 86 ad 61 f3 46 95 51 86 a0 d8 55 bd 2c 96 5e 8b 71 5d ce 70 00 7d d5 6c 6e 38 6a 53 2e 3b 60 32 ff 00 28 45 d1 13 90 dc 36 04 f7 71 43 a2 77 14 79 4f b3 c5 3a 6e 77 20 a5 f4 5e d1 Data Ascii: *sP,D(3A\1(MJ)=:T49Jd,TUXl2*2pVf>KlLSy7/.hV'<)) j*<AEXF2'yM'fFc[Zj5SXMj4jQ=e?j9\$;yaFQU,^qjp])ln8jS. ;'2(E6qCwyO:nw ^
2021-09-16 04:29:08 UTC	1787	IN	Data Raw: 8d 5f bc d3 63 b1 c3 78 ec 73 f4 4a 6e 8f 48 1b 9d 67 6e 0a 9d 26 36 30 88 5f 89 bf 76 85 5b fe df 42 e8 59 0b 05 61 0b 35 2a e8 13 6a 4d 3e 6b 0e 50 16 76 ec f5 df 2e f8 5b 72 8b 41 ea e9 fc 2d db cc fb 30 d1 ea 1f 5a c1 63 f1 0f d4 7b 0e 1b b5 6a 54 f0 2b 17 7b f8 4a 93 8a 67 28 c9 11 5e 83 5c 77 c4 1f 08 44 e8 d5 a3 f2 54 fd 54 56 a6 5b c7 67 61 8d b9 ee f4 7f 65 d2 8f fc 66 82 03 0b fd e3 4f 26 3f c3 22 ba 9a e3 93 86 4e 1b c7 a7 9f a5 d2 1c dd b0 2c 2c 12 e3 de 76 d3 d1 f8 b1 ff 00 e1 54 51 e9 58 f4 66 80 f7 50 68 10 a1 71 25 0e c0 8c 58 df f0 b5 10 0f 56 cd cd fd 7a 63 d9 43 9a 48 20 c8 23 62 14 b4 82 1b 57 20 76 3b fa fb 06 1b b5 d1 f5 5b 55 aa 3b 10 b7 05 15 43 6a 73 52 26 9b 8e 5b 91 73 5e 1e 06 f3 0b d7 52 b7 10 8b a8 9e ad db b6 28 a8 d8 dc Data Ascii: _cxsJnHgn&60_vfBYa5*jM>kPv.[rA-0Zc{]T+[Jg('wDdTTV[gaefO&?^N,.vTQXfPhq%XVzcCH #bW v;[U:CjsR&[s^R(
2021-09-16 04:29:08 UTC	1789	IN	Data Raw: a9 52 a5 7a 57 a5 d5 eb 0c 74 60 cf 17 e5 96 c3 81 aa 3f 6e 73 f4 07 97 c6 61 00 b6 40 5b e2 b9 83 88 57 f6 9c 0b c4 dd 19 2e 20 be ed a9 83 b1 14 0d af ee 3e a3 0a 44 55 b5 7a a7 32 98 b2 95 15 e7 a6 68 f7 83 50 19 a3 44 3a 84 b9 40 a9 6d b6 f1 7d e1 20 e2 0d 07 85 5d e6 08 6b 2d f2 71 e7 11 88 ce 18 1b 47 4e 8c 31 c2 08 14 17 c5 fd b0 04 c2 14 d5 50 c5 5c 4c bf 07 13 63 50 40 83 cf 33 85 7a f1 2b d5 3d 2a 54 af 4a 95 fc 2a 67 d3 9e 6a 31 8a 23 2a 04 af 40 83 2a 0a 76 73 4f 51 c3 1d 3a 4a e4 47 06 30 85 52 62 60 5b 2d 4d 38 a6 08 54 df 44 1a 53 05 7d b4 01 d2 d4 8c e4 50 f0 b2 b2 19 50 d0 d1 c9 ef 2d 02 ed 37 9e 3b 1d a5 d7 50 c3 c2 e9 b5 b7 0d 44 30 f6 4b 47 c8 5b de 5c 64 ba a2 4e d4 7e 4a 06 80 2a 64 bd ed 2b 4a ce 1a dc 50 4d fb 20 92 41 aa 02 aa c5 Data Ascii: RzWt'?nsa@[W. >DUZ2hPD:@m]) k-qGN1PLcP@3z+*=TJ*gj1#*^vsOQ:JG0Rb[-M8TDS]KaPP-7;PD0KG[\dN~J*d+JPM A
2021-09-16 04:29:08 UTC	1790	IN	Data Raw: ec 32 94 a2 f8 fc 3e 0d 80 ac 6d 2a d5 d4 8b d7 0a ee 7c c3 cc ad 7d 96 83 0f 20 b8 c0 15 32 c4 0f 7f 22 36 45 07 9a a8 52 a0 73 a6 23 4a 80 e6 89 54 45 9d ce 67 c7 cb 49 a1 65 99 6c ba 86 5d 93 24 4e 3a ba 1c aa 3a ba 3a 94 b8 33 30 9c 9f 63 a9 72 50 eb ab 8c ac 61 63 0b 16 01 71 44 58 b1 7c 0f d8 3e 07 e4 af f2 bd 25 0a 15 c6 32 7c e0 3e c5 c0 b8 40 65 c3 86 7b d4 d2 c3 53 91 65 90 d0 b4 48 73 59 f1 82 15 c7 a3 d4 ac d7 21 70 19 41 0c 5a 30 5e 85 8c 3a a0 68 2a f5 d5 e4 80 05 0b 35 69 c1 c1 84 ec a2 5d 55 0e b7 cf 36 44 e2 2d 46 80 5d b7 5d 7c 66 31 7b 8a 0b 7b 8b 30 da d2 f8 01 ac d6 13 50 8d 85 41 95 36 d1 8e f1 40 17 6a 49 79 d0 d5 42 f0 ba 07 cf 18 c1 b8 d5 76 7c d2 d1 fe e6 48 50 82 39 e2 17 c9 0c 1c ee ec 6d 85 5e 57 35 b5 ec 45 a5 40 2e db af 3c fd Data Ascii: >2>m*}] 2^6ERsJTEjle]j\$N:::30crPacqDX[>%2]>@e{SeHsY!pAZO^:h^5i]U6D-Fj]]f1x[0PA6@]jlyBvHr9m^W5E@.<

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1791	IN	Data Raw: 85 1d 77 d2 2a 68 5e 2d 60 f7 94 43 3b 39 35 6f a2 69 c8 d9 2b 48 f4 9b 2e 53 a9 cb 98 b1 e2 a7 7b 0b c4 47 98 78 68 b0 71 3d 4c 27 88 15 45 56 68 48 cb 9c 4b 8b 16 31 fc 0f d9 f4 5f 9f c4 f4 c7 f2 ab 88 48 dd d4 51 4d 89 ec 95 29 1a 96 69 c9 53 fd c7 77 b0 98 19 79 24 a9 08 cf 1a d7 83 d2 2d 26 25 55 54 75 a9 65 81 46 2e 37 c0 e3 52 be 06 d2 eb 06 f5 fd c5 47 5b 25 eb 94 90 55 9d 80 9d 9a 97 f0 66 50 5a 3a 16 38 b9 54 b0 17 de 4a c5 ca 86 70 57 bc cc d0 5d 8b f0 8e 8a c5 2b 05 0d d7 4d 41 28 4a e8 15 af 75 79 84 94 2c 5d 60 01 79 1d 79 b9 99 44 2d 45 35 ff 00 d8 00 4e 10 7e 60 3a 2e 8d 62 11 aa 68 80 2f 8f 12 ce b2 95 8b 65 bc 87 dc 00 4a 3d 2b d2 bf 85 46 c9 ea ce 7d 46 3d 6f d1 58 fa 92 30 ad d0 19 ec 12 c6 06 c1 06 1d 08 66 a3 05 5b 5b a0 2d 1d d7 Data Ascii: w'h^~C;95oi+H.S{Gxhq=L'EVhHK1_HQM)iSwy\$-&%UTueF.7RG[%UfPZ:8TPwJ]+MA(Juy,)yyD-E5N-`:.bh/eJ=+F)F=oX0f[[-
2021-09-16 04:29:08 UTC	1793	IN	Data Raw: 00 16 d6 1e ac c4 80 3c 2b 7c e6 54 70 16 84 7b df f5 2c bb 03 25 e4 68 17 1e 61 b8 46 ea f4 5f 97 50 84 51 44 80 63 80 e0 9b e4 73 99 5d 84 b1 85 77 8e 30 ca b9 83 8c cd a0 b2 e5 ff 00 00 fe 17 2f d1 66 oc b8 b9 f5 0b 55 7a 36 06 6b ba 31 5a 3c f5 6b b7 7a 86 84 2b 47 4b 43 9f a4 a9 4f 1d 37 57 89 1d 24 61 ce b4 bf 00 70 e9 8e fe f1 da a0 5d b8 84 30 84 9a 6e 32 f1 02 9e ca 83 47 3c 75 95 d4 48 30 54 30 2c 1c 9b 61 50 79 00 d0 6b 5c 9d 61 67 03 8b 16 95 e5 bf 29 16 b2 2b 91 17 da cc 43 3b 60 c0 1f ad 6f da aa 01 45 0e 70 38 c2 58 8b 37 6d dd 03 e0 c4 12 d0 86 d7 b7 7b 39 f1 1a 15 10 34 3a 4e 86 28 f3 12 37 97 22 bb 03 b7 58 f9 e1 a5 a1 4e eb a7 d1 82 8d 2e a1 ca 73 8e db 3d e2 4b ce 40 36 62 9f da 42 18 93 61 49 64 41 e8 fc cb 16 21 09 78 39 ae 97 b9 Data Ascii: <+ Tp ,%haF_PQDcs]w0/fUz6k1Z<kz+GKCO7W\$ap0n2G<uH0T0,aPyKlag)+C;`oEp8X7m[94(N(7"XN.s=K@6bBaldA!x9
2021-09-16 04:29:08 UTC	1794	IN	Data Raw: 7c c6 6d 43 d5 a4 4f ee e0 2d 70 b7 c5 ab 9f 98 fc 2c 89 57 41 47 58 01 28 eb 81 a3 4f 52 0e da 05 a3 63 ca 1d 2a c0 3b 95 fd 40 7d ee a6 c8 f9 18 f1 0a 2e ba 1e 5d 98 e8 11 1a 48 c6 31 1f 43 f0 3f 60 f8 5f 92 bf c8 ab 3d a5 aa 4f f6 2b 31 f8 31 45 d6 5c 6e c6 0d ca b8 92 02 98 ab cd d7 38 8b 45 4b 5f 8c 45 b0 a0 8a df 13 c2 73 a5 d5 ca 83 50 7b f5 9f d8 06 55 08 3e 13 2c e5 a7 5d 31 fe a2 aa 00 db 34 64 59 63 f7 01 c3 43 ee 04 14 b5 8f 60 ff 00 70 d8 1a 7d eb f1 97 f9 97 9e 4d 9f ea 35 9a b3 47 1b a9 5e 38 08 ed 65 ec 4b 1d 8d 16 31 86 1f 0c 54 b6 39 aa fe ba ca b1 51 6e a4 0a 6d c2 a6 74 e2 81 ed 98 88 43 40 5f 98 c0 b7 21 17 74 72 62 00 b1 ed 3e 63 0b bb 3a 55 24 2a cc 41 83 52 e1 84 c2 04 b0 3f 80 c5 97 2e 2c cc 62 cc 40 73 1c ca 97 58 f3 0d 41 Data Ascii:]mCO-p,WAGX(ORc*;@;).]H1C?`_=O+11Eln8EK_EsP{U>.,]14dYcC`p)M5G^8eK1T9QnTlC@_!trb>c:U\$*AR?._b@sXA
2021-09-16 04:29:08 UTC	1795	IN	Data Raw: a2 a3 7d 85 c1 c7 d9 de 73 b3 3e f3 a6 b0 66 0b 96 1d 77 2c e4 c1 57 2b 17 cf 0e 09 c6 63 a9 71 19 a1 7b 39 cc 52 b5 97 15 82 21 16 8f c4 db 4a fa 84 02 d4 ed 98 10 d0 3a cc 91 76 6a a3 a6 87 50 e2 a1 6a 34 b0 36 30 73 d9 98 40 a5 72 5b 51 ad d4 f1 f5 08 b3 26 ca 98 29 8b a8 c9 72 a9 1e 63 43 a3 75 75 f9 14 9d 3c 99 94 20 81 72 f4 32 1b 86 21 56 fc d4 b5 90 04 ab 9b 54 bf 98 f6 19 1e c5 d5 ff 00 b2 f0 ea 6a be 58 02 04 04 79 38 c2 2c 6d 53 b7 6f 68 91 f5 48 91 2a 7d 47 ec fa 0f cf f2 1b a5 04 be 25 b9 4e d0 8a 01 e1 97 bb 0f 68 ef 75 dc 0f 47 13 8c bb 8e 21 e1 14 f5 18 7a 36 62 ac f6 b8 81 c2 5d a5 e7 4d 42 61 e0 6a ed 89 40 c5 f5 d4 59 48 ba 5e 75 f0 cd a5 cc 17 cf 29 7c 75 20 5d d0 0f b2 59 7a 9c e2 bf a8 d4 3b c9 be 18 6d 0b 0c f2 2b d9 4c 58 8f 8c Data Ascii:]s>fw,W+cq[9RlJ:v]Pj460s@r[Q&]rcCuuc r22!VTj]Xy8,mSohH^]G%NhuG1z6b]MBaj@YH^u)u] Yz;+m+LX
2021-09-16 04:29:08 UTC	1797	IN	Data Raw: f6 9f b3 e8 3f 3d 3b 2c fe a0 05 68 c3 d9 04 1f b8 f6 a0 5f 35 aa 58 a4 01 a1 bb 0b 47 5c e2 1d 14 05 1a d5 7e 31 83 bc 09 85 84 ff 00 e8 d6 de b1 dd ab e8 d9 9a 2b 6c cd cb b9 79 96 b4 ba 2e e3 86 43 b0 c4 11 4a 74 42 64 00 3c d4 00 d3 98 8b c0 f6 96 43 f9 2b 81 03 d2 6c c4 55 a9 b7 11 88 49 41 5b a9 7a f2 ea 10 9b 53 63 d2 1d 97 2d d2 62 39 6e 4c 1b be 8f bc 2b 45 91 21 45 1b 99 01 90 30 f2 ed 8c 65 a7 99 ac b8 b4 d6 7f b7 49 9a 81 e9 ac 7f 04 94 4a 89 99 ac 8b 4c b2 6e 31 28 ad 2f 05 ea d6 09 a9 90 98 a1 19 79 1b 39 eb 2f 44 c4 f6 35 8e fd 66 ce 72 e6 a2 43 8a b6 eb e1 60 d8 e1 d3 65 ea 0e a5 9a a5 06 2c d2 96 73 88 96 b3 39 73 de e1 90 b2 ca 14 1c 93 61 49 a5 86 5a 6a cb 8c 8b 07 cb 01 60 05 69 3a 42 10 58 e7 a3 14 c5 56 90 24 e4 a7 fa 12 dd c8 cb cc Data Ascii: ?=+_h_5XG[-1+!y.C]Bd<C+U!A[zSc-b9nL+!E!Oe!JLn1/(y9/D5frC`e,sk9saZj`i:BXV\$
2021-09-16 04:29:08 UTC	1798	IN	Data Raw: 24 25 7a 54 bc 39 3e 71 b1 4e 09 e7 fe 03 0e 80 c5 07 ec a0 56 61 ca b9 88 e3 4c 3a a1 00 97 fc 18 b1 9b 7a 2d c6 78 54 3e ec b1 21 91 9b 01 7b e2 21 5c cb c0 23 34 a5 18 ff 00 ec 2c db 6e 5e 60 22 b0 73 03 47 d8 73 0a 50 5f cc bc 70 23 12 28 cf 82 56 36 2d c7 48 04 5c e7 da 14 84 09 75 45 4b 64 2f 74 45 bb 92 60 6a 5e f7 57 0e 20 a6 a8 ef 14 d1 cb fa 94 4c 0c 8b c9 50 25 28 70 d6 2a 63 40 18 20 af 84 2a cb da e7 8b 82 c8 75 d4 10 98 6f f6 a2 0a 8a 2e 27 90 61 2f 42 d8 3e 22 d3 aa 1c e0 5b b5 72 a3 11 75 d4 da ca 6e fb d9 1f 41 10 dc 59 a9 03 e9 9b 40 17 cf 87 eb a2 62 9d d1 8c 67 d4 7e cf a2 fc ff 00 09 2b 11 81 e2 06 90 0a ea 6a 5a 47 3d 90 50 bf 50 5c 61 f8 0c 12 c8 81 53 f1 1c 0c f5 4a 04 36 92 88 de 85 d8 99 ca a8 28 22 20 c3 9a 96 9d e2 8f be 65 1b Data Ascii: \$%zT9>qNVaL:z-xT>!{!#4,n^^"sGsP_#(V6-HluEKd/tE]j^W LP%(p*c@`*uo.'a/B>"[runAY@g--+jZG=PP!aSJ6("e
2021-09-16 04:29:08 UTC	1799	IN	Data Raw: 6e 30 92 fb 41 aa ef 2c 66 af 2b 85 36 59 5b 33 16 61 d8 c7 33 1a d8 d7 91 8c b8 7b be 3f dc 5e 2a 29 58 ce 05 c7 81 aa aa 80 12 87 79 77 c3 62 c6 5c 6a f4 5f 2c b6 5c b8 4b 8b 16 5c 7f 03 f6 7d 17 e7 f1 cf a2 f0 21 5d 1f 71 82 cb 5e c7 d4 d5 c8 e1 a0 c6 d7 97 f2 75 52 3f 56 a9 bb ed 51 4c 02 af 07 7e f1 44 01 37 41 96 f3 a2 01 7a 30 79 ea be 59 56 aa bc b2 fd 62 5e b1 32 1c 37 da 5e 61 f5 5a 3e 66 e6 4e 06 1e c2 c3 ea 33 41 58 5e 1a a8 9c ec 0c 11 7d a5 22 41 56 64 1e f3 14 ea e0 9b 1d db 51 99 13 a6 39 63 f4 dd bf d5 ee 5d b0 71 37 d8 be b0 07 ad 30 68 46 94 b5 8a 39 89 47 d6 c6 81 e6 f5 ac c3 4a 84 e9 95 c0 b1 ea 2c 12 da 57 59 58 fd c4 bb 44 29 f5 17 10 13 a1 1b 01 e4 b2 36 31 49 1c 26 07 b0 84 a0 54 03 af 67 65 87 69 02 38 e8 1e b5 c4 02 ac 6d 0f eb Data Ascii: n0A,f+6Y[3a3{?^*)Xywbj_\.K])]q^uR?VQL-D7Az0yYVb^27^a>fN3AX^j"AVdQ9c]q70hF9GJ,WYXD)6lI&Tgei8m
2021-09-16 04:29:08 UTC	1801	IN	Data Raw: c2 e9 72 ce 98 c9 34 70 16 f4 d4 74 5c 32 52 db bd 33 45 6b a4 5b 88 b2 75 5f ea 57 ac a5 1c 5f 2c cd 72 0a 75 38 97 8e dd 0e 7f e6 63 d9 be 0c 60 bc d2 cb 8b dd 48 e7 5e 23 e5 4e 43 4b 46 89 ab 29 a5 f4 6a 28 e6 17 de e2 45 d6 05 92 dc 56 f0 e8 73 f2 c5 56 1c bf 3c 54 a8 e0 00 c5 60 9d c4 72 d4 72 08 a3 9a 38 9c 04 22 12 d5 d8 b1 1e 9a 83 60 a6 8b ea 3d 65 16 54 dd 5f 27 58 d5 08 2f 16 62 c8 db 93 4f dc fc f4 33 2a 24 59 78 97 0d 4b 22 9e 8b e0 7e c6 ac aa d3 7e 3f 98 f9 5f c8 61 e5 83 dc c0 3c 59 cb d8 12 13 63 6b d9 18 fb 97 99 e2 39 18 8f 2e 3a 42 2e 47 b5 e8 f7 94 95 52 de 70 66 fd ce 18 99 ca 92 25 9e 25 35 0b 91 af 33 07 51 6d 33 e8 4a 54 57 7d b2 da e2 e1 94 c3 89 50 f3 00 3b c5 c6 9b 39 84 66 30 18 16 c2 4a 87 4a bb 06 df 90 a8 0d 43 d7 bc 2a 80 Data Ascii: r4ptl2R3Ek[u_W_,ru8c`H^#NCKF)j(EVsV<T`rMr8"=eT`_X/bO3^\$YxK"---?_a<Yck9;.B.GRpf%53Qm3JTWjP;9f0JJC*
2021-09-16 04:29:08 UTC	1802	IN	Data Raw: bf a8 f7 b8 9f 49 55 ab c3 6f 70 a8 ab 36 b0 fb 3f e9 98 8e 91 8d bd a5 a8 87 f3 65 c5 94 2a 05 d3 41 9e b8 45 65 ea 0f cc 6a 62 31 20 82 24 63 2c 88 01 5e 2f fd 99 5d 54 f2 47 77 92 30 e3 47 57 b4 e1 8c 21 38 51 d5 f5 ed 06 14 cf 4a 53 b4 11 87 a3 71 d0 1d aa e0 25 88 23 6e ac ed 7c c2 62 95 8e 4a 4c 80 72 ca eb b8 15 f3 2f 21 2e 27 d5 fb c5 ad 11 77 29 b8 df 32 da 97 35 da 66 2b ad 1d 60 bc b2 2f 95 ae 28 e5 97 38 42 ee ba 44 e7 68 db 51 b6 b5 56 b8 eb 10 57 2f 42 9e 23 9f c5 93 ab 32 b3 58 14 1c 6c f1 15 cb d2 c9 7e 83 1f 4e 3d 38 f4 7d 3e 8b f6 7d 17 e7 a9 e9 51 31 29 6d 1e a4 0d ae 76 bb 66 24 26 4e 36 e8 95 50 5c e5 e9 1f e6 14 90 77 38 bb 96 bc 81 11 91 a0 02 a9 5d 3c 18 94 aa 79 57 b8 30 d8 ee c2 b8 c1 7f 65 96 4c 04 d1 12 a3 cb c2 04 85 45 94 34 Data Ascii: !Uop6?e*AEejb1 \$c,^/jTGwOGW!8QJSq%#n]bJLr/!.w)25f+`/(8BdhQVWV/B#2XI-N=8}>}Q1)mvf\$&N6P\w8j]>yW0eLE4

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:08 UTC	1803	IN	Data Raw: 68 69 cb 10 98 8a f0 55 6b ae 8c 54 58 45 00 55 60 ff 00 4c b0 d6 cd b2 1f 91 53 4c ea a2 8a 6b 70 06 99 fe a5 81 a9 62 ba 87 46 ff 00 11 43 2a 2d 44 6e 03 07 e8 3d 06 5e d8 cb 08 93 ea 3f 65 3d 87 e7 f3 5a 99 65 0c 23 a8 60 49 93 91 ea 3c 24 a0 b9 a8 78 55 4f e2 12 5c cc e0 9c 6c 64 3e 66 6b 00 d0 bd c0 c2 c3 11 4d 47 a2 b1 8e 1c 56 fb 42 59 74 b7 bf 09 05 ca 6b e6 1d 20 52 47 98 e3 60 d3 de 51 c6 42 f8 e9 37 a6 3d f2 56 a0 40 12 9d 22 2e 6d 95 ea 0d 64 c0 de ec 8b 01 a4 38 e4 d4 b4 b2 6a 86 e5 ec 00 b4 70 74 82 b0 6b 98 86 88 36 d8 4f ee cf 50 af 22 7e 21 61 4b 10 0b 96 ce 39 8c 6f 30 05 ab 81 0b 61 70 4e 6a ba ee eb 1d 0d 5a bf 63 a3 c3 55 ef 0a 41 3f c2 ca 81 12 24 da 28 b1 63 19 b4 b8 ea 28 0d a8 46 61 44 2c 77 81 9b b9 ed d6 e5 2d 26 88 6d 77 39 aa Data Ascii: hiUKTXEU`LSLkpbFC*-Dn=?e=Ze#`I<\$xUOIld>fkMGVBVtk RG`QB7=V@`.md8jptk6OP`~!aK9o0apNjZcUA?\$(c(FaD,w-&mw9
2021-09-16 04:29:08 UTC	1805	IN	Data Raw: 78 cb 29 82 98 e7 11 8b 78 e2 22 a2 59 1a dd 42 1c 62 12 91 60 5a a7 66 33 03 4f 58 c8 5b 2f 30 34 1a e5 94 50 1d ba 9b 0e 26 76 d0 af 68 a9 74 8a 9a 95 b5 d7 2a f2 59 04 70 11 02 c6 6f 70 5d 2b 48 c3 0a 55 1a 16 cf b8 c5 7a 12 bf 92 20 82 92 01 fc 43 31 f0 4f d9 f4 1f 9f e1 af 4b 08 0e 54 7a 9e 04 cd 61 02 ab c0 46 0d 96 d9 e9 3b dc 40 0e 08 1a 33 2e 38 f9 88 b0 03 31 87 93 b9 33 e7 6c cf 5d b9 21 62 f1 07 83 b9 92 58 1b 2e a8 1e 46 98 1b 3f 21 14 37 55 87 70 66 f0 e7 48 8b c3 af fe 63 c7 4e 59 a7 6e 08 30 9d f6 8a 7b c6 94 01 6b a1 ff 00 a8 21 58 43 1a 2d a7 d4 c4 5c 8b f1 44 fd 89 c5 59 19 bc e0 40 6e a2 e2 e2 80 57 f0 c4 aa 08 66 20 86 bf 9d 7a 15 52 e2 ab 9a 05 ac be 16 6d b3 5d e2 82 bc 1d ca e5 63 19 15 bd 1b 95 f7 6a 29 46 08 c4 a1 47 b4 ca 57 85 Data Ascii: x)x"YBb`Zf3OX[/04P&vht`Ypop]+HUz C1OKTZaF;@3.813j]bX.F?17UpfHcNyn0{k(Xc-IDY@nWf zRm[cj]FGW
2021-09-16 04:29:08 UTC	1806	IN	Data Raw: 11 64 17 0a aa 2b ad 15 cc 58 8f 43 00 87 79 61 a5 6e af dc e2 24 a6 b6 61 1d e0 1a 01 d6 fa b2 f9 85 93 0b 30 3e 01 fd cb 06 b8 59 5e 13 0c 05 b5 9e ef 98 5c ce d2 a3 51 a8 65 98 80 ba 3d ff 00 d4 4a 0a d5 d4 34 10 0b 7a df f3 bc b8 df bf b4 c1 56 cb 40 0c db 6c 4b 93 19 e2 67 c6 e4 97 30 7a fc 4b 45 75 d2 fb c0 7e 9c 4b 8e 7e 62 bd e3 e8 94 95 9f 68 14 bc c2 dd 76 84 d5 3c c1 b1 b8 6b 7b ed 28 23 03 de 02 2e 88 9f 79 cd a7 bf 78 08 79 69 b3 ab 04 e6 64 cd 7d a5 47 60 2b ac c6 c3 46 ea 38 c1 a3 35 98 4b ad e1 49 96 3a e4 81 b3 0a 39 7f a9 b4 ad f3 2e 93 8c bb 09 6f 99 4b a5 7c c5 0b e5 8c 68 a8 bd b3 3e b1 f9 fe 04 16 87 76 9e ee 89 90 73 1a d4 ef b4 56 d4 b6 1d 5a 4a 88 60 5b 96 50 54 d9 0c 82 04 67 9e 20 74 62 27 5f b3 8f a1 6c cc 5c 04 a2 f2 4a 54 4c Data Ascii: d+XCyan\$a0>Y^Qe=J4zsV@lKg0zEu]-K-bhv<k{(#,xyid)}G`+F85KI:9.oK[!vsVZJ`[PTg tb`_lJTL
2021-09-16 04:29:08 UTC	1807	IN	Data Raw: 77 72 72 3b 5e 1e dd fd 29 98 44 23 0e c2 37 32 9e 1f d8 9d ed 73 37 dc 60 3a 6c b2 bc 5e 6a 76 62 1e 21 0e 26 fe 73 f7 5f af a7 98 ad 4c e8 8b c5 e8 6b 81 8e c2 b7 54 30 28 b9 ff 00 cc e1 81 80 4a ea 45 c5 dc 6f 8c 22 8e 43 98 86 65 2f 93 50 38 a0 de 0f fa 7f 04 94 7a 5e 00 ed 29 0d 82 f8 9b 00 26 46 3d f8 9b 0e f5 43 d2 f3 2c c5 da 01 46 8d 2c 40 76 ff 00 e4 63 6b d6 28 8a 18 25 e4 b6 26 5e de 23 c3 25 27 7a 8f 38 cd 1f a8 02 21 b2 ae 55 72 42 ba 84 a6 34 77 0d 81 99 73 05 3b 47 d1 84 bd 53 41 4c a3 8b c4 2a b9 a8 d6 c3 50 43 b4 13 fd c7 a2 37 b1 2e 0c 6a 05 1a 8c 6c 4a 92 18 38 f3 0b d2 89 89 89 0d 4a e4 dc 62 58 45 ac bc f4 83 48 d4 5a 3d 20 ac 3a 75 33 53 11 78 08 99 ef 0c 15 ab 15 70 82 8a f6 a9 fa 94 16 ba 1d 7f 50 4a ee a5 bf ab 23 be b0 fd 54 Data Ascii: wrr;^D#72s7`!^jvb!&s_LkTO(JEo`Ce/P8z^)&F=8xE],F,@vck(%&#%#z8!UrB4ws;GSAL*PC7,jlJ8bXEHZ=:u3SxpPJ#T
2021-09-16 04:29:08 UTC	1809	IN	Data Raw: 36 ef a1 4d 2d 60 37 57 ff 00 70 9c fd e4 df 01 32 51 ba 9b 94 5e e2 33 85 f1 0d 00 4a 7b a8 e1 45 30 38 35 68 80 88 da dc 59 1d 7c d1 0d 22 da 7d d3 5c 4b 76 9f 70 8c 96 df 98 e7 8b 4d 0f fb dd 39 af d5 46 5a f1 7d 7a ad a4 20 9a 48 e0 ad d6 9b f6 32 0a 3b bc 88 3f e5 6b 5d ba 5a 1e 4a 50 ee 07 f4 4c 8a 4d b5 9f c5 36 22 05 0b 5f 0c 0f a8 8f 64 1a de 9c 2d ad be 4a d1 91 f0 c0 03 a7 d8 d2 a4 51 ee 88 0d c7 cc 05 24 8d 2d a0 71 7f 89 45 cc f5 f6 01 36 58 47 0d 23 d5 19 19 78 25 3a 46 df 38 f5 41 ac ae 6f f1 4e 63 33 9c a0 f7 34 5d 83 e8 9b 39 f3 fc d7 c4 1c 83 ee 13 a8 8b bf ff 00 11 3b 85 1e 6b f4 51 bb e4 19 c3 0a 39 4b 1e 0f 4b a2 9a e2 e0 32 82 08 26 d7 d8 b8 d3 4a 98 35 ce a2 9b 13 41 e4 af 89 18 c2 2e 69 45 b7 94 01 0b 71 b5 a1 b0 d5 47 ec 29 04 51 Data Ascii: 6M-`7Wp2Q`3J[E085hY"]\KvpM9FZ]z H2;?kZJPLM6"_d-JQ%-qE6XG#%#;F8A0n34j9;kQ9KK2&J5A.iEQg)Q
2021-09-16 04:29:08 UTC	1810	IN	Data Raw: 36 a6 47 32 9c 41 cf 44 fe 02 ab 41 d1 83 c7 e6 9d 3b 2b e8 6a 33 37 a6 10 92 f8 28 bc d2 33 00 53 66 78 18 14 8c e4 f2 6d 44 f7 6d ae 88 56 f0 7c 8a d3 9c 20 7c 21 01 dc 02 0a 79 4b 20 14 32 4a 9f 12 12 8b b0 be a7 52 68 68 6e 53 9e 4e 07 08 38 b5 58 70 ca 90 61 34 85 b8 d2 dd 61 01 85 2b d8 25 0c 77 05 b6 b4 8d 24 90 0f ca 06 4a 35 d3 81 c2 01 01 dc 07 86 96 b5 ac 74 14 ef 30 42 9d e0 0a ea 99 b9 cd 16 9d 7d 14 50 fc 53 f5 35 be e5 4b a7 86 17 96 49 2d 3b 66 ee 30 7d 94 9a 49 db 0b 64 6f cc d7 0b 03 af e4 a3 0f 07 20 85 20 a6 04 d8 1e 48 aa c9 e4 a7 c5 0e 9d df c4 0e 7b 4b 2c 39 bc 5f 96 17 c1 d1 36 06 39 ed da f7 0f a4 66 91 23 7f cb 75 e6 8f bf 80 79 80 b4 a5 cd 3b 4f 3c 78 85 21 16 dc 16 14 ac de cd b7 5d 42 d4 02 28 13 66 86 7c d5 60 ad c4 1c 28 85 f2 Data Ascii: 6G2ADA;+j37(35fmdmV] jlyK 2JRhnSN8Xpa4a+%w\$J5t0B)PS5KI-;f0)do H(K,9_69f#uy;O<x]B(f](f`(`
2021-09-16 04:29:08 UTC	1811	IN	Data Raw: 68 a0 78 c0 da 7c c2 9b 43 3b 2e 86 e1 e8 8d 83 4a d0 3e 30 57 6a 6a 32 18 3a 64 a0 6d 52 22 c5 1c 84 63 7b 3e 9c 8f 2f f0 be 38 1c d8 f7 43 50 df 30 83 c1 c8 04 ad 14 85 84 38 ff 00 c8 26 fd 2a eb 0b 71 47 c5 a3 d2 99 9f 67 e9 1c a6 86 b0 6d 68 a1 e4 8b 95 f7 5a b5 3e 9e 29 85 39 a0 d7 1e 8b b6 3b 33 53 a7 3f 12 36 39 d7 21 b0 d1 78 c9 bf 4a ea 0a 8b 51 21 cd 06 f0 50 92 d3 85 f0 83 4f 92 63 0a 68 3e cb 7d 05 2c d4 39 52 ea db a6 ce 2d 5b c9 cc 94 c6 fa 92 bf d3 c2 7f 71 d4 8f e6 8f d1 07 2f 88 02 12 02 a4 82 19 47 cc d1 ef d5 3f b3 23 3f 4b c8 f7 4f d2 ce cb b6 9a f3 f1 eb 35 ce 88 6d 69 05 df a2 73 cb 9d 67 9e e6 9e ea ee 20 23 69 ae a8 c2 d1 cc 24 80 1e a3 07 ec 62 85 b1 c6 1a 38 0b 6f a9 44 10 ac 77 0e f7 b1 ae 04 11 60 af da 2e cc 6e 8a 13 aa 85 a7 e1 Data Ascii: hx[C,.->WVjj2:dmR`c`{>8CP08&*qGgmhZ>}>9;3S?69!xJIPOch>},9R-[q/G?#?KO5misg #b8oDw`.n
2021-09-16 04:29:08 UTC	1813	IN	Data Raw: c4 d2 e7 80 2b 53 5a ac 2e 0c 46 d0 46 e4 6a 53 1b 92 87 33 d5 39 af ad 49 6f ea 9a 1a 09 ac c7 ea 9a c1 67 42 10 68 ab 4f 05 ba 80 69 5d 8e 49 bf 17 e9 7b 2c c6 c0 3f 2f 24 69 ae cc 00 a3 a1 51 b2 89 cb b7 21 fb 7c d3 83 1d 60 0d f6 fe 16 3f 87 88 c9 2d 06 b7 0a a8 f6 0d 3b 6b dc 44 74 2d ff 00 20 47 f0 b8 64 79 62 04 f5 b5 15 1d f5 d3 9a 95 d1 e7 e4 9b 2c 77 76 3d 4f ec 17 b4 f1 78 01 f5 e6 9b d5 c2 ca 9d cf 3b 50 e4 17 12 07 db 12 4f 3f 77 5a 76 73 5c 3b 08 00 f6 84 73 a0 99 13 81 d4 12 4a 66 1a 6a e4 0f 9a 7e 07 10 77 78 3e 5b 7e 8b ee 98 86 81 6c 1f 22 84 52 8e 46 fd 17 8e fa a6 97 5f 31 e4 9b 19 2e f2 ea 9d 08 e8 84 3b d8 3e bd 10 cc c7 96 90 0f ee 9a ec af b1 b7 f2 a4 35 21 15 bf 89 4d 13 65 8f 2e f6 2c 2c 6c 26 29 cb 7e 9d c1 ee 58 2d c3 d5 40 e7 Data Ascii: +SZ.FFjS39logBhOj {./?SiQl`?;-kDt- Gdyb,wv=Ox:PO?wZvs;Sjff-wx>[~!RF_1.;>5!Me.,l&)-X-@
2021-09-16 04:29:08 UTC	1814	IN	Data Raw: 29 73 cb 2d 00 6b a2 88 be 22 2c 15 18 88 d1 22 c1 53 e1 0b 01 73 4e 89 ce 7e 5a 28 ef e6 85 94 68 15 38 cf 20 1c d7 0e 2d 76 14 30 81 63 45 f6 97 13 93 85 fb 01 ce 73 ee f8 68 f1 d7 32 7f 44 c6 06 35 ca 73 20 2b d1 17 0a 4e 92 93 dc 86 a8 02 d2 28 dc 83 b9 ec be f1 11 fc 40 fa 23 2b 4b 74 36 9c 7c 0e f4 58 a6 91 29 ef 74 7c 15 db 82 c4 c5 ff 00 48 6c 54 4b 88 cc 0f 4a dd 40 e1 93 ad 84 d6 37 45 13 23 6d 10 14 8d 64 a4 17 1d 1b c9 41 36 1f 39 a1 a8 ea 14 d8 a8 58 db 73 6f d0 5a c3 c9 86 c4 82 63 24 1e 94 42 32 e5 6d 6e 46 8a 78 9b 56 9c cd 51 d0 d2 3f 10 2a 2d 66 ba b0 37 4f c6 96 e2 d8 d8 6d 80 9a 37 ff 00 95 f6 92 70 ec 4b 63 06 c3 45 93 e6 7d d6 17 0c e9 a5 d0 d4 0e 65 61 f0 58 78 a4 0e 68 3b 56 a5 17 17 38 5f 45 98 a2 d9 48 df e9 a2 18 79 73 7c 4e 43 Data Ascii:)s-k`,`SsN-Z(h8 -v0cEsh2D5s +N(@#>Kt6X)thITKJ@7E#mdA69XsoZc\$B2mnFvXQ?*-f0m7pKcE)JeaXxh;V8_EHys]NC
2021-09-16 04:29:08 UTC	1815	IN	Data Raw: 72 1c 93 11 26 f5 5f 65 31 9c 3a c4 4f 8d 8c 9b 93 e8 1c df 5e 6a 4c 43 63 3a b8 ed d1 33 11 67 e1 a0 79 e5 58 80 df 64 ec ce 68 15 ad 8b fd 57 16 9f 08 fc 73 fe ee d1 90 1a cc 05 66 3d 54 ee 27 c3 f5 4d c6 e0 e3 71 12 b4 b8 72 d0 1f d5 4d c6 30 2d 87 d9 41 19 d7 a8 a1 af 32 9c fc d3 93 d6 d7 3e ca ed d5 52 1b f6 8e ce 0d ff 00 78 2f a2 ca 0b 75 e8 a4 c1 c8 35 61 dd 3d 98 a6 ba a8 a7 3f 14 d2 84 d3 bb a1 76 54 58 69 09 d4 a6 61 da c0 80 b2 8f c2 b8 ad 1c 61 16 2f 28 d1 10 46 fd 94 ab b2 89 55 47 dc 05 82 69 8e 16 01 c8 27 44 32 e6 66 dc c7 4f fc 2b 43 7b 06 8a c2 fd a7 e2 b8 76 e5 f6 8d 91 a3 61 20 cd f9 ee bf f5 a7 13 22 83 20 1f fc 4f f2 b1 dc 67 89 63 85 4d 3b 8b 7f ca 78 47 d0 27 10 16 2f 15 5e 16 9d 4e e7 a2 95 da 76 37 e2 1e a8 77 46 dd 96 9a c7 1d Data Ascii: r&_e1:O^jLLc:3gyXdhWsf=T`MqrM0-A2>Rx/u5a=?AvTXiaa/(FUGiD2fO+C[va " OgcM;XG/^Nv7wF

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
157	192.168.2.3	49952	104.244.42.193	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:09 UTC	1832	OUT	GET /arianalife0/status/1437939259609128967 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: twitter.com Connection: Keep-Alive
2021-09-16 04:29:09 UTC	1832	IN	HTTP/1.1 400 Bad Request date: Thu, 16 Sep 2021 04:29:09 GMT server: tsa_o set-cookie: personalization_id="v1_0BzkXBkP5H/xy2J8BbpxEA=="; Max-Age=63072000; Expires=Sat, 16 Sep 2023 04:29:09 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None set-cookie: guest_id=v1%3A163176654944197621; Max-Age=63072000; Expires=Sat, 16 Sep 2023 04:29:09 GMT; Path=/; Domain=.twitter.com; Secure; SameSite=None content-type: text/html; charset=utf-8 x-powered-by: Express cache-control: no-cache, no-store, max-age=0 x-xss-protection: 0 strict-transport-security: max-age=631138519 x-connection-hash: c8026bda6bff4715e578099aaf476f33341dd3e3e84288513fd67d8b7fbab742 connection: close transfer-encoding: chunked
2021-09-16 04:29:09 UTC	1833	IN	Data Raw: 64 35 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 0a 20 20 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 2c 76 69 65 77 70 6f 72 74 2 d 66 69 74 3d 63 6f 76 65 72 22 20 2f 3e 0a 20 20 3c 73 74 79 6c 65 3e 0d 0a 33 63 63 0d 0a 0a 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d Data Ascii: d5<!DOCTYPE html><html dir="ltr" lang="en"><head> <meta charset="utf-8" /> <meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0,viewport-fit=cover" /> <style>3cc body { -ms-overflow-
2021-09-16 04:29:09 UTC	1835	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
158	192.168.2.3	49954	152.199.21.141	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:09 UTC	1835	OUT	GET /errors/logo46x38.png HTTP/1.1 Accept: image/png, image/svg+xml, image/jxr, image/*;q=0.8, */*;q=0.5 Referer: https://twitter.com/arianalife0/status/1437939259609128967 Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: abs.twimg.com Connection: Keep-Alive
2021-09-16 04:29:09 UTC	1835	IN	HTTP/1.1 200 OK Accept-Ranges: bytes access-control-allow-origin: * Age: 23712508 Content-Type: image/png Date: Thu, 16 Sep 2021 04:29:09 GMT Etag: "7vm/v2DloVVWH9dCWPBNBA==" expires: Fri, 16 Sep 2022 04:29:09 GMT Last-Modified: Wed, 02 Dec 2020 16:55:43 GMT Server: ECAcc (frc/8FE9) strict-transport-security: max-age=631138519 surrogate-key: twitter-assets X-Cache: HIT x-connection-hash: 5c1c965232f405d897958ce5152b0791 x-content-type-options: nosniff x-response-time: 10 x-ton-expected-size: 1015 Content-Length: 1015 Connection: close
2021-09-16 04:29:09 UTC	1836	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 2e 00 00 00 26 08 06 00 00 00 bb ea a9 5a 00 00 00 09 70 48 59 73 00 00 0b 13 01 00 9a 9c 18 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 03 8c 49 44 41 54 78 01 e5 58 5d 52 1a 41 10 ee 99 25 6f 2a f0 96 aa 88 b5 9e 40 6e 20 9e 20 de 00 f6 04 e8 09 22 27 c0 9c 60 59 2f a0 9e 20 e4 04 e1 06 4e c4 54 e5 0d 44 ab f2 a0 3b 9d ee 5d 59 56 dc 5d 16 18 90 54 be 17 d8 f9 fd a6 a7 a7 ff 00 fe 51 08 58 23 4a ee a0 b4 03 b2 81 96 f8 0c 88 36 6d 6f 73 3b 02 f6 84 10 3d f0 e1 ba ef ec 5c 65 ad f1 d1 1d d8 bf 9d b2 12 d3 0b 0f 9d f2 10 56 80 3d ef b1 89 a0 cf 78 9b 19 43 d5 93 f6 8f 98 5c bc 71 d7 7d a8 09 0b bf d0 e1 3c 3a 5c 47 bc ea 90 e8 26 4d 5a 16 Data Ascii: PNGiHDR.&ZpHYssRGBgAMAaIDATxXJRA%o*@n ""Y/ NTD;JYVJTX#J6mos;=leV=xClq]<:lG&MZ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
159	192.168.2.3	49955	152.199.21.141	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:29:18 UTC	1837	OUT	GET /favicons/favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: abs.twimg.com Connection: Keep-Alive
2021-09-16 04:29:18 UTC	1837	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Age: 230155 Content-Type: image/vnd.microsoft.icon Date: Thu, 16 Sep 2021 04:29:18 GMT Etag: "iUCzHM6HSq2WUv1D606pCw==" expires: Thu, 23 Sep 2021 04:29:18 GMT Last-Modified: Sat, 04 Sep 2021 01:11:20 GMT Server: ECAcc (frc/8F52) strict-transport-security: max-age=631138519 surrogate-key: twitter-assets timing-allow-origin: https://twitter.com, https://mobile.twitter.com X-Cache: HIT x-connection-hash: 370ca7063cb2c6185e3ab27e1740bcc2340b11f0a354b981c7a915c47bb0732a x-content-type-options: nosniff x-response-time: 8 x-ton-expected-size: 481 Content-Length: 481 Connection: close
2021-09-16 04:29:18 UTC	1838	IN	Data Raw: 00 00 01 00 01 00 20 20 00 00 01 00 20 00 cb 01 00 00 16 00 00 00 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 20 00 00 00 20 08 06 00 00 00 73 7a 7a f4 00 00 01 92 49 44 41 54 78 01 62 18 36 60 14 c8 2e 04 f0 5a cf 00 7a 04 40 14 c7 63 db b6 d1 c5 aa 62 76 b1 6d 54 b1 ba d8 e8 d2 c5 ae 62 f6 b1 6d e3 6c cc fd cf 5a cd aa f8 7d c2 bc b7 42 74 39 2c c4 5d 44 20 1e cf b0 15 0d 0d 7e df 0d a5 73 df 94 c1 7c 0f e1 6d f0 14 62 22 06 13 d0 00 d3 71 0d 27 0a 0e 18 03 c1 62 17 e1 75 f1 09 62 23 0d e9 10 fc 42 a3 82 43 f6 40 90 8e 0d ca 02 47 20 0a 6f 30 18 d3 b1 30 77 c8 51 48 01 e7 50 cb 41 78 0d 24 43 14 12 21 78 8c ea b9 83 f6 42 8a f8 8e e9 28 69 51 60 0c c4 85 07 a8 5f 70 d0 58 88 89 27 98 85 4a 06 05 e6 40 94 1e a1 72 d1 41 e5 f1 05 62 21 0e a7 Data Ascii: PNGIHDR szzIDATxb6`.Zz@cbvmTbmlZ}Bt9,JD ~s mb"q'ubub@BC@G o00wQHPAx\$C!xB(iQ`_pX'J@rAb!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49773	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	585	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWWTDMbViWw
2021-09-16 04:28:35 UTC	585	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfz.AWWjpGKWh_0; expires=Wed, 15-Dec-2021 04:28:34 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 4q61ENeOTztykeW8mlUmUbusHK3HSVo/aEbLOXNYblxg79MnH6LZN//UJ+g+I4Dkzfeow3ils3eBKOfedln6A== Date: Thu, 16 Sep 2021 04:28:35 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49774	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	586	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfz.wZ.AAA.0.0.BhQsfz.AWWjpGKWh_0
2021-09-16 04:28:35 UTC	587	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 9EI+sP8kzLzHfiCurRUWCHdsVPuYB6uRZvTtRdPKoA2CyBSoope9lufTLj5X1GxouhT6y7+QvnkCjW5ldbqEA== Date: Thu, 16 Sep 2021 04:28:35 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:35 UTC	588	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6d 6c 36 5a 6a 59 73 7a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ml6ZjYsz">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:35 UTC	588	IN	Data Raw: 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6d 6c 36 5a 6a 59 73 7a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 78 4d 6e 4c 62 63 31 51 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a 2f Data Ascii: "u003Cstyle nonce="ml6ZjYsz">body * {display:none !important;}u003Cstyle>u003Ca href="#" onlick="!top.location.href>window.location.href" style="!display:block !important;padding:10px!">Gehe zu facebook.com/u003C/a>")/*xMnLbc1Q*/}}))/*...*/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49776	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	589	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfz.wZ.AAA.0.0.BhQsfz.AWWjpGKWh_0
2021-09-16 04:28:35 UTC	590	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfz.wZ.AAA.0.0.BhQsfz.AWWjpGKWIVU; expires=Wed, 15-Dec-2021 04:28:34 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: VHuW8bjSLQzYqESyCulum78cblucB6Hnb2qW5PRTuqfwf9q2uLSW9EOWJlH89eWokTZpqS38Aw5UVAIwTA== Date: Thu, 16 Sep 2021 04:28:35 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49775	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	591	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html,application/xhtml+xml,image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfz.AWWjpGKWIVU
2021-09-16 04:28:35 UTC	592	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: uFjPYlygU3v7zdwA0S12+pLlgo4fl4LKuGE0TmdnWQd0stbOIbPrfXeftcsVEXH8Z3ExE908QfkxGkOth8luzA== Date: Thu, 16 Sep 2021 04:28:35 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:35 UTC	592	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 45 72 72 4c 6c 45 4b 76 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ErrLIEKv">*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=8
2021-09-16 04:28:35 UTC	593	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 45 72 72 4c 6c 45 4b 76 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 69 62 37 63 65 Data Ascii: ow.document.write("����Cstyle nonce="ErrLIEKv">body * {display:none !important;}����Cvstyle>����Ca href="\#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com����C/a>")/*ib7ce

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49733	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:27:58 UTC	126	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:27:58 UTC	126	IN	HTTP/1.1 200 OK Content-Type: image/png Content-Length: 903 Connection: close Date: Thu, 16 Sep 2021 04:27:58 GMT Cache-Control: max-age=3600 Apigw-Requestid: FvQoTh_doAMEPgw= X-Cache: Miss from cloudfront Via: 1.1 bafba29f1325f15932567e0ae2d444a5.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: FJfJJeolkAbGWGoas5vmOF-eSo3ly4QIBDVHcJLzyHpVJmV9LDoT6Q==
2021-09-16 04:27:58 UTC	127	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 20 00 00 00 20 08 06 00 00 00 73 7a 7a f4 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 38 65 58 49 66 4d 4d 00 2a 00 00 00 08 00 01 87 69 00 04 00 00 00 01 00 00 00 1a 00 00 00 00 02 a0 02 00 04 00 00 00 01 00 00 00 20 a0 03 00 04 00 00 00 01 00 00 00 20 00 00 00 00 8f 4e 40 c9 00 00 02 fa 49 44 41 54 58 09 ed 97 4d 48 54 51 14 c7 cf b9 77 66 12 22 30 47 a7 a2 a4 08 2c 2a e8 63 51 9b 40 c8 45 7e a4 23 08 ee 25 c2 8c 40 a2 45 a4 eb a2 45 14 b4 69 17 0a 12 45 8b 72 f4 39 8c 14 b5 2b dc 95 d5 a2 5c 24 56 9 8 33 99 52 0b 6d c6 79 a7 f3 c6 ae dc b9 73 b5 41 1f b9 f1 2d e6 9c f3 9b 73 cf f9 bf 3b 33 e7 be 01 d8 b8 d6 79 07 d0 d6 3f 59 d7 78 83 88 ae da de b3 32 c4 39 04 9a 05 c0 8f 88 30 42 Data Ascii: PNGIHDR szzgAMAA8eXlFMM*i N@IDATXMHTQwf"0G,*cQ@E~-%@EEIEr9+\\$V3RmysA-s;3y?Yx290B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49777	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	594	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfz.AWWjpGKWIVU
2021-09-16 04:28:35 UTC	595	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfz.AWWjpGKWMXs; expires=Wed, 15-Dec-2021 04:28:34 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 8WNCf94XVVgU1jILyAyH1BudYeS+GQFRbhMvKwXbXHQz8R9N1WvHcofcx1zDTJlMNvsUlmo++OUB/0U63nFag== Date: Thu, 16 Sep 2021 04:28:35 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49778	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:35 UTC	596	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfz.AWWjpGKWMXs
2021-09-16 04:28:35 UTC	596	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: wfiZegcjf9BdZWbD09LoMcGiXt4q3+yPIC+H0kelm8jUZYaufCRhkjJSuKWOHRoFtllyVg/QxzIS/1PPnsMw== Date: Thu, 16 Sep 2021 04:28:35 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:35 UTC	597	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 5a 38 4d 4f 53 66 4d 37 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 37 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="Z8MOSfM7">/*! [CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=7

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	601	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 51 62 66 6a 35 51 55 47 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="Qbfj5QUG">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:36 UTC	602	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 51 62 66 6a 35 51 55 47 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6d 75 61 37 7a 32 78 65 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="Qbfj5QUG">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="\n!display:block !important;padding:10px">Gehe zu facebook.com/u003Cv>");/*mua7z2xe*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49781	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	603	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9aaw
2021-09-16 04:28:36 UTC	604	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9348; expires=Wed, 15-Dec-2021 04:28:35 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: PMJXbgkX0XTWJvIphgJ7JWxgySqxnOHxrSGIKfzWznqjeHpTisFiXiWYiRYAGtKzNpwEv2KONkFNm ZtfDz4Pw== Date: Thu, 16 Sep 2021 04:28:36 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49782	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	605	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9348

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	606	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: TVmXajJxnWqDTi3We1EN+ntIJv9t7I4CGmci32skJ5AJIMqOnmLXKmMjdlh6z8epWJBpzcsWOuHDIR vsiWcgTQ== Date: Thu, 16 Sep 2021 04:28:36 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:36 UTC	606	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 65 67 6f 49 4d 53 6d 39 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="egoIMSm9"> /*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:36 UTC	607	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 65 67 6f 49 4d 53 6d 39 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 78 49 77 59 66 Data Ascii: ow.document.write("\u003Cstyle nonce=\"egoIMSm9\">body * {display:none !important;} \u003C/vstyle>\u003Cahref=\"\#\" onclick=\"\top.location.href=window.location.href\" style=\"\display:block !important;padding:10px\">Gehe zu facebook.com\u003C/a>)/\"/*xlwYf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49783	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	608	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9348
2021-09-16 04:28:36 UTC	609	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9348; expires=Wed, 15-Dec-2021 04:28:35 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: cqbzZnP7H850bWPZkByxGQJmTr/POP06wDX22MWX5QKCiIph8HoJkzMkifkwLi+H8fGofci2/uBIU L4yGPQGw== Date: Thu, 16 Sep 2021 04:28:36 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49784	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	610	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9CR0
2021-09-16 04:28:36 UTC	610	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: dTstSEEljATBQpg19Pbeex3DNMIVpE0HpXyTL75blOz7fmDbdnDHIrrgtqRVr40D8xM15zhu3KKchs sa7QvEUA== Date: Thu, 16 Sep 2021 04:28:36 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:36 UTC	611	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4f 52 7a 5a 37 74 54 5a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ORzZ7tTZ">*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=8
2021-09-16 04:28:36 UTC	612	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4f 52 7a 5a 37 74 54 5a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6a 30 6c 53 55 Data Ascii: ow.document.write("<u003Cstyle nonce=\"ORzZ7tTZ\">body * {display:none !important;}<u003C\\style><u003Ca href=\"#\" onclick=\"\"top.location.href=window.location.href\" style=\"display:block !important;padding:10px!>Gehe zu facebook.com<u003C\\a>\";)*<u003C\\script>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49785	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	613	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX9CR0

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	613	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfX.wZ.AAA.0.0.BhQsf0.AWW8dwX95Z0; expires=Wed, 15-Dec-2021 04:28:35 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: fMLNF/8O+6/D3uILfJyGwJ/48TJJbjKjeD/Z2ANjBLDD4tOrTLKTKjKebQIdAvH7vNJWsp+nL9XimeQ0ILY7Q== Date: Thu, 16 Sep 2021 04:28:36 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49786	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:36 UTC	614	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfX.wZ.AAA.0.0.BhQsf0.AWW8dwX95Z0
2021-09-16 04:28:37 UTC	615	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: VgfMTFWgIkbbPhZKQcbGXX+m5OGk+K1hgZUOImlCz487bIZtR2A3M6JVx0bbgKIkHwNtU71pLWj7mjg4IDhFMQ== Date: Thu, 16 Sep 2021 04:28:37 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:37 UTC	615	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 66 48 46 62 58 4a 4d 7a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 36 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="fHFbXJMz"/><![CDATA*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=6
2021-09-16 04:28:37 UTC	616	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 66 48 46 62 58 4a 4d 7a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 7f 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 79 59 53 78 4d Data Ascii: ow.document.write("\u003Cstyle nonce="fHFbXJMz">body * {display:none !important;}lu003Cvstyle>\u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003C/a>)/?yYSxM

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49757	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:28 UTC	128	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:28:29 UTC	128	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 390494 Connection: close Date: Thu, 16 Sep 2021 04:28:29 GMT content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Cache-Control: s-maxage=60 Apigw-Requestid: FvQtDh9OIAMEPSQ= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 a23fc047c59f0902384fa94644607c00.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: Qi2KI7dV6Hf2foHcqFNQdrsP1BATvq3lh7oAGjxShyU9_dJuyEkM2Q==
2021-09-16 04:28:29 UTC	128	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:28:29 UTC	135	IN	Data Raw: 31 35 30 20 30 20 32 33 31 2d 37 34 20 32 33 31 2d 31 38 30 20 30 2d 38 31 2d 34 37 2d 31 35 37 2d 31 37 32 2d 31 38 34 7a 4d 32 31 34 20 35 31 68 36 39 63 37 39 20 30 20 31 30 39 20 35 39 20 31 30 39 20 31 33 34 20 30 20 38 33 2d 33 37 20 31 33 38 2d 31 31 37 20 31 33 38 6c 2d 36 31 2d 31 56 35 31 7a 6d 32 30 31 20 34 37 38 63 30 20 37 31 2d 32 33 20 31 33 39 2d 31 32 31 20 31 33 39 68 2d 38 30 56 33 37 30 68 36 34 63 39 36 20 30 20 31 33 38 20 36 32 20 31 33 37 20 31 35 39 7a 4d 31 33 30 33 20 32 38 31 63 30 2d 34 39 20 34 35 2d 37 36 20 38 38 2d 37 36 20 35 31 20 30 20 31 30 34 20 33 37 20 31 31 36 20 31 31 34 68 33 33 6c 2d 39 2d 31 33 30 63 2d 34 33 2d 31 39 2d 31 30 36 2d 33 31 2d 31 36 30 2d 33 31 2d 31 32 35 20 30 2d 31 39 30 20 36 32 2d 31 39 30 Data Ascii: 150 0 231-74 231-180 0-81-47-157-172-184zM214 51h69c79 0 109 59 109 134 0 83-37 138-117 138l-61-1V 51zm201 478c0 71-23 139-121 139h-80V370h64c96 0 138 62 137 159zM1303 281c0-49 45-76 88-76 51 0 104 37 116 114h33l-9-130c-43-19-106-31-160-31-125 0-190 62-190
2021-09-16 04:28:29 UTC	137	IN	Data Raw: 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 34 2f 63 61 38 32 38 62 37 34 2d 37 66 39 65 2d 34 63 61 30 2d 39 33 30 62 2d 66 31 38 39 36 65 37 36 64 65 33 38 2d 6b 72 69 73 74 69 6e 63 61 76 61 6c 6c 61 72 69 5f 74 65 61 73 65 72 2e 6a 70 67 3f 77 3d 34 39 32 26 61 6d 70 3b 68 3d 34 39 32 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 66 70 2d 78 3d 30 2e 34 39 36 26 61 6d 70 3b 66 70 2d 79 3d 30 2e 37 30 35 33 22 20 73 72 63 73 65 74 3d 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 Data Ascii: .com/uploads/image/2021/9/14/ca828b74-7f9e-4ca0-930b-f1896e76de38-kristincavallari_teaser.jpg?w=49 2&h=492&fit=crop&crop=focalpoint&auto=format%2Ccompress&fp-x=0.496&fp-y=0.7053" srcset="https://imgix.bustle.com/uploads/image/2021/9
2021-09-16 04:28:29 UTC	150	IN	Data Raw: 22 6d 7a 6e 20 4f 55 74 22 3e 3c 6c 61 62 65 6c 20 63 6c 61 73 73 3d 22 41 47 7a 20 45 42 78 22 20 66 6f 72 3d 22 72 61 64 69 6f 2d 30 2d 32 37 36 32 34 33 36 39 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 58 61 48 22 3e 30 31 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 44 77 54 22 3e 42 75 73 74 6c 65 20 4d 69 78 74 61 70 65 3c 2f 64 69 76 3e 3c 2f 6c 61 62 65 6c 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6d 6d 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 4e 69 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 49 57 47 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 77 75 51 22 3e 3c 61 20 63 6c 61 73 73 3d 22 77 72 4f 22 20 68 72 65 66 3d 22 2f 65 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2f 63 68 76 72 63 68 65 73 2d 73 63 72 65 65 6e 2d 76 69 6f 6c 65 6e 63 65 2d Data Ascii: "mzn OUt"><label class="AGz EBx" for="radio-0-27624369"><div class="XaH">01</div><div class="DwT"> Bustle Mixtape</div></label><div class="imm"><div class="mNi"><div class="IWG"><div class="wuQ"><a class="wrO" href="/entertainment/chvrches-screen-violence-
2021-09-16 04:28:29 UTC	154	IN	Data Raw: 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 22 20 73 72 63 73 65 74 3d 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 30 2f 63 66 63 31 35 64 65 64 2d 34 32 34 37 2d 34 34 38 34 2d 61 63 64 35 2d 34 62 33 39 39 30 31 63 65 31 33 63 2d 77 74 77 5f 61 6d 61 72 61 6c 61 6e 65 67 72 61 2e 6a 70 67 3f 77 3d 31 39 37 26 61 6d 70 3b 68 3d 31 39 37 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 20 31 39 37 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f Data Ascii: auto=format%2Ccompress" srcset="https://imgix.bustle.com/uploads/image/2021/9/10/cfc15ded-4247-4484-acd5-4b39901ce13c-wtw_amaralanegra.jpg?w=197&h=197&fit=crop&crop=faces&auto=format %2Ccompress 197w, https://imgix.bustle.com/uploads/image/
2021-09-16 04:28:29 UTC	166	IN	Data Raw: 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 20 31 39 35 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 38 2f 34 2f 65 64 61 61 66 63 34 65 2d 36 34 30 35 2d 34 39 35 35 2d 39 33 38 65 2d 31 33 38 61 35 35 30 35 62 64 63 64 2d 7a 6f 6c 61 5f 73 6f 63 69 61 6c 63 6f 76 65 72 5f 62 6f 74 68 2e 70 6e 67 3f 77 3d 31 39 35 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 33 39 30 77 2c 20 68 Data Ascii: fit=crop&crop=faces&auto=format%2Ccompress 195w, https://imgix.bustle.com/uploads/image/20 21/8/4/edaafc4e-6405-4955-938e-138a5505bdcd-zola_socialcover_both.png?w=195&fit=crop&crop=fa ces&auto=format%2Ccompress&q=50&dpr=2 390w, h

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:29 UTC	169	IN	Data Raw: 72 69 70 74 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 45 57 79 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6e 78 45 22 3e 3c 2f 64 69 76 3e 3c 70 20 63 6c 61 73 73 3d 22 72 6d 65 20 47 47 74 22 3e 41 6c 69 63 69 61 20 4b 65 79 73 20 43 6f 6d 65 73 20 48 6f 6d 65 3c 2f 70 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 50 59 22 3e 3c 70 20 63 6c 61 73 73 3d 22 44 6f 41 22 3e 4f 6e 20 74 68 65 20 32 30 74 68 20 61 6e 6e 69 76 65 72 73 61 72 79 20 6f 66 20 53 6f 6e 67 73 20 69 6e 20 41 20 4d 69 6e 6f 72 2c 20 74 68 65 20 61 72 74 69 73 74 20 72 65 66 6c 65 63 74 73 20 6f 6e 20 77 68 6f 20 73 68 65 20 77 61 73 20 74 68 65 6e 20 e2 80 94 20 61 6e 64 20 77 68 6f 20 73 68 65 27 73 20 62 65 65 6e 20 61 6c 6c 20 61 6c 6f Data Ascii: ript></div></div><div class="EWy"><div class="nxE"></div><p class="rme GGt">Alicia Keys Comes Home</p></div><div class="cPY"><p class="DoA">On the 20th anniversary of Songs in A Minor, the artist reflects on who she was then and who she's been all along
2021-09-16 04:28:29 UTC	185	IN	Data Raw: 3e 3c 73 70 61 6e 3e 42 79 20 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 4e 65 75 22 3e 42 72 69 61 6e 20 41 6e 74 68 6f 6e 79 20 48 65 72 6e 61 6e 64 65 7a 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 2f 61 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6e 4c 74 30 20 47 74 75 22 3e 3c 61 20 63 6c 61 73 73 3d 22 4d 66 4a 20 4e 5f 41 22 20 68 72 65 66 3d 22 2f 65 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2f 66 61 6c 61 2d 63 68 65 6e 2d 6d 63 75 2d 77 6f 6d 65 6e 2d 6a 69 61 6e 67 2d 6c 69 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 4f 48 5f 20 41 43 59 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 76 78 5a 20 74 67 50 20 61 70 4b 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 30 30 25 3b 22 3e 3c 6e 6f 73 63 72 69 70 74 Data Ascii: >By Brian Anthony Hernandez</div></div><div class="nLt0 Gtu"><div class="OH_ ACY"><div class="vxZ tgP apK" style="padding-top: 100%;"><noscript
2021-09-16 04:28:29 UTC	189	IN	Data Raw: 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 33 2f 36 66 63 38 35 61 62 38 2d 34 31 64 30 2d 34 35 64 36 2d 38 61 33 32 2d 38 61 65 63 32 66 63 35 37 63 65 32 2d 73 61 6c 6c 79 72 6f 6f 6e 65 79 5f 74 65 61 73 65 72 2e 6a 70 67 3f 77 3d 31 39 36 26 61 6d 70 3b 68 3d 31 39 36 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 20 31 39 36 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 33 2f 36 66 63 38 35 61 62 38 2d 34 31 64 30 2d 34 35 64 36 2d 38 61 33 32 2d 38 61 65 63 32 Data Ascii: mgix.bustle.com/uploads/image/2021/9/13/6fc85ab8-41d0-45d6-8a32-8aec2fc57ce2-sallyrooney_teaser.jpg?w=196&h=196&fit=crop&crop=faces&auto=format%2Ccompress 196w, https://imgix.bustle.com/uploads/image/2021/9/13/6fc85ab8-41d0-45d6-8a32-8aec2
2021-09-16 04:28:29 UTC	195	IN	Data Raw: 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 34 2f 63 61 38 32 38 62 37 34 2d 37 66 39 65 2d 34 63 61 30 2d 39 33 30 62 2d 66 31 38 39 36 65 37 36 64 65 33 38 2d 6b 72 69 73 74 69 6e 63 61 76 61 6c 6c 61 72 69 5f 74 65 61 73 65 72 2e 6a 70 67 3f 77 3d 31 39 36 26 61 6d 70 3b 68 3d 31 39 36 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 66 70 2d 78 3d 30 2e 34 39 36 26 61 6d 70 3b 66 70 2d 79 3d 30 2e 37 30 35 33 26 61 6d 70 3b 64 70 72 3d 32 20 33 39 32 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f Data Ascii: bustle.com/uploads/image/2021/9/14/ca828b74-7f9e-4ca0-930b-f1896e76de38-kristincavallari_teaser.jpg?w=196&h=196&fit=crop&crop=focalpoint&auto=format%2Ccompress&q=50&fp-x=0.496&fp-y=0.7053&dpr=2 392w, https://imgix.bustle.co
2021-09-16 04:28:29 UTC	198	IN	Data Raw: 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 66 70 2d 78 3d 30 2e 34 38 36 37 26 61 6d 70 3b 66 70 2d 79 3d 30 2e 35 38 34 26 61 6d 70 3b 64 70 72 3d 32 20 33 39 32 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 33 2f 38 63 32 39 65 65 61 65 2d 65 66 32 61 2d 34 61 36 62 2d 61 33 63 33 2d 64 31 31 38 31 65 39 37 39 62 64 38 2d 74 65 6e 74 65 6e 72 65 63 6f 6d 6d 65 6e 64 5f 74 65 61 73 65 72 2e 6a 70 67 3f 77 3d 32 31 36 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 61 6d 70 3b 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f Data Ascii: amp;auto=format%2Ccompress&q=50&fp-x=0.4867&fp-y=0.584&dpr=2 392w, https://imgix.bustle.com/uploads/image/2021/9/13/8c29eeae-ef2a-4a6b-a3c3-d1181e979bd8-tentenrecommend_teaser.jpg?w=216&h=216&fit=crop&crop=focalpoint&auto=format%2Cco
2021-09-16 04:28:29 UTC	212	IN	Data Raw: 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 33 2f 37 65 33 62 33 61 33 33 2d 61 62 33 34 2d 34 65 34 33 2d 62 34 65 61 2d 35 38 62 62 63 64 65 38 33 39 61 61 2d 73 69 64 65 62 79 73 69 64 65 5f 74 65 6d 70 6c 61 74 65 30 30 31 2e 6a 70 65 67 3f 77 3d 31 39 36 26 61 6d 70 3b 68 3d 31 39 36 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 6f 63 61 6c 70 6f 69 6e 74 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 66 70 2d 78 3d 30 2e 34 39 33 33 26 61 6d 70 3b 66 70 2d 79 3d 30 2e 35 36 34 20 31 39 36 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f Data Ascii: ix.bustle.com/uploads/image/2021/9/13/7e3b3a33-ab34-4e43-b4ea-58bbcd839aa-sidebyside_template001.jpeg?w=196&h=196&fit=crop&crop=focalpoint&auto=format%2Ccompress&fp-x=0.4933&fp-y=0.564 196w, https://imgix.bustle.com/uploads/image/
2021-09-16 04:28:29 UTC	220	IN	Data Raw: 20 4b 72 61 76 69 73 2c 20 26 61 6d 70 3b 20 31 36 20 4f 74 68 65 72 20 46 75 6e 20 43 65 6c 65 62 20 43 6f 75 70 6c 65 73 20 48 61 6c 6c 6f 77 65 65 6e 20 43 6f 73 74 75 6d 65 20 49 64 65 61 73 3c 2f 70 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 51 47 69 20 44 70 50 22 3e 3c 70 20 63 6c 61 73 73 3d 22 4e 69 70 20 46 61 62 22 3e 50 61 70 61 72 61 7a 7a 69 20 6e 6f 74 20 69 6e 63 6c 75 64 65 64 2e 3c 2f 70 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 61 44 20 54 61 49 22 3e 3c 73 70 61 6e 3e 42 79 20 3c 2f 73 70 61 6e 3e 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 4e 65 75 22 3e 45 6d 6d 61 20 43 61 72 65 79 3c 2f 73 70 61 6e 3e 3c 2f 64 69 76 3e 3c 2f 61 3e 3c 61 20 63 6c 61 73 73 3d 22 4d 66 4a 20 50 56 63 22 20 68 72 65 66 3d 22 2f 6c 69 66 65 2f Data Ascii: Kravis, & 16 Other Fun Celeb Couples Halloween Costume Ideas</p><div class="QGt DpP"><p class="Nip Fab">Paparazzi not included.</p><div class="laD Tal">By Emma Carey</div></div><a class="MfJ Pvc" href="/life/
2021-09-16 04:28:29 UTC	228	IN	Data Raw: 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 20 31 39 36 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 30 2f 37 62 65 33 38 66 34 32 2d 33 37 66 30 2d 34 31 31 37 2d 62 31 62 64 2d 34 64 63 39 65 31 36 63 39 61 63 62 2d 62 69 67 5f 61 67 65 5f 70 6f 72 74 37 30 2e 6a 70 67 3f 77 3d 31 39 36 26 61 6d 70 3b 68 3d 31 33 39 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 33 39 32 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d Data Ascii: crop=faces&auto=format%2Ccompress 196w, https://imgix.bustle.com/uploads/image/2021/9/10/7be38f42-37f0-4117-b1bd-4dc9e16c9acb-big_age_port70.jpg?w=196&h=139&fit=crop&crop=faces&auto=format%2Ccompress&q=50&dpr=2 392w, https://im

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:29 UTC	244	IN	Data Raw: 25 32 43 63 6f 6d 70 72 65 73 73 20 31 32 33 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 35 2f 64 32 65 36 34 31 62 35 2d 39 64 34 61 2d 34 34 37 31 2d 61 66 39 63 2d 36 61 38 65 31 39 31 31 61 37 37 31 2d 73 63 72 65 65 6e 2d 73 68 6f 74 2d 32 30 32 31 2d 30 39 2d 31 35 2d 61 74 2d 35 33 30 35 38 2d 70 6d 2e 70 6e 67 3f 77 3d 31 32 33 26 61 6d 70 3b 68 3d 31 32 33 26 61 6d 70 3b 66 69 74 3d 63 72 6f 70 26 61 6d 70 3b 63 72 6f 70 3d 66 61 63 65 73 26 61 6d 70 3b 61 75 74 6f 3d 66 6f 72 6d 61 74 25 32 43 63 6f 6d 70 72 65 73 73 26 61 6d 70 3b 71 3d 35 30 26 61 6d 70 3b 64 70 72 3d 32 20 32 34 36 77 2c 20 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 Data Ascii: %2Ccompress 123w, https://imgix.bustle.com/uploads/image/2021/9/15/d2e641b5-9d4a-4471-af9c-6a8e1911a771-screen-shot-2021-09-15-at-53058-pm.png?w=123&h=123&fit=crop&crop=faces&auto=fo rmat%2Ccompress&q=50&dpr=2 246w, https://imgix.bu
2021-09-16 04:28:30 UTC	260	IN	Data Raw: 2f 70 2d 78 50 6d 63 72 46 4e 47 66 48 6b 42 67 2e 67 69 66 22 20 2f 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 73 62 2e 73 63 6f 72 65 63 61 72 64 72 65 73 65 61 72 63 68 2e 63 6f 6d 2f 70 3f 63 31 3d 32 26 61 6d 70 3b 63 32 3d 31 37 35 31 39 32 39 39 26 61 6d 70 3b 63 73 5f 75 63 66 72 3d 30 26 61 6d 70 3b 63 76 3d 32 2e 30 26 61 6d 70 3b 63 6a 3d 31 22 20 2f 3e 3c 69 6d 67 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 2f 74 72 3f 69 64 3d 31 36 33 36 36 37 33 37 36 33 32 32 37 37 33 34 26 61 6d 70 3b 65 76 3d 50 61 67 65 56 69 65 77 26 61 6d 70 3b 6e 6f 73 63 72 69 70 74 3d 31 22 20 2f 3e 3c 2f 6e 6f 73 63 72 69 70 74 3e 3c 2f 64 69 76 3e 3c 73 63 72 69 70 74 20 69 64 3d 22 5f 5f 49 4e 49 54 49 Data Ascii: /p-xPmcFNGfHkBg.gif" /></noscript></div><script id="__INITI
2021-09-16 04:28:30 UTC	276	IN	Data Raw: 65 20 6d 69 67 68 74 20 62 65 20 61 20 73 65 63 72 65 74 20 70 72 69 7a 65 20 61 74 20 74 68 65 20 65 6e 64 20 6f 66 20 74 68 65 20 73 65 61 73 6f 6e 2e 20 22 2c 22 69 6d 61 67 65 22 3a 7b 22 75 72 6c 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 62 63 34 66 39 39 39 62 2d 35 62 36 61 2d 34 63 35 63 2d 39 30 33 33 2d 37 33 35 39 39 64 65 61 30 30 35 31 2d 67 65 74 74 79 2d 34 35 31 31 39 37 35 31 33 2e 6a 70 67 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 5c 22 53 75 72 76 69 76 6f 72 5c 22 20 68 6f 73 74 20 4a 65 66 6e 20 50 72 6f 62 73 74 20 70 6f 73 65 73 20 66 6f 72 20 70 68 6f 74 6f 67 72 61 70 68 2e 22 2c 22 77 69 64 74 68 22 3a 32 31 Data Ascii: e might be a secret prize at the end of the season. ", "image": {"url": "https://imgix.bustle.com/uploads/getty /2021/9/15/bc4f999b-5b6a-4c5c-9033-73599dea0051-getty-451197513.jpg", "description": "\u201cSurvivor\u201d host Jeff Probst poses for photograph.", "width": 21
2021-09-16 04:28:30 UTC	292	IN	Data Raw: 69 6e 74 22 3a 6e 75 6c 6c 7d 2c 22 76 69 64 65 6f 22 3a 6e 75 6c 6c 7d 7d 7d 2c 7b 22 69 64 22 3a 22 37 37 30 31 32 30 35 31 22 2c 22 5f 5f 74 79 70 65 6e 61 6d 65 22 3a 22 43 61 72 64 50 61 67 65 22 2c 22 74 65 61 73 65 72 22 3a 7b 22 74 69 74 6c 65 22 3a 22 54 59 53 4f 4e 20 4f 6e 20 52 65 67 61 69 6e 69 6e 67 20 48 65 72 20 56 6f 69 63 65 20 5c 75 30 30 32 36 20 42 65 69 6e 67 20 41 20 54 79 70 69 63 61 6c 20 50 69 73 63 65 73 22 2c 22 73 75 6d 6d 61 72 79 22 3a 22 54 68 65 20 73 69 6e 67 65 72 2f 73 6f 6e 67 77 72 69 74 65 61 6e 64 20 73 69 73 74 65 72 20 6f 66 20 4d 61 62 65 6c 20 68 61 73 20 6a 75 73 74 20 72 65 6c 65 61 73 65 64 20 68 65 72 20 64 65 62 75 74 20 45 50 2e 22 2c 22 69 6d 61 67 65 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a Data Ascii: int":null},"video":null}}},{ "id":"77012051", "__typename":"CardPage", "teaser":{"title":"TYSON On Regaining Her Voice \u0026 Being A Typical Pisces", "summary":"The singer/songwriter and sister of Mabel has just released her debut EP.", "image":{"url":"https:
2021-09-16 04:28:30 UTC	308	IN	Data Raw: 72 20 42 61 6e 64 20 41 66 74 65 72 20 57 61 74 63 68 69 6e 67 20 22 5d 2c 5b 30 2c 5b 30 5d 2c 31 2c 22 4a 6f 73 69 65 20 41 6e 64 20 54 68 65 20 50 75 73 73 79 63 61 74 73 22 5d 5d 5d 5d 7d 2c 22 64 65 6b 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 5c 22 57 65 20 77 65 72 65 20 6c 69 6b 65 2c 20 27 4f 68 20 77 65 20 63 6f 75 6c 64 20 74 6f 74 61 6c 6c 79 20 64 6f 20 74 68 61 74 2e 27 5c 22 22 5d 5d 5d 5d 7d 2c 22 66 6f 6e 74 53 69 7a 65 44 65 73 6b 74 6f 70 22 3a 22 73 6d 61 6c 6c 22 2c 22 66 6f 6e 74 53 69 7a 65 4d 6f 62 69 6c 65 22 3a 22 73 6d Data Ascii: r Band After Watching "[, [0, [0], 1, "Josie And The Pussycats"]]]]]], "dek":{"version":"0.3.2", "markups":[], "atoms": [], "cards":[], "sections": [[1, "p", [[0, [], 0, "\u201cWe were like, \u201cOh we could totally do that.\u201c]]]]]], "fontSizeDesktop":"small", "fo ntSizeMobile":"sm
2021-09-16 04:28:30 UTC	324	IN	Data Raw: 2c 22 66 6f 6e 74 53 69 7a 65 44 65 73 6b 74 6f 70 22 3a 22 72 65 67 75 6c 61 72 22 2c 22 66 6f 6e 74 53 69 7a 65 4d 6f 62 69 6c 65 22 3a 22 73 6d 61 6c 6c 22 7d 2c 22 69 6d 61 67 65 22 3a 7b 22 69 64 22 3a 22 38 32 34 39 37 35 32 34 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 37 2f 31 35 2f 32 38 34 65 34 33 61 65 2d 39 64 36 31 2d 34 35 35 32 2d 38 64 38 35 2d 37 66 33 66 65 33 62 61 35 37 37 2d 75 6e 6e 61 6d 65 64 2d 35 2e 6a 70 67 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 22 3a 22 43 6f 75 72 74 65 73 79 20 6f 66 20 4e 61 64 69 61 20 4f 64 75 6e 61 79 6f 22 2c 22 61 74 74 72 69 62 75 74 69 6f 6e 55 72 6c 22 3a 6e 75 6c 6c 2c 22 64 65 Data Ascii: ", "fontSizeDesktop":"regular", "fontSizeMobile":"small"}, "image": {"id":"82497524", "url":"https://imgix.bustle.com/uploads/image/2021/7/15/284e43ae-9d61-4552-8d85-7f3fe3ba5777-unnamed-5.jpg", "attribution":"Courtesy of Nadia Odunayo", "attributionUrl":null, "de
2021-09-16 04:28:30 UTC	340	IN	Data Raw: 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 69 6d 70 6c 65 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 54 68 65 20 42 65 70 68 69 65 73 20 42 65 61 75 74 79 20 53 75 70 70 6c 79 20 44 65 73 69 6 7 6e 65 72 20 4f 6e 20 54 68 65 20 49 6d 70 6f 72 74 61 6e 63 65 20 4f 66 20 27 43 72 6f 77 6e 20 44 61 79 27 22 5d 5d 5 d 5d 7d 2c 22 64 65 6b 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 Data Ascii: ct":null,"palette":null},"palette":null,"variant":"simple", "fields":{"headline":{"version":"0.3.2", "markups":[], "atoms": [], "cards":[], "sections": [[1, "p", [[0, [], 0, "The Bepbies Beauty Supply Designer On The Importance Of \u201cCrown Day\u201c]]]]]], "dek":{"version":
2021-09-16 04:28:30 UTC	356	IN	Data Raw: 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 70 6c 69 74 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 41 74 20 32 38 2c 20 4b 65 6c 6c 79 20 52 69 70 61 20 57 61 73 20 41 20 57 6f 72 6b 69 6e 67 20 4d 6f 6d 20 57 68 6f 20 54 6f 6c 65 72 61 74 65 64 20 54 6f 6f 20 4d 75 63 68 20 e2 80 9c 42 75 6c 6c 73 68 69 74 e2 80 9d 22 5d 5d 5d 5d 7d 2c 22 64 65 6b 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 3 3 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5b 22 65 6d 22 5d Data Ascii: ette":null,"variant":"split", "fields":{"headline":{"version":"0.3.2", "markups":[], "atoms":[], "cards":[], "sections": [[1, "p", [[0, [], 0, "At 28, Kelly Ripa Was A Working Mom Who Tolerated Too Much Bullshit"]]]]]], "dek":{"version":"0.3.2", "markups": [["em"]

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:30 UTC	372	IN	Data Raw: 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 70 6c 69 74 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 41 74 20 32 38 2c 20 4c 65 67 65 6e 64 61 72 79 20 4d 75 73 69 63 20 57 72 69 74 65 72 20 44 61 6e 79 65 6c 2 0 53 6d 69 74 68 20 4c 65 61 72 6e 65 64 20 46 72 6f 6d 20 4c 65 61 76 69 6e 67 22 5d 5d 5d 5d 7d 2c 22 64 65 6b 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 Data Ascii: ull,"palette":null,"palette":null,"variant":"split","fields":{"headline":{"version":"0.3.2","markups":[],"atoms":[],"cards":[],"sections":[{"l","p",[[0,],0,"At 28, Legendary Music Writer Danyel Smith Learned From Leaving"]]}],"dek":{"version":"0.3.2","ma
2021-09-16 04:28:30 UTC	388	IN	Data Raw: 79 70 65 22 3a 22 68 65 61 64 6c 69 6e 65 22 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 74 72 65 61 74 6d 65 6e 74 22 3a 6e 75 6c 6c 2c 22 65 66 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 69 6d 70 6c 65 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 54 68 65 20 5c 22 57 65 69 72 64 5c 22 20 57 65 6c 6c 6e 65 7 3 73 20 52 69 74 75 61 6c 20 53 68 61 79 20 4d 69 74 63 68 65 6c Data Ascii: ype":{"headline"},"settings":{"treatment":null,"effect":null,"palette":null},"palette":null,"variant":"simple","fields":{"headline":{"version":"0.3.2","markups":[],"atoms":[],"cards":[],"sections":[{"l","p",[[0,],0,"The \"Weird\" Wellness Ritual Shay Mitchel
2021-09-16 04:28:30 UTC	404	IN	Data Raw: 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 65 74 74 65 22 3a 22 61 63 63 65 6e 74 65 64 5f 62 6c 61 63 6b 22 7d 2c 22 70 61 6c 65 74 74 65 22 3a 7b 22 63 6f 6c 6f 72 73 22 3a 5b 22 23 30 30 30 30 2c 22 23 66 66 66 66 66 66 66 22 2c 22 23 31 61 31 61 31 61 22 2c 22 23 61 62 61 62 61 62 22 2c 22 36 66 66 66 66 66 22 5d 7d 2c 22 7a 61 72 69 61 6e 74 22 3a 22 6f 76 65 72 6c 61 79 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 3 0 2c 22 4b 65 68 6c 61 6e 69 20 49 73 20 46 65 65 6c 69 6e 67 20 Data Ascii: fect":null,"palette":"accented_black"},"palette":{"colors":["#000000","#####","#1a1a1a","#ababab","#ffffff"],"variant":"overlay","fields":{"headline":{"version":"0.3.2","atoms":[],"cards":[],"markups":[],"sections":[{"l","p",[[0,],0,"Kehlani Is Feeling
2021-09-16 04:28:30 UTC	420	IN	Data Raw: 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 35 2f 61 30 64 33 39 32 37 61 2d 66 63 61 30 2d 34 39 61 36 2d 38 62 64 32 2d 37 30 39 66 61 30 66 63 66 64 33 61 2d 67 65 74 74 79 2d 31 33 34 30 31 37 38 36 36 31 2e 6a 70 67 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4a 75 73 74 69 6e 20 42 69 65 62 65 72 20 61 70 70 65 61 72 73 20 74 6f 20 62 65 20 63 6f 6e 73 6f 6c 69 6e 67 20 48 61 69 6c 65 79 20 42 69 65 62 65 72 20 61 74 20 74 68 65 20 32 30 32 31 20 4d 65 74 20 4f 61 6c 61 20 72 69 67 68 74 20 62 65 66 6f 72 65 20 73 68 65 20 70 75 74 20 6f 6e 20 68 65 72 20 73 75 6e 67 6c 61 73 73 65 73 2e 22 2c 22 77 69 64 74 68 22 3a 33 34 36 38 2c 22 68 65 69 67 68 74 22 3a 32 36 34 38 2c 22 66 Data Ascii: ix.bustle.com/uploads/getty/2021/9/15/a0d3927a-fca0-49a6-8bd2-709fa0cfcd3a-getty-1340178661.jpg),"description":"","Justin Bieber appears to be consoling Hailey Bieber at the 2021 Met Gala right before she put on her sungl asses.", "width":3468,"height":2648,"f
2021-09-16 04:28:30 UTC	436	IN	Data Raw: 61 72 64 53 74 6f 72 79 50 61 67 65 22 2c 22 74 65 61 73 65 72 22 3a 7b 22 74 69 74 6c 65 22 3a 22 41 6c 6c 20 4f 66 20 54 68 65 20 27 39 30 73 2d 49 6e 73 70 69 72 65 64 20 48 61 69 72 73 74 79 6c 65 73 20 41 74 20 54 68 65 20 32 30 32 31 20 4d 65 74 20 47 61 6c 61 22 2c 22 73 75 6d 6d 61 72 79 22 3a 22 4d 75 6c 6e 65 74 73 2c 20 74 77 69 73 74 65 64 20 75 70 64 6f 73 2c 20 61 6e 64 20 6d 6f 72 65 2e 22 2c 22 69 6d 61 67 65 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 69 6d 61 67 65 2f 32 30 32 31 2f 39 2f 31 34 2f 34 38 66 33 32 39 34 38 2d 61 36 37 65 2d 34 34 63 65 2d 62 66 64 38 2d 35 39 63 33 33 65 36 66 65 31 35 38 2d 67 65 74 74 79 69 6d 61 67 65 73 2d 31 33 34 30 Data Ascii: ardStoryPage","teaser":{"title":"All Of The '90s-Inspired Hairstyles At The 2021 Met Gala"},"summary":"Mulletts, twisted updos, and more.", "image":{"url":"https://imgix.bustle.com/uploads/image/2021/9/14/48f32948-a67e-44ce-bfd8-59c33e6fe158-gettyimages-1340
2021-09-16 04:28:30 UTC	452	IN	Data Raw: 2c 22 77 69 64 74 68 22 3a 36 30 30 30 2c 22 68 65 69 67 68 74 22 3a 34 30 30 30 2c 22 66 6f 63 61 6c 70 6f 69 6e 74 22 3a 6e 75 6c 6c 7d 2c 22 76 69 64 65 6f 22 3a 6e 75 6c 6c 2c 22 64 61 74 65 22 3a 31 36 33 31 37 33 38 33 30 33 38 39 33 2c 22 68 72 65 66 22 3a 22 2f 77 65 6c 6c 6e 65 73 73 2f 72 65 6c 61 74 69 6f 6e 73 68 69 70 2d 6f 63 64 2d 77 68 61 74 2d 69 74 2d 69 73 2d 68 6f 77 2d 74 6f 2d 64 65 61 6c 2d 77 69 74 68 2d 69 74 2d 6c 6f 6e 67 2d 74 65 72 6d 22 2c 22 73 70 6f 6e 73 6f 72 65 64 22 3a 66 61 6c 73 65 2c 22 62 79 6c 69 6e 65 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 49 72 69 73 20 47 6f 6c 64 73 7a 74 61 6a 6e 22 7d 5d 2c 22 65 79 65 62 72 6f 77 22 3a 7b 22 70 61 74 68 22 3a 22 2f 77 65 6c 6c 6e 65 73 73 22 2c 22 74 65 78 74 22 3a 22 53 65 78 Data Ascii: ,"width":6000,"height":4000,"focalpoint":null,"video":null,"date":"1631738303893","href":"/wellness/relationship-ocd-what-it-is-how-to-deal-with-it-long-term","sponsored":false,"byline":[{"name":"Iris Goldstajn"}],"eyebrow":{"path":"/wellness","text":"Sex
2021-09-16 04:28:30 UTC	468	IN	Data Raw: 20 52 65 6c 61 74 69 6f 6e 73 68 69 70 73 20 57 69 74 68 20 43 65 6c 65 62 72 69 74 69 65 73 20 41 72 65 6e 27 74 20 4e 65 63 65 73 73 61 72 69 6c 79 20 41 20 42 61 64 20 54 68 69 6e 67 22 2c 22 73 75 6d 6d 61 72 79 22 3a 22 4a 75 73 74 20 72 65 6d 65 6d 62 65 72 2c 20 61 6c 6c 20 79 6f 75 72 20 66 61 76 65 73 20 61 72 65 20 66 6c 61 77 65 64 2e 20 22 2c 22 69 6d 61 67 65 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 69 6d 67 69 78 2e 62 75 73 74 6c 65 2e 63 6f 6d 2f 75 70 6c 6f 61 64 73 2f 67 65 74 74 79 2f 32 30 32 31 2f 39 2f 31 34 2f 30 35 66 30 64 30 61 38 2d 37 35 35 61 2d 34 35 34 35 2d 61 37 37 63 2d 34 37 31 65 39 65 30 65 64 30 66 2d 67 65 74 74 79 2d 31 31 39 34 33 39 39 34 32 35 2e 6a 70 67 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e Data Ascii: Relationships With Celebrities Aren't Necessarily A Bad Thing"},"summary":"Just remember, all your faves are flawed.", "image":{"url":"https://imgix.bustle.com/uploads/getty/2021/9/14/05f0d0a8-755a-4545-a77c-471e9e0eed0f-getty-1194399425.jpg"},"description
2021-09-16 04:28:30 UTC	484	IN	Data Raw: 77 22 3a 7b 22 70 61 74 68 22 3a 22 2f 77 65 6c 6c 6e 65 73 73 22 2c 22 74 65 78 74 22 3a 22 4f 6c 79 6d 70 69 63 73 20 32 30 32 31 22 2c 22 76 69 73 69 62 6c 65 22 3a 74 72 75 65 7d 2c 22 68 65 61 64 65 72 22 3a 7b 22 69 64 22 3a 22 38 32 33 33 32 38 38 34 22 2c 22 74 79 70 65 22 3a 22 68 65 61 64 6c 69 6e 65 22 2c 22 73 65 74 74 69 6e 67 73 22 3a 7b 22 74 72 65 61 74 6d 65 6e 74 22 3a 6e 75 6c 6c 2c 22 65 66 66 65 63 74 22 3a 6e 75 6c 6c 2c 22 70 61 6c 6 5 74 74 65 22 3a 6e 75 6c 6c 7d 2c 22 70 61 6c 65 74 74 65 22 3a 6e 75 6c 6c 2c 22 76 61 72 69 61 6e 74 22 3a 22 73 69 6d 70 6c 65 22 2c 22 66 69 65 6c 64 73 22 3a 7b 22 68 65 61 64 6c 69 6e 65 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 Data Ascii: w":{"path":"/wellness","text":"Olympics 2021","visible":true},"header":{"id":"82332884","type":"headline"},"settings":{"treatment":null,"effect":null,"palette":null},"palette":null,"variant":"simple","fields":{"headline":{"version":"0.3.2","markups":[]},"at

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:30 UTC	500	IN	Data Raw: 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5b 22 65 6d 22 5d 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 22 3a 5b 5b 31 2c 22 70 22 2c 5b 5b 30 2c 5b 5d 2c 30 2c 22 48 65 72 65 e2 80 99 73 20 45 76 65 72 79 74 68 69 6e 67 20 59 6f 75 20 4e 65 65 64 20 54 6f 20 4b 6e 6f 77 20 41 62 6f 75 74 20 50 6c 61 79 69 6e 67 22 5d 2c 5b 30 2c 5b 30 5d 2c 31 2c 22 20 53 75 72 76 69 76 6f 72 20 34 31 22 5d 2c 5b 30 2c 5b 5d 2c 30 2c 22 20 41 74 20 48 6f 6d 65 22 5d 5d 5d 5d 7d 2c 22 64 65 6b 22 3a 7b 22 76 65 72 73 69 6f 6e 22 3a 22 30 2e 33 2e 32 22 2c 22 6d 61 72 6b 75 70 73 22 3a 5b 5d 2c 22 61 74 6f 6d 73 22 3a 5b 5d 2c 22 63 61 72 64 73 22 3a 5b 5d 2c 22 73 65 63 74 69 6f 6e 73 Data Ascii: sion:"0.3.2","markups":{"em":"","atoms":"","cards":"","sections":["1,p","0,0,0,"Heres Everything You Need To Know About Playing"],[0,0,1," Survivor 41"],[0,0,0," At Home"]}},"dek":{"version":"0.3.2","markups":"","atoms":"","cards":"","sections

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49788	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	617	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf0.AWW8dwX95Z0
2021-09-16 04:28:37 UTC	618	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDQgA; expires=Wed, 15-Dec-2021 04:28:36 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: kaYko6Zqw3ooN4ULRNB1guFwxrrfEDd5KmqfkyOFuoODftlmV3MmCgMMIM9VitRBEeQ6EosX1VqNSE Oh5oh0CA== Date: Thu, 16 Sep 2021 04:28:37 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49787	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	619	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDQgA
2021-09-16 04:28:37 UTC	620	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: dkezyZu+SZdPYBZCFCCD08w00d8uJReUP0V8XFszyef9XHMje9X0j9yEjF4ZtOJxe1LJld8juNaAZp GLQfoj+Q== Date: Thu, 16 Sep 2021 04:28:37 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	620	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 79 5a 31 53 6c 31 77 55 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 37 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="yZ1S1wU"/>*<![CDATA[*](function){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/common/vscribe_endpoint.php?c=si_clickjacking&t=7
2021-09-16 04:28:37 UTC	621	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 79 5a 31 53 6c 31 77 55 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 53 54 6c 58 61 Data Ascii: ow.document.write("&#003Cstyle nonce="yZ1S1wU">body * {display:none !important;}&#003Cvstyle>&#003Ca href=&quot;#&quot; onclick=&quot;top.location.href=window.location.href&quot; style=&quot;display:block !important;padding:10px!&quot;>Gehe zu facebook.com&#003CVa>");/*STIXa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49789	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	622	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MnVCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDQgA
2021-09-16 04:28:37 UTC	623	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MnVCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDVk0; expires=Wed, 15-Dec-2021 04:28:36 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: T0Pjz4l31P/bYnJEnnC6b3pTYrb0o/xBG4WVXXkY1yEju6l9e0RqxjBnWeZRGINSuzX7IUourjQjA ILlxvW1A== Date: Thu, 16 Sep 2021 04:28:37 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49790	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	624	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, /* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDVk0

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	624	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: MltIdUv1iBDIcgPmH0mfMIISP33k+oLH3i0F2EKfJ9SiHb38lDjJlB37VzCH6ljTjb6F/PE69AcyW6kTbqfhQ== Date: Thu, 16 Sep 2021 04:28:37 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:37 UTC	625	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 35 75 61 6e 49 66 5a 59 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 39 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="5uanlfZY"/>*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=9
2021-09-16 04:28:37 UTC	626	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 35 75 61 6e 49 66 5a 59 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 5a 64 35 42 50 4f 61 42 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="5uanlfZY"body * {display:none !important;}u003CVstyle>u003Ca href="#" onclick="\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003CVa>");/*Zd5BPOaB*/}}()/)*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49791	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	626	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, /* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDVk0
2021-09-16 04:28:37 UTC	627	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDUK8; expires=Wed, 15-Dec-2021 04:28:36 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: J1TXeMFVvpEk7wvEVoAYo3UqY8rxA62lKN4r5BcfZL3VM/9HsYHruXR0E2d23bi6wcV9jSkiqiwMpxE5X57fNw== Date: Thu, 16 Sep 2021 04:28:37 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49792	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:37 UTC	628	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDUK8
2021-09-16 04:28:38 UTC	629	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: MkhkOzx069x814Xt+8D14tcl0REdML4JNgIAf0p46wSec2XpuHfFSEijxx3luEjaSdlBk53OtGkwi dYdn7VVw== Date: Thu, 16 Sep 2021 04:28:37 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:38 UTC	629	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 64 56 55 69 6d 50 37 79 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="dVUimP7y"/>*<![CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:38 UTC	630	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 64 56 55 69 6d 50 37 79 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4f 71 47 33 39 Data Ascii: ow.document.write("lu003Cstyle nonce="dVUimP7y">body * {display:none !important;}lu003Cvstyle>lu003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comlu003Cva>);/*OqG39

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49793	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	631	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf1.AWWZxUGDUK8

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	632	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayq0_o; expires=Wed, 15-Dec-2021 04:28:37 GMT; Max-Age=7775999; path=/; domain=facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: hjSiLz67/4VY4ywtzGsl1trq6a7ymBlPrpgSUCRSOVQJHXGLpY92ELVhJoY6FqvXV32w1LkpbSQJby VLSirWaw== Date: Thu, 16 Sep 2021 04:28:38 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49794	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	633	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayq0_o
2021-09-16 04:28:38 UTC	634	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: qcEHJC4nEAnjTnr1hobqstEDgnJajs8eUlgIHb/hL+nR/CdvOMU2MdaHJuJOuiJRSGz+K65nEDSbt tpJYEavw== Date: Thu, 16 Sep 2021 04:28:38 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:38 UTC	634	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 50 42 31 30 34 4a 7a 74 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 39 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="PB104Jzt"/>*<![CDATA[*]/(function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=9
2021-09-16 04:28:38 UTC	635	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 50 42 31 30 34 4a 7a 74 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 44 50 4c 42 49 Data Ascii: ow.document.write("<u003Cstyle nonce=<PB104Jzt>">body * {display:none !important;}<u003Cvstyle><u003Ca href="#\" onclick=<\"top.location.href=window.location.href\" style=<\"display:block !important;padding:10px\">Gehe zu facebook.com<u003Cv>");/*DPLBI

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49795	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	636	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf2.wZ.AAA.0.0.BhQsf2.AWXnUayq0_o
2021-09-16 04:28:38 UTC	636	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsf2.AWXnUayqsp4; expires=Wed, 15-Dec-2021 04:28:37 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: sQw5aXBTG03c7fXdcQRBdotodMo9R/ZiEhZQa9V7w1bGSaIHjSv/JO/ZrAZrtKLEWzIFXPO0b/UoQc j64d7JEw== Date: Thu, 16 Sep 2021 04:28:38 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49796	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	637	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf2.wZ.AAA.0.0.BhQsf2.AWXnUayqsp4
2021-09-16 04:28:38 UTC	638	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 9KCpNfINiH1v3DMEnAy9zb8zCzsrAXF70SAd1DP+7Zkdh6cAs+onUmk9n77+Aw75K1g0Th31hNCmV qPp8k6Sw== Date: Thu, 16 Sep 2021 04:28:38 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:38 UTC	639	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 65 36 6f 4c 55 76 4b 39 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="e6oLUvK9"/>*<![CDATA[*(function(){function s_i_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=s_i_clickjacking&t=1

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	640	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 65 36 6f 4c 55 76 4b 39 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 64 6a 73 51 78 Data Ascii: ow.document.write("u003Cstyle nonce=\"e6oLUvK9l\">body * {display:none !important;}u003C/vstyle>u003Ca href=\"#l\" onclick=\"top.location.href=window.location.hrefl\" style=\"display:block !important;padding:10pxl\">Gehe zu facebook.comu003C/va>);/*djsQx

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49756	52.222.214.86	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:32 UTC	510	OUT	GET /profile/brian-anthony-hernandez-63990196 HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.bustle.com Connection: Keep-Alive
2021-09-16 04:28:32 UTC	510	IN	HTTP/1.1 200 OK Content-Type: text/html Content-Length: 49721 Connection: close Date: Thu, 16 Sep 2021 04:28:32 GMT Cache-Control: max-age=600 content-security-policy: frame-ancestors 'self' http://localhost:* https://*.bustle.com Apigw-Requestid: FvQtjhFzoAMEJIQ= Vary: Accept-Encoding X-Cache: Miss from cloudfront Via: 1.1 081c7bef6b5d3c12829ac4c99182ccea.cloudfront.net (CloudFront) X-Amz-Cf-Pop: FRA56-P3 X-Amz-Cf-Id: -wW0LsmQ1DxUUzDda54LTlCNwErKbcsLaAYcWtX5nd9SIPaVw7n0Sg==
2021-09-16 04:28:32 UTC	511	IN	Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 70 72 65 66 69 78 3d 22 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 75 6e 73 61 66 65 2d 75 72 6c 22 20 2f 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 77 69 74 74 65 72 3a 73 69 74 65 22 20 63 6f 6e 74 65 6e 74 3d 22 40 62 75 73 74 6c 65 22 20 2f 3e 3c 6d 65 Data Ascii: <!doctype html><html lang="en" prefix="og: http://ogp.me/ns#/"><head><meta charset="utf-8" /><meta name="viewport" content="width=device-width,initial-scale=1" /><meta name="referrer" content="unsafe-url" /><meta name="twitter:site" content="@bustle" /><me
2021-09-16 04:28:32 UTC	519	IN	Data Raw: 43 67 6b 22 20 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 3e 3c 2f 62 75 74 74 6f 6e 3e 3c 2f 6c 61 62 65 6c 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 68 65 61 64 65 72 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 49 68 46 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 43 56 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 43 43 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 46 78 5a 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 75 6c 59 22 3e 3c 68 31 20 63 6c 61 73 73 3d 22 79 72 5a 22 3e 42 72 69 61 6e 20 41 6e 74 68 6f 6e 79 20 48 65 72 6e 61 6e 64 65 7a 3c 2f 68 31 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 72 41 6a 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 76 78 5a 20 77 6a 6e 20 61 70 4b 22 20 73 74 79 6c 65 3d 22 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 30 30 25 3b 22 3e Data Ascii: Cgk" type="button"></button></label></div></div></header><div class="lhF"><div class="cCV"><div class="sCC"><div class="FxZ"><div class="uLY"><h1 class="yrZ">Brian Anthony Hernandez</h1><div class="rAJ"><div class="vxZ wjn apk" style="padding-top: 100%;">
2021-09-16 04:28:32 UTC	535	IN	Data Raw: 70 61 6e 3e 3c 61 20 68 72 65 66 3d 22 2f 70 72 6f 66 69 6c 65 2f 62 72 69 61 6e 2d 61 6e 74 68 6f 6e 79 2d 68 65 72 6e 61 6e 64 65 7a 2d 36 33 39 39 30 31 39 36 22 20 63 6c 61 73 73 3d 22 4e 65 75 22 3e 42 72 69 61 6e 20 41 6e 74 68 6f 6e 79 20 48 65 72 6e 61 6e 64 65 7a 3c 2f 61 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 61 3e 3c 61 20 63 6c 61 73 73 3d 22 77 53 5f 22 20 68 72 65 66 3d 22 2f 65 6e 74 65 72 74 61 69 6e 6d 65 6e 74 2f 72 75 74 68 65 72 66 6f 72 64 2d 66 61 6c 6c 73 2d 72 65 61 67 61 6e 2d 77 65 6c 6c 73 2d 6a 61 6e 61 2d 73 63 68 6d 69 65 64 69 6e 67 2d 6e 61 74 69 76 65 2d 64 69 76 65 72 73 69 74 79 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 64 6e 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 76 78 5a 20 61 70 4b 22 20 73 74 79 6c 65 3d Data Ascii: pan>Brian Anthony Hernandez</div></div><div class="cdn"><div class="vxZ apk" style=
2021-09-16 04:28:32 UTC	546	IN	Data Raw: 6c 6f 72 20 53 77 69 66 74 2c 20 53 68 61 6e 69 61 20 54 77 61 69 6e 2c 20 61 6e 64 20 4c 61 64 79 20 47 61 67 61 20 69 6e 20 70 65 72 73 6f 6e 2c 20 68 65 e2 80 99 73 20 65 6e 67 61 67 69 6e 67 20 69 6e 20 73 6f 63 69 61 6c 20 69 73 73 75 65 73 2c 20 61 64 76 6f 63 61 74 69 6e 67 20 66 6f 72 20 64 69 76 65 72 73 69 74 79 2c 20 61 6e 64 20 69 6e 74 65 72 61 63 74 69 6e 67 20 6f 6e 6c 69 6e 65 20 77 69 74 68 20 63 65 6c 65 62 72 69 74 69 65 73 2e 20 42 41 48 20 61 74 74 65 6e 64 65 64 20 74 68 65 20 55 6e 69 76 65 72 73 69 74 79 20 6f 66 20 4e 65 62 72 61 73 6b 61 2d 4c 69 6e 63 6f 6c 6e 2c 20 61 6e 64 20 68 65 20 74 72 61 69 6e 65 64 20 68 69 73 20 65 64 69 74 69 6e 67 20 73 6b 69 6c 6c 73 2 0 61 73 20 70 61 72 74 20 6f 66 20 74 68 65 20 41 6d 65 72 69 63 Data Ascii: lor Swift, Shania Twain, and Lady Gaga in person, hes engaging in social issues, advocating for diversity, and interacting online with celebrities. BAH attended the University of Nebraska-Lincoln, and he trained his editing skills as part of the Americ

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49797	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	640	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsf2.AWXnUayqsp4
2021-09-16 04:28:38 UTC	641	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsf2.AWXnUayqwOE; expires=Wed, 15-Dec-2021 04:28:37 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: /JVWILh+9CioM70qqTn70b967PyowMX3LxV7QWXP0JQKtXxNjI37UR4DYru5ZHIJ5li+h+XpPZQdO GEF/348g== Date: Thu, 16 Sep 2021 04:28:38 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49798	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	642	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsf2.AWXnUayqwOE
2021-09-16 04:28:38 UTC	643	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: t/k48aMhSPIArAL+FvL2faWJvhkFkaoSZcz9PF5UYr7284BLWqzoOrb93rUiB+6G7i5SelgPL/alA LKHQgtMA== Date: Thu, 16 Sep 2021 04:28:38 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:38 UTC	643	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 44 35 67 55 7a 31 4c 45 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="D5gUz1LE"/>*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=8

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	644	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 44 35 67 55 7a 31 4c 45 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 38 6d 45 5f 55 Data Ascii: ow.document.write("\u003Cstyle nonce=\"D5gUz1LE\">body * {display:none !important;}\u003C/style>\u003Ca href=\"#\" onclick=\"top.location.href=window.location.href\" style=\"display:block !important;padding:10px\">Gehe zu facebook.com\u003C/a>);/*8mE_U

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49799	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	645	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayqwOE
2021-09-16 04:28:38 UTC	646	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayqlr0; expires=Wed, 15-Dec-2021 04:28:37 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: MJyYG+eUkKLNfPLrEIIRHXWEstW5GMI6CTReW0l8FGd7hjRzKILTdl+QvJNDR7a4tsdH14ki0QK9kZ5O2A2+A== Date: Thu, 16 Sep 2021 04:28:38 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49800	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	647	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayqlr0
2021-09-16 04:28:38 UTC	647	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: BHefymp6wOwEeO7ZfP+Qf/1SHXdHMH7GYN8sKLVWQ9uOvaYfpWm9n/fmMklhTS5UnDSSaAYuHMM0ioIWkq389A== Date: Thu, 16 Sep 2021 04:28:38 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:38 UTC	648	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 68 42 51 31 57 52 64 31 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="hBQ1WRd1">/*!l[C DATA[*](function(){function si_cj(m){setTimeout(function(){new Image()).src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:38 UTC	649	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 68 42 51 31 57 52 64 31 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4f 33 59 46 4d 6b 48 70 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="hBQ1WRd1">body * {display:none !important;}u003C/vstyle>u003Ca href="#" onclick="\top.location.href=window.location.href" style="\display:block !important;padding:10px">Gehe zu facebook.com u003C/va>");/*O3YFMkHp*/}}()/)*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49801	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	650	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf2.AWXnUayqlr0
2021-09-16 04:28:39 UTC	650	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkebXU; expires=Wed, 15-Dec-2021 04:28:38 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: H2AR/Z00iKcd2ofEwKiCB4Ti5JNqrZ0AAXJmwjr+wJ7raUvq3g2HQEpeGvkFcIRzdBW55jfhW/I1oe0i0vKpg== Date: Thu, 16 Sep 2021 04:28:39 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49802	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	651	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkebXU

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	652	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: A6pO3USD38uecCu3yej/CM9iZkyxaii7YW+A6UrVyCEoZiZ8v55kuJ+BftibZh0Zz65/SEZYlyRZIV28sRtFg== Date: Thu, 16 Sep 2021 04:28:39 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:39 UTC	653	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 66 59 63 6e 66 49 67 68 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="fYcnflgh">/*<![CDATA[*/*(function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=sl_clickjacking&t=5
2021-09-16 04:28:39 UTC	654	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 66 59 63 6e 66 49 67 68 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4f 66 61 4b 57 Data Ascii: ow.document.write("u003Cstyle nonce="fYcnflgh">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003Cv>")/*OfaKW

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49803	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	654	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUKXNkebXU
2021-09-16 04:28:39 UTC	655	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUKXNkeTlk; expires=Wed, 15-Dec-2021 04:28:38 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: ewivJV57YShW7mwyepMb7849bXQuQBKGKsufwKW01txZy82q7Gi4oSDO55xbS+lkK2cSjMKA5x5mYV S9ycHVJw== Date: Thu, 16 Sep 2021 04:28:39 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49804	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	656	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkeTlk
2021-09-16 04:28:39 UTC	657	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 6kRFYQ9RRG6CXyq+ptmgvjETr/Ww/nszED1GmDS2ac3o4RyE33qnd2PCF9ISma0zt+qmm0+Nlg2RFmtaBz83rQ== Date: Thu, 16 Sep 2021 04:28:39 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:39 UTC	657	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 64 59 31 46 6d 63 49 71 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="dY1Fmclq">/*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3
2021-09-16 04:28:39 UTC	658	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 64 59 31 46 6d 63 49 71 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 5a 38 47 71 31 4d 49 39 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="dY1Fmclq">body * {display:none !important;}u003C/vstyle>u003Ca href="#" onclick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comu003C/va>");/*Z8Gq1MI9*/}}})();/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49805	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	659	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkeTlk
2021-09-16 04:28:39 UTC	660	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkeEJU; expires=Wed, 15-Dec-2021 04:28:38 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-lafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: aYfaxEG3B+BBBhK/YtTfjVIXFnavgsoWyu8Gjl28tW4gFdoKM1pC4kxzLISgYgROpH0+X17LQy9jxz/obUSIA== Date: Thu, 16 Sep 2021 04:28:39 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49806	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	661	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUKXNkeEJU
2021-09-16 04:28:39 UTC	661	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: XYBkFc5kNfCFESI69PA3zDpUqU8ZyR7hv57P7ZPwsc5WUNE7U+uroitPBRczhcZSFkvhQk0gA3vAdg iDwuqGeA== Date: Thu, 16 Sep 2021 04:28:39 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:39 UTC	662	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6b 79 6b 4e 31 67 4c 72 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="kykN1gLr">/*!CDATA["/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:39 UTC	663	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6b 79 6b 4e 31 67 4c 72 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 72 64 6c 6f 73 72 51 57 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="kykN1gLr">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003Cv>");/*rdlosQW*/}}()/)*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49762	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:33 UTC	559	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: www.facebook.com Connection: Keep-Alive
2021-09-16 04:28:33 UTC	560	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: H1ScQ8l69hvxrt9elqAwH32Hlxh+Ts2CxxwEmCZPqDj5ssA1q8cRso1Xgw4Y07FiByBwzVG+qtXBF KIQFnYoQ== Date: Thu, 16 Sep 2021 04:28:33 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:33 UTC	560	IN	Data Raw: 35 35 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 72 32 44 43 58 71 62 76 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 555<html><head><title>Redirecting...</title><script type="text/javascript" nonce="r2DCXqvb">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:33 UTC	561	IN	Data Raw: 77 77 2e 62 75 73 74 6c 65 2e 63 6f 6d 5c 75 30 30 32 35 32 46 65 6e 74 65 72 74 61 69 6e 6d 65 6e 74 5c 75 30 30 32 35 32 46 68 61 69 6c 65 79 2d 62 69 65 62 65 72 2d 63 72 79 69 6e 67 2d 74 69 6b 74 6f 6b 2d 76 69 64 65 6f 2d 6d 65 74 2d 67 61 6c 61 2d 73 65 6c 65 6e 61 2d 67 6f 6d 65 7a 2d 63 68 61 6e 74 5c 75 30 30 32 35 33 46 75 74 6d 5f 74 65 72 6d 5c 75 30 30 32 35 33 44 73 68 61 72 65 26 5f 72 64 72 22 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 72 65 66 72 65 73 68 22 20 63 6f 6e 74 65 6e 74 3d 22 30 3b 75 72 6c 3d 68 74 74 70 73 3a 2f 2f 6d 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 2f 73 68 61 72 65 72 2f 73 68 61 72 65 72 2e 70 68 70 3f 75 3d 68 74 74 70 73 25 33 41 25 32 46 25 32 46 77 77 77 2e 62 75 73 Data Ascii: ww.bustle.com/u00252Fentertainment/u00252Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant/u00253Futm_term/u00253Dshare&_rdr");</script><meta http-equiv="refresh" content="0";url=https://m.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant/u00253Futm_term%3Dshare&_rdr HTTP/1.1

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49807	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	664	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfX.wZ.AAA.0.0.BhQsf3.AWUkXNkeEJU
2021-09-16 04:28:39 UTC	664	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfX.wZ.AAA.0.0.BhQsf3.AWUkXNkeCZQ; expires=Wed, 15-Dec-2021 04:28:38 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: bWDB3nYuWshKNGn1PawxVXTvjLY6Z0qBzAUQkv85708DWTsBrDBanMxTW8bBESZneKF CAB+Yahm4vf4Xoj3iw== Date: Thu, 16 Sep 2021 04:28:39 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49808	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	665	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfX.wZ.AAA.0.0.BhQsf3.AWUkXNkeCZQ

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:39 UTC	666	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: ijNUo33TzayOcenFG6vmH5EM8Dyrw4bXx38ykpCpiUbTOoIoVCKPpG66sDPM1bgs3kMdz7SA/Um7etp9XrXDeQ== Date: Thu, 16 Sep 2021 04:28:39 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:39 UTC	667	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 7a 57 6c 5a 67 38 75 4a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="zWlZg8uJ"> /*<![CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=8
2021-09-16 04:28:39 UTC	667	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 7a 57 6c 5a 67 38 75 4a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6f 34 6d 6e 6c Data Ascii: ow.document.write("\u003Cstyle nonce="\u003Cscript nonce="zWlZg8uJ">body * {display:none !important;}\u003Cvstyle>\u003Cahref="\u003Cva>")/*>Gehe zu facebook.com/\u003Cva>")/*>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49809	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	668	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf3.AWUkXNkeCZQ
2021-09-16 04:28:40 UTC	669	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyR4g; expires=Wed, 15-Dec-2021 04:28:39 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: w5U9VI3+xhysGdrvMjbn4vfgW/mwDN4jEiyrP3F6dlbpmb7u+AVz2KP0zV7gnnpc7/Z6WyA4OJmF6DRhbYkCVA== Date: Thu, 16 Sep 2021 04:28:40 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49810	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	670	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyR4g
2021-09-16 04:28:40 UTC	671	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: Ga5kik9IHvon1IMtKnaMMvOrGKKDAD0dHjDRUR/LcFul3bUZBSTdlvP+7aUId0ndDk5gHCdA2Kp3/vHKm/q0hQ== Date: Thu, 16 Sep 2021 04:28:40 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:40 UTC	671	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 69 45 4c 59 41 44 63 62 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="iELYADcb">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:40 UTC	672	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 69 45 4c 59 41 44 63 62 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 55 6e 5f 4a 44 Data Ascii: ow.document.write("u003Cstyle nonce="iELYADcb">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comu003Cva>);/*Un_JD

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49811	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	673	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyR4g

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	678	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyZyY
2021-09-16 04:28:40 UTC	678	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyLW8; expires=Wed, 15-Dec-2021 04:28:39 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: ZjFyFlvBqu+hLQz8mDldsqugYVc5K38EY7+C0CDGB+5h9PruwX2GNJkH2913/xclVt17K1ZKqCR2iygt5GS4mw== Date: Thu, 16 Sep 2021 04:28:40 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49814	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	679	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyLW8
2021-09-16 04:28:40 UTC	680	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: grYLzCc7clkiFNIrca0l9EeYMZF+g4hf+Q6yIfWpuMjrf9lDj4jqQiDBjw7AyXxuP/acj92/cwsySXlInXxS6A== Date: Thu, 16 Sep 2021 04:28:40 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:40 UTC	680	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4f 42 4b 6d 77 4d 33 35 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="OBKmwM35">*<![CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:40 UTC	681	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4f 42 4b 6d 77 4d 33 35 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4b 30 6b 34 53 Data Ascii: ow.document.write("u003Cstyle nonce="OBKmwM35">body * {display:none !important;}u003Cvstyle>\u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com\u003C/va>");/*K0k4S

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49815	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	682	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKlyLW8
2021-09-16 04:28:40 UTC	683	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKly2UY; expires=Wed, 15-Dec-2021 04:28:39 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: KEmRNPSOaCuZmRhnMYDnVfQCJe08WCrPkRn3dQ39gMTahN3leuER1t/5MK4TNmJwlSD8+kwqPVo9dj1Occ9wg== Date: Thu, 16 Sep 2021 04:28:40 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49816	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	684	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKly2UY
2021-09-16 04:28:40 UTC	685	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: /8EMZzYCyz2BvKffXV+6MW3fsr9bWyWEotd9LejGgtTZ98z6czPxGQyWHVtiqdxin3Gp0zkIh0nu sgEdex5g== Date: Thu, 16 Sep 2021 04:28:40 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:40 UTC	685	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 65 37 54 71 4e 32 68 41 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 36 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="e7TqN2hA">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=6

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	686	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 65 37 54 71 4e 32 68 41 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6b 31 38 39 56 Data Ascii: ow.document.write("u003Cstyle nonce="e7TqN2hA">body * {display:none !important;}u003C\style>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comu003C\va>");/*k189V

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49764	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:33 UTC	561	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive
2021-09-16 04:28:33 UTC	562	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; expires=Sat, 16-Sep-2023 04:28:33 GMT; Max-Age=63072000; path=/; domain=.facebook.com; secure; httponly Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfx.AWUBBy_mcJKM; expires=Wed, 15-Dec-2021 04:28:32 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: 5RsXonBdoHAk5mp7M792wkTmOd+dVJE8bHA17i62NpullNt52enymGB0/4+TxQFxiUjDfVegTQtp o82ipysQ== Date: Thu, 16 Sep 2021 04:28:33 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49817	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:40 UTC	687	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf4.AWU5rKly2UY

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	688	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWWfoE_b7LA; expires=Wed, 15-Dec-2021 04:28:40 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: VTCq7GxIsr7B9aqwtypks+L8kays/0kDgAla2RI4SJ1b+xKHlmJi1acQJKFRIHj7YpkK3tdSS+2Cy8tsQvMKQ== Date: Thu, 16 Sep 2021 04:28:41 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49818	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	689	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWVfoE_b7LA
2021-09-16 04:28:41 UTC	689	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: htgQqMzA+Z5yyMWY+C8vVUMALgiu6vR+idfD549J6KEE36/dC8Wdg0DfcYNs/GaolSicI+bTZ+iMda syayyxSg== Date: Thu, 16 Sep 2021 04:28:41 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:41 UTC	690	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4e 4a 36 35 47 68 65 74 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="NJ65Ghet"/>*<![CDATA[*]/(function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=8
2021-09-16 04:28:41 UTC	691	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4e 4a 36 35 47 68 65 74 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 7f 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 46 43 78 41 62 6a 53 52 2a 2f 7d 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="NJ65Ghet">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick=\ "top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.com/u003Cv>");/*FCxAbjSR*}}})/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49819	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	692	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWWfoE_b7LA
2021-09-16 04:28:41 UTC	692	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWWfoE_bj_A; expires=Wed, 15-Dec-2021 04:28:40 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: na0GVpxzjo6aGsCtPOjO791YEj59tf9URuJGkAaeHTPZEjlfu1Gc0N0GnmnPn5yLv5OA+PFHM7xqV5H5JoybA== Date: Thu, 16 Sep 2021 04:28:41 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49820	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	693	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWWfoE_bj_A
2021-09-16 04:28:41 UTC	694	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: w4M9IPUI8822uH1Br2M1XJ7Mr1vo+Gv3sk0L13Eo0hZvoal2WWni7MbraXd8FPkK1qn5EWbO/scEzCjR86UHPA== Date: Thu, 16 Sep 2021 04:28:41 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:41 UTC	694	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 54 50 79 68 72 55 36 4a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="TPyhrU6J"/>*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	695	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 54 50 79 68 72 55 36 4a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 53 44 79 6f 61 Data Ascii: ow.document.write("u003Cstyle nonce="TPyhrU6Jl">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comu003C/a>");/*SDyoa

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49821	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	696	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWVfoE_bj_A
2021-09-16 04:28:41 UTC	697	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWVfoE_baSE; expires=Wed, 15-Dec-2021 04:28:40 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: XgAOi9gWdPrI2NsFgsX0mDy+qKCM42XNcVXNSGbph4G6LsIFe5xlxmOQKrIX6bhcb6OF9D0B8FZBVuvSjXERg== Date: Thu, 16 Sep 2021 04:28:41 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49822	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	698	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWVfoE_baSE
2021-09-16 04:28:41 UTC	699	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 542LVFKeUZl4pNTRzI5JacVYKYINi9lyRU9Ym9xK3L7uwKrl3JDbn/85MN7Prlxw297wtfkBA5+KdeEbeiBtwv== Date: Thu, 16 Sep 2021 04:28:41 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	699	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 75 68 5a 79 79 71 56 71 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="uhZyyqVq">/*<!CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/common/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:41 UTC	700	IN	Data Raw: 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 75 68 5a 79 79 71 56 71 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 6c 4f 30 65 51 79 Data Ascii: w.document.write("\u003Cstyle nonce="\u003Cstyle>\u003Ca href="#" onclick="\u003Cstyle>\u003C/a>");/*IO0eQy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	192.168.2.3	49823	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:41 UTC	701	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MnVCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf5.AWWfoE_baSE
2021-09-16 04:28:42 UTC	702	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MnVCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf6.AWU-LDXIFUU; expires=Wed, 15-Dec-2021 04:28:41 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: soNTce6sAHfuETKvWtomJmCd7o8zbE4UXuDKKcV6ktWAwvwx7Ar341r15p3hpNggoXumPFfcQXX/NSTOefBhw== Date: Thu, 16 Sep 2021 04:28:42 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	192.168.2.3	49824	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:42 UTC	703	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf6.AWU-LDxiFUU
2021-09-16 04:28:42 UTC	703	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: lpr/xJqgZKMjOsQiRq9ULCZwHnflor21h8u8TkvjzIN8is946tTOHYSOxJN4iVR5glQdnCmoO9K +nPS6eTQ== Date: Thu, 16 Sep 2021 04:28:42 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:42 UTC	704	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6c 35 6f 44 4e 56 33 69 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="!5oDNV3i!">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:42 UTC	705	IN	Data Raw: 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6c 35 6f 44 4e 56 33 69 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 2d 4d 4b 47 69 6a Data Ascii: w.document.write("<u003Cstyle nonce="!5oDNV3i!">body * {display:none !important;}<u003Cvstyle>u003Ca href="#" onclick="!\"top.location.href=window.location.href!\" style="!\"display:block !important;padding:10px!\">Gehe zu facebook.com/u003Cv/a>");/*-MKGij

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.3	49825	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:43 UTC	705	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf6.AWU-LDxiFUU

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:33 UTC	563	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfx.AWUBy_mcJKM
2021-09-16 04:28:34 UTC	564	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 4z/MpNi86fbZ96sq8EuP/hzSmeEAuZzgIM60nN0k2PktBWckzthQUEw8TUC8xxUfAGNiZAxstW2Cj4K6k/KKA== Date: Thu, 16 Sep 2021 04:28:34 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:34 UTC	564	IN	Data Raw: 36 66 62 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 34 68 4f 58 31 45 78 65 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 6fb<html><head><title>Redirecting...</title><script type="text/javascript" nonce="4hOX1Exe">*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=2
2021-09-16 04:28:34 UTC	565	IN	Data Raw: 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 34 68 4f 58 31 45 78 65 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 38 48 75 66 4f 52 54 4a 2a 2f 7d 7d 7d 28 29 Data Ascii: t.write("\u003Cstyle nonce="\u003Cstyle>\u003Cbody * {display:none !important;} \u003Cstyle>\u003Ca href="\u003Cstyle>\u003C/a>");/*8HufORTJ*/}}()

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.3	49827	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	710	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9ILqYs

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	711	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9IL31c; expires=Wed, 15-Dec-2021 04:28:43 GMT; Max-Age=7775999; path=/; domain=facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: uvDGT6JogjUbEaYmSUBvHbtdVG66Zrb91rKso973KLkildKjO5iEjglexxiOn4zAaNwxYXoaDWgUgu x7xzurJA== Date: Thu, 16 Sep 2021 04:28:44 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.3	49828	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	712	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9IL31c
2021-09-16 04:28:44 UTC	713	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: eWj9e434QgRHR/ng6a2aZHlwX4EnEVsHSg+ZN7HXXYcyDpCQJxSBV8qYs7VayeaK9oF17KW1SHRnTNZYnpPQaw== Date: Thu, 16 Sep 2021 04:28:44 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:44 UTC	713	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 74 51 67 55 33 59 32 75 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="tQgU3Y2u">/<![CDATA[/*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:44 UTC	714	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 74 51 67 55 33 59 32 75 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 7f 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 75 54 6e 7a 6e 78 79 34 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("����Cstyle nonce=\tQgU3Y2u\>body * {display:none !important;}����Cstyle>����Ca href="#"#\" onclick=\\"top.location.href=window.location.href\>Gehe zu facebook.com����C/va>");/*uTznxy4*/}})}/*...

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	192.168.2.3	49829	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	715	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsf8.wZ.AAA.0.0.BhQsf8.AWWQc9IL31c
2021-09-16 04:28:44 UTC	715	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsf8.wZ.AAA.0.0.BhQsf8.AWWQc9ILTil; expires=Wed, 15-Dec-2021 04:28:43 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: st4o1T3YdTrMdRajpziuTyzxamxvpZppXRkt6GuWkplMLw1zwir6IRc7JMVvn/EKNfqXqHZooxhyd VOi6skOQ== Date: Thu, 16 Sep 2021 04:28:44 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
73	192.168.2.3	49830	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	716	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsf8.wZ.AAA.0.0.BhQsf8.AWWQc9ILTil
2021-09-16 04:28:44 UTC	717	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: /BMMvYVpliY903kEDOf7jvy4VUmvkLdVN12P3Pt9/Cw7/9lpytB2zkR0wN0U4KauwwCIVuXZNdRFj a10AXA7A== Date: Thu, 16 Sep 2021 04:28:44 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:44 UTC	718	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 56 4d 55 59 71 65 34 4d 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 36 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="VMUYqe4M"/>*<![CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=6

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	719	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 56 4d 55 59 71 65 34 4d 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4b 64 65 67 4d 31 61 6f 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="VMUYqe4M">body * {display:none !important;}u003Cv/style>u003Ca href="#" ononclick="\"top.location.href=window.location.href\" style=\"display:block !important;padding:10px\">Gehe zu facebook.com u003C/a>");/*KdegM1ao*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
74	192.168.2.3	49831	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	719	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9ILTil
2021-09-16 04:28:44 UTC	720	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9ILPOk; expires=Wed, 15-Dec-2021 04:28:43 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: YBd8oDVQzByVJzSV6gJFL5b9y7ovQOqlePk3t8C/pELAlbGZNH8GhR890FyluOegRFSIExMRlrUxeJXz4YSDHw== Date: Thu, 16 Sep 2021 04:28:44 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	192.168.2.3	49832	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	721	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9ILPOk
2021-09-16 04:28:44 UTC	722	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: ngOdrXwwBzp4opRiCOTyS26P6hBe+vjNMxQa4GJ7UzDqcB9erh9exFwSuAwfv+4uaRsunkgP99mU4ATar4JUZW== Date: Thu, 16 Sep 2021 04:28:44 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	722	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4f 65 6f 6e 6b 55 71 51 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 37 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="OeonkUqQ">/*! DATA[*(function(){function si_cj(m){setTimeout(function(){new Image()).src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=7
2021-09-16 04:28:44 UTC	723	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4f 65 6f 6e 6b 55 71 51 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 45 30 30 62 54 58 36 4d 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="OeonkUqQ">body * {display:none !important;}}u003Cv>u003Ca href="#" onclick="\top.location.href=window.location.href" style="\display:block !important;padding:10px">Gehe zu facebook.com u003Cva>");/*E00bTX6M*/}}))/...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.3	49833	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:44 UTC	724	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf8.AWWQc9ILPOk
2021-09-16 04:28:45 UTC	725	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwrv; expires=Wed, 15-Dec-2021 04:28:44 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: H1bEwWTmsmaM+OmmiDOZa96MmD1majjgu7QVlKlq+pVbye31jUWo/QJegrepZs4rlapLK5lVtr9gL plfib+Ew== Date: Thu, 16 Sep 2021 04:28:45 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.3	49834	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	726	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwrv

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	726	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 8XKGYe9RKkDnkgvtDkKklgE4ppjcmjsdYU+6qX13zqmSEjJPJ8ar8e/vC0YPAZANoFE/BJxL95WgyrAOC58oA== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:45 UTC	727	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 49 57 50 68 6b 49 50 44 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 6f 72 6e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="IWPhkiPD"/>*<![CDATA[*]/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=4
2021-09-16 04:28:45 UTC	728	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 49 57 50 68 6b 49 50 44 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 41 35 6a 34 50 Data Ascii: ow.document.write("\u003Cstyle nonce="IWPhkiPD">body * {display:none !important;}\u003Cvstyle>\u003Ca href="\#\" onclick="\top.location.href=window.location.href\" style="\display:block !important;padding:10px\">Gehe zu facebook.com\u003C/a>");/*A5j4P

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	192.168.2.3	49835	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	729	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwrvvc
2021-09-16 04:28:45 UTC	729	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwqnm; expires=Wed, 15-Dec-2021 04:28:44 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: qfQGPQt0XsO1kDft9Wygcyw4PDml350lbpXhqlv1UOLCD7+ilJEOK1saMTxOKJIKLD9NPsDtA2qz7t742PLJw== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	192.168.2.3	49836	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	730	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwqnM
2021-09-16 04:28:45 UTC	731	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: WdmXz4EOVRGoRedGULtgEH3Pgo9PgDoTGyucbtOoGkG3AzoE/OW0grrh0Xco6M0xk/4AlztCRwwve mCF0A2UQ== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:45 UTC	732	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 78 79 36 4f 55 69 5a 47 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="xy6OUiZG">/*!CDATA*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:45 UTC	733	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 78 79 36 4f 55 69 5a 47 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 77 62 38 5f 5a Data Ascii: ow.document.write("lu003Cstyle nonce="xy6OUiZG">body * {display:none !important;}lu003C/style>lu003Ca href="#" onclick="top.location.href=window.location.href" style="display:block !important;padding:10px">Gehe zu facebook.comlu003C/a>);/*wb8_Z

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49765	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	566	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfx.AWUBy_mcJKM

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	567	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvHdw; expires=Wed, 15-Dec-2021 04:28:33 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: JtBJuNHyz3dvNmXte2Lz+s12z0XNZ12ST4Skqs9Fp3FvCLnUT3CRKe/kyXOusDBgla+NPABb8NCojuYBkikA== Date: Thu, 16 Sep 2021 04:28:34 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.3	49837	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	733	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwqnM
2021-09-16 04:28:45 UTC	734	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwnUA; expires=Wed, 15-Dec-2021 04:28:44 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: zhrKp4SusuyvGB/t5wwfqYjGCcqBOgGiS/cVa5zh0Xmypykbj+OSXnNMllaCHSbsFpL9DTRg2neF0pZ A/zxg/jw== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.3	49838	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	735	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqylSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwnUA

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	736	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: ycnSvritPYw4QGgN/p1PuN3p/AXtSGPMkGuU/MOfPvfoSWyWRrRud/74QkTy3PbBRMJJzmdvpf8QW01REbvpMQ== Date: Thu, 16 Sep 2021 04:28:45 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:45 UTC	736	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 51 6b 42 32 77 5a 36 44 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="QkB2wZ6D">/*<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:45 UTC	737	IN	Data Raw: 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 51 6b 42 32 77 5a 36 44 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 41 53 55 2d 61 4c 72 38 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a 2f Data Ascii: "u003Cstyle nonce="\QkB2wZ6D">body * {display:none !important;}\u003C/style>\u003Ca href="\#" onclick="\top.location.href=window.location.href" style="\display:block !important;padding:10px">Gehe zu facebook.com\u003C/a>");/*ASU-aLr8*/}}()/*...*/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	192.168.2.3	49840	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	738	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwnUA
2021-09-16 04:28:45 UTC	739	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwnu4; expires=Wed, 15-Dec-2021 04:28:44 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: MDsbKKKD0+RHEHG3eJmRL6e5OF5Fr0/LSpQhJl1yguoWAYSMVALgvC83duKbxlzBEDEsuHBXrlyvZUIf7nhdA== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	192.168.2.3	49839	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	740	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwNu4
2021-09-16 04:28:45 UTC	740	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: qazGmhAlGr/BHlwtcF2Dqh2IL/ODn3MmdNho36XaqDO25+oz3Ouel+IKv3esh5P8dy15NxAskXob HJYs+Tdg== Date: Thu, 16 Sep 2021 04:28:45 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:45 UTC	741	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 31 34 77 6d 56 6d 56 49 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="14wmVmVI">/*! [CDATA[*/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:45 UTC	742	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 31 34 77 6d 56 6d 56 49 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 4d 44 57 50 70 Data Ascii: ow.document.write("\u003Cstyle nonce="14wmVmVI">body * {display:none !important;}\u003Cstyle>\u003Ca href="#" onclick="\"top.location.href=window.location.href\" style="display:block !important;padding:10px!>Gehe zu facebook.com\u003C/a>");/*MDWPP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.3	49841	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:45 UTC	743	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDwNu4

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	743	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDw7_k; expires=Wed, 15-Dec-2021 04:28:44 GMT; Max-Age=7775999; path=/; domain=facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: aBMS52PEjZzwMaDkQpeZLENHG2iXg2QRry5kBta8zSREJsWqlogmXL0tOi20EvrxrPF9Y8F0rg3Jie/m7z6Lw== Date: Thu, 16 Sep 2021 04:28:45 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.3	49842	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	744	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDw7_k
2021-09-16 04:28:46 UTC	745	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: yxnqd5x4sgAQns9PYk+NumUI/VJvZMNMWx9nl+uQ4Vw5eJb0shGGbLPfesS1QadPDRFI7+hCMqVvDFDzlwQZyig== Date: Thu, 16 Sep 2021 04:28:46 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:46 UTC	746	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 61 32 6f 69 78 53 74 37 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 37 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="a2oixSt7">/*!CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=7
2021-09-16 04:28:46 UTC	746	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 61 32 6f 69 78 53 74 37 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 64 56 47 49 35 6f 32 35 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="a2oixSt7">body * {display:none !important;}u003Cvstyle>u003Ca href="#" onlick=\n"top.location.href=window.location.href" style="display:block !important;padding:10px!>Gehe zu facebook.com\u003C/va>");/*dVG15o25*/}}))/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	192.168.2.3	49843	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	747	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf9.AWUNrVDw7_k
2021-09-16 04:28:46 UTC	748	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-AWX9vYrEUEs; expires=Wed, 15-Dec-2021 04:28:45 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: UqeqpiElvz6em6M6rN5/z0P04L0cxuwMeDF8y6jk/P6Gs7XunC39CI/QC4eVuGnx+09+VAXt4JqqI2 O0ayhlTA== Date: Thu, 16 Sep 2021 04:28:46 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	192.168.2.3	49844	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	749	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-AWX9vYrEUEs
2021-09-16 04:28:46 UTC	750	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: wpaMsp45Zqn4oRjnPn0trU7cn3yJsKaPIJuLWKuQyxUPAKA0IljHq7njZUz7jWgQ+X0vsQHUGeou8vfhR0tucQ== Date: Thu, 16 Sep 2021 04:28:46 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:46 UTC	750	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 66 54 57 53 7a 6f 33 49 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 33 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="fTWSzo3l">/*!<CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://verror.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=3

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	751	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 66 54 57 53 7a 6f 33 49 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 68 46 4f 79 6c 50 47 78 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="fTWSzo3lI">body * {display:none !important;}\u003C/vstyle>\u003Ca href="\#a" onclick="\n"top.location.href=window.location.href\" style="display:block !important;padding:10px!>Gehe zu facebook.com\u003C/va>");/*hFOyIPGx*/}})}/*...*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
88	192.168.2.3	49846	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	752	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrEUEs
2021-09-16 04:28:46 UTC	753	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrE1zU; expires=Wed, 15-Dec-2021 04:28:45 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: AapM/OxMABD/v3y2ezmh8XFZuPv3FEQPdDgLijmc4fNfYGSPsBqELhEHTXdyNJ5xTGBuvNpyHmyJWw2uGtLZeA== Date: Thu, 16 Sep 2021 04:28:46 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
89	192.168.2.3	49845	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	754	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrE1zU
2021-09-16 04:28:46 UTC	754	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: xvjQW+wmyt+YkzLprq/MxWH6C+DcE80xKiSJ+2OY+ftVwtXRe8JEaf4p1yk2mLJCeB4xulxnHAhyqcsNHIQQ== Date: Thu, 16 Sep 2021 04:28:46 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	755	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 41 53 79 4f 61 78 6e 42 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 32 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ASyOaxnB"/>*<![CDATA[/fu nction(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/common/vscribe_endpoint. php?c=si_clickjacking&t=2
2021-09-16 04:28:46 UTC	756	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 41 53 79 4f 61 78 6e 42 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 52 4c 55 66 6f Data Ascii: ow.document.write("\u003Cstyle nonce="\u003Cstyle>\u003Cbody * {display:none !important;}\u003Cstyle>\u003Ca href="\u003Cstyle>\u003Cscript type="text/javascript" nonce="ASyOaxnB"/>*<![CDATA[/fu nction(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/common/vscribe_endpoint. php?c=si_clickjacking&t=2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49767	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:34 UTC	568	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MnVcqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsfy.AWVTDMBvHdw
2021-09-16 04:28:34 UTC	568	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: qFXDO5VOik/gPgwfng4IkOOLUXp/JpBFSXVmFNPV4j5FXvKzZ+ZGb50ZncrrCU8AQleqICZnOLRZL6IDUKkKQ== Date: Thu, 16 Sep 2021 04:28:34 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:34 UTC	569	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 69 68 43 6e 47 44 39 32 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 39 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="ihCnGD92">/<![CDATA[*](function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=9
2021-09-16 04:28:34 UTC	570	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 69 68 43 6e 47 44 39 32 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 34 39 32 53 39 Data Ascii: ow.document.write("\u003Cstyle nonce="\u003Cstyle>\u003C/href="\u003C/a>")/*492S9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
90	192.168.2.3	49847	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	757	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf-.AWX9vYrE1zU
2021-09-16 04:28:46 UTC	757	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf-.AWX9vYrEkW8; expires=Wed, 15-Dec-2021 04:28:45 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: pj9LuPSRHZZ4EnvThENJWGB8MjEOiN5wMMtzfGrfAN/c5MqiFi5I/hLbgylPLL/bCcEhCTiIGSSeK BjRfnVYA== Date: Thu, 16 Sep 2021 04:28:46 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
91	192.168.2.3	49848	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	758	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf-.AWX9vYrEkW8
2021-09-16 04:28:46 UTC	759	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: kr4cS1jY3pS188eE025pq0ZE4OwlWFX3PNz77GW610TPY/PO/3JpR4TJpqowPAZQU8ztJyiP3sVMel Qj2qlQWw== Date: Thu, 16 Sep 2021 04:28:46 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:46 UTC	759	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 61 57 4b 6f 57 7a 55 52 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 36 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="aWkoWzUR">/*! [C DATA["/(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe _endpoint.php?c=si_clickjacking&t=6

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	760	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 61 57 4b 6f 57 7a 55 52 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 50 54 75 5a 6a Data Ascii: ow.document.write("\u003Cstyle nonce=\"aWkoWzUR\">body * {display:none !important;}\u003Cstyle>\u003Ca href=\"#\" onclick=\"\u003Ctop.location.href=window.location.href\" style=\"display:block !important;padding:10px\">Gehe zu facebook.com\u003C/a>\";/*PTuZj

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
92	192.168.2.3	49849	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	761	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrEkw8
2021-09-16 04:28:46 UTC	762	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrEAnw; expires=Wed, 15-Dec-2021 04:28:45 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: RLxx1ujplb8H9B/sDs0bQ3xpQ1iINNjQFpY0WU6cMpBNzC7ELmbzf9bVOQMvAbvEk2mF5hDW9CgZ+PonyYWQVw== Date: Thu, 16 Sep 2021 04:28:46 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
93	192.168.2.3	49850	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:46 UTC	763	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNvCqyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf-.AWX9vYrEAnw
2021-09-16 04:28:47 UTC	764	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: fasD/fU5Ysg3x3J2GUSaO3s5GdEq+9V9023m2s5s3NeJ1fn34aYPoLSDUKGdeaCHgadu+LVA82x6t+Ky7Wo8w== Date: Thu, 16 Sep 2021 04:28:47 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	764	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 70 38 44 59 58 4b 54 71 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 35 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="p8DYXKTq">/*! DATA[*/(function(){}function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=5
2021-09-16 04:28:47 UTC	765	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 70 38 44 59 58 4b 54 71 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 70 64 4f 67 39 Data Ascii: ow.document.write("\u003Cstyle nonce="\u003Cstyle>\u003Cbody * {display:none !important;}\u003Cstyle>\u003Cahref="\u003Cva>")/*pdOg9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
94	192.168.2.3	49851	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	766	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf..AWX9vYrEAnw
2021-09-16 04:28:47 UTC	767	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf..AWVfEUScGFA; expires=Wed, 15-Dec-2021 04:28:46 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: sRXsLf6Hi+ko4yPW64swwSXGw64aZsE/69/prz0n+HhBfBThGQUcTSw/UIBCzR/MiJdq03HIVgNuXbgVQ26kqA== Date: Thu, 16 Sep 2021 04:28:47 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
95	192.168.2.3	49852	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	768	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf_AWWfEUScGFA
2021-09-16 04:28:47 UTC	768	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: 6NrGgq84HqVLnngnnQbptso3kSN0YrQx0TYyq8D9LhFO2k4mmXXYDaYZKLozJUarlyNRgy2ZEnnUN0hHaLkw== Date: Thu, 16 Sep 2021 04:28:47 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:47 UTC	769	IN	Data Raw: 37 30 34 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 4d 38 30 38 37 6a 57 7a 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 31 Data Ascii: 704<html><head><title>Redirecting...</title><script type="text/javascript" nonce="M8087jWz">/*!CDATA[*/(function(){function si_cj(m){setTimeout(function(){(new Image()).src="https://verror.facebook.com/vcommonVscribe_endpoint.php?c=si_clickjacking&t=1
2021-09-16 04:28:47 UTC	770	IN	Data Raw: 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 4d 38 30 38 37 6a 57 7a 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 74 4b 4c 63 61 4c Data Ascii: w.document.write(""+u003Cstyle nonce=""M8087jWzl">body * {display:none !important;}u003Cvstyle>u003Ca href=""#"" onclick=""top.location.href=window.location.href"" style=""display:block !important;padding:10px!>Gehe zu facebook.com/u003Cv/a>");/*KLCaL

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
96	192.168.2.3	49853	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	771	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqYlSSeKJ7Dd..BhQsfx.wZ.AAA.0.0.BhQsf_AWWfEUScGFA

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	771	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcqylSseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf_.AWVfEUScAK0; expires=Wed, 15-Dec-2021 04:28:46 GMT; Max-Age=7775999; path=/; domain=facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: VrhJL4llmhROuk6Fa1mlOZaloULa6g+pJ/6CmsnFHhesv2CvD9eWp9IM1fdxpKK5QK65dbfo/72rzq uHOu9RiA== Date: Thu, 16 Sep 2021 04:28:47 GMT Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
97	192.168.2.3	49854	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	772	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcqylSseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf_.AWVfEUScAK0
2021-09-16 04:28:47 UTC	773	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: iOKcsA/BbB01GH1ID03fTYtpPPPCYv9tjKcxKhX532ZISKV8aTRdzVZcOL+TKRZ1N+sNhQ1AUm1gWYfHcWw== Date: Thu, 16 Sep 2021 04:28:47 GMT Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600, h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:47 UTC	773	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 6d 55 77 58 39 64 65 6e 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 38 Data Ascii: 705<html><head><title>Redirecting...</title><<script type="text/javascript" nonce="mUwX9den"/>/*!<[CDATA[*(function(){function si_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=si_clickjacking&t=8
2021-09-16 04:28:47 UTC	774	IN	Data Raw: 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 6d 55 77 58 39 64 65 6e 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 6e 61 74 69 6f 6e 2e 68 72 65 66 3d 7f 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 61 75 6e 4a 44 33 4a 4e 2a 2f 7d 7d 28 29 29 2f 2a 5d 5d 3e 2a Data Ascii: ("u003Cstyle nonce="mUwX9den">body * {display:none !important;}u003Cvstyle="u003Ca href="#" onclick="\"top.location.href=window.location.href\" style="display:block !important;padding:10px!>Gehe zu facebook.com u003Cv>");/*aunJD3JN*}}{}}/*...

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
98	192.168.2.3	49855	157.240.17.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	775	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Host: m.facebook.com Connection: Keep-Alive Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf__AWVfEUScAK0
2021-09-16 04:28:47 UTC	776	IN	HTTP/1.1 302 Found P3P: CP="Facebook has no P3P policy fb.me/p3p" Set-Cookie: fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf__AWVfEUScgKE; expires=Wed, 15-Dec-2021 04:28:46 GMT; Max-Age=7775999; path=/; domain=.facebook.com; secure; httponly Location: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr facebook-api-version: v2.3 x-fb-rlafr: 0 Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT X-Content-Type-Options: nosniff X-XSS-Protection: 0 Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload; includeSubDomains X-FB-Debug: DeLQc1o45ZH/+aZ/j9L1ZIVOTZT8h3ebf6Hx5kk7Rx1ko84YBV7W+pLMX3gJ1/fmO5jyw0of3tkict HvQU/n8g== Date: Thu, 16 Sep 2021 04:28:47 GMT Priority: u=3,i Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
99	192.168.2.3	49856	157.240.9.35	443	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	777	OUT	GET /sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Referer: https://www.facebook.com/sharer/sharer.php?u=https%3A%2F%2Fwww.bustle.com%2Fentertainment%2Fhailey-bieber-crying-tiktok-video-met-gala-selena-gomez-chant%3Futm_term%3Dshare&_rdr Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: www.facebook.com Cookie: datr=8cdCYaLR4mVj1FP4cixboqka; fr=18MNVcQyISseKJ7Dd..BhQsf.wZ.AAA.0.0.BhQsf__AWVfEUScgKE
2021-09-16 04:28:47 UTC	778	IN	HTTP/1.1 200 OK Vary: Accept-Encoding Pragma: no-cache Cache-Control: private, no-cache, no-store, must-revalidate Expires: Sat, 01 Jan 2000 00:00:00 GMT Content-Type: text/html; charset=utf-8 Strict-Transport-Security: max-age=15552000; preload X-FB-Debug: MXl65ADyabb2lR3JKeuVcUuV/khf4LpWe4Qam8lb+LiZHnpctlOIHX+QLwhxFlgVwIMNUoSibQss4d 2WqjFvQ== Date: Thu, 16 Sep 2021 04:28:47 GMT Priority: u=3,i Transfer-Encoding: chunked Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600,h3-27=":443"; ma=3600 Connection: close
2021-09-16 04:28:47 UTC	778	IN	Data Raw: 37 30 35 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 52 65 64 69 72 65 63 74 69 6e 67 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6e 6f 6e 63 65 3d 22 52 75 42 34 37 67 34 73 22 3e 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 73 69 5f 63 6a 28 6d 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 6e 65 77 20 49 6d 61 67 65 28 29 2e 73 72 63 3d 22 68 74 74 70 73 3a 5c 2f 5c 2f 65 72 72 6f 72 2e 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 2f 63 6f 6d 6d 6f 6e 5c 2f 73 63 72 69 62 65 5f 65 6e 64 70 6f 69 6e 74 2e 70 68 70 3f 63 3d 73 69 5f 63 6c 69 63 6b 6a 61 63 6b 69 6e 67 26 74 3d 34 Data Ascii: 705<html><head><title>Redirecting...</title><script type="text/javascript" nonce="RuB47g4s">*<![CDATA[*(function(){function s_i_cj(m){setTimeout(function(){new Image().src="https://error.facebook.com/vcommon/vscribe_endpoint.php?c=s_i_clickjacking&t=4

Timestamp	kBytes transferred	Direction	Data
2021-09-16 04:28:47 UTC	779	IN	Data Raw: 6f 77 2e 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 22 5c 75 30 30 33 43 73 74 79 6c 65 20 6e 6f 6e 63 65 3d 5c 22 52 75 42 34 37 67 34 73 5c 22 3e 62 6f 64 79 20 2a 20 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 7d 5c 75 30 30 33 43 5c 2f 73 74 79 6c 65 3e 5c 75 30 30 33 43 61 20 68 72 65 66 3d 5c 22 23 5c 22 20 6f 6e 63 6c 69 63 6b 3d 5c 22 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 3d 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 5c 22 20 73 74 79 6c 65 3d 5c 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 20 21 69 6d 70 6f 72 74 61 6e 74 3b 70 61 64 64 69 6e 67 3a 31 30 70 78 5c 22 3e 47 65 68 65 20 7a 75 20 66 61 63 65 62 6f 6f 6b 2e 63 6f 6d 5c 75 30 30 33 43 5c 2f 61 3e 22 29 3b 2f 2a 67 58 5f 39 44 Data Ascii: ow.document.write("\u003Cstyle nonce=\"RuB47g4s\">body * {display:none !important;} \u003C\style>\u003Ca href=\"#\" onclick=\"\u003Ctop.location.href=window.location.href\" style=\"display:block !important;padding:10px\">Gehe zu facebook.com\u003C\va>\";/*gX_9D

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5672 Parent PID: 792

General

Start time:	06:27:53
Start date:	16/09/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff771390000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 1744 Parent PID: 5672

General

Start time:	06:27:53
Start date:	16/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\Internet Explorer\EXPLORE.EXE' SCODEF:5672 CREDAT:17410 /prefetch:2
Imagebase:	0x1360000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

[File Activities](#)

Show Windows behavior

[Registry Activities](#)

Show Windows behavior

Disassembly