

JoeSandbox Cloud BASIC



ID: 532946

Sample Name:

PaymentReceipt.html

Cookbook:

defaultwindowhtmlcookbook.jbs

Time: 21:21:22

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report PaymentReceipt.html	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Initial Sample	3
Sigma Overview	3
Jbx Signature Overview	4
Phishing:	4
System Summary:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	7
URLs	7
Domains and IPs	7
Contacted Domains	7
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
Private	9
General Information	9
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	11
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	13
Static File Info	41
General	41
Network Behavior	41
Network Port Distribution	42
TCP Packets	42
UDP Packets	42
DNS Queries	42
DNS Answers	42
HTTP Request Dependency Graph	43
HTTPS Proxied Packets	43
Code Manipulations	128
Statistics	128
Behavior	128
System Behavior	128
Analysis Process: chrome.exe PID: 6464 Parent PID: 980	128
General	128
File Activities	128
Registry Activities	128
Key Value Modified	128
Analysis Process: chrome.exe PID: 6636 Parent PID: 6464	128
General	128
File Activities	129
Disassembly	129
Code Analysis	129

Windows Analysis Report PaymentReceipt.html

Overview

General Information

Sample Name:

PaymentReceipt.html

Analysis ID:

532946

MD5:

7f46a4fc70dab89..

SHA1:

9132215cc4c7f24..

SHA256:

d657257086a46a..

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Yara detected HtmlPhish10

Yara detected HtmlPhish44

Yara detected obfuscated html page

HTML document with suspicious title

HTML document with suspicious nam...

Found iframes

None HTTPS page querying sensitiv...

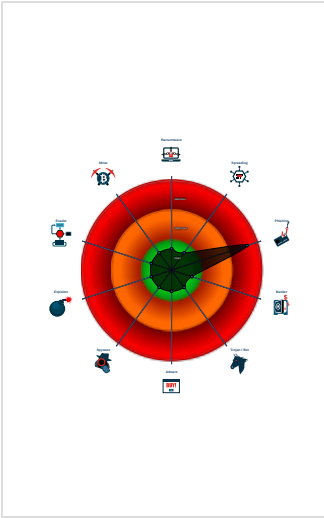
No HTML title found

JA3 SSL client fingerprint seen in co...

HTML body contains low number of ...

IP address seen in connection with o...

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 6464 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\PaymentReceipt.html" MD5: C139654B5C1438A95B321BB01AD63EF6)
 - chrome.exe (PID: 6636 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,6213295624667690040,7919256905441255605,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
PaymentReceipt.html	JoeSecurity_Obshtml	Yara detected obfuscated html page	Joe Security	
PaymentReceipt.html	JoeSecurity_HtmlPhish_44	Yara detected HtmlPhish_44	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

Phishing:



- Yara detected HtmlPhish10
- Yara detected HtmlPhish44
- Yara detected obfuscated html page

System Summary:

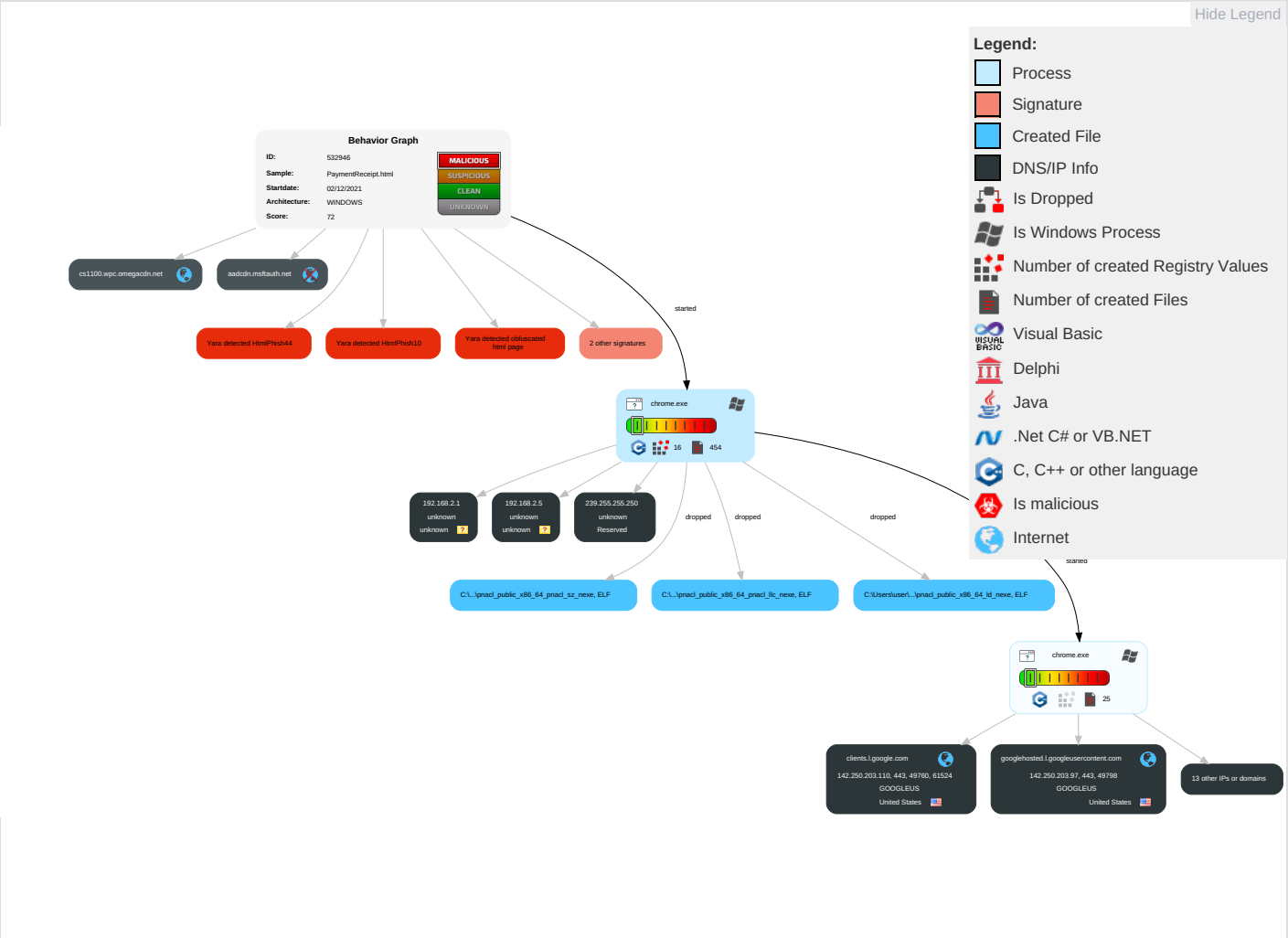


- HTML document with suspicious title
- HTML document with suspicious name

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
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
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 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
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 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
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	

Behavior Graph

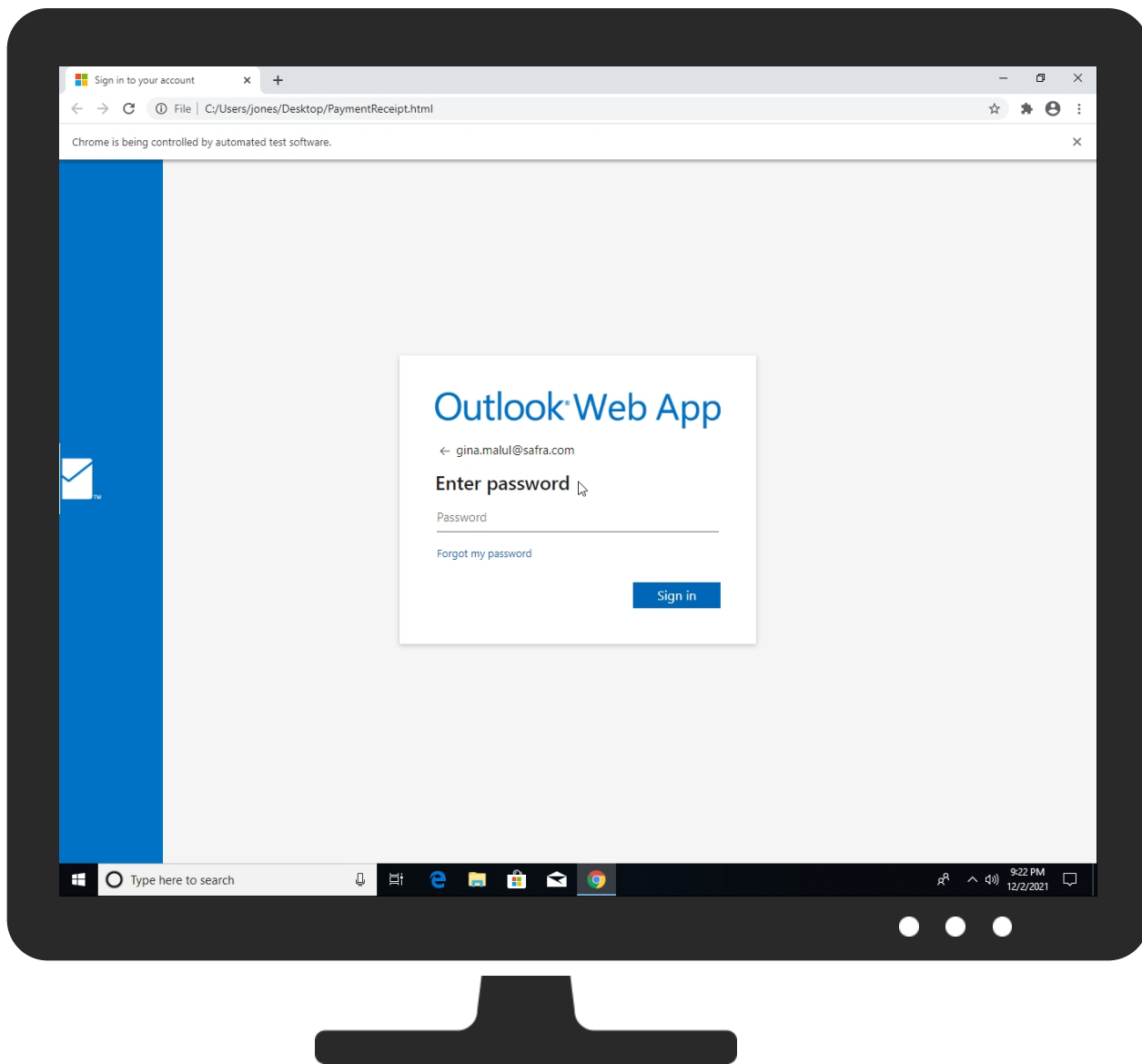


Screenshots

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
PaymentReceipt.html	4%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_id_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_pnacl_illc_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_pnacl_illc_nexe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\6464_913451637\platform_specific\x86_64\pnacl_public_x86_64_pnacl_sz_nexe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cs1100.wpc.omegacdn.net	0%	Virustotal		Browse
aadcdn.msftauth.net	0%	Virustotal		Browse
aadcdn.msauth.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_kfhrfyf-sm2tmkm5ficc	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f.jpg	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_ktc4wemsewhydsbdjhhsja2.jsz	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnq3xbrj5zv5ionvww2.css	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.sv	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/hosted-libraries-pushers	0%	URL Reputation	safe	
http://https://dns.google	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b	0%	Avira URL Cloud	safe	
http://https://www.google.com ;	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.sv	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/hosted-libraries-pushers	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_ktc4wemsewhydsbdjhhsja2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnq3xbrj5zv5ionvww	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_kfhrfyf-sm2tmkm5ficcw2.css	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/hosted-libraries-pushersCross-Origin-Resource-Policy :	0%	URL Reputation	safe	
http://https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js	0%	Avira URL Cloud	safe	
http://https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cs1100.wpc.omegacdn.net	152.199.23.37	true	false	0%, Virustotal, Browse	unknown
accounts.google.com	172.217.168.45	true	false		high
cdnjs.cloudflare.com	104.16.19.94	true	false		high
maxcdn.bootstrapcdn.com	104.18.10.207	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
aadcdn.msftauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
login.microsoftonline.com	unknown	unknown	false		high
aadcdn.msauth.net	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
https://login.microsoftonline.com/logout.srf?ct=1548343592&rver=64.4.6456.0&lc=1033&id=501392	false		high
file:///C:/Users/user/Desktop/PaymentReceipt.html	true		low
https://aadcdn.msftauth.net/shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png	false	• Avira URL Cloud: safe	unknown
https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js	false		high
https://clients2.googleusercontent.com/crx/blobs/Acy1k0bLljHsvnKaKN_oRpVaYYvFs25d7GKYF1WXrT6yizCMksBO0c_ggE0B6tx6HPRHe6q1GOEe3_NclbSiGG8kXeLMUY0sAKVvC6R89zvKM13s5VqoAMZSmuUgjQL5vlygJuArQghXXE_qTL7NIQ/extension_8520_615_0_5.crx	false		high
https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2_7916a894ebde7d29c2cc29b267f1299f.jpg	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_lgjnfg3xbrj5zv5ionvww2.css	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/shared/1.0/content/images/favicon_a_eupayfgghqiai7k9sol6lg2.ico	false	• URL Reputation: safe	unknown
https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
https://aadcdn.msftauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/ests/2.1/content/images/microsoft_logo.png	false	• Avira URL Cloud: safe	unknown
https://clients2.google.com/service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmhkhkcgccagldldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkddefgdpdelbpcmbmeomcjbemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/aad.login.min_ktc4wemsewhydsbdjhhsja2.js	false	• Avira URL Cloud: safe	unknown
https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.0/umd/popper.min.js	false		high
https://aadcdn.msftauth.net/shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/converged.v2.login.min_kfhrfyf-sm2tmkm5ficcw2.css	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnv2.js	false	• Avira URL Cloud: safe	unknown
https://aadcdn.msftauth.net/shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.18.10.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.110	clients.l.google.com	United States		15169	GOOGLEUS	false
172.217.168.45	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.203.97	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.23.37	cs1100.wpc.omegacdn.net	United States		15133	EDGECASTUS	false
104.16.19.94	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1
192.168.2.5
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532946
Start date:	02.12.2021
Start time:	21:21:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PaymentReceipt.html
Cookbook file name:	defaultwindowshtmlcookbook.jbs
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:	18
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 • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.winHTML@36/274@10/10
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .html
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.18.10.207	_0.html	Get hash	malicious	Browse	
	wXvjhk5m3v.html	Get hash	malicious	Browse	
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	
	VM845.html	Get hash	malicious	Browse	
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	
	ATT14851.html	Get hash	malicious	Browse	
	DHL Receipt.html	Get hash	malicious	Browse	
	ATT29220.html	Get hash	malicious	Browse	
	Updated Proposal and Statements.docx	Get hash	malicious	Browse	
	ATT17593.html	Get hash	malicious	Browse	
	ATT91376.html	Get hash	malicious	Browse	
	Statement.html	Get hash	malicious	Browse	
	50837%%fax838393839379he8883838298272738383.htm	Get hash	malicious	Browse	
	WMHighfield.html	Get hash	malicious	Browse	
	Employee payment plan.HTM	Get hash	malicious	Browse	
	V-M RTAmpcapital5EG1-TGQ02F-IOC8.htm	Get hash	malicious	Browse	
	File211124.html	Get hash	malicious	Browse	
239.255.255.250	ATT01313.html	Get hash	malicious	Browse	
	IM-87678A-1A1.msi	Get hash	malicious	Browse	
	IM-87678A-1A1.msi	Get hash	malicious	Browse	
	PaymentReceiptPDF.html	Get hash	malicious	Browse	
	fel.com.html	Get hash	malicious	Browse	
	_0.html	Get hash	malicious	Browse	
	wXvjhk5m3v.html	Get hash	malicious	Browse	
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	
	leco.com-FAX-59087-pdf.htm	Get hash	malicious	Browse	
	EmployeeAssessment.html	Get hash	malicious	Browse	
	(MT-103-USD)___717.htm	Get hash	malicious	Browse	
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	LockBit_Ransomware.hta	Get hash	malicious	Browse	
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	
	'Vm Note'jessica.mancel On Wed, 01 Dec 2021 210259 +0100.html	Get hash	malicious	Browse	
	'Vm Note'username On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdnjs.cloudflare.com	PaymentReceiptPDF.html	Get hash	malicious	Browse	104.16.19.94
	_0.html	Get hash	malicious	Browse	104.16.19.94
	wXvjhk5m3v.html	Get hash	malicious	Browse	104.16.18.94
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	104.16.19.94
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	104.16.18.94
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	104.16.18.94
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	104.16.18.94
	'Vm Note'username On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	104.16.19.94
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	104.16.19.94
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	104.16.18.94
	ATT01159.html	Get hash	malicious	Browse	104.16.18.94
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	104.16.19.94
	ATT14851.html	Get hash	malicious	Browse	104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	WMHighfield.html	Get hash	malicious	Browse	• 104.16.18.94
	Gracehealthmi.org7X9YCEB6AI.htm	Get hash	malicious	Browse	• 104.16.18.94
	DHL Receipt.html	Get hash	malicious	Browse	• 104.16.19.94
	phish.htm	Get hash	malicious	Browse	• 104.16.19.94
	html.html	Get hash	malicious	Browse	• 104.16.18.94
	ATT03144.htm	Get hash	malicious	Browse	• 104.16.19.94
	#Ud83d#Udce9-susan.hinds6459831.htm	Get hash	malicious	Browse	• 104.16.18.94
cs1100.wpc.omegacdn.net	_0.html	Get hash	malicious	Browse	• 152.199.23.37
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 152.199.23.37
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 152.199.23.37
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	ATT14851.html	Get hash	malicious	Browse	• 152.199.23.37
	html.html	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#Udce9-susan.hinds6459831.htm	Get hash	malicious	Browse	• 152.199.23.37
	Download_Statement_(0 seconds).htm	Get hash	malicious	Browse	• 152.199.23.37
	Download_Statement_.htm	Get hash	malicious	Browse	• 152.199.23.37
	Statement.html	Get hash	malicious	Browse	• 152.199.23.37
	Fax059-j.metternich-SwiftMT109-INV.html	Get hash	malicious	Browse	• 152.199.23.37
	Fax059-j.metternich-SwiftMT109-INV.html	Get hash	malicious	Browse	• 152.199.23.37
	Statement.html	Get hash	malicious	Browse	• 152.199.23.37
	Michal November 23, 2021.html	Get hash	malicious	Browse	• 152.199.23.37
	V-M RTAmpcapital5EG1-TGQO2F-IOC8.htm	Get hash	malicious	Browse	• 152.199.23.37
	Omegabuilders-FAX84216.html	Get hash	malicious	Browse	• 152.199.23.37
	#U266b_789_89676.htm	Get hash	malicious	Browse	• 152.199.23.37
	Brewin PAYMENT copy.html	Get hash	malicious	Browse	• 152.199.23.37
	Clti.xlsx	Get hash	malicious	Browse	• 152.199.23.37
	Vernon.xlsx	Get hash	malicious	Browse	• 152.199.23.37

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EDGECASTUS	ATT01313.html	Get hash	malicious	Browse	• 152.199.23.37
	_0.html	Get hash	malicious	Browse	• 152.199.23.37
	DHL_Original AWB Document.exe	Get hash	malicious	Browse	• 93.184.216.34
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	• 152.199.21.175
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 152.199.23.37
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	• 152.199.23.37
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 152.199.21.175
	DHL Express shipment notification.exe	Get hash	malicious	Browse	• 93.184.220.29
	mp3_Message_wav_###JBTDKV.HTM	Get hash	malicious	Browse	• 152.199.23.72
	ATT14851.html	Get hash	malicious	Browse	• 152.199.23.37
	WMHighfield.html	Get hash	malicious	Browse	• 152.199.21.175
	phish.htm	Get hash	malicious	Browse	• 152.199.21.175
	html.html	Get hash	malicious	Browse	• 152.199.23.37
	#Ud83d#Udce9-susan.hinds6459831.htm	Get hash	malicious	Browse	• 152.199.23.37
	phish.htm	Get hash	malicious	Browse	• 152.199.21.175
	ph.htm	Get hash	malicious	Browse	• 152.199.21.175
	forensic_challenge(1).html	Get hash	malicious	Browse	• 93.184.220.70
	Download_Statement_(0 seconds).htm	Get hash	malicious	Browse	• 152.199.23.37
	Download_Statement_.htm	Get hash	malicious	Browse	• 152.199.23.37
	Statement.html	Get hash	malicious	Browse	• 152.199.23.37
CLOUDFLARENETUS	ATT01313.html	Get hash	malicious	Browse	• 104.16.18.94
	1D4I9eROW4.exe	Get hash	malicious	Browse	• 23.227.38.74
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 104.26.6.139
	j6cSSIGZK8.dll	Get hash	malicious	Browse	• 104.26.6.139
	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 172.67.70.134
	QEuPmJ4IVYW4nj1.exe	Get hash	malicious	Browse	• 104.21.19.200
	200098765245699000000.exe	Get hash	malicious	Browse	• 104.21.19.200
	nakit.exe	Get hash	malicious	Browse	• 104.21.19.200
	S8TePU9taH.dll	Get hash	malicious	Browse	• 104.26.6.139
	Token Grabber.exe	Get hash	malicious	Browse	• 162.159.13 5.232
	PRO.exe	Get hash	malicious	Browse	• 162.159.13 0.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ-18072 QPHN .doc	Get hash	malicious	Browse	162.159.13 4.233
	RFQ-CIF DT22.doc	Get hash	malicious	Browse	162.159.13 5.233
	RFQ00_3779028392.doc	Get hash	malicious	Browse	162.159.13 4.233
	aRo4FhRug5.dll	Get hash	malicious	Browse	104.26.2.70
	PaymentReceiptPDF.html	Get hash	malicious	Browse	104.16.19.94
	Milleniumbpc.xlsx	Get hash	malicious	Browse	23.227.38.74
	uATT8vAUK9.exe	Get hash	malicious	Browse	162.159.13 5.233
	1Y0xc70fbX.exe	Get hash	malicious	Browse	162.159.12 9.233
	Document.exe	Get hash	malicious	Browse	162.159.12 9.233

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	ATT01313.html	Get hash	malicious	Browse	152.199.23.37
	CTvjbMY3DK.dll	Get hash	malicious	Browse	152.199.23.37
	CTvjbMY3DK.dll	Get hash	malicious	Browse	152.199.23.37
	FT A75619637369.vbs	Get hash	malicious	Browse	152.199.23.37
	OSJIMxel05.exe	Get hash	malicious	Browse	152.199.23.37
	fel.com.html	Get hash	malicious	Browse	152.199.23.37
	S6RqSs1LsE.exe	Get hash	malicious	Browse	152.199.23.37
	4RXRHeZIG8.exe	Get hash	malicious	Browse	152.199.23.37
	kEwLLWnIG5.exe	Get hash	malicious	Browse	152.199.23.37
	kEwLLWnIG5.exe	Get hash	malicious	Browse	152.199.23.37
	SecuriteInfo.com.W32.AIDetect.malware2.32340.exe	Get hash	malicious	Browse	152.199.23.37
	mUYEdn5OC0.exe	Get hash	malicious	Browse	152.199.23.37
	new offers885111832.docx	Get hash	malicious	Browse	152.199.23.37
	_0.html	Get hash	malicious	Browse	152.199.23.37
	lifehacks_6582318243.docx	Get hash	malicious	Browse	152.199.23.37
	counter-1248368226.xls	Get hash	malicious	Browse	152.199.23.37
	counter-1248368226.xls	Get hash	malicious	Browse	152.199.23.37
	ukmxWblFcs.exe	Get hash	malicious	Browse	152.199.23.37
	Narudzba.0953635637.PDF.exe	Get hash	malicious	Browse	152.199.23.37
	Orden de compra.exe	Get hash	malicious	Browse	152.199.23.37

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\6464_913451637_platform_specific\86_64\nacl_public_x86_64_id_nexe	ATT01313.html	Get hash	malicious	Browse	
	IM-87678A-1A1.msi	Get hash	malicious	Browse	
	PaymentReceiptPDF.html	Get hash	malicious	Browse	
	fel.com.html	Get hash	malicious	Browse	
	_0.html	Get hash	malicious	Browse	
	wXvjhk5m3v.html	Get hash	malicious	Browse	
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	
	leco.com-FAX-59087-pdf.htm	Get hash	malicious	Browse	
	EmployeeAssessment.html	Get hash	malicious	Browse	
	(MT-103-USD)___717.htm	Get hash	malicious	Browse	
	#U0420R#U04223445FM.htm	Get hash	malicious	Browse	
	SMK_EFT_BILLPAY.html	Get hash	malicious	Browse	
	LockBit_Ransomware.hta	Get hash	malicious	Browse	
	GlobalfoundriesINV33-45776648.htm	Get hash	malicious	Browse	
	'Vm Note'jessica.mancel On Wed, 01 Dec 2021 210259 +0100.html	Get hash	malicious	Browse	
	'Vm Note'username On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	
	'Vm Note'steven_spangle On Wed, 01 Dec 2021 194608 +0100.html	Get hash	malicious	Browse	
	ATT01159.html	Get hash	malicious	Browse	
	mp3_Message_wav_###JBTDKV.HTM	Get hash	malicious	Browse	
	'Vm Note'info On Wed, 01 Dec 2021 152453 +0100.html	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Google\Chrome\User Data\361f5925-d805-4496-9db2-2160427f22e7.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	197438
Entropy (8bit):	6.074748537402838
Encrypted:	false
SSDEEP:	3072:yVZLbGk/IQPEv31IFxUI7Raebo7N9QhAyZQa5sFcbXaflB0u1GOJmA3iuRw:EZ5xe1jxhfmP3yl6aqfllUOoSiuRw
MD5:	28928D3D07F4A2DF1C0F9326DC48EB19
SHA1:	D5A2C69C01B6B9122063E1699DDFC24F3BC37EAA
SHA-256:	1EACE47D46798998E418A3FA452DAA5C3ECBCEA6A08B263938F8BC5C6161F6C5
SHA-512:	A813983E1E14D174AEE34B16C46CE98940FFD9BFCF7B6E6EBB7BC43CD12964D5524563D04AEA4F5520F0B61642C0351017BFA5160585622C091769399BFA35C
Malicious:	false
Reputation:	low
Preview:	{ "browser": { "last_redirect_origin": "", "shortcut_migration_version": "85.0.4183.121", "data_use_measurement": { "data_used": { "services": { "background": {}, "foreground": {} }, "use_r": { "background": {}, "foreground": {} }, "hardware_acceleration_mode_previous": true, "intl": { "app_locale": "en-GB", "legacy": { "profile": { "name": "migrated": true } } }, "network_time": { "network_time_mapping": { "local": "1.638476541863451e+12", "network": "1.638476544e+12", "ticks": "313275688.0", "uncertainty": "4211939.0", "os_crypt": { "encrypted_key": "RFBbUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwloHYIQKZwuwW8V0yxAAAAAIAAAAAABBMAAAAAQAAIAAAAOt4j8Zm9U1zXX6oEUpPqIYBjSIOiLGeiMKiIFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbuFgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSPRzVqkBo+yVH56WF9zMt0AAAAAYRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi", "password_manager": { "os_password_blank": true, "os_password_last_changed": "1324592715755118", "plugins": { "metadata": { "adobe-flash-player": { "d

C:\Users\user\AppData\Local\Google\Chrome\User Data\47abf5af-5e4d-44a3-9b7e-fbbb2235a5a0.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7488835214242124
Encrypted:	false
SSDEEP:	384:9DYX/FaotGp1VmsbqNTrovv3Af54HhUGkDrOJfHx45F9UruDmO5KVr/LYO5JXNX:pa61V6FggkebDdBkHruVK7VPBP
MD5:	A672026617B250543D52382F20D96B00
SHA1:	2D025BC6D6388E3BC686AC81CFC1BA17C0C0D744
SHA-256:	D5DB3648C93D68F1854DF98429B769E9F19CC92ED6892D67CEDB4CA99A1BD857
SHA-512:	00CA26A8F60758A42978719468EBB67DC6BDB4940555452C716066FD1504326FBFBE9743DC04D8031F6B88A9813C5409C69757539C79F1D9F2C2B579304E42E6
Malicious:	false
Reputation:	low
Preview:	.q.....*...C::\P.R.O.G.R.A.-~1\M.I.C.R.O.S.-~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L...P!...[]...%p.r.o.g.r.a.m.f.i.l.e.s.%\m.i.c.r.o.s.o.f.t..o.f.f.i.c.e.\o.f.f.i.c.e.1.6\.....g.r.o.o.v.e.e.x...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..2.0.1.6...*...M.i.c.r.o.s.o.f.t..O.n.e.D.r.i.v.e..f.o.r..B.u.s.i.n.e.s.s..E.x.t.e.n.s.i.o.n.s.....1.6...0...4.7.1.1...1.0.0.0....*...C::\P.R.O.G.R.A.-~1\M.I.C.R.O.S.-~1\O.f.f.i.c.e.1.6\G.R.O.O.V.E.E.X...D.L.L...M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n....L8.D...C::\P.r.o.g.r.a.m..F.i.l.e.s.\C.o.m.m.o.n..F.i.l.e.s.\M.i.c.r.o.s.o.f.t..S.h.a.r.e.d.\O.F.F.I.C.E.1.6\m.s.o.s.h.e.x.t...d.l.l.@....U/_...%c.o.m.m.o.n.p.r.o.g.r.a.m.f.i.l.e.s.%\m.i.c.r.o.s.o.f.t..s.h.a.r.e.d.\o.f.f.i.c.e.1.6\.....m.s.o.s.h.e.x.t...d.l.l.....M.i.c.r.o.s.o.f.t..O.f.f.i.c.e.)...M.i.c.r.o.s.o.f.t..O.f.f.i.c.e..S.h.e.l.l..E.x.t.e.n.s.i.o.n..H.a.n.d.l.e.r.s.....1.6...0...4.2.6.6...1.0.0.1.....D...C::\P.r.o.g.r.a.m.

C:\Users\user\AppData\Local\Google\Chrome\User Data\49689fa7-b0c6-4315-87fd-f6823261d0a6.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	189065
Entropy (8bit):	6.046276489219116
Encrypted:	false
SSDEEP:	3072:m/LbGk/IQPEv31IFxUI7Raebo7N9QhAyZQa5sFcbXaflB0u1GOJmA3iuRw:A5xe1jxhfmP3yl6aqfllUOoSiuRw
MD5:	4B4DCEd811BC6A013C14C5ECA3FC0FDE
SHA1:	C1F3807758EA131A83522BE6A25ECA6A8F4D3CAA
SHA-256:	396D50854313F1B91C8599ACAE9234DCEEAf029BD449516C759753CF1F9E55DF
SHA-512:	D72BA802382505E562882225432EBA9BAF83284C94046266F02EEF5F47CF8E7A64A8F22BBF521190C7B26B6DEC4A118B8999E68F1A9022FAEC7A575EB2055A1C
Malicious:	false
Reputation:	low
Preview:	{ "browser": { "last_redirect_origin": "", "shortcut_migration_version": "85.0.4183.121", "data_use_measurement": { "data_used": { "services": { "background": {}, "foreground": {} }, "use_r": { "background": {}, "foreground": {} }, "hardware_acceleration_mode_previous": true, "intl": { "app_locale": "en-GB", "legacy": { "profile": { "name": "migrated": true } } }, "network_time": { "network_time_mapping": { "local": "1.638476541863451e+12", "network": "1.638476544e+12", "ticks": "313275688.0", "uncertainty": "4211939.0", "os_crypt": { "encrypted_key": "RFBbUEkBAAA0lyd3wEV0RGMegDAT8KX6wEAAABaHlwloHYIQKZwuwW8V0yxAAAAAIAAAAAABBMAAAAAQAAIAAAAOt4j8Zm9U1zXX6oEUpPqIYBjSIOiLGeiMKiIFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbindD+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbuFgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSPRzVqkBo+yVH56WF9zMt0AAAAAYRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi", "password_manager": { "os_password_blank": true, "os_password_last_changed": "1324592715755118", "plugins": { "metadata": { "adobe-flash-player": { "d

C:\Users\user\AppData\Local\Google\Chrome\User Data\52f751b6-3a03-4dd0-ba94-997a2701cf00.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	188971
Entropy (8bit):	6.046010113610587
Encrypted:	false
SSDEEP:	3072:N3LbGk/IQPEv31fXUI7Raebo7N9QhAyZQa5sFcbXaflB0u1GOJmA3iuRw:J5xe1jxhfMp3yl6aqfllUOoSiuRw
MD5:	D17FC4AEA49C342EB5720CCE2C75C27B
SHA1:	0551F8C6204FFD35A3E7537E382794D3797CDA2B
SHA-256:	05F656E5CAF00AA81A47A7D9B1BC1946DE461008B36A7FF1F0E422BBBE47766C
SHA-512:	858CE0E2737FDD51EC8AC3DDB92AB9C233F64D6182252AFFC0DE44C3DC3176F00EF4A6CD876989886F1450EFEDE8C19914E434FD82ED21296B4B215C2388F37
Malicious:	false
Reputation:	low
Preview:	<pre>{"browser":{"last_redirect_origin":"","shortcut_migration_version":"","85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{},"use_r":{"background":{},"foreground":{}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"","en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638476541863451e+12,"network":1.638476544e+12,"ticks":313275688.0,"uncertainty":4211939.0},"os_crypt":{"encrypted_key":"RFBbUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABaHlwloHYIQKZwuwW8V0yAAAAAIAAAAAABBMAAAAAQAAIAAAOT4j8Zm9U1zXX6oEUpPqlyBjSIOiLGeIMKilFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbind+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMT0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"","13245922715755118"},"plugins":{"metadata":{"adobe-flash-player":{"d</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\915b8712-e93c-4e3a-b022-d9ea50c7f458.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	189255
Entropy (8bit):	6.046725037709026
Encrypted:	false
SSDEEP:	3072:VA/LbGk/IQPEv31fXUI7Raebo7N9QhAyZQa5sFcbXaflB0u1GOJmA3iuRw:VC5xe1jxhfMp3yl6aqfllUOoSiuRw
MD5:	DCBC10AB28CAE4F224705BA919DEE3CF
SHA1:	7F24A6363738E57F8BAD428503AC9857EFDD2310
SHA-256:	FA1AF1A59B21F18162D670A87334BE19D835A01F3BEE36C5D15242AFB6BFE058D
SHA-512:	7CEE1108DE2B848F720F4BCA447B6E6B8ACF4C941BC86AAF3C609355013C75D755871335A253016770801A369037916FB0CE21F25820DA886C243007AD34E0F5
Malicious:	false
Reputation:	low
Preview:	<pre>{"browser":{"last_redirect_origin":"","shortcut_migration_version":"","85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{},"use_r":{"background":{},"foreground":{}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"","en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638476541863451e+12,"network":1.638476544e+12,"ticks":313275688.0,"uncertainty":4211939.0},"os_crypt":{"encrypted_key":"RFBbUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABaHlwloHYIQKZwuwW8V0yAAAAAIAAAAAABBMAAAAAQAAIAAAOT4j8Zm9U1zXX6oEUpPqlyBjSIOiLGeIMKilFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbind+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMT0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"","13245922715755118"},"plugins":{"metadata":{"adobe-flash-player":{"d</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\92caad5e-4e36-4f9a-9d8b-82fa278c6a12.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	189065
Entropy (8bit):	6.046276489219116
Encrypted:	false
SSDEEP:	3072:m/LbGk/IQPEv31fXUI7Raebo7N9QhAyZQa5sFcbXaflB0u1GOJmA3iuRw:A5xe1jxhfMp3yl6aqfllUOoSiuRw
MD5:	4B4DCEd811BC6A013C14C5ECA3FC0FDE
SHA1:	C1F3807758EA131A83522BE6A25ECA6A8F4D3CAA
SHA-256:	396D50854313F1B91C8599ACAE9234DCEEAf029BD449516C759753CF1F9E55DF
SHA-512:	D72BA802382505E562882225432EBA9BAF83284C94046266F02EEF5F47CF8E7A64A8F22BBF521190C7B26B6DEC4A118B8999E68F1A9022FAEC7A575EB2055A1C
Malicious:	false
Reputation:	low
Preview:	<pre>{"browser":{"last_redirect_origin":"","shortcut_migration_version":"","85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{},"use_r":{"background":{},"foreground":{}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"","en-GB"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638476541863451e+12,"network":1.638476544e+12,"ticks":313275688.0,"uncertainty":4211939.0},"os_crypt":{"encrypted_key":"RFBbUEkBAAAA0lyd3wEV0RGMEgDAT8KX6wEAAABaHlwloHYIQKZwuwW8V0yAAAAAIAAAAAABBMAAAAAQAAIAAAOT4j8Zm9U1zXX6oEUpPqlyBjSIOiLGeIMKilFJZDroAAAAA6AAAAAgAAIAAAAFW1OavBhyV7qwszPZbind+KU2Osh5O7HSmDPpFnuCDMAAAAGEkmqbufgFUSmOzx4cW7Aup7spqps4DvqbPrwRgUGqSpRZvQkbO+yVH56WF9zMT0AAAAAyRwtYxjf7/AqYrFr0JZ6kbTiUt0/2PKkCw7ntLtbN2qrad7I3MeL4iNGDFgqRlhWgsb/6w0gJzQxAfL6rdzxi"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"","13245922715755118"},"plugins":{"metadata":{"adobe-flash-player":{"d</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXwgs0oRLn:+taRLn
MD5:	7AE9008C2AA5ED3E5ED52743E082F5BF
SHA1:	CD90099842F51474494BFC490433578A89C1B539
SHA-256:	94E7D9BF431A0E3F0FD02F0FBA7321F43DD8B523E3D32092AFC474D3FD5ABF62
SHA-512:	596E66D10186ADAD552F4CF7E74CD438AD19AF4C30950D2D6EB80E9F9430CA475D12BB79423EC8D15EAF37ABE0AD1DCCAE459C356A00055A82155C24A35C614
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	sdPC.....UO..E.D.Q.o....

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default	34179be7-304b-4382-aed3-67d725d118d0.tmp
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.5778035011573985
Encrypted:	false
SSDEEP:	384:7Hq/Xto7LIAcpNX3N1kXqKf/pUZNCgVLH2HfD/lrU+9n5O4V:/LIL91kXqKf/pUZNCgVLH2HfhrUW5Om
MD5:	7545AEC72F372A01D4490E2B553DD0E
SHA1:	F9521720A5499012CA8A8E83E0EBFB5CE6D629A
SHA-256:	1D841675A784212441F6F4C095BC02CA827C279FB179B7A6D0A1B9A57483D646
SHA-512:	D98090CAE5E91C613D44244700CA42431D40E6BBDB793DCFCCEED2923D8C5096DB16FF3EA618BD4780ADBFA3AF1C0208C7472279751A572F11EE19991C061C4C6
Malicious:	false
Reputation:	low
Preview:	{ "extensions": { }, "settings": { "ahfgeienlihckogmhjhadlkjgocpleb": { "active_permissions": { "api": ["management", "system.display", "system.storage", "webstorePrivate", "system.cpu", "system.memory", "system.network"], "manifest_permissions": [] }, "app_launcher_ordinal": "t", "commands": { }, "content_settings": [], "creation_flags": 1, "events": [], "from_bookmark": false, "from_webstore": false, "incognito_content_settings": [], "incognito_preferences": { }, "install_time": "13282950139620142", "location": 5, "manifest": { "app": { "launch": { "web_url": "https://chrome.google.com/webstore/" }, "urls": ["https://chrome.google.com/webstore/"], "description": "Discover great apps, games, extensions and themes for Google Chrome." }, "icons": { "128": "webstore_icon_128.png", "16": "webstore_icon_16.png" }, "key": "MIGfMA0GCsqGSIb3DQEBAQUAA4GNADCBiQKBgcQtI3rtOosjuZRsfxdtD2SKxPITfuoy7AWoObysitBPvH5FE1NaAA1/2JkPWkVDhdLBWLalBPYeXbzlHp3y4Vw/4XG+aNsEqFE3z+1RU/NqkzVYhtlpVScf3DjTYtkVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDP76wR6ijFzsYwQIDAQAB", "name": "Web Store ", "pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\39081f31-579f-472d-adb4-df1fc4b5136c.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5529
Entropy (8bit):	5.171651398660184
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6121b419-90ee-4b46-b976-a4b0cdbf995c.tmp	
SHA-256:	B9F7A197B34038C9AAA60DB61DE7656B7F9EEFFE83CD2B4E97610A72F5F123AC
SHA-512:	9F8396775893EA8E365F2DC211557E9C52B136F4DD9AE72C5D913B114599CA4A7D9C1376A8DD9AAF6AFBB0BA7C198FF3AAAA4048FA22D037101007D01FED32C0
Malicious:	false
Preview:	{ "extensions": {}, "settings": { "ahfgeienlihckogmhjhadlkgocpleb": { "active_permissions": { "api": ["management", "system.display", "system.storage", "webstorePrivate", "system.cpu", "system.memory", "system.network", "manifest_permissions": [], "app_launcher_ordinal": "t", "commands": {}, "content_settings": [], "creation_flags": 1, "events": [], "from_bookmark": false, "from_webstore": false, "incognito_content_settings": [], "incognito_preferences": {}, "install_time": "13282950139620142", "location": 5, "manifest": { "app": { "launch": { "web_url": "https://chrome.google.com/webstore/ ", "urls": ["https://chrome.google.com/webstore/ "], "description": "Discover great apps, games, extensions and themes for Google Chrome.", "icons": { "128": "webstore_icon_128.png", "16": "webstore_icon_16.png", "key": "MIGfMA0GCsQGSib3DQEBAQUAA4GNADCBiQKBgQCtI3tO0osjuzRsf6xtD2SKxPITfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLalBPYeXbzIHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB", "name": "Web Store", "pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\90f943bc-fbd8-4308-acf3-6a694c15b069.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	modified
Size (bytes):	1637
Entropy (8bit):	4.8333059816411845
Encrypted:	false
SSDEEP:	48:Y2nzM3qK6qDHGXctwWs3RLs4yKstoMHxYhbw:JnzMaKxDHGXCOJPHGehM
MD5:	747DBD27A8CF35595D66CB9C5EBCE936
SHA1:	7D8E90CA26F6095FF07E753EB8725E3FFCFD1F6B
SHA-256:	0123531977215458D22945D4A21F093659ACA4E5FFE6FC28674C4988BE814B29
SHA-512:	B918D592FF36C5D173A6E531A0321C702A95845D7F46C8104AFDFEBAF0A719A8DCE6B0CEC2DD7CF71849369BD1E7A98B699FF7D1AA9BDC07A6D286B0EF5A6EEC
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { "isolation": [], "server": "https://www.google.com", "supports_spdy": true, "isolation": [], "server": "https://dns.google", "supports_spdy": true, "isolation": [], "server": "https://www.googleapis.com", "supports_spdy": true, "isolation": [], "server": "https://redirector.gvt1.com", "supports_spdy": true, "isolation": [], "server": "https://fonts.googleapis.com", "supports_spdy": true, "isolation": [], "server": "https://ogs.google.com", "supports_spdy": true, "isolation": [], "server": "https://play.google.com", "supports_spdy": true, "isolation": [], "server": "https://apis.google.com", "supports_spdy": true, "isolation": [], "server": "https://fonts.gstatic.com", "supports_spdy": true, "isolation": [], "server": "https://ssl.gstatic.com", "supports_spdy": true, "isolation": [], "server": "https://www.gstatic.com", "supports_spdy": true, "alternative_service": { "advertised_versions": [50], "expiration": "13285542142319644", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.127200182248586
Encrypted:	false
SSDEEP:	6:mNXvDN+q2Pwkn23iKkKdK9RXXTZIFUtMXvNaZmwKXv/dNVkwOwkn23iKkKdK9RXX5d:iUvYf5Kk7XT2FutMk/KH95Jf5Kk7XVJ
MD5:	37CF6DE3C802D8FE8F32A66F40FDF1D5
SHA1:	0FDD64C4E0DB4561C76E4CBF5449B880C1F69D90
SHA-256:	DDCB2812CC9A0CA849A8D75BE5ADD44C3B29C33F8408ADCE63253D1FD342ED70
SHA-512:	85F4355553B3A13C991AC0DFC51F82B669DCB5B5DFDAA93A87695A8A771D97BCF885C5C06FF155DF08EE412233137DD1163A6C9C23D5A460719DA1C3CB4E0B4
Malicious:	false
Preview:	2021/12/02-21:22:29.881 1998 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/12/02-21:22:29.882 1998 Recovering log #3.2021/12/02-21:22:29.883 1998 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.oldNT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.127200182248586
Encrypted:	false
SSDEEP:	6:mNXvDN+q2Pwkn23iKkKdK9RXXTZIFUtMXvNaZmwKXv/dNVkwOwkn23iKkKdK9RXX5d:iUvYf5Kk7XT2FutMk/KH95Jf5Kk7XVJ
MD5:	37CF6DE3C802D8FE8F32A66F40FDF1D5
SHA1:	0FDD64C4E0DB4561C76E4CBF5449B880C1F69D90
SHA-256:	DDCB2812CC9A0CA849A8D75BE5ADD44C3B29C33F8408ADCE63253D1FD342ED70
SHA-512:	85F4355553B3A13C991AC0DFC51F82B669DCB5B5DFDAA93A87695A8A771D97BCF885C5C06FF155DF08EE412233137DD1163A6C9C23D5A460719DA1C3CB4E0B4
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.oldNT (copy)

Preview:	2021/12/02-21:22:29.881 1998 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/12/02-21:22:29.882 1998 Recovering log #3.2021/12/02-21:22:29.883 1998 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\000003.log .
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.159714474141012
Encrypted:	false
SSDEEP:	6:mNXvu+q2Pwkn23iKkDKyDZIFUtMXvwdXZmwKXvIF+NVkwOwkn23iKkDKyJLJ:iXvYf5Kk02FUtMI5/KHz5Jf5KkKwJ
MD5:	128B3D734C378BFED9C23CA41F9DB371
SHA1:	5A7EB20F04E78F345E84CA4D9EB09002CCE9546A
SHA-256:	FCD7159DF12449C9401AC8945C16F7F8BD48B1021D015070C4882E6E6091168E
SHA-512:	BDE13102B8B48ABE22EA77168B1DE25B628A312B6BB38115EE6C3F6D83933825E982839430B01EA766D895CF1624D776E71F73A2BF488FF9CFBDCEE8CE48052B
Malicious:	false
Preview:	2021/12/02-21:22:29.875 1998 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/12/02-21:22:29.877 1998 Recovering log #3.2021/12/02-21:22:29.878 1998 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG.old. (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.159714474141012
Encrypted:	false
SSDEEP:	6:mNXvu+q2Pwkn23iKkDKyDZIFUtMXvwdXZmwKXvIF+NVkwOwkn23iKkDKyJLJ:iXvYf5Kk02FUtMI5/KHz5Jf5KkKwJ
MD5:	128B3D734C378BFED9C23CA41F9DB371
SHA1:	5A7EB20F04E78F345E84CA4D9EB09002CCE9546A
SHA-256:	FCD7159DF12449C9401AC8945C16F7F8BD48B1021D015070C4882E6E6091168E
SHA-512:	BDE13102B8B48ABE22EA77168B1DE25B628A312B6BB38115EE6C3F6D83933825E982839430B01EA766D895CF1624D776E71F73A2BF488FF9CFBDCEE8CE48052B
Malicious:	false
Preview:	2021/12/02-21:22:29.875 1998 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/12/02-21:22:29.877 1998 Recovering log #3.2021/12/02-21:22:29.878 1998 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_0

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	45056
Entropy (8bit):	0.14146969160930184
Encrypted:	false
SSDEEP:	24:d0SXW8lcZMBkY2zn6fU1jRq06zN/PNmjWZtf:/vWCl2zgSRq06zN/PRtf/
MD5:	B975D9629C9056773A9AA09BD6AE74CD
SHA1:	5A31E5CECE892E64B70240F8A491E06D19B080FA
SHA-256:	3D82FA0A0A4E31C1C7FBFA14931D5B52A1F17F9EBA8461A19896A3AA7FED60C4
SHA-512:	F6D0BDFCD5C04914B59D6C7DA02861E74C39E5725D1AF76DEE11C41B543FC4DA55831566498736D86EF42313A92F48F57C4AF0E246AA14DFCBB1C20967019E5
Malicious:	false
Preview:	\$.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.22579843759768567
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_1	
SSDEEP:	96:gv31MqT7P3O7LgJci8z0F3YM9o63oaZ+1goNKlheE4RE22+/p:aDf3O7LId9RsGVf4R0+x
MD5:	E2C82FEEC2F3A2CCAF225396FD1FD683
SHA1:	48A1189A00574D462E257554B9759110C60928DA
SHA-256:	4D47BA7065B3B4BA75FEE05D3376853043E5842077EDF462BD82D836F34F8F6C
SHA-512:	A1E6DBE9F645D96311505CF396B82D38F64BAB4C3228E7213C7EA63E8B1FF9230506BAF6CFB537995DA62EE78F1701DDB5D123B1146F845FAFC22CEA58DB3F6
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_2	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1056768
Entropy (8bit):	0.7619366583824888
Encrypted:	false
SSDEEP:	1536:CyOU0+tF110m2OAO+OY0O6OG+OHIOxO8O:EE3usvJcFYo0r
MD5:	A29B876ED194951BFB48DFE0EF5558E1
SHA1:	BE2DD9CF297D9DC0FBB6B07E54ADEC8C092532D
SHA-256:	394466709B0B3A549C8CAE63DFD2F663967FD17BE6AB8FEB17403BC0DBF7443A7
SHA-512:	499CAB1012AC3D0D6CE23FF7EE42726439C9D73817AFB5DCB79370CCA2515E0C00C8313048D268C9EFEC5B0F33393A37C2AC92DAE01F658CC86E931E68A8957
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	4202496
Entropy (8bit):	0.025248344107966243
Encrypted:	false
SSDEEP:	96:E63r9xD3XmSEzQG8fRTasm8EskBsls8isQs5sMsrXFTfOsu4MsWsnqsOsqsC4:pb7EZqPRCFB4CJZbtME
MD5:	18C39579CE975B49FF31FA796F867A9F
SHA1:	A0557FB8FEDDB9F383CD24B96FC99DA072F9C282
SHA-256:	1EC456DCDBA40E5C944ECF12D207335FEF393397988F97DFB5F6244B96463508D
SHA-512:	CB3F9EAA706F196A41587E88F11CEB016F9C47B29D15AB110BEAD6C69D922AD22DAA70D43F629BDB5F4EB4892F4D84D50B9FCDEACDBEE626A749C4DE0691E93
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	2.2208508836702423
Encrypted:	false
SSDEEP:	96:dNw/bscbkGsGg8sb1qs4vzsOMsfNshinhsjsEzLsHSRishfKWAsHXm0ds8swzscQ:duUcgT1OX3p6/4N0Jxd
MD5:	16561581D6E6807D1302C81C11C1860D
SHA1:	64494DD73D9A84FA658EC85926E2AD08885BB506
SHA-256:	079D921AF7FE8F5714646D9D015CBB68044BC805A99E9498E65D537ECCA83E5A
SHA-512:	C84D758413D81EE022D1604B6EA090D3604F9AD180D8EF4E4D4EFEB1224E06F8205DE80ED0C22CBA36E4D79FED7B747F56D66AA11D33685A7AAB532702025B9
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.073250990329037
Encrypted:	false
SSDEEP:	6:mNXIQ+q2Pwkn2iIKKdK8NIFUtMXRdWZmwKX2ZQVkwOwkn23iKKdK8+eLJ:i4Q+vYf5KkpFUtMBdW/K4QV5Jf5KkqJ
MD5:	59F05A7AAA43B1FC6CB6A56F4609174A
SHA1:	79D3470AA85FA0F251D5CED16BAE927E26F8AE17
SHA-256:	391BBE6C8257F60AFB1E583695D34DF4A7DDEC44ED9EE72DDCA2836E4E95D201
SHA-512:	46C17DAD1B2F28945A142B11E4D199A02BF94480F1E4CF5D678478DC3332E7EAAC993FCF58BD293DD40285604D15E9CBAEB61A66EEE2E13B99E12233C0AE7D0
Malicious:	false
Preview:	2021/12/02-21:22:22.038 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\MANIFEST-000001.2021/12/02-21:22:22.040 19cc Recovering log #3.2021/12/02-21:22:22.041 19cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\lnmmhkkeggccagldldgiimedpiccmgmieda1.0.0.6_0\metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJniTWGb7V9Hne4qasKxXltmLG48gcLg/Pkl:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Preview:	{ "file_hashes": [{ "block_hashes": ["A+1PYW3V6CJbBuQ7aqrqYhyH3bT8PKyBxp3hN2slpI0=", "WSOpQRkYTHjPSIG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=", "jDctR8lmG5KZrQKmn4KdJUB7FokSJfjo/pmvFowRVlaY=", "LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=", "nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjjiCPdtHE=", "wifibc1QfMBN2jrtUtLgsCefuuceTpAatmLvul11RJA=", "dHjWISlIdj7MWqg3T8MG58RuugRXk32vqi/13JqEgA=", "zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFLADaEeTI=", "DpjXcO85FFFY9KJFPkGNfUtdQIOsGwO5jUckiUwY14=", "gqid6l1+mk/6yWgUECRofl9IMipXgXh2jEN2+CxmPE0=", "prDB91X2Mmfg/MtxVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zfKEt3Cn2j0q2v9QOSThVFWn8EzCM=", "EPQ3jzdrLkAHyvf3920B5Y3aAkO1Ijdn/UtbAmq6T0=", "+oOc6ca+ChKUptu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=", "3mBGNAiRITANEQkzU3TEi+5wJ0ubR5uwtS4/9OOM7=", "1A9NNawxuhu95H5eThv1rewJ4QQWhhPNxJXO1C/n68=", "E3vWLQxzmj+e5QxYbUscIIJ5n0lTpW5JBHV1Kph3/KM=", "i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=", "R8B8qYabnMSILPhrtu0hGYrHn3llsMHqBbi70gkljEE=", "rhIzuEvv2KRAFmms896xFwkNgPrw6WvmgPn6xrBSa2Y=", "LAMXv6sRb0VzY34aVXF3Ftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1\metadata\computed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6lcafusK4H1IIGRIhKikIALQWdynQh2RX4K6M1tVztzr7XSNyZH:7dOscSRKc1nGRSkhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Preview:	{ "file_hashes": [{ "block_hashes": ["DOZdV3jFvk12AM2JNDYKo3KZrIVRpmJ+sVGWkqqE4Q=", "rVEIW3Hu3T52S2zDDUqGT5YiJTBGUv2h3pNuBKFIhZ1U=", "X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxCxs=", "VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=", "EchCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whIE=", "block_size": "4096", "path": "locales/iw/messages.json", { "block_hashes": ["xklkoZ7iSU1+7cd6DAteMUC5IPFd+EgcbnzxkOiFwlk=", "3KbsvoxKY/3AwggF2aAdVQRpMhsNVrKQ3rx2A6Z2Z+Y=", "o9+tsohquaCMj+70zeinRG/hBhA2uLoDI/WoC1uokME=", "xv/K8xucyWJELVT8Cqn+ugFjobBV/mg8pnmACF+2PP4Y=", "p/mvJm2wuCl32Rx3it654MjKAsMe3S9IDEabc1A8mE=", "j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=", "nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDZTXc=", "eToQyJUuNuF9yCga/fXGYFCj/pysSceanhBzksdx23s=", "Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=", "VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAx0Lw=", "iDgLXQqXjP8nCNZxgLuC9LXM45DGfufvGnXvmHsn18wc=", "g+RfdDfrWTUKOPkcsbot7NJ4SC9wVVR/vdVVMuHAtEj8=", "2oC4HCuCuXu3VjF6wnKlzt9uqQNaebcuWpm/mWj69U=", "aMUlpuFqPMiieSaWhlktCK62v2P3OZQAWupWsYzCnvk=", "L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Size (bytes):	26624
Entropy (8bit):	0.8469095552016908
Encrypted:	false
SSDEEP:	24:LLitYxh0GY/I1rWR1PmCx9fZjsBX+T6UwcE85fB9KpJNwMBly0tsaDc90R4sAqwn:tBmw6fU1zBQJNwAbtjI90R47zGMJ2tw
MD5:	0059B6DE4191006E3A7DD494727F942F
SHA1:	92ACA9851C8B1B2A0582C5D8D278E54CC59D91BA
SHA-256:	D1529069BB2CB23AC8237749EA311C8892A5BF9D90BA6569C44033338B37FD9
SHA-512:	0E9AE06D740BD6FC62C4389F051E689D5FC8864E72E4688EEE843313E83B8CF5BF3440D624B20700D07E149F4B1FD2DD076DF3DB4F3BDE40A318AF21B0CA2A2
Malicious:	false
Preview:	SQLite format 3.....@C.....g....._c...~.2.....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxIXNQxIX:qTCT
MD5:	51A2CBB807F5085530DEC18E45CB8569
SHA1:	7AD88CD3DE5844C7FC269C4500228A630016AB5B
SHA-256:	1C43A1BDA1E458863C46DFAE7FB43BFB3E27802169F37320399B1DD799A819AC
SHA-512:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEE985DF
Malicious:	false
Preview:	.f.5.....f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.210422729137975
Encrypted:	false
SSDEEP:	6:mNXvnXSq2Pwkn23iKKdK25+Xqx8chl+IFUtMXvnCEWXXmwKXvnRxkwOwkn23iKKN:i/SvYf5KkTXfchl3FUtMVW/KL5Jf5Kkl
MD5:	382AF65219444E37EA050D5666FF4BA5
SHA1:	65EBC5B5A7486FED7C7B9AC5E88F23D0794B0DB8
SHA-256:	941CD54BB45E543C381B5CF78B72D8CC2F4BEDF709E4269374B97C5BD1A48FC2
SHA-512:	9714B46D00B94F4DF98999C7467992140934FEC921A72007D6901620A0EBA44DF0D3C00B1D3B79FD74FB9858206EC4E5E55AABEC2D13218F32F9452C41AA9D2F
Malicious:	false
Preview:	2021/12/02-21:22:29.712 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/12/02-21:22:29.713 1834 Recovering log #3.2021/12/02-21:22:29.714 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.210422729137975
Encrypted:	false
SSDEEP:	6:mNXvnXSq2Pwkn23iKKdK25+Xqx8chl+IFUtMXvnCEWXXmwKXvnRxkwOwkn23iKKN:i/SvYf5KkTXfchl3FUtMVW/KL5Jf5Kkl
MD5:	382AF65219444E37EA050D5666FF4BA5
SHA1:	65EBC5B5A7486FED7C7B9AC5E88F23D0794B0DB8
SHA-256:	941CD54BB45E543C381B5CF78B72D8CC2F4BEDF709E4269374B97C5BD1A48FC2
SHA-512:	9714B46D00B94F4DF98999C7467992140934FEC921A72007D6901620A0EBA44DF0D3C00B1D3B79FD74FB9858206EC4E5E55AABEC2D13218F32F9452C41AA9D2F
Malicious:	false
Preview:	2021/12/02-21:22:29.712 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/12/02-21:22:29.713 1834 Recovering log #3.2021/12/02-21:22:29.714 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.187277567179511
Encrypted:	false
SSDEEP:	6:mNXvLoq2Pwkn23iKKdK25+XuoIFUtMXvGZmwKXv/kwOwkn23iKKdK25+XuxWLJ:i6vYf5KkTXFYUtMe/KX5Jf5KkTXHJ
MD5:	AB600AA98F5638CC5538BE237F62AB81
SHA1:	6E71CDB5E1E9F3171920292C02E751B9C506F2E0
SHA-256:	51D1E47ACC87FBE83A0C8072C33EF8FBD0608A0BCD049726A4083B3FB271D99D
SHA-512:	33632DD7DBF059B4CD71E144382C3C34F23B3D29C0D2A8AEA3A385A5E8F8541FF53D2D3195EBC6889BDE33A11A07C2AABDA49A7D0605D2CEA603B625280111E5
Malicious:	false
Preview:	2021/12/02-21:22:29.705 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/12/02-21:22:29.706 1834 Recovering log #3.2021/12/02-21:22:29.707 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.187277567179511
Encrypted:	false
SSDEEP:	6:mNXvLoq2Pwkn23iKKdK25+XuoIFUtMXvGZmwKXv/kwOwkn23iKKdK25+XuxWLJ:i6vYf5KkTXFYUtMe/KX5Jf5KkTXHJ
MD5:	AB600AA98F5638CC5538BE237F62AB81
SHA1:	6E71CDB5E1E9F3171920292C02E751B9C506F2E0
SHA-256:	51D1E47ACC87FBE83A0C8072C33EF8FBD0608A0BCD049726A4083B3FB271D99D
SHA-512:	33632DD7DBF059B4CD71E144382C3C34F23B3D29C0D2A8AEA3A385A5E8F8541FF53D2D3195EBC6889BDE33A11A07C2AABDA49A7D0605D2CEA603B625280111E5
Malicious:	false
Preview:	2021/12/02-21:22:29.705 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/12/02-21:22:29.706 1834 Recovering log #3.2021/12/02-21:22:29.707 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.233581454613651
Encrypted:	false
SSDEEP:	6:mNXvyq2Pwkn23iKKdKWT5g1ldqIFUtMXvmZmwKXvcdWFkwOwkn23iKKdKWT5g1lu:iavYf5Kkg5gSRFUtM+/KpF5Jf5Kkg5gZ
MD5:	6014FC9F74023AA70422849ECF245892
SHA1:	4319078A44A5FCF078B8BC19BDD699CF8EBCB4EB
SHA-256:	7622D9CDDDD202516C25FA82BD83A8EF5DE3661E981D4D9CFE821155E0020267E
SHA-512:	464B257040418915150F5D7E20D5F8F9AFE6A7809ED3B3937446C5F7ACBFC980C4D59401019E199133F18AEA4072A1907871CF8A1479D1DDA42ABEB509DBD14C
Malicious:	false
Preview:	2021/12/02-21:22:29.565 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/12/02-21:22:29.566 1834 Recovering log #3.2021/12/02-21:22:29.567 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldg (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.233581454613651
Encrypted:	false
SSDEEP:	6:mNXvyq2Pwkn23iKKdKWT5g1ldqIFUtMXvmZmwKXvcdWFkwOwkn23iKKdKWT5g1lu:iavYf5Kkg5gSRFUtM+/KpF5Jf5Kkg5gZ
MD5:	6014FC9F74023AA70422849ECF245892
SHA1:	4319078A44A5FCF078B8BC19BDD699CF8EBCB4EB
SHA-256:	7622D9CDDDD202516C25FA82BD83A8EF5DE3661E981D4D9CFE821155E0020267E
SHA-512:	464B257040418915150F5D7E20D5F8F9AFE6A7809ED3B3937446C5F7ACBFC980C4D59401019E199133F18AEA4072A1907871CF8A1479D1DDA42ABEB509DBD14C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.oldg (copy)

Malicious:	false
Preview:	2021/12/02-21:22:29.565 1834 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/12/02-21:22:29.566 1834 Recovering log #3.2021/12/02-21:22:29.567 1834 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.48129034211055716
Encrypted:	false
SSDEEP:	96:v8XnKU+bDoYysX0uhnjdVjN9DLjGQLBE3uw:U3h+bDo3irhnydVj3XBBE3uw
MD5:	FFA11668EE240BC05E544DD351FDDD6D
SHA1:	061D68A57166EC248D03156F3A0C74CAECFB68BF
SHA-256:	41DE45BEA6E5841AF722D09E3CFCD9C19DA18B7D2BA763A85E4E42D1AAE7B8B0
SHA-512:	669A5CE282F1F73EA29D738AE39739AE4D71BC5F3DA2850436495F2C964285AADBCA203FD4DE2BD98648A1D9EF00CB1A08AC6EDD850629EC1D65FE09219FE7A3
Malicious:	false
Preview:	SQLite format 3.....@C.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	705
Entropy (8bit):	5.1972483059176495
Encrypted:	false
SSDEEP:	12:Al3XOV2eZfHxQA0V/LNxtvtxq/wsy7SUuJeKbK778B/xgskZBa9sNiyDRMztGsBW:AKXa7RzSjjxhsyOeIY78BJgskfa9yBDT
MD5:	1CD2B434ECFDC202384CA49CBBFE6164
SHA1:	DBB465B9E4FDC436969CCCEADAA288065D68AB40
SHA-256:	5179317A1FC94EE889E5428B65F2D3A4FCD4563C0C09A61828194DB0C5E040C4
SHA-512:	26500B8E8FE8AA4A2AF7FEE7C2AE0B1F8C858F6D6537AA937893DA1AF118B555F475D2E94195379BE44303ACDE7EF4EF53B3CC1CEC78BDD10A78CF80E4A6FAC0
Malicious:	false
Preview:	"U....account..c..desktop..file..html..in..user..paymentreceipt..sign..to..users..your*.....account.....c.....desktop.....file.....html.....in.....user.....paymentrecep t.....sign.....to.....users.....your..2.....a.....c.....d.....e.....f.....g.....h.....i.....j.....k.....l.....m.....n.....o.....p.....r.....s.....t.....u.....y.....n.....Bq..m.....*2file:///C:/Users/user/Desktop/PaymentReceipt.html2.Sign in to your account:.....J.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8720
Entropy (8bit):	0.3291324012332043
Encrypted:	false
SSDEEP:	6:+o4/fMt76Y4QZeS/rG99pG/POqR4EZY4QZv8fOg;j4nMWQASjG9LwFBQZ8fOg
MD5:	3EF6692EE7DD756B805CBB037A79E5DC
SHA1:	08E864E8E2680D9C9775FE419B99C8EA6313650D
SHA-256:	F781F61CE97A8DCDED5E71BB89E0764AA168FA4EA8018F55F9C54CB958BFB988
SHA-512:	51C70589ABCAFE90F827BB246A7CBE23E056A47B6D3B639F188DBC5CE5ABC8C30147F0721EF2809F6F65D6A101E62B9BB07E354D3D39119E81FD74FC9293C074
Malicious:	false
Preview:	K.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Last Sessiona (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Sessiona (copy)

Size (bytes):	2267
Entropy (8bit):	3.2484167149339025
Encrypted:	false
SSDEEP:	48:34dlXxwuJqyhBwJqNjIBle6IgVord+LSJqT:34dlel88lgcd+NT
MD5:	C6556007FD9C9251C8D9DA71B65AB859
SHA1:	18C0FFE52EDFD45D9591DB36D20CA2F8789BEB00
SHA-256:	DA8DF99478E6BF520EF85C4B1BE602A8A5DC431EA33C3678FC9B6C606008F68C
SHA-512:	EF5F18C915F9B2E128068D58923F24FB2C7579294EAE7FD53532924449AEC261A25BE37DBB6914860E11894EE2CA4C73643F9BB8D4387220865DA18EC7583945
Malicious:	false
Preview:	SNSS.....!.....1.....\$.21de891f_3c73_4556_ae9d_dc70eb5c52dc.....4.....,.....2...file:///C:/Users/user/Desktop/PaymentReceipt.html.....h.....`...../...../.....(.....l...2...f.i.l.e.:/..C.:/..U.s.e.r.s./j.o.n.e.s./D.e.s.k.t.o.p./P.a.y.m.e.n.t.R.e.c.e.i.p.t...h.t.m.l.....8.....0.....8.....2...file:///C:/Users/user/Desktop/PaymentReceipt.html.....0/..... 5..0.....&...{730C75E3-B87A-4292-818B-DC8F984D08AE}.....2...file:///C:/Us

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsle (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	1.8112781244591325
Encrypted:	false
SSDEEP:	3:3Dtn:3h
MD5:	0686D6159557E1162D04C44240103333
SHA1:	053E9DB58E20A67D1E158E407094359BF61D0639
SHA-256:	3303D5EED881951B0BB52CF1C6BFA758770034D0120C197F9F7A3520B92A86FB
SHA-512:	884C0D3594390E2FC0AEAB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	7826
Entropy (8bit):	5.381454228469331
Encrypted:	false
SSDEEP:	192:9OMpd3fvE5fgPVZHgQKYicdvHXtE5fgyOq:IWLV5zE1
MD5:	425C66A9D75F0C45E417140B3E8A504B
SHA1:	FFD1718DFDB043574D39D775CA886B8835C51FBB
SHA-256:	EE3AC302A6AECF8CB46C7C0FDDDC93C99D109313B74FE2110C10902275EDD5A9
SHA-512:	9D394C05315C35AE0758A59874BFEDF25C33DCBBF25C04F5C4053D6774808E474400D3A513493EB58C13342156E1BE582407D60A1CDEE246132741919FC30774
Malicious:	false
Preview:	.ch@.....VERSION.1.8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Q_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.CloudProvider7,{\"cloudEnabled\":false,\"notifiedHangoutsPrivacy\":false},S_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.persistent.IdentityService6,{\"signedIn\":false,\"userEmail\":null,\"kioskAuth\":false},Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService,{\"cache\":{\"sinks\":{},\"g\":{},\"h\":null},\"manualHangouts\":{}}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..285164000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...[\"[2020-09-30 09:28:42.02][INFO][mr.Init] MR instance ID: a3f601d9-09ed-4d73-b6cf-2acd12d4689c\\n\", \"[2020-09-30 09:28:42.02][INFO][mr.Init] Native Cast MRP is disabled.\\n\", \"[2020-09-30 09:28:42.02][INFO][mr.Init] Native Mirroring Service is enabled.\\n\", \"[2020-09-30 09:28:42.02][INFO

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.103451081705806
Encrypted:	false
SSDEEP:	6:mNXsywyq2Pwkn23iKKdK8a2jMGIFUIMXsfVm1ZmwKXsJRkwOwkn23iKKdK8a2jM4:i8ywyvYf5Kk8EFUtM8fu/K8JR5Jf5Kkw
MD5:	742B5B880F02D62E0F860D0970AF4E45
SHA1:	2AFA8373D918E26C0AD5E24C42C851980563334C
SHA-256:	539A4D28512BAA305E0F18826F232A0CB410B5A45722FF5ABA29CC82156DF188
SHA-512:	6BA1EB93692EE03A86F13DA4974BE12D73E7D8FFE97EF550608503AB836943DB4DC05DDB01DE7ACD7EBDF4FD8773D63FE6C6949EACBDF4FC565824951A271:34
Malicious:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG

Preview:	2021/12/02-21:22:19.652 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/12/02-21:22:19.662 19c0 Recovering log #3.2021/12/02-21:22:19.670 19c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log .
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	332
Entropy (8bit):	5.103451081705806
Encrypted:	false
SSDEEP:	6:mNXsywyq2Pwkn23iKKdK8a2jMGIFUtMXsfVm1ZmwkXsJRkwOwkn23iKKdK8a2jM4:i8ywyvYf5Kk8EFUtM8fu/K8JR5Jf5Kkw
MD5:	742B5B880F02D62E0F860D0970AF4E45
SHA1:	2AFA8373D918E26C0AD5E24C42C851980563334C
SHA-256:	539A4D28512BAA305E0F18826F232A0CB410B5A45722FF5ABA29CC82156DF188
SHA-512:	6BA1EB93692EE03A86F13DA4974BE12D73E7D8FFE97EF550608503AB836943DB4DC05DDB01DE7ACD7EBDF4FD8773D63FE6C6949EACBDF4FC565824951A271C34
Malicious:	false
Preview:	2021/12/02-21:22:19.652 19c0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/12/02-21:22:19.662 19c0 Recovering log #3.2021/12/02-21:22:19.670 19c0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State3} (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { { "alternative_service": { { "advertised_versions": [], "expiration": "13248516607497410", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 27387 }, "server": "https://www.gstatic.com", "supports_spdy": true }, { "alternative_service": { { "advertised_versions": [], "expiration": "13248516607334226", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 34287 }, "server": "https://ssl.gstatic.com", "supports_spdy": true }, { "alternative_service": { { "advertised_versions": [], "expiration": "13248516607463627", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 31787 }, "server": "https://fonts.gstatic.com", "supports_spdy": true }, { "alternative_service": { { "advertised_versions": [], "expiration": "13248516607318875", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 23359 }, "server": "https://apis.google.com", "supports_spdy": true }, { "alternative_service": { { "advertised_versions": [], "expiration": "13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statemp (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1637
Entropy (8bit):	4.8333059816411845
Encrypted:	false
SSDEEP:	48:Y2nzM3qK6qDHGXctwWs3RLs4yKstoMhXyHbw:JnzMaKxDHGXCOJPHGehM
MD5:	747DBD27A8CF35595D66CB9C5EBCE936
SHA1:	7D8E90CA26F6095FF07E753EB8725E3FFCFD1F6B
SHA-256:	0123531977215458D22945D4A21F093659ACA4E5FFE6FC28674C4988BE814B29
SHA-512:	B918D592FF36C5D173A6E531A0321C702A95845D7F46C8104AFDFEBFA0F19A8DCE6B0CEC2DD7CF71849369BD1E7A98B699FF7D1AA9BDC07A6D286B0EF5A6EEC
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { { "isolation": [], "server": "https://www.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://dns.google", "supports_spdy": true }, { "isolation": [], "server": "https://www.googleapis.com", "supports_spdy": true }, { "isolation": [], "server": "https://redirector.gvt1.com", "supports_spdy": true }, { "isolation": [], "server": "https://fonts.googleapis.com", "supports_spdy": true }, { "isolation": [], "server": "https://ogs.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://play.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://apis.google.com", "supports_spdy": true }, { "isolation": [], "server": "https://fonts.gstatic.com", "supports_spdy": true }, { "isolation": [], "server": "https://ssl.gstatic.com", "supports_spdy": true }, { "isolation": [], "server": "https://www.gstatic.com", "supports_spdy": true }, { "alternative_service": { { "advertised_versions": [50], "expiration": "13285542142319644", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Category:	dropped
Size (bytes):	320
Entropy (8bit):	4.988529178046013
Encrypted:	false
SSDEEP:	6:mNXFlq2Pwkn23iKkKdKrQMxIFUtMXbHZZmwKXakwOwkn23iKkKdKrQMFLJ:i1vYf5KkCFUtMrZ/Kq5Jf5KktJ
MD5:	CD91D0CD6A63A83071B4C127A6C6201A
SHA1:	F0EA79581565C6D09BA22081F7E6C0BAEC55140F
SHA-256:	6357C60C0D308ED93A0C7D38500C5C6223B71C8DCAAF22871E6A65AAA6565188
SHA-512:	8D2F8E7888D55F0BFCB6C404100BDC693774821E57319169F0017892D44CD0C098D7B860B8C38131DD6BC4960C7B9A572FA73AD424A0FBA1D5BE8C63CB612B7
Malicious:	false
Preview:	2021/12/02-21:22:20.260 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000001.2021/12/02-21:22:20.262 1a30 Recovering log #3.2021/12/02-21:22:20.256 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.121032635057007
Encrypted:	false
SSDEEP:	6:mNXsyq2Pwkn23iKkKdK7Uh2ghZIFUtMXsbuZmwKXsoFkwOwkn23iKkKdK7Uh2gnLJ:i8yvYf5KklhHh2FUtM8bus/K8oF5Jf5m
MD5:	F75A508989A99C65DDC971024022A1EE
SHA1:	1D2745261C30D574BAB94B95A555A7FD8F368C94
SHA-256:	631E44B929294D38A150B630CC44F0658282563C253B18D2FD89F768E6B9FE5E
SHA-512:	3936586A75990D8FB2FEE64C221EC565A30B2630839E6D127951629A52A7EDF10E547489C0C3F5105A2D77F4EAAE9404FD20A7459A9EC3D04CD3F73F67077B68
Malicious:	false
Preview:	2021/12/02-21:22:19.616 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/12/02-21:22:19.629 1994 Recovering log #3.2021/12/02-21:22:19.635 1994 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.oldQ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.121032635057007
Encrypted:	false
SSDEEP:	6:mNXsyq2Pwkn23iKkKdK7Uh2ghZIFUtMXsbuZmwKXsoFkwOwkn23iKkKdK7Uh2gnLJ:i8yvYf5KklhHh2FUtM8bus/K8oF5Jf5m
MD5:	F75A508989A99C65DDC971024022A1EE
SHA1:	1D2745261C30D574BAB94B95A555A7FD8F368C94
SHA-256:	631E44B929294D38A150B630CC44F0658282563C253B18D2FD89F768E6B9FE5E
SHA-512:	3936586A75990D8FB2FEE64C221EC565A30B2630839E6D127951629A52A7EDF10E547489C0C3F5105A2D77F4EAAE9404FD20A7459A9EC3D04CD3F73F67077B68
Malicious:	false
Preview:	2021/12/02-21:22:19.616 1994 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/12/02-21:22:19.629 1994 Recovering log #3.2021/12/02-21:22:19.635 1994 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejcic\def9ea5879b-4edd-4707-9385-950525085747.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B61DD08061EAE25A510642228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F8
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": [{ "alternative_service": { ["advertised_versions": [50], "expiration": "13248516514667526", "port": 443, "protocol_str": "quic"] }, "isolation": [], "server": "https://dns.google", "supports_spdy": true }], "version": 5, "network_qualities": { "CAESABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "4G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIIkEthXllkI2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898158
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.1562323013600295
Encrypted:	false
SSDEEP:	12:iEQ+vYf5KkFFUtMjZdW/KjZQV5Jf5KkOJ:iGYf5KkfgMrAJf5Kkk
MD5:	02596CB6F5E65816227F6E82E291E318
SHA1:	DBE63CFECE1192F0042307714976A2DA8244E308
SHA-256:	D6E05F2871BD1538320DA0878B38A02CE61CB8B400A99BF0107CB7FB9C8D3A7A
SHA-512:	261D47506FCF0F3F88E310EB4A6F544696600935C75B547CBC9A08FFF4B7B57DA77285A99D1B54FA8D9C59501A06F78454926F46E566026807CA4264D61C2670
Malicious:	false
Preview:	2021/12/02-21:22:20.278 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\MANIFEST-000001.2021/12/02-21:22:20.280 19cc Recovering log #3.2021/12/02-21:22:20.280 19cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.1562323013600295
Encrypted:	false
SSDEEP:	12:iEQ+vYf5KkFFUtMjZdW/KjZQV5Jf5KkOJ:iGYf5KkfgMrAJf5Kkk
MD5:	02596CB6F5E65816227F6E82E291E318
SHA1:	DBE63CFECE1192F0042307714976A2DA8244E308
SHA-256:	D6E05F2871BD1538320DA0878B38A02CE61CB8B400A99BF0107CB7FB9C8D3A7A
SHA-512:	261D47506FCF0F3F88E310EB4A6F544696600935C75B547CBC9A08FFF4B7B57DA77285A99D1B54FA8D9C59501A06F78454926F46E566026807CA4264D61C2670
Malicious:	false
Preview:	2021/12/02-21:22:20.278 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\MANIFEST-000001.2021/12/02-21:22:20.280 19cc Recovering log #3.2021/12/02-21:22:20.280 19cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Network Persistent State.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.971623449303805
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5p7DHJShsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHfHYhsBdLJlyH7E4f3K33y
MD5:	8CA9278965B437DFC789E755E4C61B82
SHA1:	5776B6C90CA1D2DDC765ED673B5E6DC8E167F0D6
SHA-256:	A57D9231244C1FBDE58A1BF50CAD3A1E3EA28D042BFA272782B65139446E7C51
SHA-512:	3065FE0743AD88E02F8C8FF6CF03B832B616DD08061EAE25A510642228D45EB999EE2CBE4E9C96D5FFC108CB817766240E27BF97E3E5C2A58081D369E2968F6

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Network Persistent State.. (copy)	
Malicious:	false
Preview:	<pre>{"net":{"http_server_properties":{"servers":{"alternative_service":{"advertised_versions":[50],"expiration":"13248516514667526","port":443,"protocol_str":"quic"},"isolation":[],"server":"https://dns.google","supports_spdy":true},"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.189884539645095
Encrypted:	false
SSDEEP:	6:mNXbr+q2Pwkn23iKKdKusNpqz4rRIFUtMXbaXZmwKXb6SVkwOwkn23iKKdKusNpH:i3+vYf5KkmiuFUtMWX/KbV5Jf5Kkm2J
MD5:	F34D080B5CB18465380789BDCDB64DA3
SHA1:	E7BB65AAA9A10CE71B4C33071CD76BC77E09F50E
SHA-256:	5B4406889E3A2C335378D0DDACF272D2861384B8030BDB59881B81315E3A1258
SHA-512:	38736BCBF2AEECF3880AD21DCE11CB18D48B81549A5AD71A0FBAC60F28C10B8572188E3064571D60934ACA536B105E590FAF3724FF315A525ACB9C2E732E3B19
Malicious:	false
Preview:	<pre>2021/12/02-21:22:20.354 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\MANIFEST-000001.2021/12/02-21:22:20.357 1a2c Recovering log #3.2021/12/02-21:22:20.358 1a2c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\000003.log .</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.189884539645095
Encrypted:	false
SSDEEP:	6:mNXbr+q2Pwkn23iKKdKusNpqz4rRIFUtMXbaXZmwKXb6SVkwOwkn23iKKdKusNpH:i3+vYf5KkmiuFUtMWX/KbV5Jf5Kkm2J
MD5:	F34D080B5CB18465380789BDCDB64DA3
SHA1:	E7BB65AAA9A10CE71B4C33071CD76BC77E09F50E
SHA-256:	5B4406889E3A2C335378D0DDACF272D2861384B8030BDB59881B81315E3A1258
SHA-512:	38736BCBF2AEECF3880AD21DCE11CB18D48B81549A5AD71A0FBAC60F28C10B8572188E3064571D60934ACA536B105E590FAF3724FF315A525ACB9C2E732E3B19
Malicious:	false
Preview:	<pre>2021/12/02-21:22:20.354 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\MANIFEST-000001.2021/12/02-21:22:20.357 1a2c Recovering log #3.2021/12/02-21:22:20.358 1a2c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\000003.log .</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHIS+QUI1ASEGhTFjji:S85aEFjl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Preview:	<pre>*...#.version.1..namespace-..&f.....&f.....</pre>

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.160934450101568
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\LOG	
SSDEEP:	6:mNXFnIq2Pwkn23iKKdKusNpZQMxiFUtMXFLSZmwKXFZvzkwOwkn23iKKdKusNpZb:iVnlvYf5KkMFUtMV2/KVRz5Jf5KkTJ
MD5:	1AAF16BBD9C4E1806D26899C5A3D4855
SHA1:	D1187B7F2A99848EE437BF079BAC8F039DC6FEC1
SHA-256:	F04309D82F121F809D6B7E3DDCF880BCE990913CB6FC9AC561162140AA567035
SHA-512:	FF71B5ABE8C953A287DF73A0071D58F3D5D90C575B40F727B526B3C21223626039160B8B7E9208B6EC777FC5E799BE0D2807BF0B83DDB41D87208F7731C5CC3
Malicious:	false
Preview:	2021/12/02-21:22:36.070 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage/MANIFEST-000001.2021/12/02-21:22:36.071 1a30 Recovering log #3.2021/12/02-21:22:36.072 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.160934450101568
Encrypted:	false
SSDEEP:	6:mNXFnIq2Pwkn23iKKdKusNpZQMxiFUtMXFLSZmwKXFZvzkwOwkn23iKKdKusNpZb:iVnlvYf5KkMFUtMV2/KVRz5Jf5KkTJ
MD5:	1AAF16BBD9C4E1806D26899C5A3D4855
SHA1:	D1187B7F2A99848EE437BF079BAC8F039DC6FEC1
SHA-256:	F04309D82F121F809D6B7E3DDCF880BCE990913CB6FC9AC561162140AA567035
SHA-512:	FF71B5ABE8C953A287DF73A0071D58F3D5D90C575B40F727B526B3C21223626039160B8B7E9208B6EC777FC5E799BE0D2807BF0B83DDB41D87208F7731C5CC3
Malicious:	false
Preview:	2021/12/02-21:22:36.070 1a30 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage/MANIFEST-000001.2021/12/02-21:22:36.071 1a30 Recovering log #3.2021/12/02-21:22:36.072 1a30 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lnmmhkkegccagdldgiimedpiccgmgmiedaldefl034e55e0-9b94-480d-b81a-068c9b343130.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { { "alternative_service": { { "advertised_versions": [50], "expiration": "13248516523181804", "port": 443, "protocol_str": "quic" } }, "isolation": [], "server": "https://dns.google", "supports_spdy": true } }, "version": 5, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "4G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lnmmhkkegccagdldgiimedpiccgmgmiedaldeflGPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.0012471779557650352
Encrypted:	false
SSDEEP:	3:MsEIIllkEthXllkI2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898F58
Malicious:	false
Preview:	

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.1720399350881925
Encrypted:	false
SSDEEP:	12:ih+vYf5KkkGHArBFUtMiW/KUV5Jf5KkkGHArJ:iWYf5KkkGgPgMin+Jf5KkkGga
MD5:	3ABB9D6C0BC10D1F5D7882DEAA1A4961
SHA1:	9EB1EA4437947D3860D78ECD4131942A8A2D3E4A
SHA-256:	027D2D662D401C91C190092F26B2402BB1BC9C5CA86FFACF9ED1054707818716
SHA-512:	EDC238D4E21DD47E35B3E491AD940D20F5577CF449C06EE2D66033CF958DF21EEDA8F070DBDA7BCCAFD2788F3FB9D8837E8436B7142A6A69ADC6751E26A11B2
Malicious:	false
Preview:	2021/12/02-21:23:14.596 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\MANIFEST-000001.2021/12/02-21:23:14.598 1a2c Recovering log #3.2021/12/02-21:23:14.599 1a2c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.1720399350881925
Encrypted:	false
SSDEEP:	12:ih+vYf5KkkGHArBFUtMiW/KUV5Jf5KkkGHArJ:iWYf5KkkGgPgMin+Jf5KkkGga
MD5:	3ABB9D6C0BC10D1F5D7882DEAA1A4961
SHA1:	9EB1EA4437947D3860D78ECD4131942A8A2D3E4A
SHA-256:	027D2D662D401C91C190092F26B2402BB1BC9C5CA86FFACF9ED1054707818716
SHA-512:	EDC238D4E21DD47E35B3E491AD940D20F5577CF449C06EE2D66033CF958DF21EEDA8F070DBDA7BCCAFD2788F3FB9D8837E8436B7142A6A69ADC6751E26A11B2
Malicious:	false
Preview:	2021/12/02-21:23:14.596 1a2c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\MANIFEST-000001.2021/12/02-21:23:14.598 1a2c Recovering log #3.2021/12/02-21:23:14.599 1a2c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflNetwork Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	325
Entropy (8bit):	4.9616384877719995
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5pirhsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdHirhsBdLJlyH7E4f3K33y
MD5:	B0429187E1BE99DE4D548DC5B2EDEA0A
SHA1:	B3E07BEE5D753BF1B613BD2DE665C7C21E8184F6
SHA-256:	D8DABBF936DAB4F17437ECA255020EA847D76D6B789F9486010C95E995CFED03
SHA-512:	233F7BDAA848A295E9F58CA52761829FE1044DA1DE1FBCAC407FADC8C7ABA1E4FFD7CA7A4FBE649E83FD1815DC2E3619ACB2A22CE5B2C7241E474CDB9AF2F7ED
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [50], "expiration": "13248516523181804", "port": 443, "protocol_str": "quic" }] }, "isolation": [], "server": "https://dns.google", "supports_spdy": true }] }, "version": 5 }, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "4G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflPlatform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.210036353336588
Encrypted:	false
SSDEEP:	12:i3Q+vYf5KkkGHArqiuFUtMBg/KKQV5Jf5KkkGHArq2J:i35Yf5KkkGgCgMBNKSJf5KkkGg7
MD5:	7FD14BFA24F46CDF9F1E10BF05585439
SHA1:	8AAFB1A296C17226724E53C1ECA4C8DC8CB9FFE7
SHA-256:	FCAE2A0D6E10855887317A7DDA6C29811F8CCA05859EF1692555C0CBCFD71565
SHA-512:	C3724C9C692EBAEC5433ACF40381F9D07274396E0C743BACADF4A93FF99015348DFFA41F326BD10316042DA59F15D188B6FEB2C5A7661F32223A9FF57A3B1026

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\LOG	
Malicious:	false
Preview:	2021/12/02-21:23:14.623 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\MANIFEST-000001.2021/12/02-21:23:14.625 19bc Recovering log #3.2021/12/02-21:23:14.626 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.210036353336588
Encrypted:	false
SSDEEP:	12:i3Q+vYf5KkkGHArquFutMBg/KKQV5Jf5KkkGHArq2J:i35Yf5KkkGgCgMBNKSJf5KkkGg7
MD5:	7FD14BFA24F46CDF9F1E10BF05585439
SHA1:	8AAFB1A296C17226724E53C1ECA4C8DC8CB9FFE7
SHA-256:	FCAE2A0D6E10855887317A7DDA6C29811F8CCA05859EF1692555C0CBCFD71565
SHA-512:	C3724C9C692EBAEC5433ACF40381F9D07274396E0C743BACADF4A93FF99015348DFFA41F326BD10316042DA59F15D188B6FEB2C5A7661F32223A9FF57A3B102C
Malicious:	false
Preview:	2021/12/02-21:23:14.623 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\MANIFEST-000001.2021/12/02-21:23:14.625 19bc Recovering log #3.2021/12/02-21:23:14.626 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	3.4921535629071894
Encrypted:	false
SSDEEP:	3:S8ltHIS+QUI1ASEGhTFjl:S85aEFjl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E1773DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.152573892187503
Encrypted:	false
SSDEEP:	12:iaR39+vYf5KkkGHArAFutMaueSJ/Ka5F39V5Jf5KkkGHArfJ:iaYYf5KkkGgkgMaj5a5F1Jf5KkkGgV
MD5:	B038D2D93E1AC1E1C0C2518DE3AEC9EE
SHA1:	D396C132EE279F366DADE1C9901C1566B3A212A0
SHA-256:	91F66ED6068F0048B5275723BF584E7213FD77A7F6001F66E73864B61EB2C2E3
SHA-512:	A0FDB846C534FD1F9C9FF65F97786D450CDCBBB0F72D056A9EAAA87EDC60FF919A4C0643F6729BDA7D8AE1E4772AD85FA5E0810B499C59387F02888DC7D35A6
Malicious:	false
Preview:	2021/12/02-21:23:31.304 1b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\MANIFEST-000001.2021/12/02-21:23:31.305 1b4c Recovering log #3.2021/12/02-21:23:31.306 1b4c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	418
Entropy (8bit):	5.152573892187503

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\LOG.olde/ (copy)	
Encrypted:	false
SSDEEP:	12:iaR39+vYf5KkkGHArAFUtMaueSJ/Ka5F39V5Jf5KkkGHArfJ:iaYYf5KkkGkgMaj5a5FfJf5KkkGgV
MD5:	B038D2D93E1AC1E1C0C2518DE3AEC9EE
SHA1:	D396C132EE279F366DADE1C9901C1566B3A212A0
SHA-256:	91F66ED6068F0048B5275723BF584E7213FD77A7F6001F66E73864B61EB2C2E3
SHA-512:	A0FDB846C534FD1F9C9FF65F97786D450CDCBBB0F72D056A9EAAA87EDC60FF919A4C0643F6729BDFA7D8AE1E4772AD85FA5E0810B499C59387F02888DC7D3E A6
Malicious:	false
Preview:	2021/12/02-21:23:31.304 1b4c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda \deflSession Storage\MANIFEST-000001.2021/12/02-21:23:31.305 1b4c Recovering log #3.2021/12/02-21:23:31.306 1b4c Reusing old log C:\Users\user\AppData \Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedaldeflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	198
Entropy (8bit):	2.871724756892511
Encrypted:	false
SSDEEP:	3:sLolltz6sjlGXU2tk0lkGgGgGgGgGgGgGgGg:qolXtWswXU2tkEttttt
MD5:	1F7F208858A1F652FA7AE45C3C7510C9
SHA1:	E3B7E0FB73EE579B9E8B6E29F9D9CCD783050A5D
SHA-256:	81B396566964F665632A83714FF09AFE24C96E8E5401A588B943D721669DE6F4
SHA-512:	CFB0EA1566CD946F39159F01DCECCCD98FF4DCC10CD30F85E9BB86AF8661ACF8B9AD0E6C3E915FDAC93959C64158723673EB877ECFEC078C1C82A2E11066E A01
Malicious:	false
Preview:	...n'....._mts_schema_descriptor.....F.....F.....F.....F.....F.....F.....F.....F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.18962010090269
Encrypted:	false
SSDEEP:	6:mNXslJq+q2Pwkn23iKkKdKplFutMXsdegZmwKXsdGpQVkwOwkn23iKkKdKa/WLJ:i8HQ+vYf5KkmFutM80g/K8QpQV5Jf5Ka
MD5:	BA791345D68A1F3D95086AFC147D3F0E
SHA1:	4D76DD04F8792F409196C720388447A5A15EC228
SHA-256:	3A8C0E0DE034F6B35AF31F61D0123DB832559AEACE4DD87E256DEB36DB519F61
SHA-512:	794650FBBC6E75913B3FE1110613B3A32DCF01FBC386C52CD1CC338E15AB0B9CD45722497FB679FE9BD61005831BBB44504541A9DDDD628372545810888FE27E/ A01
Malicious:	false
Preview:	2021/12/02-21:22:19.633 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/12/02- 21:22:19.641 19bc Recovering log #3.2021/12/02-21:22:19.643 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/ 000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.18962010090269
Encrypted:	false
SSDEEP:	6:mNXslJq+q2Pwkn23iKkKdKplFutMXsdegZmwKXsdGpQVkwOwkn23iKkKdKa/WLJ:i8HQ+vYf5KkmFutM80g/K8QpQV5Jf5Ka
MD5:	BA791345D68A1F3D95086AFC147D3F0E
SHA1:	4D76DD04F8792F409196C720388447A5A15EC228
SHA-256:	3A8C0E0DE034F6B35AF31F61D0123DB832559AEACE4DD87E256DEB36DB519F61
SHA-512:	794650FBBC6E75913B3FE1110613B3A32DCF01FBC386C52CD1CC338E15AB0B9CD45722497FB679FE9BD61005831BBB44504541A9DDDD628372545810888FE27E/ A01
Malicious:	false
Preview:	2021/12/02-21:22:19.633 19bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/12/02- 21:22:19.641 19bc Recovering log #3.2021/12/02-21:22:19.643 19bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/ 000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.283823581679113
Encrypted:	false
SSDEEP:	6:mNXoJt9+q2Pwkn23iKkKs8Y5JKKhdlFUtMXotF3JZmwKXoE9VkwOwkn23iKKde:i5vYf5KkkOrsFUtMUX/Kx5Jf5KkkOrzJ
MD5:	498CBBA082E10DFF7822398E495AF2B9
SHA1:	138CFADBF2D7FAAF9C487F13F6005B27AB873648
SHA-256:	58E6028F6E4D6B4E1F40F4FC7AA0304AE02500A2D0F7D73517B20094D46CB25B
SHA-512:	C17A1A1539D3F2AC2248C661FDDb29602DD792189C384894998BB812277857E841EB156CD27E65951D6ED6F09BD0662A37DB174AD6CD7F7543BC60361ACE16C
Malicious:	false
Preview:	2021/12/02-21:24:13.859 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\MANIFEST-000001.2021/12/02-21:24:13.860 1a48 Recovering log #3.2021/12/02-21:24:13.861 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.olds (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.283823581679113
Encrypted:	false
SSDEEP:	6:mNXoJt9+q2Pwkn23iKkKs8Y5JKKhdlFUtMXotF3JZmwKXoE9VkwOwkn23iKKde:i5vYf5KkkOrsFUtMUX/Kx5Jf5KkkOrzJ
MD5:	498CBBA082E10DFF7822398E495AF2B9
SHA1:	138CFADBF2D7FAAF9C487F13F6005B27AB873648
SHA-256:	58E6028F6E4D6B4E1F40F4FC7AA0304AE02500A2D0F7D73517B20094D46CB25B
SHA-512:	C17A1A1539D3F2AC2248C661FDDb29602DD792189C384894998BB812277857E841EB156CD27E65951D6ED6F09BD0662A37DB174AD6CD7F7543BC60361ACE16C
Malicious:	false
Preview:	2021/12/02-21:24:13.859 1a48 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\MANIFEST-000001.2021/12/02-21:24:13.860 1a48 Recovering log #3.2021/12/02-21:24:13.861 1a48 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.0033769341339387224
Encrypted:	false
SSDEEP:	3:ImtVuQ+Xa/IT7sTyC:liVuQAe3A
MD5:	87295D85683FFF6BD1BD0B99644BD7B2
SHA1:	21E06D78C0C4F16F0658905D450D82C74129125A
SHA-256:	38E479A3578A3433ECA57F9C6D7EC4B2480822C9BA8BF099D28D42E996CDA7D1
SHA-512:	00EDC5D6314BC4C125B57CDC7F30E113D7AA92146E07EF3D058CF32734A26560EE6B55934CDB58043CE878C38A4D4FEBF8A8E619A8303398055BFFFD8C9EDE4
Malicious:	false
Preview:	VLnk.....?.....g..H.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\la1bb12ef-742c-4867-9744-0dce5c4e8cb4.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	22602
Entropy (8bit):	5.53647185270196
Encrypted:	false
SSDEEP:	384:7Hq/XiZ7LIAcpNX3N1kXqKf/pUZNCgVLH2HfD/lrU/HGPnZmanEO49L.wLIL91kXqKf/pUZNCgVLH2HfhrUvGPni
MD5:	6FA24A75732211BEA78DDF3FF67BB8EF
SHA1:	5E5F507C4EA534B4DE24B33447D98B99B8EEBB82
SHA-256:	CD3132D1461C066A165E85DE798384B9A95A5AA507795A79A19240E97758702A
SHA-512:	251CA4D0BB760A5AF575151DCB93B66054A4EBC201385A5F3B5C54BAA573B5AC0F00A09F3D24CCC8AA6BB0C20E173464AF20B33529B28AB4C41072E8D0A3BFD

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\la1bb12ef-742c-4867-9744-0dce5c4e8cb4.tmp

Malicious:	false
Preview:	{ "extensions":{ "settings":{ "ahfgeienlihckogmohjhadllkjgocpleb":{ "active_permissions":{ "api":{ "management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"},"manifest_permissions":[]},"app_launcher_ordinal":"","commands":{},"content_settings":{},"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":{},"incognito_preferences":{},"install_time":"13282950139620142","location":5,"manifest":{ "a pp":{ "launch":{ "web_url":"https://chrome.google.com/webstore"},"urls":{ "https://chrome.google.com/webstore"},"description":"Discover great apps, games, extensions and themes for Google Chrome."},"icons":{ "128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCsqGSib3DQEBAQUAA4GNADCBiQKBgQCtI3tO0osjuzRsf6xtD2SKxPITfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLbWLalBPYeXbzIHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB"},"name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\cfccf2c5-14ca-479b-aae0-515fb5cf24aa.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	19184
Entropy (8bit):	5.570710263102561
Encrypted:	false
SSDEEP:	384:7Hq/XiZ7LIAcpxN3N1kXqkF/pUZNCgVLH2HfD/lrU/HGmandaO4r:wLIL91kXqkF/pUZNCgVLH2HfhrUvGFdC
MD5:	027A37469028C9D744FB5CE9310E1346
SHA1:	E97ED98E1ED518153D568998E014B8530DA5BBA3
SHA-256:	3A508D5147651D75DE75FD879F829D21BB56E7A19A818405D691916E016DB643
SHA-512:	EA3C53F2E53E61914219EF4A8D125CE26F05CFEECFF7FA83F0B344683056289A8B8B3B45752AF60629F193052FB41275DAA493ADDED6C164224937B26B7394B4
Malicious:	false
Preview:	{ "extensions":{ "settings":{ "ahfgeienlihckogmohjhadllkjgocpleb":{ "active_permissions":{ "api":{ "management","system.display","system.storage","webstorePrivate","system.cpu","system.memory","system.network"},"manifest_permissions":[]},"app_launcher_ordinal":"","commands":{},"content_settings":{},"creation_flags":1,"events":[],"from_bookmark":false,"from_webstore":false,"incognito_content_settings":{},"incognito_preferences":{},"install_time":"13282950139620142","location":5,"manifest":{ "a pp":{ "launch":{ "web_url":"https://chrome.google.com/webstore"},"urls":{ "https://chrome.google.com/webstore"},"description":"Discover great apps, games, extensions and themes for Google Chrome."},"icons":{ "128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCsqGSib3DQEBAQUAA4GNADCBiQKBgQCtI3tO0osjuzRsf6xtD2SKxPITfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLbWLalBPYeXbzIHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB"},"name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fd465a11c-f402-458e-bde3-df63323407ae.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCDBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\000004.dbtmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qlFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENTf (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ldb\CURRENTf (copy)	
Size (bytes):	16
Entropy (8bit):	3.2743974703476995
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qlFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.276606754741003
Encrypted:	false
SSDEEP:	3:tUKQXZBt5Zmwv21XC0mdkJ0V8t1XC0mdkJ0WGv:mNXZBvZmwKXlIdhVqXldhtv
MD5:	A24367FB42AC8E73F0623CE41051BA97
SHA1:	AC4DA3913BC034EE19728089D44089CBE6664ED0
SHA-256:	B7AAF6BC92597920A25C2116E92D4058B4898825EAE58F73DE67FC30FE92EF7D
SHA-512:	24EDB078881A52BFF3BD269F01C631E1C7CCF934671F4FFCCBDE885B64BE9B7DB2AE7B653CBD39253F307AE3D8DD66D537C9F799EE69A8DF28B940E0DEC43C02
Malicious:	false
Preview:	2021/12/02-21:22:28.565 1998 Recovering log #3.2021/12/02-21:22:28.999 1998 Delete type=0 #3.2021/12/02-21:22:28.999 1998 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.276606754741003
Encrypted:	false
SSDEEP:	3:tUKQXZBt5Zmwv21XC0mdkJ0V8t1XC0mdkJ0WGv:mNXZBvZmwKXlIdhVqXldhtv
MD5:	A24367FB42AC8E73F0623CE41051BA97
SHA1:	AC4DA3913BC034EE19728089D44089CBE6664ED0
SHA-256:	B7AAF6BC92597920A25C2116E92D4058B4898825EAE58F73DE67FC30FE92EF7D
SHA-512:	24EDB078881A52BFF3BD269F01C631E1C7CCF934671F4FFCCBDE885B64BE9B7DB2AE7B653CBD39253F307AE3D8DD66D537C9F799EE69A8DF28B940E0DEC43C02
Malicious:	false
Preview:	2021/12/02-21:22:28.565 1998 Recovering log #3.2021/12/02-21:22:28.999 1998 Delete type=0 #3.2021/12/02-21:22:28.999 1998 Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKIVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF04
Malicious:	false
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ldb20bc3-becd-422c-ab5c-b0e065e43fc9.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\edb20bc3-becd-422c-ab5c-b0e065e43fc9.tmp	
Category:	dropped
Size (bytes):	3473
Entropy (8bit):	4.884843136744451
Encrypted:	false
SSDEEP:	96:6FGX0G70GhIGpyGzRDYLiEHYDBKGzUGaCGjHGESHG/OG6mhM:6Fe0i0sIlyGzRDYLiEHYDBKSUpCQHrSP
MD5:	494384A177157C36E9017D1FFB39F0BF
SHA1:	CE5D9754A70CD84CEE77C9180DB92C69715BE105
SHA-256:	07CF0A5189FAD30A4AA721F4F6DA1B15100991115833EACFA1E2DC84A1B54337
SHA-512:	BFB80EEC0C0B5D9E487047703BE49826321A4D249422E0C81E978E6C8A310F41C7B4B8F849229BA87484FDF4831DD6A98FF994D0FDA5CE3D341CE615C15F2F1
Malicious:	false
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [], "expiration": "13248516607497410", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 27387, "server": "https://www.gstatic.com", "supports_spdy": true }, { "alternative_service": { [{ "advertised_versions": [], "expiration": "13248516607334226", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 34287, "server": "https://ssl.gstatic.com", "supports_spdy": true }, { "advertised_versions": [], "expiration": "13248516607463627", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 31787, "server": "https://fonts.gstatic.com", "supports_spdy": true }, { "alternative_service": { [{ "advertised_versions": [], "expiration": "13248516607318875", "port": 443, "protocol_str": "quic" }], "isolation": [], "network_stats": { "srtt": 23359, "server": "https://apis.google.com", "supports_spdy": true }, { "alternative_service": { [{ "advertised_versions": [], "expiration": "13248

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	338
Entropy (8bit):	5.111377739988368
Encrypted:	false
SSDEEP:	6:mNXvnzQ+q2Pwkn23iKKdKfrzAdIFUtMXvn6pdWZmwkXvnHpQVkwOwkn23iKKdKfa:ibQ+vYf5Kk9FUtMipdW/KPpQV5Jf5KkS
MD5:	74ADD54830F86D94750D5FC202697DED
SHA1:	11904D3BCA73D85AD9A5DB988A601C156D7A1BAD
SHA-256:	701B0E3F93967B131E8E5F523826797B3F23A179AB1187693073A71A37C6C97A
SHA-512:	085CCB766BB501B78D2FAA72D6C9A8F86BF929EA93922B2964ACB4A0FCEECEAA799B0217475D514F7D2FE5214A6C54B16F97180E9932207C089A50E72F8DA4E
Malicious:	false
Preview:	2021/12/02-21:22:29.931 19cc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\MANIFEST-000001.2021/12/02-21:22:29.932 19cc Recovering log #3.2021/12/02-21:22:29.933 19cc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000003.log .

Static File Info

General	
File type:	HTML document, ASCII text, with very long lines
Entropy (8bit):	4.166448552327814
TrID:	HyperText Markup Language (28028/1) 100.00%
File name:	PaymentReceipt.html
File size:	710487
MD5:	7f46a4fc70dab897f514fbb609cc47c1
SHA1:	9132215cc4c7f2421df985e978c2081f4c88f562
SHA256:	d657257086a46a67c1227a386d881e71f8fd7d9f15c9d8f592c5e55419e85d76
SHA512:	3c829765d3219072eae678c573c07ae384fc38313a15f8244e79f9683695874ea1e526db37254679c567f2b7bf1e02c7c4a18b98416e5f2d26dfe9ee9450b4
SSDEEP:	12288:j0dlCRsefOh9hriOS5z163C8H7hhSCvZF77Qpmgo9yhvAlQwk8wu2OM27N1LZVfb:jiao7AW2TDRp7yxC+NiTegeD2jYiZkjJ
File Content Preview:	<script language=javascript>function _0x262d02(_0x3012ce,_0x2106bc,_0x7ddb06,_0xd9c00a,_0x21daf6,_0x15dd8a,_0x5c4050){return _0x571a(_0x2106bc-_0x1f1,_0x15dd8a);}function _0x571a(_0x16b3d8,_0x2f8f19){var _0xbb2ca4=_0x3651();return _0x571a=function(_0x148

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 21:22:22.924787045 CET	192.168.2.4	8.8.8.8	0xbb0f	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.929083109 CET	192.168.2.4	8.8.8.8	0xd4a5	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.939133883 CET	192.168.2.4	8.8.8.8	0x16e9	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.943612099 CET	192.168.2.4	8.8.8.8	0xd0e	Standard query (0)	aadcdn.msfauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.948373079 CET	192.168.2.4	8.8.8.8	0x39f6	Standard query (0)	aadcdn.msaauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.571468115 CET	192.168.2.4	8.8.8.8	0x2cfd	Standard query (0)	cdnjs.cloudflare.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.574718952 CET	192.168.2.4	8.8.8.8	0x88fb	Standard query (0)	maxcdn.bootstrapcdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.610963106 CET	192.168.2.4	8.8.8.8	0x3df0	Standard query (0)	code.jquery.com	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:26.573801994 CET	192.168.2.4	8.8.8.8	0x6ef8	Standard query (0)	aadcdn.msfauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:31.031642914 CET	192.168.2.4	8.8.8.8	0x288e	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 21:22:22.935949087 CET	8.8.8.8	192.168.2.4	0xc6a7	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:22.952516079 CET	8.8.8.8	192.168.2.4	0xbb0f	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:22.952516079 CET	8.8.8.8	192.168.2.4	0xbb0f	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.958736897 CET	8.8.8.8	192.168.2.4	0x16e9	No error (0)	login.microsoftonline.com	ak.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:22.958736897 CET	8.8.8.8	192.168.2.4	0x16e9	No error (0)	ak.private.link.msidentity.com	www.tm.ak.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:22.963118076 CET	8.8.8.8	192.168.2.4	0xd0e	No error (0)	aadcdn.msfauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:22.963118076 CET	8.8.8.8	192.168.2.4	0xd0e	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.969810963 CET	8.8.8.8	192.168.2.4	0xd4a5	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:22.977467060 CET	8.8.8.8	192.168.2.4	0x39f6	No error (0)	aadcdn.msaauth.net	aadcdnoriginwus2.azureedge.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:24.593303919 CET	8.8.8.8	192.168.2.4	0x2cfd	No error (0)	cdnjs.cloudflare.com		104.16.19.94	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.593303919 CET	8.8.8.8	192.168.2.4	0x2cfd	No error (0)	cdnjs.cloudflare.com		104.16.18.94	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.593857050 CET	8.8.8.8	192.168.2.4	0x88fb	No error (0)	maxcdn.bootstrapcdn.com		104.18.10.207	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 21:22:24.593857050 CET	8.8.8.8	192.168.2.4	0x88fb	No error (0)	maxcdn.bootstrapcdn.com		104.18.11.207	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:24.630379915 CET	8.8.8.8	192.168.2.4	0x3df0	No error (0)	code.jquery.com	cds.s5x3j6q5.hwcdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:26.593477964 CET	8.8.8.8	192.168.2.4	0x6ef8	No error (0)	aadcdn.msftauth.net	cs1100.wpc.omegacdn.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:26.593477964 CET	8.8.8.8	192.168.2.4	0x6ef8	No error (0)	cs1100.wpc.omegacdn.net		152.199.23.37	A (IP address)	IN (0x0001)
Dec 2, 2021 21:22:31.059487104 CET	8.8.8.8	192.168.2.4	0x288e	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 21:22:31.059487104 CET	8.8.8.8	192.168.2.4	0x288e	No error (0)	googlehosted.l.googleusercontent.com		142.250.203.97	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- accounts.google.com - aadcdn.msftauth.net - clients2.google.com - maxcdn.bootstrapcdn.com - cdnjs.cloudflare.com - https: - clients2.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49764	172.217.168.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	0	OUT	POST /ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard HTTP/1.1 Host: accounts.google.com Connection: keep-alive Content-Length: 1 Origin: https://www.google.com Content-Type: application/x-www-form-urlencoded Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:23 UTC	0	OUT	Data Raw: 20 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	113	IN	HTTP/1.1 200 OK Content-Type: application/json; charset=utf-8 Access-Control-Allow-Origin: https://www.google.com Access-Control-Allow-Credentials: true X-Content-Type-Options: nosniff Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 02 Dec 2021 20:22:23 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: script-src 'report-sample' 'nonce-gGDQixVc2Np9Xi4AKuS7+g' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-gGDQixVc2Np9Xi4AKuS7+g' 'self' https://apis.google.com https://ssl.gstatic.com https://www.google.com https://www.gstatic.com https://www.google-analytics.com;report-uri /_/IdentityListAccountsHttp/cspreport Cross-Origin-Resource-Policy: cross-origin Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-02 20:22:23 UTC	114	IN	Data Raw: 31 31 0d 0a 5b 22 67 61 69 61 2e 6c 2e 61 2e 72 22 2c 5b 5d 5d 0d 0a Data Ascii: 11["gaia.l.a.r",[]]
2021-12-02 20:22:23 UTC	114	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49763	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	0	OUT	GET /shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.8 Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:23 UTC	2	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 16213098 Cache-Control: public, max-age=31536000 Content-MD5: TjUQkZ0p0Y7rbj6LJofS9Q== Content-Type: image/svg+xml Date: Thu, 02 Dec 2021 20:22:23 GMT Etag: 0x8D79A1B9B05915D Last-Modified: Thu, 16 Jan 2020 00:32:45 GMT Server: ECAcc (frc/8F6C) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlobBlob x-ms-lease-status: unlocked x-ms-request-id: c711e8bd-e01e-0094-3b45-547244000000 x-ms-version: 2009-09-19 Content-Length: 513 Connection: close
2021-12-02 20:22:23 UTC	3	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 32 34 22 20 68 65 69 67 68 74 3d 22 32 34 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 32 34 20 32 34 22 3e 3c 74 69 74 6c 65 3e 61 73 73 65 74 73 3c 2f 74 69 74 6c 65 3e 3c 70 61 74 68 20 64 3d 22 4d 31 38 2c 31 31 2e 35 37 38 76 2e 38 34 34 48 37 2e 36 31 37 6c 33 2e 39 32 31 2c 33 2e 39 32 38 2d 2e 35 39 34 2e 35 39 34 4c 36 2c 31 32 6c 34 2e 39 34 34 2d 34 2e 39 34 34 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 38 5a 22 20 66 69 6c 6c 3d 22 23 34 30 34 30 34 30 22 2f 3e 3c 70 61 74 68 20 64 3d 22 4d 31 30 2e 39 34 34 2c 37 2e 30 35 36 6c 2e 35 39 34 2e 35 39 34 4c 37 2e 36 31 37 2c 31 31 2e 35 37 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 24 24"><title>assets</title><path d="M18,11.578v.844H7.617l3.928-.594.594L6,12l4.944-4.944.594.594L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056l.594.594L7.617,11.57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49782	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	176	OUT	GET /shared/1.0/content/images/personal_account_0f72b5950600f24e7f9a604b186f3945.png HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	198	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 15366314 Cache-Control: public, max-age=31536000 Content-MD5: D3K1QYA8k5/mmBLGG85RQ== Content-Type: image/png Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D79A1B9F5B2B36 Last-Modified: Thu, 16 Jan 2020 00:32:52 GMT Server: ECAcc (frc/8F8E) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: b29f51a7-b01e-0055-38f8-5b88ae000000 x-ms-version: 2009-09-19 Content-Length: 1335 Connection: close
2021-12-02 20:22:25 UTC	199	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 33 00 00 00 33 08 06 00 00 00 3a a1 30 2a 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 04 c4 49 44 41 54 78 da cc 9a 4d 68 13 41 14 c7 27 69 a1 16 c 1 a6 15 0a 55 a4 29 ed 41 68 a1 7b d0 8b a0 59 2f 5e 13 4f 7a eb f6 a8 97 a6 e8 dd f4 2e 65 7b d1 63 d3 9b 37 b7 47 3d a 5 8a 5e 2a 98 42 7b b3 98 28 56 a8 98 26 42 b1 05 a5 be 17 67 36 b3 eb ee 66 66 76 ba e6 c1 b0 21 64 37 f3 db f7 f5 9f d 9 4d 9d 9c 9c 10 5d 96 7a f8 36 0b 07 83 8e 2c 1d bc 35 61 54 61 d4 f0 78 f2 f8 5a 95 68 b4 54 5c 18 00 28 c0 01 87 09 63 5c f2 f4 16 8c 0a 0c 07 07 c0 35 13 87 01 80 0c 1c 2c 18 45 05 Data Ascii: PNGIHDR33:0*PHYstEXtSoftwareAdobe ImageReadyqe<IDATxMhA'iU)Ah{Y/^Oz.e{c7G=^*B{(V&Bg6ffv!d7M]z6,5aTaxZhT(c\5,E

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49783	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	176	OUT	GET /ests/2.1/content/cdnbundles/converged.v2.login.min_kfhrfyfy-sm2tmkm5ficw2.css HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	202	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 5198719 Cache-Control: public, max-age=31536000 Content-MD5: 0O2H9juGYL0zkzcYWwR0Nlg== Content-Type: text/css Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D982C8F03AF4D4 Last-Modified: Tue, 28 Sep 2021 21:42:58 GMT Server: ECAcc (frc/8FCC) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 4cd84846-501e-0061-5f72-b8a27b000000 x-ms-version: 2009-09-19 Content-Length: 110118 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	310	OUT	GET /ests/2.1/content/cdnbundles/jquery.3.5.min_dc940oomzau4rsu8qesnvg2.js HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	311	IN	HTTP/1.1 200 OK Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Content-Encoding,Cache-Control ,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 4734403 Cache-Control: public, max-age=31536000 Content-MD5: HWW92uTq7vx3y5z+zFZbXQ== Content-Type: application/x-javascript Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D8DA1D9D23143A Last-Modified: Fri, 26 Feb 2021 06:13:19 GMT Server: ECAcc (frc/8F5A) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 30219252-601e-007f-4fab-bcdcbd000000 x-ms-version: 2009-09-19 Content-Length: 119648 Connection: close
2021-12-02 20:22:25 UTC	312	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 33 2e 35 2e 31 20 7c 20 28 63 29 20 4a 53 20 46 6f 75 6e 64 61 74 69 6f 6e 20 61 6e 64 20 6f 74 68 65 72 20 63 6f 6e 74 72 69 62 75 74 6f 72 73 20 7c 20 6a 71 75 65 72 79 2e 6f 72 6f 2f 6c 69 63 65 6e 73 65 20 2a 2f 0d 0a 21 66 75 6e 63 74 69 6f 6e 2e 68 65 2c 74 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 65 2e 64 6f 63 75 6d 65 6e 74 3f 74 28 65 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 2e 68 65 29 7b 69 66 28 21 65 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 Data Ascii: /*! jQuery v3.5.1 (c) JS Foundation and other contributors jquery.org/license */function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery
2021-12-02 20:22:25 UTC	328	IN	Data Raw: 3d Data Ascii: =
2021-12-02 20:22:25 UTC	328	IN	Data Raw: 28 61 3d 65 29 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 7c 7c 5b 5d 29 5b 30 5d 3d 3d 6b 26 26 72 5b 31 5d 29 2c 21 31 3d 3d 3d 64 29 77 68 69 6c 65 28 61 3d 2b 2b 73 26 26 61 26 26 61 5b 6c 5d 7c 7c 28 64 3d 73 3d 30 29 7c 7c 75 2e 70 6f 70 28 29 29 69 66 28 28 78 3f 61 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3d 3d 3d 66 3a 31 3d 3d 3d 61 2e 6e 6f 64 65 54 79 70 65 29 26 26 2b 2b 64 26 26 28 70 26 26 28 28 69 3d 28 6f 3d 61 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 3d 5b 6b 2c 64 5d 29 2c 61 3d 3d 3d 65 Data Ascii: (a=e)[S] (a[S]={})[a.uniqueID] (o[a.uniqueID]={})[h] [])[0]===k&&r[1],!1===d)while(a+=+s&s&a&a[!])(d=s=0) u.pop())if((x?a.nodeName.toLowerCase()===f:1===a.nodeType)&&+d&&(p&&((i=o=a[S])[(a[S]={})[a.uniqueID] (o[a.uniqueID]={})[h]=[k,d],a===
2021-12-02 20:22:25 UTC	377	IN	Data Raw: 65 29 7b 72 65 74 75 72 6e 20 31 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 39 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 21 2b 65 2e 6e 6f 64 65 54 79 70 65 7d 3b 66 75 6e 63 74 69 6f 6e 20 47 28 29 7b 74 68 69 73 2e 65 78 70 61 6e 64 6f 3d 53 2e 65 78 70 61 6e 64 6f 2b 47 2e 75 69 64 2b 2b 7d 47 2e 75 69 64 3d 31 2c 47 2e 70 72 6f 74 6f 74 79 70 65 3d 7b 63 61 63 68 65 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 70 74 3d 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3b 72 65 74 75 72 6e 20 74 7c 7c 28 74 3d 7b 7d 2c 56 28 65 29 26 26 28 65 2e 6e 6f 64 65 54 79 70 65 3f 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3d 74 3a 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 74 68 69 73 2e 65 78 70 61 6e 64 6f 2c 7b 76 61 6c 75 Data Ascii: e){return 1===e.nodeType 9===e.nodeType !+e.nodeType};function G(){this.expando=S.expando+G.uid++}G.uid=1,G.prototype={cache:function(e){var t=e[this.expando];return t (t={},v(e)&&(e.nodeType?[this.expando]:t).Object.defineProperty(e,this.expando,{valu
2021-12-02 20:22:25 UTC	393	IN	Data Raw: 65 73 74 28 73 2e 74 79 70 65 29 3f 75 2e 63 68 65 63 6b 65 64 3d 73 2e 63 68 65 63 6b 65 64 3a 22 69 6e 70 75 74 22 21 3d 3d 6c 26 26 22 74 65 78 74 61 72 65 61 22 21 3d 3d 6c 7c 7c 28 75 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 3d 73 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 29 3b 69 66 28 74 29 69 66 28 6e 29 66 6f 72 28 6f 3d 6f 7c 7c 76 65 28 65 29 2c 61 3d 61 7c 7c 76 65 28 63 29 2c 72 3d 30 2c 69 3d 6f 2e 6c 65 6e 67 74 68 3b 72 3c 69 3b 72 2b 2b 29 4f 65 28 6f 5b 72 5d 2c 61 5b 72 5d 29 3b 65 6c 73 65 20 4f 65 28 65 2c 63 29 3b 72 65 74 75 72 6e 20 30 3c 28 61 3d 76 65 28 63 2c 22 73 63 72 69 70 74 22 29 29 2e 6c 65 6e 67 74 68 26 26 79 65 28 61 2c 21 66 26 26 76 65 28 65 2c 22 73 63 72 69 70 74 22 29 29 2c 63 7d 2c 63 6c 65 61 6e 44 61 74 61 3a 66 75 Data Ascii: est(s.type)?u.checked=s.checked:"input"!==l&&"textarea"!==l (u.defaultValue=s.defaultValue);if(t){if(n)for(o=0 ve(e),a=a ve(c),r=0,i=o.length;r<i;r++)Oe(o[r],a[r]);else Oe(e,c);return O(c=a+ve(c,"script")).length&&ye(a,!f&&ve(e,"script")),c,cleanData:fu
2021-12-02 20:22:25 UTC	409	IN	Data Raw: 65 78 74 65 6e 64 28 7b 61 74 74 72 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 72 2c 69 2c 6f 3d 65 2e 6e 6f 64 65 54 79 70 65 3b 69 66 28 33 21 3d 3d 6f 26 26 38 21 3d 3d 6f 26 26 32 21 3d 3d 6f 29 72 65 74 75 72 6e 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 65 2e 67 65 74 41 74 74 72 69 62 75 74 65 3f 53 2e 70 72 6f 70 28 65 2c 74 2c 6e 29 3a 28 31 3d 3d 3d 6f 26 26 53 2e 69 73 58 4d 4c 44 6f 63 28 65 29 7c 7c 28 69 3d 53 2e 61 74 74 72 48 6f 6f 6b 73 5b 74 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 5d 7c 7c 28 53 2e 65 78 70 72 2e 6d 61 74 63 68 2e 62 6f 6f 6c 2e 74 65 73 74 28 74 29 3f 70 74 3a 76 6f 69 64 20 29 29 2c 76 6f 69 64 20 30 21 3d 3d 6e 3f 6e 75 6c 6c 3d 3d 3d 6e 3f 76 6f 69 64 20 53 2e 72 65 6d 6f 76 Data Ascii: extend({attr:function(e,t,n){var r,i,o=e.nodeType;if(3!==(o&&8)!==(o&&2)!==o)return"undefined"==typeof e.getAttribute?S.prop(e,t,n):(1===o&&S.isXMLDoc(e)) (i=S.attrHooks[t.toLowerCase()]) (S.expr.match.bool.test(t)?pt:void 0)),void 0!==(n?null===n?void S.remove

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1171	IN	Data Raw: 4c 4b e4 28 58 a2 e0 40 93 33 b8 e8 f5 80 03 e8 92 6b 47 88 3e 84 e4 e2 d1 6e 5b 42 dc c4 62 c5 62 4e c1 83 2e a6 76 23 5f 03 f2 5b 59 ec d5 d3 75 a0 4f 01 7a c6 c4 e8 a5 4b ae 07 28 8e f8 ac c3 e4 ee 4c db 46 6b 85 1a f7 3f 6f f2 ce fa 7f ad c9 20 f2 18 4d 7e 6c a7 f4 53 38 0b 0a 79 25 9a b9 df 87 de d3 a7 7e b9 e8 8e ba 65 58 ba 63 fa cb ec 39 7e fb de 43 57 25 f7 47 6e fa 6f 60 71 34 6e 1d 68 3f b0 e3 41 12 06 ef 7b 2a 0a 46 d1 fd 04 3a 50 23 f4 98 16 7c 05 ee ad 48 8a 36 fa b0 3a e0 98 46 f2 b8 12 48 9b be 3f ca f3 e3 80 63 dc ff df 52 11 c6 11 c7 1f be 15 ab 16 02 17 95 d7 d4 8d 35 75 63 38 e9 59 e5 75 75 63 5d dd a8 c7 13 ab 6c 91 3d 14 fa 1b 8c 3c 7f 54 e1 bf 24 19 8d b2 fd 57 8e 90 a4 d5 f1 57 2c 4b 08 51 81 81 8c 5e 11 1c 5d 07 18 e2 d5 12 b2 12 Data Ascii: LK(X@3kG>n[BbbbN.v#_[YuOzK(LFk?o M-!S8y%-eXc9-CW%Gno`q4nh?A(*F:P#l6:FH?cR5uc8Yuuc)=<T\$WW,KQ^]
2021-12-02 20:22:31 UTC	1172	IN	Data Raw: 41 5b 17 c3 d2 e4 61 11 c7 66 b5 29 87 a5 fe 9a 61 41 6c 74 6d 58 fe 0f 28 8c 07 f2 a9 20 11 6f 5c eb 8f 12 0e 13 71 57 72 98 e2 99 3b 7e d5 da e8 ff 66 6d 2c a4 17 47 84 63 51 cc 59 23 af 59 22 4c 47 d4 fa 70 78 c0 d2 6b a4 a2 b6 c4 eb 16 ca bc 11 49 2d 1c 93 85 bf cd 91 c0 40 10 ae 47 51 fd 06 e4 37 5f e9 33 b5 dc e3 28 c3 59 37 96 80 6c 00 f9 48 84 05 94 de 77 f5 8c 03 56 69 73 6d ad b4 51 7c fb 7e 7d bd f4 fe fd db e2 fa 26 b4 c7 9d ce 2f b0 b1 b6 f1 76 03 9e de 78 f7 fe dd fa da db 8d d2 fb b7 50 e0 71 7e 81 cd 0f 1f 4a 1b 6b ef 36 36 df af bd 7f bf b1 b1 51 2c 15 a1 c0 a7 d6 dc 02 6f 8b 6f d7 3f 94 8a 1b 6f 4b ef 3e bc fb b0 b6 58 c4 1c ba ee af f9 6f 78 f7 6e 7d f3 ed 87 cd 52 71 6d 63 a3 b4 f1 61 f3 dd fb 0f 50 60 eb 85 3e 6c be db 5c 5f 5f fb b0 Data Ascii: A[af)aAltM(X(olqWr;-fm,GcQY#Y"Lgpxkl-@GQ7_3(Y7lEwVismQl-)&VxPq-Jk66Q.oo?oK>Xoxn)RqmcaP`>!_
2021-12-02 20:22:31 UTC	1173	IN	Data Raw: f7 78 17 3e de b9 8f 7b f0 f1 de fd fc 0b 3e 3e b8 d3 4f e5 8d 12 74 a1 06 1f 25 77 17 1e 29 ad b9 63 78 a4 b4 ee fe c2 8f 0d 37 f8 0c 1f 9b ee 14 7f bd 75 a7 f0 a2 d2 3b f7 27 bc 7d 6d cd ad c3 1b d6 e0 49 b8 b8 b6 e1 ee 41 f1 b5 f7 6e 0d ef 7d 70 27 50 60 bd e4 9e dd 97 37 a1 b9 fb 3b f0 51 72 4f a6 f0 b1 e6 fe dc 87 8f 75 f7 ee 13 7c 6c b8 61 0d 3e 36 dd 01 7e bc 73 07 f0 24 b4 e5 eb 6e b9 b4 b6 b6 2e a2 d9 d3 87 8e 01 af 46 bd 57 84 53 8b d4 c1 c3 d1 e0 02 11 e5 78 11 e3 8e f4 e4 75 05 a2 76 df eb 0e 62 c5 02 d2 3d 4f 2a c5 03 07 eb e4 8b 88 0e 76 34 22 ec 36 0a 16 1c a5 d5 f5 c7 23 ca 60 e8 d3 7b a4 37 d9 52 b1 22 c9 18 6f d4 24 c6 b6 7a c2 05 e4 0b 9c ea 52 b1 bc b4 04 bf 19 2e 80 88 4b a1 8e 49 ce 74 a6 4f 66 af e2 c2 a8 8a a3 78 f5 bf d2 63 c3 a0 Data Ascii: x>{>Ot(%w)cx7u;`jmlAn)pP`7;QrOu la>6-s\$n.FWSxuvb=O`v4"6#{7R"o\$zR.KltOfxc
2021-12-02 20:22:31 UTC	1174	IN	Data Raw: 27 a6 d2 50 ba 8c 4e 50 c6 1a 64 f8 44 2a 5f c7 64 8c 64 1a a7 2b 1f 0d ac d0 05 89 80 2e de 0b 1d 09 aa b6 0f d7 af 02 e0 97 7f 04 36 b9 11 14 3d 2f 09 69 b2 39 a9 f9 a2 aa 49 86 3f ac 22 50 3a c9 02 c2 c8 32 ce 3d 64 59 e5 c2 2d 0d 39 61 67 ba 99 91 f7 13 e1 8d 30 57 34 3a 13 11 be d8 d8 e6 86 f0 e5 4c 6b c4 d3 3e b5 43 53 3c e6 0d e3 56 db cc 2a e1 93 23 a9 3e 8c ca 95 a0 a2 12 59 8b f1 14 de 75 21 46 b7 68 ae a5 62 30 28 ad 37 da 8d 22 e5 21 0b 2b 66 65 25 80 6d 61 63 36 5f 54 53 e9 a3 17 8a d0 69 68 f5 2c 99 7a 9a aa 71 ee c2 f5 69 00 02 ad b1 38 93 ab 25 c2 f0 09 78 55 f2 a3 c6 9c fa 30 9f 02 62 7a c1 18 11 10 e1 24 eb 9a 3b 5b c9 59 89 e9 ea aa fa 28 95 c9 9f 56 3d 10 c8 41 ff 15 ca 04 ad 3a c4 a0 1c 2b 4c 6c d0 f8 28 5d cb 2b 2b 2b 3c a6 36 70 26 Data Ascii: 'PNPdD*_dd+.6=~/9I?*"P:2=dY-9ag0W4:Lk>CS<V*#>Yu!Fhb0(7"!+fe%mac6_TSiH,zqi8%U00bz\$;[Y(V=A: +Ll[+++<6p&
2021-12-02 20:22:31 UTC	1176	IN	Data Raw: fd 4c 9c 85 bb c2 49 d6 a8 ef 0a 65 ef 6e 92 1b 92 b0 16 c2 0a e6 d7 de 75 64 28 3d f2 93 a2 df 15 49 3b b1 1f 70 9c 51 5c 60 56 45 e6 b0 d9 eb 92 60 db 13 da ac af 8d 4b c7 cf ea 83 43 1d 0b c1 af c8 5a 22 ac e5 38 a4 94 73 33 49 39 03 8d 25 08 8c ed 52 af d4 71 bb 30 ff 4c e9 bc 50 9d 01 bc 6a e1 1e e4 09 dc 2d 3e 90 f4 78 6c 37 c3 ec 1d ed 4a 49 5c 51 2f cc e1 3f 92 97 b8 d9 82 8a b8 c2 f4 05 06 20 2e 2c 89 ed 00 ae 65 96 1c 1c 6b 8e b9 b6 60 fe 98 02 e7 cd b6 66 07 3b 26 ae 5f d9 b6 e0 11 68 07 2f 01 72 c9 ca 67 b7 d4 76 31 8a 13 1f 24 39 35 63 55 43 03 b3 ba a8 63 a1 b7 3c 4e f4 0b 68 ba 34 0b de d7 33 91 a9 42 c3 74 0c 47 9f 6a 37 8b a3 7e 72 3e 50 d0 ac 38 02 35 67 f8 a5 a2 fb 7b b1 b6 6e 1e 82 da f1 18 24 b1 0e ea 7c 43 5f 39 3c df ea 74 bc d5 e9 Data Ascii: Llenud(=!pQ\`VE"KCZ"8s3l9%Rq0LPj>x7Jl Q/? .ek`f;&_h/rgv1\$95cUCC<Nh43BtGj7-r>P85g{ns C_9<t
2021-12-02 20:22:31 UTC	1177	IN	Data Raw: ff 49 a3 ae dd a0 57 7e 92 e1 09 98 d3 e6 3f 6c 62 41 54 8d 9e 9f d8 5c a3 b5 98 c6 ae db 54 25 db 74 8e 1b 9a d3 f6 32 d6 66 e9 63 ca 39 03 9f c4 03 e5 c0 d5 fa f5 fa ce 44 18 2f 9e a4 76 e9 0e 17 cf 69 a1 48 2f cf c5 49 6b d8 5c 3c d8 c6 5c b3 18 e2 a0 87 a8 a4 66 87 33 f5 a5 7a 9c 80 5a 53 90 f9 d3 0c a4 b0 ae bd 37 46 ed d9 00 8d 34 18 df d4 25 fa 52 01 d9 2b ea 75 11 83 4e 5e 72 40 08 14 58 0f 28 33 a3 f9 1a dd 0b 58 81 cf e7 11 54 85 84 b2 8e 98 0d 11 39 84 e6 0d ed e5 ab 97 6a 6a 58 23 97 b7 75 ec 0f ee ca e1 df 18 d8 e4 6c 6d 48 52 72 30 26 05 22 6f 14 7a 4a d7 0e 0d 96 68 56 39 9c 23 1c 1d 8d b3 cc 0c 7b bf 35 d8 b7 0d 46 f6 33 ea 56 05 88 2d 0a bc c1 55 e9 9a d0 81 e9 31 2f d0 bd 25 b0 82 e3 b1 7b 92 7a fd 27 fb 64 ec 1e 8e f9 60 3b cd d3 Data Ascii: !W~?lbatYtM2fC9D/viH/Ik<l3zZS7F4%R+uN`r@X(3XT9jX#ulmHrR0"&ozJhV9#{5F3V-U1l/%{z'd`;
2021-12-02 20:22:31 UTC	1178	IN	Data Raw: ad 2e bc ad 5e 48 5f 72 05 a7 8e f7 e4 57 b4 57 a9 3d 71 cb 8a 99 d8 6d a4 bd dd 74 74 e3 47 66 c2 3a ee 03 e9 0c 48 dd d7 44 24 b5 27 c2 4f 3b 88 ca 84 ab c6 40 64 65 b4 d9 b9 62 31 94 3b 2e c3 8f 95 1f dc 43 60 b6 be ec 9c 6c 1f 9c ec dd 6c 7d f9 72 76 fa 75 eb 88 32 c2 08 70 1f 9a c3 94 37 51 93 04 9e 8e 47 f5 3f 78 02 02 6d a2 c3 a9 55 1e 0a ad c1 27 04 13 45 8c 18 60 e2 f7 10 5e bd e3 be 43 cc b4 ed 96 fd 20 90 dc c8 d8 29 56 ca 7d 9a c6 89 6e b7 27 a8 06 c9 81 79 4c 21 da e1 b6 bf a9 d9 ed 6c ef 9c 5c 1c 6c 1d 9d 5b ee 93 4e b5 c3 99 c3 2e 04 8c 6b 27 9c 6f e7 10 80 66 a2 0f 4f 36 f5 cc ed 67 57 b2 e6 ab 9b 3b 39 f5 04 d7 4f f2 7f 4c 4e 24 17 88 58 9a 56 d9 c4 36 36 2c 01 06 3e 3c 8a 76 dd b8 9d c0 c4 39 15 16 84 18 2e ce cc 89 c6 f4 6a b1 e9 23 53 Data Ascii: ^H_rWWW=qmttGf:HD\$`O;@deb1;.C`lljrvu2p7QG?xmU'E`^C`Jv)nYl!l[N.kofO6gW;9OLN\$XV66,><v9.j#S
2021-12-02 20:22:31 UTC	1180	IN	Data Raw: 72 02 a5 5e 3d 8a de 02 29 ad 55 b6 f6 f9 1c dd bc 3b 09 ba b6 35 12 d2 7b d4 b8 29 6e 8b 5b 8b ec 16 66 aa c2 b1 60 56 88 35 ff 03 0e 23 43 c0 6e 31 22 6e 24 82 02 eb 42 49 96 98 f8 66 ee ee 1c 7d 19 0e 4c b2 39 b2 04 d8 79 52 e0 74 af 1c a1 99 c1 8d 8b 3e 25 81 40 c9 cb e4 aa 20 ef 54 9e 71 cb 0d 95 18 bc 3f 61 84 99 03 83 7d 3c bc d7 68 d8 a6 9b d7 22 03 5f c1 ca 3e 72 de ea de 6d b7 06 21 82 cd 3e 4a 71 d9 d5 16 7e af 2b f4 61 ce 6f f6 b1 f9 26 22 a7 07 13 f7 f0 de a9 1c e8 f4 ab d7 ca 58 96 97 97 cd 3d e5 09 bc 5b b8 de 23 ef 5d 3d 24 35 22 67 ce c4 aa 67 dc a0 3f 92 18 24 81 0c b6 7e b7 e2 4b c4 42 04 a3 69 45 24 c9 3b 3a a9 4b ec 61 61 dc 1a c3 4c 69 3b 50 5f 75 b8 e8 d0 98 67 5b 2b c1 8a e5 58 e8 26 3b 53 ec 3e 47 4f 18 f3 c5 26 86 fd 09 9c a4 Data Ascii: r^=)U;5`0]n[f`V5#Cn1"n\$Bif)L9yRt>%%@ Tq?a]<h"__>rm!>Jq--+ao&"X=[#]=5'gg?&-KBiE\$;KaaLi;P_ug [+X&;S>GO&

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1263	IN	Data Raw: c2 22 7b 65 47 d9 2b 63 5a 2e 27 c3 02 b7 06 4a cb 65 f3 dc a4 c8 10 75 b9 59 1c fc 1a dc f0 5f 80 2c cd 97 f3 f4 33 8e 08 b3 87 d5 e1 21 3f 1d d8 1f de 4b bb 94 5e 2d b3 e1 9a ed 73 b4 bf c0 0b 03 d9 aa 67 8b a5 31 2a c3 23 3c f4 f0 a1 07 0f e1 c2 c0 b3 f0 68 a1 fb c7 f3 34 65 62 e3 b9 8c f0 5d 16 ef 15 db 06 06 bc b6 c8 cb 46 df a6 92 b2 d9 3c 23 1b 13 8e 4b d2 83 09 5b a3 fd ae 1d 38 83 e0 30 31 d2 fe 24 0a 4a 22 d1 a0 c7 42 1d 58 b5 34 47 fb 08 13 de 71 74 25 19 b7 20 e3 ba d8 d2 95 84 44 f0 6f 35 06 b6 9c a4 c8 d3 a4 21 9f d3 6e be 2c 5c 63 d8 ef 04 37 9c d7 c2 7e 76 e7 5a 0c 44 72 04 50 46 f8 92 7e e3 a1 8b c9 08 b9 1e 16 46 63 ea 73 58 93 9f 59 1f a9 55 ce 05 72 ba 54 21 d4 ba c8 87 04 6c 97 32 4d 97 61 a6 c8 72 ae 5c 2a b7 61 f3 50 4e 34 3c 9a 22 Data Ascii: "[eG+cZ.'JeuY_,3l?K^-sg1*#<hA4ebJF<#KJ[801\$J"BX4Gqt% Do5In,lc7~vZDRPF~FcsXYUrT!2Mar^aPN4~"
2021-12-02 20:22:31 UTC	1264	IN	Data Raw: a8 03 6c f6 f3 2e 4d 39 1c 44 ee be d8 ca 24 67 8d f8 4f 72 e0 89 51 5f 86 37 20 49 10 24 9d f4 97 8c 98 a2 a4 ed 18 16 4e f2 38 a2 83 6d 11 09 42 ec 03 91 9e 2b b4 5b c4 aa 8a e6 02 b3 e4 f3 05 96 3a b8 24 df 10 b1 53 c4 eb e1 d8 03 d4 a2 5d 33 21 a1 e0 d3 d4 d5 6a f2 3c 50 52 b1 66 93 aa 6d 03 6d 5a b3 07 ec e2 30 3a 7f 30 55 63 d8 16 30 88 2f 7c 3b ae ad af 87 61 b8 58 06 fe 74 3d 87 39 69 0d ed 02 36 58 4c 5a 66 61 84 b6 c9 69 ae 17 9a 47 5d 69 57 65 e0 4b c1 6e e4 a9 f5 f0 43 da f0 79 47 94 a3 4f 7b 8c 29 e4 78 15 9e ca 4f 7b 8a 39 fb 6c 3d 3f 5f 62 8d 50 06 3f 7c cd 4d 32 26 aa 5d cc 32 50 df 0b d9 4b 2b 0b d0 5d 69 00 5a 91 e6 e0 31 27 2c bc fc e3 5c 6a ad 77 b4 3e 3f b7 32 df cd f6 ba 3c 39 5c 82 02 45 d9 56 77 d0 a8 5a eb 44 81 70 3e 32 72 b2 4a 91 Data Ascii: l.M9D\$gOrQ_7 l\$N8mB+{.\$Sj3j<PRfmmZ0:0Uc0l; aXt=9l6XLZfaiGjIWeKnCyGoj XoQl=?_bp?lM2&J2P K+}jZ1'.jw>?2<9lEVwZdp>2rJ
2021-12-02 20:22:31 UTC	1265	IN	Data Raw: c4 d5 0e 5d ed 88 ab 5d ba da 15 57 c7 74 75 2c ae 7c ba f2 c5 15 8d 0c c3 27 8b dd 6a f2 7c a6 62 c3 e2 55 53 5c 1d e0 c5 c1 a4 54 8d 38 88 a9 4d 37 c5 47 ac ce c1 c3 1f a1 10 0f a2 7f 69 00 5a 31 c5 c4 2c e6 e4 c9 94 8f da d2 bb 52 0c 42 7c bb f8 68 f1 7d 62 7a c4 9c c9 4e 76 4d 49 99 13 61 f8 47 88 46 b5 12 c6 8b c0 a9 7a d9 3d e1 88 da fa e3 4e e3 20 ac 6a 1c b2 68 67 5d 83 00 d1 63 3f 29 59 d5 f9 8e 3a c5 51 99 72 d4 fd cf 8e ba 33 00 7e 15 37 79 b0 73 09 3c cc b1 b3 43 e3 9b 63 59 fd 48 93 ea 67 1b c0 ae ce d8 00 6d b5 68 ba 1b 2d c6 28 9f 94 ec ea 3c eb 66 55 43 eb 66 57 b5 75 73 12 d6 ad 81 a4 ec a5 60 e7 00 34 fa 01 3c 9e 58 1d 2f 58 b8 fa a0 37 ee 53 88 98 72 b0 a8 62 7d 1b c3 4b af 4d 42 2a 5c fe 49 c9 09 af ee c1 10 a0 4f 6c 9c ef 80 de c5 bb Data Ascii: j]Wtu, j]bUSlT8M7GiZ1,RBj]bzNvMlaGFz'=N jhg c?)Y:Qr3~7ys<CcYHgmh-<fUCfWus~4~X/X7SrbjKMB^lOI
2021-12-02 20:22:31 UTC	1267	IN	Data Raw: 8b d9 e1 36 2b 7c 66 8f 39 29 d2 23 a7 b7 31 7b b7 01 12 4e 64 be bc 6e 98 6a 7f 79 4a 08 18 09 78 f1 b9 d1 75 7b cf 12 0a c8 48 91 75 0c 0a 85 ea 73 f1 a1 6d 38 0d ba 1a ad 69 02 eb cd 6b ca 2e e0 b5 5b e9 6e 95 bd 3c c1 d4 4d 3f 2c f0 a8 62 87 8f 86 22 4a d2 43 19 a8 52 11 17 9c 24 08 93 cd 5c 54 11 7a 47 3b ae c9 89 0f 90 d9 d2 da 8b 22 ba 07 96 d6 56 39 ee d0 08 83 7e 10 51 4a 99 ed f0 16 ff 25 69 24 1d 07 8b f9 91 d3 dd 9b 67 ba 37 9a 68 27 57 cf 18 fa ac b7 cd 7c 76 f9 87 dc 7a 9c 4d 39 6b bc 78 ed 0b 34 f2 df 28 18 79 f9 fd 2f 3a 2d a6 22 56 8a 86 04 36 8e 11 c9 6c c4 ee a4 53 e9 4e a3 fb 9d 2c 45 c7 38 44 63 01 de e9 f6 fb 2f 19 b6 90 fe fe ec d9 ad c6 e8 3b 56 e1 af ff de c7 f7 f7 27 2f 03 aa 9a 49 71 62 02 d7 b8 c7 d7 b8 57 0d b9 57 03 d8 8e 6d Data Ascii: 6+{f9)#1(NdnjyJxu{Husm8ik,[n<M?,b"JCR\$!TzG;"V9~QJ%i\$g7h"W vzM9xk4(yl/:"~V6lSN,ED8c;V/lqbWWm
2021-12-02 20:22:31 UTC	1268	IN	Data Raw: 58 62 8d 0a c5 03 6f 57 28 10 78 a7 42 81 c0 9b 15 0a 04 de ad 50 20 f0 56 85 02 81 ef f2 c0 d4 3b 2f 14 98 7a bc 45 81 a9 47 5b 14 5f fa 70 8f e2 4b 1f ec 51 7c 69 bf 42 f1 a5 eb 15 0a 2c fd f3 85 02 4b 5f bf 50 60 e9 eb 1d 0a 2c 7d b5 43 81 a5 9d 1d 0a 2c 6d ed 50 60 69 7b 87 02 4b fb db 14 58 ba be 4d 81 a5 fb 9b 14 58 ba b4 14 58 ba b7 45 81 a5 bf 5c ec 51 64 e9 d3 3d 8a 2c 7d be 47 91 a5 cf f6 28 b2 f4 db 36 45 96 7e dd a6 c8 d2 77 3b 14 59 fa 76 87 22 4b ef f3 c8 d2 95 3d 8a 2c bd bd 47 91 a5 77 f6 28 c8 f6 ee 1e 05 d9 de db a3 20 db d7 9b 14 63 fb 6a 93 62 6c 9f f1 18 db a7 3c c6 f6 d5 1b 05 d0 3e 7f a3 88 d4 de 16 45 a4 76 b7 28 22 f5 e1 26 45 a4 3e d8 a4 88 d4 fb 9b 14 91 fa f2 8d 22 52 5f bc 51 44 ea bd 17 8a 48 5d 79 a5 88 d4 65 Data Ascii: XboW(xBP V/zEG_pKQjIB,K_P'_)C,mP`i{KXMXI[XE Qd=,}G(6E~w;Yv"K=,Gw(cjb <~Ev"l"&E"R_QDHj]ye
2021-12-02 20:22:31 UTC	1269	IN	Data Raw: 91 f6 05 36 e9 62 be b4 a0 e2 d4 6f 86 57 bb 66 be e4 26 bd da cd 38 f7 ee f7 bc fe 6a f7 a1 64 05 52 2a 6b 83 14 16 86 85 d1 c2 30 c0 13 0f 88 3a 6b 92 2a 82 1f 46 5b 30 31 5d 4c ed 37 c3 62 07 4d 03 b3 6d 91 54 a6 f9 cf 4e d7 dd 5c d3 d5 82 7a ff bf 9a ad dc 44 ea 9f 2a d1 63 46 f9 94 ca dc 85 7f ab ca 60 51 a6 04 c8 b5 1d 49 81 a5 f8 03 05 21 78 75 53 a1 ec ab 2a d7 92 8d c7 bf 54 99 da 47 ea 5b da 41 d0 52 00 12 e9 7f 8f 6b 5e ae 46 a0 05 2e 57 c4 65 86 c7 b0 93 f9 98 b0 43 ee 9a e9 f3 a0 8e 94 fe 93 03 98 ed aa 32 92 1f 8f af 7c cf 4e b1 1a a6 4f 4e 55 97 9b ab eb 0e f4 7c b9 e3 df ed d9 c2 64 7e 27 24 eb 8c 03 96 24 78 52 76 a2 10 04 81 c6 0e 01 8d 9d cf 4c a0 02 61 da 6e 58 b4 b5 13 b2 82 08 81 ae e9 3a fd dd 2a db a9 66 4a bb 9f bd 35 3c ac Data Ascii: 6boWf&8jdR*k0:k*F[01]L7bMmTNlzd*cF6QjqxlxuS*TG[ARK^F.WeC2 NONUjd~\$xRvLanX:~fJ5<
2021-12-02 20:22:31 UTC	1270	IN	Data Raw: 14 da cf 2e 5c 36 e0 b4 2f 94 31 63 c6 25 9a 0c a5 30 0e e6 e3 98 a2 ff 60 a3 05 d5 6a 21 dd b2 fb c3 0c 54 50 bd 4e a9 f1 30 51 a8 41 f1 09 d2 0f ae 87 26 90 78 e0 ad 5f ec 67 15 03 5a ff d2 e6 ec 36 39 0c 0c 00 dc fb c3 0c 17 96 80 cb 34 35 b5 a8 f3 57 1e f6 12 fc 01 36 5c 54 5a ca 61 ce 63 ad 8e a5 ea 36 51 a6 04 c8 b5 42 a1 c9 75 02 a2 bd 91 5d 59 fe 93 ff cf 96 2d 2e ff 09 3b 9f 3b 6f c1 47 00 b1 03 7f 30 26 32 ab 53 02 e2 fc f2 df f6 86 4c 83 68 d6 0d e0 f7 79 d3 1f 0e 56 e3 5f ff f5 ab 2b cd 17 fd 45 0c 6c 55 e7 1e 6d 3d e8 ae b0 5d fc f1 7c 91 ae 53 aa 23 e1 46 b7 d9 32 1c b6 e3 c3 89 3b 41 a7 79 db 36 6c d6 b4 8d 1a db b6 0c 0f b8 e8 d0 9c e9 27 5b 8b 74 79 e2 93 61 4f d3 2e c1 1e df b6 3e 3e 30 9f 72 55 a0 10 7b a3 b8 ba b4 6a 14 57 Data Ascii: .\6/1c%0`j!TPN0QA&x_gZ6945W6\TZac`10Bu Y-;;oG0&2SLhyV_+ElUm=]]S#F2;Ay6f t[yaO.~>>0rUj W
2021-12-02 20:22:31 UTC	1272	IN	Data Raw: 00 15 3f 01 ea d0 62 41 80 6d 68 b3 20 1b 69 54 e2 6d 70 84 5f 2f e4 4c 85 48 47 21 9f c2 39 6b 70 20 dd 32 1b bf 42 72 94 98 60 44 ac 42 aa ed 9c 2c 03 51 14 7b 99 af 82 b6 d0 6b ef 54 60 8d 2f ad 99 40 3f c8 33 42 89 21 a2 61 66 55 72 b9 ed 1d f8 fd f1 f1 84 85 cc 90 67 62 4e 3b 24 e8 8d 74 07 e0 ef 1e c1 df 0e d4 ca c1 89 07 74 e1 b3 75 bc c8 00 19 d6 51 52 14 cc 5d e7 c1 29 aa 99 82 8c ba 55 91 0a 81 69 c9 fd 70 03 df 7a 37 8e 5c 66 8e 07 df 03 cd 10 c9 88 57 33 1c 15 4e 76 87 60 3f 5a 4d b8 61 f1 4c 90 be 90 1a ad 60 2b 1a 61 12 75 a7 9b 64 b8 19 86 99 28 30 59 2c d0 69 d7 16 a6 76 50 62 c6 1a 05 f1 13 a4 df 18 95 cd e2 58 65 00 5e e5 b7 97 90 8d be e5 49 d8 25 32 1a 3b 86 c7 7e 76 80 9b c6 7d 3d 1e 02 0b 7d 32 02 b6 1a f8 e8 fa 84 96 31 c2 3d 5b d9 Data Ascii: ?bAmh iTmp_/LHG!9kp 2Br`DB,Q kT` @?3B!afUrgbN;SttuQR)Uipz7lW3Nv~?ZMaL~+aud(OY,iVpBxe^l %2;~v)=]21=[
2021-12-02 20:22:31 UTC	1273	IN	Data Raw: e8 f1 d6 18 53 95 5f 36 de e6 90 6e 44 5b fc 1e 4c e2 ad 17 78 f3 05 6c 3f 4d 10 8d 20 a3 27 40 46 ef 3f 07 19 ca 03 19 8e ab c3 8f ab a3 83 0c 77 c3 21 90 e1 2a b9 af 4b 20 c3 41 90 e1 04 20 c3 d5 5c ed 7f 17 64 4c 1b 03 82 09 c7 54 af 29 49 f9 32 f7 57 96 87 ee 08 8e da 6f b1 49 ab d0 d9 f7 3c c1 0f 38 7f bd 79 76 dc 91 cd 67 fd 7f 0d eb 5d f6 3d cf f1 b7 5f fa 56 d7 9d 29 47 8b 56 9c 63 83 f1 26 0b bc cd 02 36 0a a3 bb 76 18 7d 01 96 ff cb 51 b2 47 21 48 00 6c a7 88 71 b1 13 43 22 4b b1 25 fb 62 4b f6 ff 67 b0 d8 f8 7f 18 8b 4d 17 7f 8d 75 f1 17 7d d7 14 f1 d7 a0 0d ad f2 b9 22 a5 2e 8c 7f 7a 48 24 e0 4f 22 86 2b c8 1c 7d 46 6a 5b 82 d4 8e 64 9b 11 f8 10 d7 52 43 87 34 01 24 c6 72 28 a5 04 1c f4 27 f8 8c db 0d 8f a5 bd aa 95 f9 4b 60 bb 6f 79 74 eb 30 Data Ascii: S_6nD[Lxl?M '@F?w!*K A lDLT)l2Wol<8yvg =~_V)GVc&6v QG!HlqC"K%bKgMuj".zH\$O"+f]FjdRC4Sr(K'koyt0
2021-12-02 20:22:31 UTC	1274	IN	Data Raw: 3e 63 00 88 d2 cc 3a 46 73 c0 a5 44 c5 01 3a 37 c6 14 f3 ca 2e be 4d 76 f1 a3 b9 74 00 75 01 88 9e 48 07 30 fe 65 a6 9f 02 d1 7e 5e 03 28 a2 b4 1e 9e f0 4f 35 ef 8b 21 a1 ff 93 50 bf 3f ff 16 34 4b f2 a4 0f e0 95 af e0 15 d6 1a 25 40 27 19 be b5 3e d3 52 05 83 53 db 75 82 53 cf 36 c1 29 58 63 97 0c e6 01 92 04 06 f3 78 81 2b 8e 36 f0 0e 45 13 40 b0 f3 de 41 38 b5 07 9c 25 9c 4e 77 c3 21 af 59 b2 86 a7 9f 21 6b f8 67 05 81 5e fe 25 c9 e1 89 37 f2 1e 11 98 0c 93 21 51 f0 fc 33 01 4e a3 bb 40 95 e9 f6 30 2c b9 f1 b5 64 52 21 15 69 4f 17 ca bc 08 60 f4 32 a7 fd 7b a2 58 46 ad d1 f6 0e c9 00 9f b0 d0 c4 32 de 86 4b 62 19 dd cd 1c 45 23 2e 8a 65 dc 40 2c e3 29 b1 8c fb db 62 99 69 63 40 d2 0d 2d 58 c5 6b 4a 81 01 bd 9b 09 44 28 9d 46 77 aa cc 24 2c ad 51 ef 51 Data Ascii: >c:Fsd:7.MvtuH0e~(O5lP?4K%@>R^SuS6)Xcx+6E@A8%Nw!Ylkg^?lQ3N@,0,dRl!O~2(XF2KbE#e@.)bic@~XkJD(Fw\$,QQ

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1276	IN	Data Raw: 75 05 3f 07 a3 51 ea 61 56 34 3c fb de 79 30 31 d1 8f dc 9b 70 fd f1 91 1a cb a5 53 87 d8 9e 30 98 73 b3 ec a4 df 4f 0e 0c 20 45 0f 8c 3c 3b 3b c0 70 f2 07 46 91 ed 1e 18 4b ec e0 c0 58 66 87 07 c6 0a 3b 3a 30 56 d9 f1 81 b1 c6 f6 0e 28 3e 3c fc cd 4f 32 6c 9b 68 5e d8 a7 66 7a fb 17 a0 96 60 93 c0 a3 fb 3c 5c 6f 8f 7c 6f 00 0b 45 37 0a 70 e3 a6 b1 d3 a0 8b 22 5d 74 f0 13 e1 6a 09 ae b6 da 63 6f d4 eb 61 d4 0f b8 b3 0c 77 8e 7b 76 a3 ed d1 e5 8a ba 5c 28 ec d2 9d d5 68 f7 6b 41 95 22 af 92 c7 21 55 c6 9d ce 2b bf c4 11 fd 3c 3b c1 0b 11 b1 f1 1f 03 2e 27 7c 33 06 90 25 2c ef 50 3a 5f 65 6d a9 59 c1 13 74 de 91 ae 60 3b 61 57 b0 f9 bc b7 12 2d 15 d1 e3 75 aa d9 23 7b 54 d6 de 64 a8 22 cc 20 f3 39 61 d4 d4 53 96 23 ca e8 fb 5b 60 ee f8 fd 11 ed 94 d0 d6 d1 Data Ascii: u?QaV4<y01pS0sO E<;pFKXf;0V(<>O2lh*fz'<loJoE7p`J]tjcoaw[v\{hKa`U!+<;' 3%,P:_emYt';aW-u#`[Td` 9aS#`[
2021-12-02 20:22:31 UTC	1277	IN	Data Raw: 34 60 6a bc 30 be 0c 3c 3e 8d 47 8c b3 97 60 2a 45 df 47 c3 e0 1e 3c 66 47 8c e1 47 07 c6 84 a9 b3 b8 89 d4 23 83 57 a3 c6 d4 31 1d db da 70 6d 2b ed 64 0c 8f 0a 82 a5 4e 4a 72 e0 e0 27 41 65 de 1d 17 46 62 48 07 24 69 18 89 1d 03 d1 00 f3 35 00 ea 92 cf dc cf 90 75 29 5c b9 04 40 5d 9d ae 11 42 cd 5e 44 3e e0 a1 7c 00 af bf 58 fa fc 58 7c 22 54 3c 27 0a 8e ec 21 04 f5 03 31 81 c8 33 e4 da 51 35 dc 6c df 51 fc 8d 1f 2e fc d9 70 0d 67 c2 f0 75 00 27 e8 7d b6 89 4c 65 6d e1 8c 08 e3 87 3c 11 45 5c 5d 77 82 31 9a a9 ae 45 93 05 63 b8 9a a6 ca 10 d1 db 4e 6c 2d 98 55 28 f8 78 a7 11 86 22 42 23 eb d9 49 bb fe f7 3f 4a 51 44 ea db 2c d8 a2 f0 5d e8 54 42 2b 2d 1a 0b cc 5a d8 5e 02 d4 ba a1 cd bf 3d 11 56 1c e1 53 f9 1b 52 19 72 ea a3 77 69 e2 99 4f 31 59 7e 6d Data Ascii: 4`j0>G*EG<fGG#W1pm+dNDr/AeFbH\$!5u)\@]B*D> XX `T<'!13Q5IQ.pgu']Lem<E\]w1EcNI-U(x"B#f?JQD ,]TB+-Z^=VSRnwiO1Y~m
2021-12-02 20:22:31 UTC	1278	IN	Data Raw: 69 9a 2c c8 32 97 72 c5 e5 24 45 34 3d 29 24 6a a0 e9 51 31 51 f5 4c 8f 96 26 56 00 24 ac 90 c8 bd 50 5c 8d d0 01 bf 4b fc 9f 24 12 ff c9 7a e9 df 54 4b b7 09 82 b4 00 82 b4 73 11 b5 34 dc 08 a9 a5 e1 3a a2 96 86 3b 89 6a e9 b6 00 2f 9d 38 7f f0 db d9 34 77 13 c2 f2 7d 1e 7f 2f 1e a3 af 1d ca 84 e4 cb 14 48 52 6e c3 c3 a8 59 b9 e9 61 d4 76 66 67 db 1c 3b 94 6d f3 d9 66 3e 25 dd 2c 79 18 a0 68 d1 cd 76 4a 70 ba ea 94 19 0b 2f d2 de c7 87 af e5 d1 dc 25 51 53 0d 45 4d a8 fe f5 36 5c 1c 55 ce e0 39 72 3a 31 51 13 e7 51 dc 5c 52 30 b7 59 a1 f7 b4 a1 8e 3a 53 86 ea eb 43 f5 63 43 dd 63 ef fb 03 18 aa 77 64 2c ca b1 fa c1 58 45 f6 cf 2f da 60 b9 24 ab 9e 30 ab 52 92 35 fe 64 56 a7 0d b5 a9 0f b5 19 1b ea b1 18 aa af 0d b5 19 0c b5 19 9b 56 2e 2f 6b 26 8c 54 06 Data Ascii: i;2r\$E4=)\$jQ1QL&V\$PK\$zTKs4:;j 84w\ /HRnYavfg;mf>%;yhwJp/%QSEm6U9r:1QQ!R0Y:SCcCcwd,XE/\$OR5dVV./k&T
2021-12-02 20:22:31 UTC	1279	IN	Data Raw: 6e db 3b 83 19 3f e9 8d 1a b5 06 10 f4 28 a4 6d 74 9f 7a 2d cf 65 0b b6 05 3b 67 61 d8 78 f3 30 fe 8d da d6 a5 20 87 20 40 05 46 d1 ca 13 5e 6e c1 0b c5 eb 81 47 e0 2f ce 2d 2a 3b f9 af 5f f3 a6 76 b1 67 4b d4 e0 cb d3 f7 25 f4 ed 7e c2 b7 63 20 9a d1 16 76 0c 04 33 2e 62 11 5f 8b 77 8f 0e 60 41 65 a8 63 78 69 06 46 9c e6 b4 6a ea e4 fc b8 3c 0e 32 22 da e6 e5 f1 bd f3 90 7d b1 f9 e2 5a 5c 33 8b e1 91 4b ce b7 6f 99 d2 a4 24 df bc f0 94 c3 97 a7 a5 c4 92 12 a0 a6 52 86 45 01 ac be 99 a9 5f a9 20 2e d3 b7 37 24 cb 78 1c ca 38 e8 b8 99 25 56 bb 30 ab b5 74 94 f3 c7 fa d9 28 3d 27 c8 a5 cb 88 26 03 e0 1b 0a aa b0 82 a0 e6 e2 46 d6 17 34 93 88 dd 33 16 25 f0 6e 18 42 0d c3 db 98 81 ba b8 d5 c9 b8 46 74 92 94 e7 09 30 9f 73 9c 97 e1 eb a3 d7 13 15 1b 89 6d Data Ascii: n;?(mtz-e;gax0 @F^nG/-*_-vgK%-c v3.b_w`AecxiFj<2"}Zl3Ko\$RE_.7x8%V0t-8'&F43%nBxFt0sm
2021-12-02 20:22:31 UTC	1281	IN	Data Raw: 56 c8 b6 b3 3f e1 13 c9 a9 b2 8d f1 88 ed ec 71 c3 74 26 ea e9 b0 96 96 92 0b 87 36 1e af 07 ab 70 05 f5 a4 44 29 fb 06 bb b2 5b 23 c3 2d 51 c1 c9 5a a4 79 b1 b5 5a 3f 0f 79 0d 86 dd b4 ea b2 00 e4 90 08 08 85 ee 10 28 08 ed e9 c5 ea b8 b1 3b 01 69 11 08 1a 63 ad ea 1a 00 54 93 b5 14 3d 13 d7 fe 3f b5 93 2c d7 15 3e 94 b0 b4 35 a2 78 d8 82 ed d1 0c 01 a5 b0 80 5e da a1 fd 04 db 09 01 13 ad af a7 89 1d 79 1a 51 3b a3 12 38 d4 b3 87 96 34 db b7 52 46 58 c4 ef d4 89 75 d6 2c f1 9f a2 55 1a 3e 1e 4e 45 1f 70 8c e6 47 44 36 ba 6c 80 0e 6d b5 96 64 e2 90 1a f0 78 a2 b5 c6 60 38 5a 20 63 58 c0 73 56 c7 43 cb 3c 47 8a fe 48 39 4f 20 6d 85 ad e5 d0 a1 12 6d 1c cc 5c 4c 1e d3 0f 6b 5d ad 2c f0 fd 30 c9 a6 64 3f 37 80 e8 3c 3d 3b db ae a4 4c 61 ce e7 6d a4 2b 3a d9 20 Data Ascii: V?qt&6pD)[#-QZyZ?y'S=#u3r]XXLj6(<B-e7w[0o-tix>S'WGE!!Y,~**W[q"]He(n;@/o[-f-kpD*]>Dxz[-Q"]U"3u#
2021-12-02 20:22:31 UTC	1282	IN	Data Raw: 04 cd 11 58 64 94 24 9d 6f 21 ce d3 14 62 9f 82 9b 87 56 ab a8 64 75 1c c5 cb 1e 2c 3f 6d 07 b9 a3 16 62 23 8f ce ad e5 47 d6 2d 18 b5 00 08 41 5b 84 09 e1 71 93 a2 8a 02 6d 07 36 36 be 2a 00 e4 90 08 08 85 ee 10 28 08 ed e9 c5 ea b8 b1 3b 01 69 11 08 1a 63 ad ea 1a 00 54 93 b5 14 3d 13 d7 fe 3f b5 93 2c d7 15 3e 94 b0 b4 35 a2 78 d8 82 ed d1 0c 01 a5 b0 80 5e da a1 fd 04 db 09 01 13 ad af a7 89 1d 79 1a 51 3b a3 12 38 d4 b3 87 96 34 db b7 52 46 58 c4 ef d4 89 75 d6 2c f1 9f a2 55 1a 3e 1e 4e 45 1f 70 8c e6 47 44 36 ba 6c 80 0e 6d b5 96 64 e2 90 1a f0 78 a2 b5 c6 60 38 5a 20 63 58 c0 73 56 c7 43 cb 3c 47 8a fe 48 39 4f 20 6d 85 ad e5 d0 a1 12 6d 1c cc 5c 4c 1e d3 0f 6b 5d ad 2c f0 fd 30 c9 a6 64 3f 37 80 e8 3c 3d 3b db ae a4 4c 61 ce e7 6d a4 2b 3a d9 20 Data Ascii: Xd\$o!bVdu,?mb#G-A[qm66\$;(icT==?,>5x*yQ;84RFXu,U>NEpGD6lmdx'8Z XsVc<GH9O mm\lKj,0d7?<=:Lam+:
2021-12-02 20:22:31 UTC	1283	IN	Data Raw: 6c 74 24 a6 b5 24 a7 d3 49 c2 b3 0e ef c7 85 03 54 4d 93 38 dc 47 e7 ec ec 16 6a 4c 3c d3 fd 96 fa 2b f5 cd 83 cf e6 5f b0 61 8b c4 df dc b4 d5 01 07 6d 42 f4 50 1c f4 da 6d 6f 20 a5 85 d5 a1 43 6a 16 3e 9d 88 88 c4 44 3a 48 95 44 26 d2 c9 f0 6f 4f a0 36 b5 41 86 e9 90 47 45 87 3c 4a f3 3e e0 93 1f 9d 34 d9 be 3a e8 6d 45 16 db f2 51 09 55 c1 2d fc 34 69 f7 84 df 49 76 dc ea eb d1 6b 12 7b d8 48 75 c6 29 23 d5 6e a4 58 87 7f 55 1d 8d c1 ad 8b 74 87 39 ac 86 86 da fc 1b dd 0d 20 85 2f 4e d3 ef 55 df a8 33 94 df 32 52 a0 a2 45 a2 08 d1 eb 61 f2 29 d6 11 5b 2e 63 9c 9d c2 74 18 38 c1 5e b6 0a ac 7d 89 8c 52 60 b2 4e f1 81 b7 f1 25 e5 00 df 99 1a 3a a9 4c e9 9c 6e 65 66 ec 31 98 1e 8d fe 76 12 e9 6f 6d 7c 7c 0d fb 36 1a e3 a0 55 8d 2b 0d 5e 50 7f e5 08 5b Data Ascii: It\$!TM8GjL<+_ad!#Cj>D:HD&oO6AGE<J>4:mEQU-4ilvk{Hu}#nXUt9 /NU32REa)[.c\$8")R`N%:Lnef1v0u]+^P[
2021-12-02 20:22:31 UTC	1284	IN	Data Raw: 3a ff ec 8f 24 cb 18 37 b0 11 73 37 92 ac e2 27 86 5b 8a af ab 87 3a 2d f4 51 76 55 67 44 36 29 cc ca ff a7 fd 97 51 c1 32 ab 6f 0e 18 f2 d3 01 07 6d 42 f4 50 1c f4 da 6d 6f 20 a5 85 d5 a1 43 6a 16 3e 9d 88 88 c4 44 3a 48 95 80 a5 b0 f2 a2 0e 93 4f 22 6f 85 5b b1 5a be aa fc 64 5b b4 11 ed 3c 6e 44 3b af ed a9 a3 76 12 66 8b f5 de 26 98 aa 80 ee 33 d9 e7 cb da 45 b2 f2 3b b0 50 bc 52 50 bf 03 10 fd 14 aa 8d 04 34 6c ee bc 0a 18 f4 6c cb 69 76 93 96 f1 35 17 89 30 a5 6c a0 02 60 bd 13 d8 77 22 87 c5 ef 29 37 8d dd 90 13 88 70 0c dc 95 de 5c 67 96 66 05 79 ab 1a fd 0c 35 6a 08 7d df 4f d9 aa 11 35 b2 01 94 55 43 5f 50 b2 53 9b 6e 49 e5 e4 b9 7a 13 05 8d f2 b7 18 f0 c8 0a bd f2 46 20 91 25 df 39 36 df 27 c2 2f 50 3a 9c 08 47 16 ed 0b 3a e6 bb 6f Data Ascii: :\$7s7[-:QvQgD6)Q2omBPmo l/\$zG:O'o[Zd[<nD;vf&3E;PRP4lliv50'w")7p]gfy5j]O5UC_PSNlzF%96/P;G:o
2021-12-02 20:22:31 UTC	1286	IN	Data Raw: d7 9f ba 71 4b 5c 4c b2 b3 55 f2 b3 63 8c 8e 84 b3 0d ac 88 f4 db 4e fb 62 ba 60 73 fa 9c 03 05 90 5f 46 4d 3c fe f5 04 a4 af 7c f2 b5 a9 0c cb 03 55 73 9c ee b0 f6 9c 2a 6c dd 0d e9 21 a2 d7 96 c3 d9 ea fe 13 01 64 58 31 f7 77 4d 55 7e 6e b4 db 0b 40 99 7b 9d fe 68 c1 aa 5b 68 8c 54 03 0e 64 81 42 88 42 ed 2f e5 a7 34 06 79 93 04 31 1e 18 40 3c 8f b0 5b 70 17 d4 be e5 d1 b8 4a 76 d7 b1 5e f8 0b 65 9f 8c 60 05 be be 49 94 21 4c d6 36 e5 28 85 fd 53 28 2e e9 6d e9 cb 86 c3 05 8b ef 6a ab eb 12 7c b1 44 87 00 4c c7 6d d8 e0 b0 79 00 c6 b9 12 c6 a1 17 b7 42 10 2e 5e fe d4 7c 25 c8 75 db e5 05 5d 1d da b0 09 6f 3c 56 e6 be 23 f0 19 a8 11 26 db 9c b4 d8 f9 b0 49 8f 30 d8 41 e4 66 c3 46 e8 8b 13 b0 dd 65 96 38 eb 28 e4 34 75 98 80 c2 eb ed 6e 02 74 e6 3c Data Ascii: qKlLUcNb's_FM<]Us*!IndXlWmU~n@{h[hTdBb/4y1@<[pJv~e!!L6(S(.mj])DLmyB.^]juo<V#&!0AIFe8(4unt<
2021-12-02 20:22:31 UTC	1287	IN	Data Raw: 19 0d 8a a1 13 8f da 9f c3 59 1a 94 d9 4a 06 03 ba 8a 8b 2f 2b c0 af 66 32 3f ef 78 9c 00 1e 94 a0 e3 b0 77 f7 d9 70 49 57 71 97 5e 5f 47 6b 33 58 08 f3 3d 6f 60 f2 d3 02 fc cd b3 22 fc 2d b0 25 f8 bb c2 96 e1 ef 2a 5b 81 bf eb 6c d5 28 e4 57 58 1e aa 16 8a c0 03 1b 85 e2 32 00 1c 28 e0 26 b4 29 ae b2 3c b4 2a ae b1 3c b4 2a ae b3 3c b4 5b ca 4d 58 85 bf 00 bb 2f 42 67 45 f8 5b c4 ee 81 8d 5e 86 df cb d0 3d de 5f a5 bf 6b 06 4a de f0 25 f9 55 ae 91 f3 a3 c2 b7 cc 7b eb 3a a4 8f 73 50 3e 1c 8d 07 db fc ff b8 7b d3 ae 36 92 a4 6d f8 3b bf 42 d4 d3 87 ae 1a 12 59 0b c6 b6 d4 ba 75 63 56 b1 37 8b 6d 4c f3 f4 a9 4d 25 81 16 d0 c2 62 d0 7f 7f 63 c9 cc ca 5a 84 dd 33 f3 7c 79 e7 4c 1b 55 55 ee 4b 64 44 64 c4 15 9a e7 65 df 87 84 d7 83 42 77 ef 27 bc 1e 22 61 1d Data Ascii: YJ/fJ2?xwplWq^_Gk3X=o'"-%*[!(WX2(&<4*<4[MX/BgE]^=_kJ%U;:sP>[6m;BYucV7mLM%bc3j]yLUUKdD deBw""a

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1288	IN	Data Raw: d2 cf 53 45 e5 71 b5 61 da c0 44 ed 53 11 12 9e e2 ef ca 36 ec bb ab c2 2a c8 bf 46 b6 ed 38 f9 ba d4 0e 1e bb 29 8c f9 13 b7 a1 10 3b 7b df 6f 7e 10 06 28 7d f8 96 6c f0 10 c3 05 20 b3 db 2b 8b 9b 13 a7 de 33 67 35 09 4e 27 f9 63 d2 a3 f6 a5 8d 01 a3 76 71 49 45 bf 17 ba 23 0d 72 2f 3b 0a 73 39 17 79 6e a1 f7 8b 1c 8e d2 5b 32 bf a0 19 95 65 ab d0 9f a2 b3 95 7a 81 a8 72 77 a8 d0 d4 af 76 e0 0d 73 08 0c 6b 27 5f 77 e0 b5 fd a5 ad 65 a9 04 92 0e ce c5 2e 33 08 0e 33 40 89 26 6e 26 d6 38 62 21 0c e4 40 58 67 30 30 77 7c 79 89 c5 92 2d 4b a1 8b ed 70 a1 44 27 19 c4 10 19 ee f5 69 d0 1d d2 79 89 cc be 90 6f 29 04 a6 7e 9b e3 27 0a b2 cc e4 41 5d b8 90 a2 5a 79 1c 0d 93 34 04 5a e6 1a b0 c1 bc 55 2c bc 21 9b e2 0e a2 5f 7d 5b 2e fc 3b 5f 62 eb 24 ba 3b 4d 17 Data Ascii: SEqADS6*F8);{o~(Jl +3g5N'cvqlE#r/:s9ynJ2ezrwvsk'_wde.33@&n&8b!@Xg00wly-KpD'iyo)~'A]Zy4ZU,!_][:_b\$;M
2021-12-02 20:22:31 UTC	1290	IN	Data Raw: 11 4f cc 83 3b 56 96 41 e3 09 da be 76 07 44 da 54 62 32 7b 2d dc 01 7f 3b c4 19 aa d9 5c fe 26 be a6 5d 36 72 07 e3 2e 0e 38 83 c8 f3 a4 c2 22 51 05 b0 f5 ec 34 86 32 fc 49 9b 6c 9e 51 ec a8 54 81 c0 af 83 06 ac 43 44 f3 40 73 fb 84 01 99 d4 58 70 ab 12 45 73 77 14 71 d6 66 c2 a6 39 6f b1 b0 ee a1 5f 02 f2 6e ee 6d 58 18 0e a0 e3 88 35 52 80 d6 f6 ba 7e 77 a2 cc 76 71 9e 17 68 c3 bd ff f0 11 b7 5a df c6 50 30 b0 de 2a 5b 55 5a ff 30 2b 70 ac e3 fe 46 69 a5 5f 87 43 ff 44 59 85 4a de a1 de d7 5c 83 69 73 42 4d df 40 ce 9a cc f7 c2 41 90 b9 c4 1a b1 b9 46 66 dd 43 43 76 1b 32 c2 98 79 3c ec 4a ab 82 93 39 57 e8 f9 a3 49 31 30 f0 1a 7a dd 53 20 2e 33 f1 1e 03 5a 43 c3 bd 84 e1 1e b6 56 95 40 51 89 c4 24 a5 17 e0 15 e9 16 0f 70 77 98 c9 e1 15 32 ba 3c 71 82 Data Ascii: O;VAvDTb2[-;&]6r.8"Q42lIQTCd@sXpEswqf9o_nmX5R~wvqhZP0*[UZ0+pFi_CDYJlisBM@AFfCCv2y<J9W1lOzS_.3ZCV@Q\$pw2<q
2021-12-02 20:22:31 UTC	1291	IN	Data Raw: 4c 6a a3 fc f7 94 5a da 26 ce 1b be 0f 1f e2 0c 3c 2b 1b 9a d1 87 3c 67 b0 fe c6 ed bc 66 7d 8c f3 7d e0 ee a6 6c 96 8c b4 9f e2 b4 3c 45 87 b1 d5 24 87 f0 db 9c 86 e7 c3 b3 ce 7a 12 c0 f6 37 b2 7e 2c 89 05 9d f7 53 3a ef 3e 08 c0 67 24 4f 1c 27 32 c5 ab e7 3d 4c 9a dc d3 8f 39 b6 21 8f dd 60 82 51 13 6f 24 0e 51 d8 8d 3a 13 bc c9 e1 67 8a 3f 73 8a 8a 65 17 51 38 1f 7f 1f 9a 9d 58 b7 b3 8e 7b 17 da 5c 81 d4 be d1 03 a2 c0 2b 7a 94 b6 9a 9e f0 7d 5c 9f ba d7 d7 6f f0 16 dd c9 34 61 6f 3c cc b9 5c 7d a1 8a 6a 71 9d 82 ab a8 19 d5 09 5d 72 2d 59 d1 2c 55 c9 5c 8b cf c5 45 a5 94 e6 4e c2 18 d1 0f f9 52 fe 11 07 93 7e c9 d7 71 17 e1 4b 5c 29 cd d0 53 39 c3 e4 4b 9c 22 a9 88 bc 61 55 40 fd e5 97 2c 0a 1f f5 95 1a e3 59 64 f9 41 b4 d0 56 bc d9 4c fc c8 26 e8 24 Data Ascii: LjZ<<+<gffj)<E\$!7~,S:>g\$O'2=L9!'Qo\$Q:g?seQ8X{z}lMo4ao<~}jjq!r-Y,UlENR~qK!)S9K"au@,YdAVL&\$
2021-12-02 20:22:31 UTC	1292	IN	Data Raw: 9e 7a de 45 50 8d 05 cf 18 b9 9e 78 f9 73 bf e6 cd 14 22 31 47 be fa f5 43 71 4f 33 11 5f ff b3 00 28 46 1c 90 f2 cf e3 80 ec a5 76 f2 bc 90 e2 3a ac 80 82 3f de ff 69 d7 d6 65 a0 1a dd b1 f5 5e 82 3b 43 ed 98 0c 69 f5 7f 42 5a e7 d0 c8 39 14 75 2e e9 cc 27 94 a9 38 50 8a 8a f7 b4 45 7f 64 18 fa 27 e3 8a 61 44 31 19 7a f4 d6 a9 1f b9 ae 79 f3 cb 48 86 8b 3e de 32 9a 2e f9 c1 76 9d e1 39 11 6a 8f a0 03 ca 1f 39 8e 22 11 de 03 22 bc b7 8d 03 13 18 ea 36 65 f8 7f 28 19 d8 b7 82 c8 43 9e 9c 09 5e dc 47 e0 ed c5 4e fb f5 15 75 a1 65 06 60 ea 8e b7 06 c8 23 cc 25 ef 3d 82 6e 18 87 93 4c 3a a5 ff d8 a0 7b 61 65 31 ab 0b c4 b7 d2 00 4d dd 74 9d df 66 02 a2 6c 0b 97 1b 72 7e 0f 06 81 f1 b9 04 42 d8 02 ad ff e6 b9 6c ee 9c 80 61 63 d3 b5 48 e1 2e 2c 2d 79 af Data Ascii: zEPxs"1GCqO3_(Fv:?'ie^;:HIBZ9u.'8PEd'aD1zyH>2.v9j9""6e(C^GNue`#%=nL:{ae1Mtf!r-jBlacH.,-y
2021-12-02 20:22:31 UTC	1293	IN	Data Raw: 85 ed 5e f9 88 70 1a cb 48 ca f2 d4 ab 64 0e 74 10 77 ae bc d4 ec b3 92 50 61 e8 ea 54 e9 36 11 19 cd 9d 89 df b2 96 89 68 27 97 28 4e 46 b7 f6 9b 2c a3 16 a8 c6 eb 1a ff 69 f8 a9 21 a1 f1 9d 73 43 e9 56 94 8e 89 e7 5a 46 16 91 7e 6f 49 34 68 49 03 fc 4a 0e b1 7b e9 d4 94 7b 6e 50 79 83 6a dd f8 06 43 1d 54 d4 11 09 af 1b 57 d5 6b 11 26 f3 ce 67 10 83 ca 2f 33 88 4f b7 24 b5 62 dc 64 6f 7e 3c 6a 17 e3 26 7b 66 3c 6a 1d bd 99 f4 0e 9a c3 3c 51 1c 26 c6 71 3e fe 19 87 59 0f 52 cb f9 90 81 66 7e 7a ca 10 b5 9d b7 7b 13 11 d2 5e 30 1c 5a 18 bf 09 c9 f3 a8 16 26 37 36 bd 53 0e 7a be 69 68 01 43 f9 bd 9c 0a d5 15 71 7a 24 82 6a ef 47 4d 3f 81 95 d5 d6 5b 18 b5 89 ed 8a f8 0e c7 48 fb 97 7b ab 36 2f 41 e0 f8 39 61 5b a4 9b 51 c3 22 cb 31 ba 55 93 de 9c 56 d2 19 Data Ascii: ^pHdtwPaT6h'(NF,i!sCVZF~ol4hJ{f{nPyjCTWk&g/3O\$bd0~<~<f<~<q<Q>YRf~z{^0Z&76SzihCqz\$}GM?{H {6/A9aQ["1UV
2021-12-02 20:22:31 UTC	1295	IN	Data Raw: 50 c3 da 7b b3 96 6d a8 65 9b 6a e9 c5 b5 c0 39 fd 56 9e 1b 82 a2 c5 3c 03 99 67 0d 76 92 b8 7b 33 d3 26 64 da a4 4c 77 32 53 75 eb fd 4c 0c 33 93 4e 3e 6d 33 71 ff 66 69 3d c2 b8 c5 d2 ee 65 69 a5 99 18 e5 66 81 29 86 c4 53 4a 3c 92 89 61 c3 cf c4 24 23 e2 ca 85 80 cb 58 8c e7 14 16 21 96 ae 72 1d 1d 73 79 04 ac a4 a1 de 67 62 fa 46 de 8e 4a 37 8d f3 76 8c bc 8f d9 56 6d c4 ad 7a 78 a3 e4 0d 55 ca 83 2a 79 c1 78 a9 20 92 32 e3 0d e7 d6 23 81 d1 16 c9 57 68 43 47 59 36 03 43 a4 3e a9 28 01 a8 42 08 1a 1b 88 de 27 d2 c1 f6 0c 2f 3f cd 2f 10 87 e1 26 22 37 86 69 f6 c2 d6 e9 05 99 32 f9 e4 7d 95 bc c8 95 36 28 33 58 26 f3 08 7e 3b 24 b1 99 70 13 46 b9 82 d8 cb ac ee d2 8d ba be 4f 8f a5 71 8a 96 cb 7c fc a2 5f 0c 86 83 b0 1e bf 72 38 0a 05 5e a8 7b 57 18 12 Data Ascii: P{mej9V<gv{3&dLw2SuL3N>m3qfi=eif)SJ<a\$a#XlrsygbFJ7VvmzxU^yx 2#WhCGY6C>(B'/?/&"7i2)6(3X&~; \$pFOql_r8^W
2021-12-02 20:22:31 UTC	1296	IN	Data Raw: 26 ad e7 08 cd 43 a0 63 04 66 75 d4 26 29 53 07 b2 8d f7 4b cd 78 30 37 75 c4 9b 5a 7d 6a dc 12 d7 a3 b3 b1 01 af 8c 61 9a 7a 3f 44 88 41 56 f8 30 f7 6e cc 8e 6c fa d9 38 57 26 d4 27 b2 52 96 88 2b 17 b1 d4 f9 d2 3c 01 ce b4 e1 b0 5f 15 f4 fc 39 97 78 dc 50 80 35 f7 97 47 50 e3 25 eb fa 80 d7 5b 2c 03 81 91 5c 66 1b d9 81 a8 f1 99 96 01 ee 48 54 45 67 af 0f 14 da 48 53 b2 32 15 e2 99 24 c7 ae d4 36 64 f6 11 1a 0b f7 1b d1 c4 be 8a 44 e7 1a c4 b7 5a e7 1e 42 17 b4 50 ae 6d aa 5c 18 ac 7d 84 41 46 f2 04 91 2a 39 d0 10 f9 eb 70 b9 a2 ff 46 c9 58 58 f1 32 68 62 79 fc b7 42 7f 5f ea 1e a9 51 02 96 69 f5 76 a1 c4 fc ee a8 5d a3 2c f4 34 ab bd 99 cd 60 20 d7 44 5c 06 1f 4b c6 f3 7e 60 3e d1 8d 24 d5 31 0a dd f1 70 e0 60 9d d5 5f af 2a 96 14 42 2e 76 4e 31 1a 0c 29 b7 94 Data Ascii: t! 8khz(m=? 8@*~Eit=KlQ9v!O>o88?^Q*oM\$!.&{>7/[sklOCpdE ~F3H;F3pt@y3qwf7]sSq8%3wR
2021-12-02 20:22:31 UTC	1297	IN	Data Raw: cc 74 f0 ed 21 7c 03 b6 e7 38 6b f2 b0 68 fa b1 7a a2 e5 ba a4 1d c0 07 e5 92 28 0f e9 ee be 6d 3d 9e 3f 7c f2 7c 38 b5 ee f6 c2 fd 0f 40 22 c4 7e 45 7f 1c fe f8 e2 ae b7 11 0e fa 69 1c 7c 3d 4b 5c 9d ee c3 51 fe a7 91 df bd 39 0c 76 21 c5 f7 4f 7f 3e 6f 85 90 fd d4 f8 38 38 0e ca 3f b0 f0 5e d0 7b b8 c7 c2 cf 8c af e7 8f de 51 1b bf ee 1c 9e dc 97 03 b9 a4 0e 2a 6f 4d 24 03 dc e2 69 cd d1 ab 2e 26 dd 1e 14 7b 3e ef 12 b7 8c 16 37 1e 5b d0 8b 2f 73 ee 6b 6c 4f 43 84 10 70 87 c7 c0 1d 64 90 45 20 9f 7e 46 af 1d 03 11 33 80 48 c9 c1 a8 ae a8 c1 93 3b 46 33 df 70 74 9e b3 40 ce b8 16 84 e3 a1 a9 d6 05 1d 79 33 71 98 77 84 7f 05 96 66 0e f0 ed 37 ba 7c 73 93 fc b5 97 a3 e1 f2 53 e8 b5 71 c3 83 99 c3 d0 c2 19 38 16 25 09 1e 33 c2 b1 16 77 52 00 d5 89 a2 90 07 Data Ascii: t! 8khz(m=? 8@*~Eit=KlQ9v!O>o88?^Q*oM\$!.&{>7/[sklOCpdE ~F3H;F3pt@y3qwf7]sSq8%3wR
2021-12-02 20:22:31 UTC	1298	IN	Data Raw: 5f f2 35 23 e9 76 6f 1b e6 50 d7 6f 8b 07 39 06 92 a4 c6 bd 2d 7e 8b d2 cc 2b 2d 49 19 6d d9 6b 18 d7 db 9e 8a 1c be a3 f6 cf 61 c3 23 80 ae f3 ce bc d9 8c a0 65 c1 d4 37 58 71 53 4e f9 c2 e6 25 bb 68 a1 cb c1 ac d0 0b 05 5a d5 ca 01 6b fe 07 05 ee c4 05 62 69 fb 73 fd a2 7f a9 b4 c3 64 69 ad b9 4b b7 53 ec 05 98 62 37 2f 85 da 79 64 e5 82 a9 de 80 a5 be 3a be 0b 47 ec e3 d8 0d 90 a1 93 04 02 63 da 8d c3 91 62 f3 78 97 23 e6 34 52 38 fd 06 9b 81 2f 1f 18 4d 56 bf df 5b b6 ae 2d b9 bb be a6 3d 6b c9 Data Ascii: _5#voPo9~--+!mka#e7XqSN%hZkbisdiKSb7/yd:Gcbx#4R8/MV!=[~k
2021-12-02 20:22:31 UTC	1299	IN	Data Raw: 06 a7 85 d7 07 88 94 35 71 23 96 e8 44 59 47 00 2e b0 8e c3 75 9a 2b 65 f4 4c fe 96 30 08 5a f7 32 64 b6 2f bd 3d ad b8 37 18 ea cd ed 91 df 5b c1 0b c3 41 21 24 7b 57 8c 2c a8 48 6e 1f 32 ac 73 92 2d f9 91 d1 f8 91 2e 7e ab 88 75 8f 19 d2 2f e9 ad a4 cc 9b 24 f9 47 01 58 fd f6 9a 6e 2d 36 9e 22 db 66 20 b4 40 aa 09 56 81 59 b4 af a1 7b 0b 9c 93 f8 9e 1c 99 83 83 4c bf 52 3a 97 58 0e 1b 03 6f 19 de f5 cd 09 ec e8 7e 51 f7 9a bb 31 1c 59 5a 6f a2 95 30 86 e9 1d 50 32 ec e1 f7 8a 38 38 70 ea df 4d 5a 29 07 29 57 ca 24 55 10 dd 7c 61 3c 5f 66 85 e9 de 8b 38 77 74 3a 30 23 36 29 85 1b 48 f6 83 20 57 ae a5 73 86 f8 df a6 c5 20 c6 ae 27 3c 9e 22 df 22 a0 33 35 75 7e 70 94 6e 51 6e 28 3c 71 0e 7b 7d 28 35 48 22 69 c7 e0 43 82 38 56 fe 6f 68 ce c8 36 3d 4e ed b7 Data Ascii: 5q#DYG.u+eLOZ2d/=7[A!\$[W,Hn2s~.-u/\$GXn-6"f @VY{LR:Xo~Q1YZo0P288pMZ))W\$Uja<_f8wt:0#6)H Ws 'c""35u~pnQn(<q){(5H"IC8Voh6=N

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1300	IN	Data Raw: 56 d9 79 72 5e 9e 4b 29 04 9f 40 dd b8 c5 57 f1 eb 37 f9 d7 e4 63 6a 8e 77 31 f7 76 57 76 7c 03 7e 2b 11 71 e4 6b ed 96 d4 4a 4a f5 e4 7d a7 e1 4d 6c b5 0a d5 05 9e e9 56 10 ab 2f 2f bd 0d 2e 66 ff bb 76 44 28 4a ad e5 66 76 0d ed 1e d9 f3 ad ee db b1 5b e9 4c 03 b9 3d f0 48 b7 18 ee 1c ed 38 95 3c ab db e0 27 5b 20 2d 09 7c dd 8e 2f 46 da c3 44 d2 1b 36 73 28 1e aa a4 6e 94 f8 fe 4d fa b1 ba 91 4a f0 7c 93 48 b0 ef 69 b5 eb 65 97 11 cd 65 43 d7 25 22 fc 30 94 2d 3e b7 65 32 a7 be c0 64 d6 cd 9f cb 5b 26 4f 7b a4 18 12 32 a9 44 47 53 d8 58 9e 6f cc c7 f7 6e 43 be 44 43 7b 53 f9 db ef 18 5d 77 6f 13 4d 3f 96 d5 4f 5c 23 8d 67 58 59 48 64 17 5a 07 1f 7b b8 8a b3 f3 19 62 b2 48 cd d5 4d 47 39 f8 55 94 7f df 44 8e 70 df a8 e4 1b c7 0a 79 b0 ab da 59 46 0e ce Data Ascii: Vyrr^K)@W7cjwt1vWVj~+qkJJjMIV///fvD(Jfv[L=H8<[-]/FD6s(nMJ)HieeC%0->e2d[&O{2DGSXonCDC{S}wom? O#gXYHdZbHMG9UDpyYF
2021-12-02 20:22:31 UTC	1301	IN	Data Raw: 2d da 6e dc 51 aa 76 e3 90 cc ac 4b 08 7e 73 27 2b 69 63 79 52 81 b0 53 a2 88 74 72 66 88 d6 f2 53 cc 7f a3 e6 27 ac 2b 3a 3a 94 8c 06 2c 06 64 23 12 d4 f0 2e 4f d9 18 0b 84 d3 a6 12 60 32 87 56 e2 ec b8 93 01 b4 3c b2 6c ad e5 7e d3 7a 35 3a 36 65 9b 80 97 a6 3b 10 a7 f0 e8 8e e9 0e 18 08 6a 86 d7 e9 75 e6 f0 a9 2c 9d f2 91 7c 1f 68 3b 3f 83 0c 42 05 7b 43 24 91 31 07 4a 46 06 68 2f 98 3d 89 e9 16 72 aa 88 a5 62 97 dc e2 8e a3 99 c2 9d ac a9 ae 32 bb ad 4a cf f1 3a a4 6a 8c f0 29 73 d8 2b e7 42 8c 6c a6 0d 8d 65 46 c8 66 08 08 ef 89 b3 f1 49 c5 ef de c6 08 39 84 c1 a4 b2 9a 08 1b 3b 6a be ef d3 e7 66 85 8a f2 9c a6 fd b9 64 a3 5f c3 b7 36 1f b8 02 ed cb c5 b8 8a aa ac 9a 1b ef 7a 60 93 e5 fc 90 9d e7 33 1e 5f 18 f8 33 c5 a1 c2 8c 7d 69 6d 7d 45 94 cc 6b Data Ascii: -nQvK-s'icyRStrfS'+::,d#.O'2V<l-z5:6e:ju,lh;?B{C\$1JFh=-rb2Jj)s+=BleFf9;jfd_6z'3_3jm)Ek
2021-12-02 20:22:31 UTC	1302	IN	Data Raw: 7f 27 2e f1 eb da e3 ad 6f 38 69 5c 55 af 31 c2 c7 a6 cf cd 85 d4 df 11 ec ba 0d 39 9e 6f 12 38 a5 c4 85 86 46 1b 10 c2 e4 06 48 55 12 b5 85 f8 c2 1e c9 c2 84 92 22 77 98 34 ac 81 fe 1a 56 69 68 12 4b a6 b0 ac 9a ec 85 7c 16 f6 66 f3 90 ec 3e 47 16 d8 49 5a 78 df 28 7d f4 86 a2 68 16 96 20 45 0f 36 84 13 05 a9 3a f7 5c ff 16 b7 7d eb 48 75 de 5a 3f 68 7d df da 64 3e d8 22 b6 89 85 41 6d fa 6d 78 08 55 61 8e 7d 94 f9 d1 d2 34 89 33 d2 b4 bd 46 a5 fc 49 c4 e7 36 0c 82 84 47 5b 24 ef 52 af f1 44 e6 89 12 e1 63 4a af a4 06 80 70 6e 1c 23 33 8c 86 18 92 a4 a5 fc d6 24 57 89 32 73 5d 12 b2 ad 5f 14 bb f6 8e 5b 47 14 4c 56 6c 27 07 59 fa d1 25 c6 59 4c ab 79 04 95 0c a5 df 10 99 b4 24 b4 15 e4 b1 25 ae e6 49 38 0a e2 af ec 2f 87 36 96 8f 1b cb 23 e5 38 f1 b3 ca Data Ascii: '.o8iU19o8FHU"w4VihK]of>GlZx{h E6:}uZ?h)d>"AmmxUaJ43F16Gj\$RDCjPjn#3\$W2s_]GLVlY%YLy%#l8/6#8
2021-12-02 20:22:31 UTC	1304	IN	Data Raw: 19 29 73 af e9 2d bd c9 84 12 b1 bd 96 f9 b0 f0 b9 cd b2 5a 6c 49 3e 7c 7b 9b 3d 1e a2 05 98 c6 48 26 d7 34 8d d3 75 fa 80 fa 08 1d fa ce 6b 98 a8 f1 0e 85 af 90 22 96 d7 84 c6 7b e8 c2 c4 7e 64 a4 8b 81 e9 a5 79 f5 33 a1 3f 8f e9 e0 a9 51 6b e3 6b 41 f1 94 e6 0b b8 f0 3b 3a 31 51 97 85 4a 2e 5f b0 03 10 88 45 27 1a 1c 83 5f 3a c6 f5 a4 2b e5 63 c5 b7 32 fd 6d fe a9 c9 10 48 ba 68 7c f5 3d 07 02 6b d0 c1 88 4e 93 74 6b 18 16 ab cf b8 58 9e 6f 5a 45 02 c9 3c ca 43 7e 90 2c 44 84 83 dc 27 49 1b 17 d6 0e 31 25 f1 2c e1 89 df ef cc c4 e9 bc db 88 ed 79 fc ad e1 a1 43 70 ee 33 b1 b0 9f bb 69 4e 59 6a e2 d8 09 92 f7 7b 7d dd 3d 62 e6 50 99 b1 4f ec 2b e8 5b 46 f7 65 78 c7 c0 ef 84 4a 2b a3 07 f5 dc cc e1 35 f2 b3 a7 35 71 ad 06 c8 6c 82 c7 f0 8c cb 77 c5 32 a6 Data Ascii: :s-ZlI}[-H&4uk{"-dy3?Qkka;:1QJ_-'_+c2mHh}=kNtkXoZE<C-,D'l%yCp3iNyj[]}=bPO+[FexJ+55qlw2
2021-12-02 20:22:31 UTC	1305	IN	Data Raw: ba bc 96 b8 c5 b8 c9 31 94 35 54 eb 1d 37 73 b7 05 b3 b9 59 95 11 20 9c 7a d2 fe 74 4b 6a d1 b7 e5 df af 34 ed 64 86 c1 ae 3f 52 83 5f ce 53 e6 13 5e 00 47 aa 34 ae 13 01 43 76 75 d2 46 7e a1 6c 09 7a a6 92 53 82 5b dc d5 16 b1 2f 5b 7c 6d cc 79 fc 38 84 c1 6c 9b 3f cc 7c e4 f3 d9 4f f8 7b 0e 3d 8b d2 76 60 39 4a 47 36 d2 f3 c9 08 0c 25 b6 97 4b 0c 56 0e 67 89 b5 88 04 05 8e a2 b2 4d 0e af 8c bc 39 4f c6 cb 9b 85 d6 a5 cd 8d c0 eb 45 19 7b 24 65 f7 1b 39 71 22 f6 e4 4e f8 d0 e3 09 44 06 8c 03 84 d3 2d f8 14 82 40 82 72 d6 3f 9b ec 29 1a e7 99 cc c6 46 55 df 40 9b b6 89 db c5 08 78 cb cf f3 45 be b4 a1 b3 42 c3 eb a1 3a f4 6e 48 21 fc f8 d0 91 1f 86 e9 0f 9b a9 d3 60 93 9f 93 df 89 f4 0e 9d 9f 60 de 11 b3 fd b3 23 06 fb 7f a7 0e 98 72 1c b2 4c b6 32 32 Data Ascii: 15T7sY ztKj4d?R_-'G4CvuF-lzS[/[[my8l?]O[=v'9JG6%KvgM9OE{\$e9q'ND-@r?)FU@xEB:nH!'?'#rL22
2021-12-02 20:22:31 UTC	1306	IN	Data Raw: 2a 86 fc 0a 5d 56 c4 cc c9 b3 b6 8a 19 d7 8c 3c 51 a3 2d f3 c0 58 35 e0 05 7d 20 4d 45 c8 6c c3 69 18 6d 3d dd d9 ef ec 66 4d e9 00 ff 7a f7 f7 eb 1d 2c 38 e8 89 f3 0e ce d3 e9 c8 0f 97 ad 77 d7 d6 32 26 bb fa bf 7f bd bb 5e fe ab c8 7f b3 29 ae fe 7a fc fb af 15 f3 cb bb ab bf 9a 90 b6 a9 5e 70 0b 5a d5 2c 9b 42 6a 32 f8 04 c3 88 46 31 c5 d2 5f cb 32 e2 16 ec 55 f5 54 92 6a d5 6b b8 e4 43 e3 83 c0 d9 0f 97 96 d4 af e2 68 3a c0 72 e9 e2 38 18 52 30 4d af 88 21 50 b0 98 e2 70 d4 8d ba 03 82 e5 4f be a2 3b dd f9 c5 bd be fa 4e 7c bd 3c 23 db 8e 06 f2 f5 23 1c 32 b6 34 f0 f4 8b d9 63 a7 db 0b a5 dd 8d 67 66 d4 b2 95 ee d8 7e 35 de 7c 1c 82 0d 44 7a ec 62 dc 42 5a d8 70 d8 36 ad c1 6d d8 ed 77 86 d1 4d 70 37 b8 f3 fd e1 b0 7d d7 eb 76 fb ae db 81 ff a0 b9 Data Ascii: *}V<Q-X5} MElim=fMz,8w2&^)z^pZ,;jBF1-2UTjkCh:r8ROM!PpO;N <##24cgf-5jDzbBZp6mwMp7jv
2021-12-02 20:22:31 UTC	1308	IN	Data Raw: 2d 3b 86 b1 36 62 c8 42 bb 41 31 a3 c6 08 1d b4 e1 df 4e 91 8c f1 cf 48 40 11 78 a9 3d 8a 6f b4 6b c0 c2 d5 2c 87 a2 04 8e d4 b5 38 bc 10 e9 6e e0 a4 9c f0 43 2b d8 1e 8e ce 5d cf d6 71 55 46 57 23 a9 31 5a 01 aa 05 1d 89 77 de 54 0f 70 86 1a bf be 82 74 31 65 5b 2a 33 b8 42 70 e5 5d b3 31 80 74 07 2e 89 08 fe eb 07 7d d2 d3 f4 51 4f 23 a9 d3 3d 24 ef 5f d7 2d 6f 34 7c 1c 93 3d fc 7d 11 17 40 33 82 1f 30 99 35 2b 02 56 42 bf ed a8 b7 fa 48 d5 df 96 96 e0 6f 77 d2 0b 81 54 25 5b 8c 28 52 ee a0 db 46 88 5e 87 4e cf a5 a5 05 38 86 a8 28 67 e6 da 2f 30 8a c0 b1 5c d0 b9 15 e2 5b 21 db a3 df 46 02 da a1 9f 3a e2 ae 37 05 1e 58 bf 68 cf 28 4c 2e af 95 97 e1 40 f2 b4 b5 17 83 75 a9 99 0b 06 c3 77 65 e6 68 38 60 bb c8 20 c1 f1 20 82 83 30 6e 86 8c 05 fb 46 09 Data Ascii: -:6bBA1NH@x=ok,8nC+)jqUFW#1ZwTpt1e[*3Bp]1t.)QO#=#_-o4=]@305+VBHwt%{([RF*N8(g/0)!F:7Xh(L .@uweh8` OnF
2021-12-02 20:22:31 UTC	1309	IN	Data Raw: 9d db cc e2 0a d4 f0 bd d2 f5 62 aa 6d 74 62 dc 76 f0 5e df 06 11 af 37 69 58 d4 23 54 0a 27 b2 3f ad 68 37 79 11 c7 b3 d9 1a a0 27 dc ca a9 dc 49 2b ad f6 0a 87 ef 74 bd 5e 68 5d 37 2c 0f b6 cb d2 9a 02 98 a5 53 5b d2 35 a4 7c f1 25 36 17 90 09 8f c2 08 fc 11 29 db b6 17 a8 ff b0 75 b8 b5 f2 85 e3 29 61 3d e5 62 89 af 96 3a 0d 6b eb 68 f3 ef e3 ed bf 4f 90 09 b4 96 7f e0 01 0f 39 36 f8 ba 79 05 17 11 e4 f8 bd 0f fb a6 0b 14 7f f2 6e 14 f6 50 3c ad 17 bc e1 74 10 b8 a3 e7 86 f5 fb 72 67 f9 77 eb 77 98 a8 07 90 15 da c2 17 91 e8 f0 dd 51 6a 54 1e 1f 1f 57 30 70 e2 ca 74 04 cd c3 d1 c0 58 90 0b 6d ba 15 bd bc 47 78 87 a0 78 1b 3e 37 83 c6 0b fc a9 d1 c3 ac 06 4f 33 47 c4 f0 4e d9 06 b6 a9 d5 eb 3e 7a 41 af 1c 00 cb 34 45 1a 72 0d 03 72 8a 61 c2 c3 81 a5 Data Ascii: bmtbv^7iX#T'?h7y1+*'h7,*S[5]%6)u)a=b:khO96ynP<trgrwWjTW0tpXmGxx?7O3GN>zA4Erra
2021-12-02 20:22:31 UTC	1310	IN	Data Raw: 33 52 2b ac 17 e4 08 49 a7 c6 a1 ef 4f 47 18 e7 c7 1d 04 84 05 49 67 67 62 32 7d 0d 67 ee a1 43 2e 5e 39 90 1e 8f 66 a1 51 fa 77 e6 ee f5 35 28 f6 a9 17 cc fe 96 14 c3 be 9b b7 ab de 4c 2e e9 60 dc 28 9a 4d ec df aa e2 7b d5 a9 ff f6 4f 59 8c fa 9c 0b 57 f2 da c6 68 53 e4 0c 33 e9 10 2c 5b 86 be b7 15 4f c2 78 0b 32 c3 c5 c4 79 d9 b0 3e 87 ee 28 c4 ed da ae 07 f6 3c 16 28 8e 5c 45 e8 71 a1 be 64 76 57 cd 13 72 26 9e 53 7a 29 13 fc ca 87 65 31 19 4d fd c9 70 84 b8 6a b0 72 2f 82 ba 83 2a 94 4d 0f ad 14 36 bd 64 12 f8 5c ec f5 89 f9 a6 5f 8d a7 90 9c 9f cc 31 91 9f 50 f6 16 4f 61 1e 9c 8c 0b 29 cc 5b e2 3e 8e 5b b2 2a 63 ea fa 2a ea 18 4d 5e 10 c8 53 45 b1 a9 32 60 3d 26 19 35 4a f5 d1 1f f7 f5 e5 e5 91 23 13 5f 8d ae 8b 17 fb d0 60 4e 0d 8f a4 52 8c Data Ascii: 3R+IOGlggb2}gC.^9fQw5(. (M{OYWhS3,[O'2y>(<(EqdvWr&Sz)e1Mprj^M6d_l_PoA)[>[*cM^SE2'=&5j;_NR
2021-12-02 20:22:31 UTC	1311	IN	Data Raw: aa d9 3a dc 3a 3a 2f 42 b5 f0 ae b0 f5 05 1e 0a 67 bb eb 07 07 58 d7 42 01 ef 69 8e 4f b1 89 85 8d e3 93 cb d3 d6 ce ee 79 61 f7 f8 60 73 0b 5e 7e de 82 b6 ad 7f 3e d8 e2 ba a0 5f 1b 07 eb ad 43 51 d8 5c 3f 5c df d9 a2 5c c7 50 0c 74 0f d3 71 03 0b 5f 77 b7 f0 1d d6 b8 0e ff df 38 6f 1d 1f 61 4f 36 8e 8f ce 4f e1 51 40 47 4f cf 75 de af ad b3 2d 51 58 3f 6d 9d e1 98 6c 9f 1e 1f 42 1f 71 4c 21 cb 31 95 22 01 b0 b1 18 1c ef e4 b4 40 12 7c be 38 db d2 25 16 36 b7 d6 0f a0 30 98 a3 a3 e4 24 e2 a4 ae fc 37 ff 07 d4 85 ec f8 d9 2d e0 47 af eb 09 b4 16 f0 3b 48 6a a6 83 00 e4 a1 e4 12 97 9b 6d a1 c0 3e 57 ef de 45 b0 a3 a7 1e a1 ec f6 5d 0c 50 fe 0e 4b 79 e7 f5 86 1e bc 18 4f e4 8b 62 07 9a ce 3f a0 07 64 0b 37 6a bb 7e a8 96 ed ef f8 ed f7 42 84 b6 81 b8 aa a7 Data Ascii: :::/BgXBiOya s^~>_CQ?\\Ptq_w8oaO6OQ@GOu-QX?mlBqL1!"@j8%60\$7-G;Hjm>WEjPKyOb?d7j-B

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1313	IN	Data Raw: 35 e8 a9 c2 4f f5 76 15 27 ac f4 54 6b 9b 6b 22 5f b5 6d 5a 54 14 0e 80 6d f5 6b 0a 54 ed d4 97 75 ca 98 87 68 7e 8d 20 9a 72 c8 e7 be e5 26 e6 ba 0c f9 14 ee 17 b7 70 04 8b 65 d3 68 54 d7 9a b4 98 b4 70 a5 59 6f 70 34 44 b7 68 ae fb 4a c7 97 2e 52 24 6a d2 68 d6 aa 30 aa d0 3a 51 09 2d b4 9b 8d 46 ad 59 d4 c2 12 57 b8 be 6e 56 f4 a2 d6 29 71 66 38 ec 2f ea f3 a0 68 9b d5 d6 46 b8 69 b6 ab 95 3a 1e aa 6d 2e 46 4f b5 76 7d 2e 94 58 31 48 03 15 74 01 48 ec ad 07 3c 92 a5 41 18 8f 8d 80 e3 b3 2f 75 df f8 a7 dd d7 0d d1 f9 2e 61 74 f1 dc 0e db 9a 1c 84 4c a0 b9 7b 08 37 36 36 9a 6d 4d 0d 4a 7e a1 f9 e5 2f 66 b5 ad a9 a4 7a 45 24 b5 0c 55 bc da 92 99 56 9a 35 3d 99 9a e3 5a 17 53 43 24 44 c1 a2 a4 bb 01 6c 4e 56 b7 fe a8 fd 8f b3 82 ae 35 1e 2a f0 66 8f ce 9a Data Ascii: 5OvTkK"_mZTmkTuh~ r&pehTpYop4DhJ.R\$jh0:Q-FYWnV)qf8/hFi:m.FOV).X1HtH<A/u.atL{766mMJ~ /fzE\$UV5=ZSC\$DINV5*f
2021-12-02 20:22:31 UTC	1314	IN	Data Raw: 74 e1 53 be 54 b2 3a 36 98 8c 60 73 56 a7 d1 b6 67 e0 af 89 f5 0b 68 9d ae ea aa 66 20 49 d7 be 4e d5 17 94 ec db b8 be 00 f5 cd a5 af 2c 7f 9d 47 3f e7 c2 54 1d dc 1e c4 20 3b 4e 51 0f 97 88 2a f1 eb 2e d1 51 22 e1 46 20 9e 8e 06 84 3b fc b4 33 86 a1 3b 38 12 4c 32 23 f5 34 b4 1b ab 35 5e 6c 1d 4a e8 ac 87 16 e1 be ce 9c 1a 2d b6 ce 39 88 25 0d 55 b1 88 22 e7 76 d7 ee a8 49 a6 fe da 15 bd cd d9 08 e6 72 c9 5a d5 0d 89 4a e2 24 35 55 ba ba d1 dd 2c 16 bb 6d 22 2f 54 6a 20 56 af a8 6c 20 96 f5 be 4f 60 64 1a 43 0b ba 44 98 4c d9 98 60 ba 8d 26 ba b2 a3 a8 0d 7c 98 b9 6e 77 ac 4e a9 a4 33 8e 7b 38 47 1e 08 66 b2 23 1a 56 a8 6b 4a 1c 44 c1 52 e9 dc 90 f9 4d dd f0 d3 19 4b 25 c0 e4 9c 47 99 78 f5 0d d9 61 01 94 22 7e fc 08 dd d1 79 2d 86 ca 86 ad 9e fd f3 cd Data Ascii: tST:6`sVghf IN,G?T `NQ*.Q"F ;3;8L2#45^IJ-9%MU"vIrZJ\$5u,m"/Tj VI O`dCDL`&[pnwN3{8Gf#VkJDRM K%Gxa"--y-
2021-12-02 20:22:31 UTC	1315	IN	Data Raw: 30 76 58 40 74 9a fb c4 ce fb f5 71 dd 45 9c e9 db e3 99 16 89 ca a2 f2 23 81 bf df 53 f8 eb 94 9d a1 44 5a fe ef ba eb 19 40 81 db a1 c1 2a 6b 87 96 5c 40 f0 6b 22 28 34 e1 b5 a6 5e 49 12 a6 5d 2f 92 54 c1 b8 5f 06 c6 35 7e 7c 62 11 91 99 08 4f cb 98 d9 c4 c0 16 03 b8 ed da 12 8f 60 b9 76 3d 30 bd 6f 11 4d d5 23 72 5e a5 29 a0 86 46 0e e3 15 1e 48 1e 1e 49 8e 90 2f fc 76 cf ee 8b 2c b7 6e ad ac f0 33 55 68 33 db 43 6f 78 02 9b 8c 97 62 51 bd 82 ff f9 e9 83 f5 62 76 8a 28 27 be fa e2 2b b2 89 ec ff 2f 24 f8 eb 63 4b b7 ee 49 f8 6b 95 b4 71 c9 c7 f1 e0 98 70 b4 85 9f de 6f 20 82 6f f9 86 b8 03 da 53 ef 45 12 ad 0d 21 21 c7 e0 b4 14 38 e7 4a f4 23 ae fa cc 5d 19 9c eb 1b 1d b1 31 96 4a 24 3c e6 94 da 7b 9d 21 bb 09 a7 01 23 27 81 10 7f a5 c8 6e 40 b8 ad Data Ascii: 0vX@tqE#SDZ@*k!@k"(4^I)/T_5- bO`v=0oM#r^*)FHI/v,n3Uh3CoxbQbv('+/&scKlkqpo oSE!!8J#1J\$<{!#n@
2021-12-02 20:22:31 UTC	1316	IN	Data Raw: 60 19 2d 47 5a 8c 4d cc c4 27 48 58 e2 42 a4 54 97 88 97 23 f5 eb a9 52 6f 92 15 7e 8e 92 85 33 1b bb 25 3d 7f 86 38 29 e5 c7 cb 40 d4 e0 f5 c5 6f 10 15 11 2b 3c 51 db f5 95 fa 84 9d 5f 64 bf f4 13 19 6e 87 d2 5b b1 bc 3d 30 92 99 58 a3 28 1e 5f 5f 88 5f 47 66 dd f5 64 56 19 ae eb 26 94 dd 91 ef bb b2 7b 6f 65 fe cf 2a 9f 2c b7 23 9b d8 96 bf 03 59 ff 61 57 fc 7e 70 54 9f af 3c 65 25 39 f3 35 d3 ac 37 a5 6f 87 db 20 99 5e ad 2a a7 fa 6e 22 79 b5 a5 5b 9f ea 9a ac 27 7e be 0d e2 67 9c 75 88 07 39 d4 5b d9 85 93 ae 9d 4b c0 c8 4f 36 a7 3a 71 93 6c ad b1 5a 8b ab bd 51 d5 4e 25 64 f8 74 5b 5c 7a c5 91 eb 63 e5 84 b1 82 a4 77 c2 eb 2e ac 3d 04 d5 13 2b 55 00 4c da 93 f0 cb be 6c 63 5f 41 53 a2 d7 81 2c f8 46 be bf ba b0 2b 49 ab 0e b5 d5 70 40 ec 87 87 17 52 Data Ascii: `GZL`HXBt#Ro~3%=8)@o+<Q_dn[=;X(____GfdV&{oe*.#YaW~pT<e%957o ^^n"y]"~gu9j KO6:qlZQN%dt zcv.=+Ullc_AS,F+lp@R
2021-12-02 20:22:31 UTC	1318	IN	Data Raw: 6f db 29 1f 4f 54 3a 22 9f 6f 88 07 be 98 5b b4 23 31 f0 2e c8 82 11 47 5e 8a 9c 2b f7 d9 81 5d a4 3c a0 e1 04 0d f5 0a 60 57 64 f0 0e 99 14 09 59 3c 28 36 9f 90 8e 6d 03 4e 64 4d f2 d7 29 9b 50 88 60 b9 52 a9 d5 a5 ed ad c4 9b 30 ab b2 a8 8b 95 8d 00 e6 71 30 4f 2c 05 3a c1 61 3d 60 fb c1 aa 11 94 78 0c ac e3 0a 1f 1e d6 6e e9 4f eb 05 13 a7 d6 06 09 74 c8 0a 39 d0 c3 37 d0 cc 8d 0e d1 b4 f5 8e ee da 1f 61 65 0f 71 8d f9 ec 96 2d 2c 02 03 7b 4d d8 be 8a e0 4b ef 02 87 43 d3 00 57 06 d6 00 03 cf b9 f4 cb f8 dd a5 07 a5 f5 18 40 8f 11 d0 4f e0 d9 e6 fa 3a 5e e9 e5 92 4a 41 91 65 d2 f3 e0 c2 0e 8b ab f4 70 d8 15 39 06 17 f4 b2 ed db 48 e1 1c 3b be fd 9f ff 68 1a be e0 34 44 7f 49 db d3 20 d2 86 c4 77 57 ff 46 9d f8 c4 da 90 58 0c 47 45 48 be 4c 27 8a bc 24 Data Ascii: o)OT:"o[#1.G^^]-`WdY<(6mNdM)P`R0q0O,:a=`xOt97aeq;,{MKCW@O:~JAep9H;h4DI wWFXGEHL'\$
2021-12-02 20:22:31 UTC	1319	IN	Data Raw: 58 cc 27 8d 5e 21 9b b1 ca 40 42 90 88 36 c3 5f 57 47 a6 81 9c 02 cd 4b d0 75 c1 79 11 eb ed 4b a5 42 20 89 9e c1 24 90 64 fa e6 9a f8 5d ad 89 df 35 53 fc 9a 15 99 40 9c 9a cc c9 ba 09 7f d3 c1 46 e9 f1 39 8c 54 13 09 21 cc 70 a0 8e 81 a6 60 53 64 a8 e9 38 95 68 3b 44 58 8d 47 f1 82 45 6f 96 9e 59 20 90 d9 40 28 59 20 51 92 27 e2 43 b2 3b 96 6e 63 61 65 56 22 6a 3d 0e 26 33 c4 12 89 b1 c7 49 a0 0e 44 aa 4e f9 62 d4 1b 6a 85 82 de 26 b8 4f 06 90 a1 3a ac f4 16 92 91 03 29 0a b6 bb 10 a1 f8 ba 99 1e 12 17 42 0e 93 17 78 48 e2 75 b1 a7 e0 97 40 3b 48 15 8c 38 89 88 8d ed 26 66 90 4f af 99 b7 a6 ba 25 19 72 51 ed c3 03 e8 10 25 c6 77 4a e4 08 84 e4 da 6b a4 1d b1 f6 92 14 aa 93 e5 7d 75 31 c4 23 7a 1b d3 04 c6 b4 2d bc c4 15 0c 38 d7 49 d5 e7 06 29 d1 7d Data Ascii: X'^! @B6_WGKuyKB \$dj5S@F9T!p`Sd8h;DXGEoY @(Y Q'C;ncaeV"]=&3IDNbj&O;)BxHuD48l8&f O%rQ%wwJk}u1#zk-8l}}
2021-12-02 20:22:31 UTC	1320	IN	Data Raw: f4 57 8d 28 8e cc ca ca 8b 2b 94 a1 9d 84 96 57 ea 03 a7 43 34 ae 53 ed 7a 3a 18 b2 1f f4 83 0e dc b4 22 c0 99 70 a8 eb 07 e3 de 4d 20 7c dd 4e 66 57 c1 d8 eb 3b 13 f8 94 4d e4 94 ec cb c7 98 65 d1 ce ea e6 ea 1a c9 1a 95 2a fe b4 f0 07 af 66 8d fe 54 e9 4f ad 51 37 ea f5 a6 89 3f f4 5a 5f 6d e0 0f 65 69 e0 43 a3 b1 2a dd 58 5c a7 89 ea 52 5c 49 37 c1 51 bc 56 ec 83 19 33 14 c4 ed cd 24 d9 57 91 7c 54 d2 d1 bb 28 50 13 c7 13 fa 94 e0 d3 9c a1 d3 bf 9b f6 bc 89 8a d1 35 18 d1 1e cd 51 e2 cb d2 77 ae 8a fa 76 28 be a8 70 ee 22 b2 9a a5 1a 79 ff 6e 31 32 93 07 92 dc b5 3d c5 63 5c 44 a7 37 dc 8d eb 03 39 3a b9 52 e5 32 c5 19 93 d3 8f a2 66 aa 30 be cb 75 47 7b c3 37 1c 4d 57 38 5c d3 54 bb 6e 20 ce 25 00 f6 69 61 ef e5 5d ae ff 49 ed 72 fd 4f f1 2e e7 46 b5 Data Ascii: W(+WC4Sz:~pM NfW;Me*FTOQ7?Z_~meiC*XIRU!7QV3\$WjT(P5Qwv(p"yn12=c D79:R2f0uG{7MW8 Tn %ia lr O.F
2021-12-02 20:22:31 UTC	1322	IN	Data Raw: 52 b6 9f 0b 5b 7b bb ba 6a c4 49 57 50 d6 b7 ab 2d 63 81 7b 78 49 9b 06 a5 af 2d a5 13 6f 48 1b 51 9b da 5b fc 22 22 67 d1 27 73 e9 13 89 60 94 5e 5d 4a 87 20 41 e2 4c 48 1f 6b 46 9a a1 79 29 48 3a 7d a9 2f 7e e1 ae d5 1a 8b c9 51 fb cd b9 71 cf 50 f2 00 a5 fb c6 59 e5 9c 38 08 fa 35 cf ed 2a 7e ab e7 76 0d bf b5 73 bb 8e df 3a 6c 28 e8 b7 71 6e 37 f1 db 84 b1 06 fd ae c2 20 83 7e 5b 30 f0 a0 df b5 73 db 44 45 ba 71 43 f5 3f 3e 18 d3 c8 3d 02 b6 ea dc f8 96 90 d0 0a ae e3 5d d2 c6 8c b8 c0 ff 56 e1 73 33 82 e0 aa d0 ba ff a6 bf 33 19 c0 46 84 f9 45 a3 a8 24 bf 14 a9 39 bf 10 0a 18 31 62 3c 74 67 d8 11 91 90 48 96 a1 fe 8d 6f 82 f1 bf 45 68 df 89 50 d9 25 c3 d9 23 f2 0a 95 9f 0d fd 48 66 c8 17 64 f0 53 3f 74 96 4e 1d 3a 09 8b c0 0b fb 62 aa 45 12 99 48 42 Data Ascii: R{[i WP-c{xI-oHQ["g`s^")J ALHKfAy)H;)/~QqPY85*~vs:(qn7 ~[osDEqC?>=] Vs33FE\$91b<tgHoEhP%~HfdS? tN:bEHB
2021-12-02 20:22:31 UTC	1323	IN	Data Raw: 71 fd eb 22 b2 77 c1 73 40 2c f0 5d 36 a8 79 dd ce 85 ab a7 8b f2 64 34 9e 6a fb 90 ab 50 07 8d 85 60 0d da 44 ab 45 b8 fc 63 dc 89 bd 5e f6 d1 a0 9d 6c f0 e1 01 17 70 53 75 89 97 41 90 66 66 09 39 b1 8a 31 d9 7c 8d d7 e6 27 65 8f f5 82 08 91 d8 2c 71 88 a1 d2 6f 16 47 7d 12 71 d4 27 ef 1e 3b 50 78 ad 0e 14 f6 d2 dc d4 a7 98 99 32 0a be 1b 1d ac 38 60 99 a7 da 5e c3 f8 24 99 89 fd c5 75 17 b9 f5 f5 02 ec 8f 5e b0 59 ea 7a 70 4d 02 43 6e 42 cb 87 07 7e fd 00 5d ea 87 2e 96 0a b2 98 6d ce 6a b6 53 1f e7 c6 ce 32 ff 7b 91 90 31 fa 91 3b 0c e9 e0 a0 2b 39 9e 9d 24 61 65 8e e2 17 eb 51 15 60 6c 6f d3 40 79 27 ad e8 68 d3 2c 99 46 74 d8 01 de 5a 7b db 30 de ea d6 db 64 ab df 33 18 d8 43 51 05 49 c8 05 a9 bf 7e f7 08 fc 8e d8 bd 11 1f 44 da c9 6a ad cb f2 eb c1 Data Ascii: q"ws@, 6yd4jP`DEc^lpSuAff9l 'e,qAoGj;q';Px28`^\$u^YzpMCnB-].mjS2{1;+9\$aeQ`lo@y/h,FtZ{0d3CQI~Dj

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1324	IN	Data Raw: 42 d6 2e 4c b5 63 3e 6c 64 90 bf 5f 46 69 15 8b 8c 29 25 da 8b 5b a3 a9 80 36 1d b7 3c 83 95 95 a0 bc ed 11 2e 32 65 f2 75 43 23 2e 4d df f4 6d 2a 82 2f a9 3e 2a 05 b8 d6 91 57 c5 69 ea f9 a0 7b 0a 33 6d bd ed 31 0c 8c c2 6c 58 d0 39 45 10 ff 6f 29 45 88 71 b2 dc d9 25 d3 e4 e4 65 27 34 31 1e f5 fb 41 14 34 58 1c 9e be 6d 24 37 87 45 db df c9 81 44 6c 65 95 e8 29 45 78 da 1c f8 62 29 e7 57 6f 29 69 c7 59 4a 1a 2e 27 7d 5d 4a e9 2c 67 ba 5d 4e 3a 58 4a f9 bc 94 72 b5 5c ec f5 72 d2 6c 39 69 ba 9c b4 b3 5c d5 52 ca db a5 94 ed 65 b0 cc 96 52 0e ed b3 4f 15 ed 67 d7 99 ba bf 95 b7 a6 46 8e c8 21 3d bd 1e 18 13 7e e8 f4 e6 ba 11 e7 f8 3e 31 44 86 ef 63 99 c1 4f 67 70 a7 32 83 37 91 19 de 5c a6 32 78 2a 83 af 32 4c 7f a4 32 04 2a c3 96 ea c3 5e ba 86 50 65 78 Data Ascii: B.Lc>ld_Fj)%[6<.2euC#u.Mm*/>*Wi{3m1IX9Eo)Eq%e'41A4Xm\$7EDle)Exb)Wo)jYJ.}}J,gJn:XJrnrIñR eROgFI=->1DcOgp27l2x*2L2*^Pex
2021-12-02 20:22:31 UTC	1325	IN	Data Raw: 0c a2 f2 56 11 a3 28 7d e1 10 40 ff c9 9a f8 8b 65 4d 3c d5 fc 51 89 22 d9 ba fa 48 c9 1b 80 c9 31 3a b6 2f 49 06 d4 b9 b0 fe 93 e5 8d 4f f8 ed 94 5f 85 52 25 fd 2a 2c fb bd c9 d5 68 12 80 3a a1 90 54 fc 86 ac 28 24 49 29 eb e6 52 dc 9b b4 30 f3 5a 98 2e 2d a4 ce 64 2a ef 59 6a 8b 82 48 f5 99 45 aa cf 0b 16 fa 44 e5 96 39 c7 b3 73 50 12 cf 99 6a 57 9a 24 14 b1 4e 58 27 52 7a a5 2d 93 ce bc 43 e3 53 84 eb b4 91 75 6c e4 24 e9 6a fa a6 66 4c fe 1a b1 07 4d d0 e9 1f 99 74 3a 8f 1d e3 89 5a 48 a6 8a 90 69 be 34 e8 6c c2 af 46 2a 8c 6d 41 db 5f 85 82 b6 5b b9 cf 8f 4b a2 52 77 2e 84 bf 88 8e 8c ef 52 ee a4 96 a0 f8 8c 6f a9 9f 2a 72 8e d8 37 5f 85 96 1f a3 8e e5 f0 1e a7 96 92 2f 4d 77 a9 7a a5 7d a7 5d 8b 36 89 bb 9f 0e c4 b7 f9 13 a2 2e ab 8c 3f 66 cb ba 2e Data Ascii: V{()@eM<Q"H1:/O_R%*,h:T(\$!)R0Z.-d*YjHED9sPj)W\$NX'Rz-CSulj\$LMt:ZH4IF*mA_[KRw.Ro*r7_/Mwz]}6.?f.
2021-12-02 20:22:31 UTC	1327	IN	Data Raw: cb 84 a4 93 86 9d c5 fb 38 62 c5 71 f7 56 e1 bb 68 61 dd 35 c4 da 30 2b 2a a1 29 13 a2 1c 55 99 50 55 09 a6 5a 9e e2 a7 22 7f 4d f9 1b e5 5b b3 fc 20 74 66 fd a9 4a 98 f5 d1 0b d6 63 6f 36 d8 1f ca 6d f6 5d 5f 98 db 64 51 90 30 1a 4f b8 44 41 5e bc fd 8e ad 68 b8 3d 1a 0e 03 6f 4a 9b 9a 4c d8 e9 4d 3c 99 b6 19 aa f5 0d 10 df 68 a1 11 2f e1 24 dd 51 56 22 76 2e 24 6e 54 e4 fb 12 a8 7c 35 5d 91 24 99 cf b7 91 2d 20 79 5a 70 70 8b e2 5d 6c 77 d2 01 a2 f2 89 97 49 f4 bc 7c 09 76 47 e7 06 92 06 80 41 9a 07 64 d3 1a bf 7c e5 6a d2 e5 93 30 1e 19 6f 5b 5d fb 48 eb 1a ec 85 b0 63 9f 6a 1d a3 69 74 23 64 38 84 57 02 18 07 e9 46 5d fe b8 ae 7a 1c c3 a1 22 f4 a8 77 bf 3d 11 22 96 18 e6 e1 9f c0 3f 83 e7 54 13 a2 28 27 4f 08 c2 99 bd 48 b4 42 73 02 58 fb f0 b1 81 ec Data Ascii: 8bqVha50+*)UPUZ"M[tfJco6m]_dQOODA*h=oJLM<h/\$QV"v.SnTj\$]-yZppj)wl/vGAdJj0oJHcjit#d8WFjz"w=? T('OHBsX
2021-12-02 20:22:31 UTC	1328	IN	Data Raw: 3f 1c e5 25 bf 98 8f 39 2c 55 4d b9 a0 7c 2c bb cd 05 06 56 7a d0 98 d8 a9 c0 3a 91 14 e0 8c ef ca c2 6f 4f ec 91 dd 51 d7 24 5c 25 45 10 65 7e b3 20 f0 1a 0b 61 47 46 db 16 7c fb 4e a5 4b 72 81 5b 38 3a 13 61 3b 02 44 8f 50 7a 19 19 34 f2 a8 2f 80 d7 87 1b 61 5a c9 88 ad a2 56 3c 68 6c 93 da c9 76 ce 68 04 46 77 87 da 4f 31 a1 b8 79 b5 e0 f1 b3 10 12 cb d9 e7 50 70 51 c4 f1 42 ec 27 91 d3 bf 79 ed 54 b1 d1 21 e5 f9 85 72 1d 19 0b 80 dd 1d 36 b5 c2 c7 6e a0 7c 3f 06 f0 02 39 19 cd c6 5e 90 ff e1 4c e0 99 31 cf 25 cb 05 c3 34 d5 26 15 b2 3c 18 2e 4f 98 6b 07 4d f9 fc 1c 38 22 47 96 24 7e 1b 5f de a8 98 24 34 2f ed cf 6f 12 54 72 7f 66 6c 75 db 5f df cc f5 14 73 b4 0d 57 47 46 e1 b0 48 4b a7 a3 bc 58 40 e0 dc f3 e0 d6 81 b5 7e 92 35 9c 1b 41 56 7f df f6 71 Data Ascii: ?%9,UMj,Vz:oOQ\$%Ee~ aGFjNKrf[8;a;DPz4/aZV<hlvhFwO1yPpQB'yTr6nJ?9^L1%4&<.OkM8"G\$~_\$/4oTr flu_sWGFkX@~5AVq
2021-12-02 20:22:31 UTC	1329	IN	Data Raw: fc 13 08 d5 d1 9f d6 1a f2 d6 5b 69 08 e5 7e 0f 44 44 4a 1a cd 56 bd 4e 13 d7 fa 13 08 a1 47 d5 d5 86 d9 a4 fd 31 93 6a ff 22 8c b0 64 cd ca 2a ad fd 5a 2d 9b 68 ff 22 88 40 6b a9 37 8d 9a d9 a8 98 7f 82 44 a0 22 d5 56 a3 42 ff 6f 55 33 37 b6 5f 84 51 95 b7 91 1a 11 c8 46 8a ee fc 2e 88 56 b1 8b 80 7c b4 ea ab 29 74 cc fd 2e 8c 40 69 89 16 b5 b0 43 36 ab bf 09 24 1a 1b 55 23 56 19 f2 34 5a ad d5 6c 1c 5a ea 4d b5 25 e1 43 e3 22 28 8b d9 aa 56 57 ab b4 ec 5b b5 cc 25 66 9a 4b 95 98 12 38 34 24 82 b0 24 40 26 71 1f 95 5a 65 61 38 11 60 9a 4b c3 69 4a c0 d0 60 08 be 12 95 69 d7 20 52 bf ba 5a af 64 02 a5 b6 58 cb da 22 4c b0 19 ae 36 6b 6b ab b4 ad 66 12 e7 5f 80 49 1d 3b c5 6a b5 b5 46 2b e1 17 60 92 cb 06 0a 98 17 b3 b6 56 6f ae 2d 50 7f df 82 09 08 20 31 Data Ascii: [i~DDJVNG1j"d*Z-h"@k7D"VB0U37_QF.Vj)t.@iC6\$U#V4ZlZM%C"(VW[%fK84\$\$_&qZea8'KiJ`i RZdX"L6kk f_IjF+`Vo-P 1
2021-12-02 20:22:31 UTC	1330	IN	Data Raw: 9e 5a 97 9d 26 c1 43 00 0e 2e 08 4e e8 a9 d7 a4 e5 97 be f2 d0 55 c7 c0 c3 26 65 40 20 63 ab 4b e0 ee e2 7e 8d c2 fd 26 2e 81 18 03 a3 cb 1e 77 ed 2e df ea 1c 35 79 99 12 5f bc c6 b7 22 32 7c 28 2f 7a 30 19 44 67 6a 83 f2 37 7f ae 6f 6a b8 4c 18 55 d4 ac 70 58 25 44 2d 4b d0 e0 08 36 ec e2 80 40 d1 d1 8d c9 21 bc 8f c6 05 71 2f 43 57 e6 ed d7 4f 9e 7b 4e f8 e0 f3 30 79 f0 79 1d 9d 61 1e e2 0c b3 7a 6e 5d 2f 9f 61 4e 0a c2 37 f5 23 21 f3 62 0f 2b 59 56 30 98 d6 f7 5b cf c4 fb c3 59 74 f9 7d 30 9e b0 Data Ascii: Z&C.NU&e@ cK~&.w.5y_"2 (/z0Dgj7oJLUpX%D-K6@!q/CWOQ[N0yyazn]/aN7#lB+YV0[Yt]0
2021-12-02 20:22:31 UTC	1331	IN	Data Raw: 43 e3 e9 49 00 c3 7d c2 b3 38 cd 9f 63 4b 0b 6d 69 2d b2 ef f7 83 6d 79 39 db ca 8c c4 bb 99 ba 1d 30 a6 29 86 91 61 1a c0 32 75 6e 1c 67 05 18 fa 1c 05 18 fa 9c 0e 30 e4 da 1c a6 f3 48 85 e9 8c 2d 4e 70 59 35 74 98 18 be 63 ff 41 f2 14 7b fe 98 4d 06 cd 65 4f d8 48 65 7b 34 eb fb 6c f5 32 71 6e 82 fc 49 e0 11 24 30 c4 d3 d9 60 e0 8c ef f2 6e e0 39 33 e2 04 60 f5 4b d3 c3 46 32 89 50 a6 05 9d 63 a6 c7 d7 4d 12 66 1b b4 ea 07 4d 2d 6e d6 12 94 fb ba c9 fe 23 92 da 4d 9b d8 ae 7c db e7 60 c5 96 72 b4 ec c1 2b 50 e2 ee d7 fb 25 34 c8 1a 43 27 98 26 86 30 79 be f3 ba f2 ae 91 60 d3 b0 99 96 9a bb 44 cd ed 33 b0 39 15 2b 58 47 b7 44 fc cf 84 33 e9 cb e0 8e 18 cf 62 e2 ee 1c bc f6 5e f8 b4 95 15 08 7f af c6 93 7f 17 70 19 36 b4 6f d0 4f 62 de e2 5c 6a f3 a1 5d Data Ascii: Cl}8cKmi-my90)a2ung0H-NpY5tcA{MeOHe{4l2qnl\$0'n93'KF2PcMfM-n#Mj`r+P%4C'&0y'D39+XGD3b^p6oO bJj]
2021-12-02 20:22:31 UTC	1332	IN	Data Raw: 34 d2 93 8f 51 d9 2f fb a7 bb 46 7e eb 64 ff 14 40 79 7d 72 7c 48 83 04 50 a9 c8 31 d7 42 05 8f 76 45 35 00 78 7a 5e 28 0b de 3f 9d ee 46 35 e6 77 76 b7 0e a8 b2 53 14 e6 51 aa cd 34 ab 82 cc 6c 6f 57 30 c1 02 03 f9 42 2b 21 f3 88 30 89 36 11 da 50 fc 60 9c ef 3b 3f 0c fe c8 08 52 92 ef 82 35 25 8c ea 79 bc d2 81 67 31 66 12 4a e6 68 d5 f6 c5 27 0e 82 4b e9 ee 68 cc 26 b3 bc 3e 05 c2 27 69 87 5c 01 bc 32 3d 5a 1e 03 22 36 f9 1f a3 71 df ff d1 23 a9 13 6b 20 99 9d 9e e3 b5 eb 47 c4 00 f4 8a be 83 a2 dd 01 6d bf 8d 66 b4 0c 78 47 e5 2e 8f 69 1f ed dd a0 5b dc 5f 85 e9 04 82 fc 7b d1 f2 8e 68 79 47 8c 0d ab c9 e9 8f 24 b9 c9 a5 fb 5c ce ef 87 58 6b b4 8c 89 70 76 a7 d3 ab 49 fb e5 4b e6 dd a8 0d 6f 34 18 d0 62 2a 8f c6 9d 97 62 54 62 50 2f ef 83 f1 e8 a5 59 Data Ascii: 4Q/F~d@y)rjHP1BvE5xz~(?F5wvSQ4loW0B+!06P';?R5%ygf1Jh'Kh&>'l2="Z"6q#k GmfxG.iL_[hyG\$IXkpv lKo4b*bTbP/Y
2021-12-02 20:22:31 UTC	1333	IN	Data Raw: 33 62 05 27 e8 9d 44 59 8b 32 f6 a8 ad c1 08 0b 5d 0e 98 64 72 47 6c 65 77 cd 89 68 ff 11 db 0e f6 2c b9 04 65 bb bc 8f 51 55 3d 54 25 50 ad 37 15 c4 fa 6a 4c 0b d2 bb 53 55 5f 89 7d 28 da 2c c4 aa fa 3f 04 a4 01 74 36 d8 60 f8 7f fd de 65 30 0c 26 c4 d5 06 57 3d 9e 34 50 da b8 cb 37 e5 a8 46 31 ad 8c 5e a0 45 b4 d5 cf 86 a1 d3 93 6b 78 da 13 57 5f 41 a3 3a ce d8 4f ec 67 0a 48 0b 42 67 4c 92 19 9b 89 48 39 9d b1 73 d5 cd d7 71 29 4b 6c ef e8 43 3e b3 0f 72 b5 8f 1d 29 a0 d3 84 4c 82 41 6f 28 29 49 bc b5 cc c4 fe 89 5d 5b f6 23 35 c2 1b 82 64 b4 a3 2b 44 9c cc c0 28 4c e4 1a a1 e5 cf b7 ee 04 aa ef f4 c6 e8 02 b1 29 6b cd 97 6b 2f 77 b7 25 33 2f 2b df 9d 21 64 07 51 9b f7 ce 98 f6 52 de 1a d1 11 c5 f1 8f 66 43 af c7 db 85 69 e6 0f e1 bc 2f 6f ae ad 3f f3 Data Ascii: 3b'DY2jdrGlewh,eQU=T%P7jLSU_J}(,?t6'e0&W=4P7F1'EkwW_A:OgHBg LH9sq)KlC<r)LaO()lJf#5d+D(L)kk /w%3/+ldQRfCi/o5

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1334	IN	Data Raw: cc 61 9e 61 28 64 5f 0e 64 26 07 a8 a4 44 79 b2 21 0f 23 31 25 b4 11 f8 00 a3 17 8c 87 4a 1a 13 a0 96 30 34 98 33 ef c5 23 81 f3 0e 84 5c 4b f5 fe 19 4d 5d aa 5d 51 0f 89 99 a0 d9 20 13 5d fa e4 b8 bd 7e 0f e2 01 b1 36 bc 0e 78 09 ca 08 19 33 62 65 14 b1 60 32 9f 93 e2 5f ac b5 14 ca 35 3e e5 9c f0 11 b6 d4 72 0a fa 27 d8 0a 3f 00 84 41 e1 3c a2 8d 24 63 1b 11 60 98 51 10 20 63 56 24 ae 84 bd db 4d 62 d6 1a 1a 0f 98 56 c0 49 ee 8d da 8c 98 f6 8f e2 aa 32 e5 93 d4 81 58 9a 44 60 8a bd c4 14 fb 12 19 27 ca b9 4b 4f 80 87 a1 c2 e1 67 12 e2 98 d2 f9 a9 03 64 d5 0d 5a ea d0 e4 08 15 57 52 bd 25 c9 3a e4 e9 0c a1 32 a2 e7 42 ab 10 cd 61 7c 92 ff 9c c8 92 a0 02 65 51 cd 6b a1 38 35 7e 71 84 09 4b 01 6c 51 01 58 52 5a e5 39 a9 a1 19 62 9a 26 46 e2 c0 7a 12 4f 72 Data Ascii: aa(d_d&Dy!#1%J043#AKM)]Q]-~x3be`2_5>r?A<\$c`Q cV\$MbVl2XD`"KOgdZWRw%:2Ba[eQk85-qKIQRZ9b&FzOr
2021-12-02 20:22:31 UTC	1336	IN	Data Raw: 21 c1 72 7c a3 1d de 60 a2 47 57 d4 52 e1 cd ee c7 02 e1 2c 42 ff 50 d2 90 f6 66 ff 8e a3 71 7a 1c ea 28 c9 b8 d5 71 15 83 33 b0 38 4b 4d 55 2b 15 15 d0 76 36 d9 f4 a2 a0 1c ec c7 8e 7d 41 7e a4 d9 d1 db 9e 0a 7b cf 86 f5 b4 e7 c1 47 ec d0 97 81 d1 a4 79 73 32 0b f6 c5 bb e4 75 ce c3 e5 bb 58 17 76 61 3a 9e 05 05 db 76 ac dd a6 f2 ea 3f 2a b5 97 55 2a ba 55 e8 6c 3a ed 57 b2 60 a2 06 f6 86 b7 bb 38 e1 af a3 c1 09 f7 b5 36 1c 87 f6 09 06 f4 d7 86 c5 f4 32 4e 44 3b 06 2f 65 8b b7 64 fc dd 74 cb 13 b1 38 88 3f 41 c8 22 f9 f6 95 97 0a 42 51 2e af 50 aa 2b 4d bc e1 8a 9c 63 2d 72 2f 40 de d5 07 23 34 33 6f 35 f9 1d 5c df 89 5d 81 e2 36 59 5d 06 b1 13 6f 8d d4 5b 53 5c bf d1 a2 bb 66 7c b9 20 7d 17 47 46 55 c4 c5 44 58 ba 77 9a 84 78 f2 96 9a da b4 1e b9 aa 16 Data Ascii: !r `GWR,BPfqz(q38KMU+v6)A~{Gys2uXva:v*U*Ui:W`862ND;/edt8?A"B.Q.P+Mc-r/!@#405j]6Y[o[SVf] GFUDXwx
2021-12-02 20:22:31 UTC	1337	IN	Data Raw: 68 4e dc 5b 63 ea b1 5b 1b c3 9f 5d b7 96 dd 81 85 1d 8a 6f bb 83 b1 da 31 8e f2 18 7f f0 d0 18 3a cc 1e 29 3a b1 03 c7 76 40 96 bf ce a0 f8 11 c5 5c 63 dc c4 01 47 76 e6 f6 c7 80 54 e6 6c 8a 6e 6a 80 9b b2 03 7f d4 a6 0c cc 38 b9 fd c2 8c 08 cc 4a a2 4f 7d c1 70 7e 0b 1a 73 6d e7 b5 d2 a1 51 7a 82 46 bd 6d 15 73 54 77 99 c4 98 8b 26 50 3a 97 85 da 90 01 6b cb a2 84 8c 86 5f 1f 44 6e 75 18 b9 14 95 1e 97 04 30 21 16 58 23 b0 a8 f9 46 ac d0 90 62 dd 37 0a 01c e5 36 89 71 9b 8a be 5b cd ef da 5f 50 c2 7a c8 01 6b 4f 8c 2f 09 f3 18 02 77 14 51 08 5c 0c 75 cb b1 6d 37 31 e0 54 01 a3 db d2 d7 36 7f 7e 89 f8 73 6d 8b bf db f7 14 cf 76 61 ed 1d b7 d4 e1 ef 35 06 61 60 c0 50 7a e0 23 54 84 48 2f 02 e6 47 c0 68 d0 ef 42 0d 8b ae 63 51 34 4d be e7 aa eb 7c 0c 8d 30 Data Ascii: hN[c[jo1.):v@!cGvTlnj8JO]p-smQzFmsTw&P:k_Dnu0!X#Fb76q[_PzkO/wQ!ua71T6--smva5a`Pz`TH/GhBcQ4M]o
2021-12-02 20:22:31 UTC	1338	IN	Data Raw: aa c4 83 2a f1 25 dd c4 07 d5 c7 50 f5 f1 23 3d 88 8e 6a a1 ad 5a 38 4a b7 30 54 05 86 aa c0 69 ba c0 48 15 18 a9 02 67 e9 02 03 55 60 a0 0a 9c a4 0b f4 55 81 be 2a 70 9c 2e d0 52 05 ee 55 81 8f e9 02 3d 55 a0 a7 0a 7c 4e 17 b8 57 05 62 55 e0 20 5d a0 ad 0a b4 54 81 c3 74 81 ae 2a d0 51 05 3e a1 81 db 9a 07 a7 62 4a ca 1d 14 9e 2f b7 48 4a 32 29 d4 2e 95 83 7d 7a 4c bc d2 8f 89 97 53 e7 b5 44 8e 17 3d 14 42 91 2e 00 bf f9 dd f9 fa d5 87 ea 3b d4 3e d7 c9 17 3a 54 7f d3 8f 72 81 21 9d 0a 8d 77 05 d4 3b 5f 5e 0e ea 41 f1 a3 1d b2 ee 41 2d 71 fe 7e b5 65 7f dd 42 87 cc f8 10 87 0a bd 8d e2 15 8a 82 72 9e 22 22 d4 8b fa d9 cc f5 6f 1a 3b a7 6b a8 18 11 2f 2f 7b 30 0f 5f 40 a3 71 61 c6 b3 87 2e d1 86 21 45 85 f9 0f 3b 39 c5 27 ac 21 64 88 f0 1b 13 c8 cf 43 b8 Data Ascii: *%P#=#J8JOtHqU`U*p.RU=UJNwbU ]T!*Q>AbJ/HJ2).}zLSD=B.=>:Trlw;_`^AA-q-eBr""o;/k!/_@_qa.IE;9!dC
2021-12-02 20:22:31 UTC	1340	IN	Data Raw: 28 83 84 84 70 72 05 f5 26 bc 0a 69 fb d7 7e 9a e4 85 69 17 06 53 a8 c8 e5 82 c5 37 cb 18 3b 21 cd 1d bc 37 cc 5d 7a df 51 03 83 f1 0c 9e 2c 45 f0 49 5d b3 ef e8 58 7e 49 99 46 90 76 3e ae c1 b1 64 6d 9e bf 87 d5 f5 fd 75 71 39 aa 6e 4f a4 8d 8f 5b fc 24 c8 c8 05 6d a6 d2 c3 f8 43 9a 17 e5 0c c6 8f c3 60 dc ca 1b 0f 5a d8 a4 63 a2 b8 72 bf 6b b4 64 a8 92 f7 0d cd c2 b6 72 f7 a3 0d e3 fe f0 00 a3 6a a3 92 1d 57 44 95 fb 4a e6 c4 78 ce a7 2f 50 ea a3 20 de e8 94 d0 5d 50 21 4a a9 b6 90 da 93 4f 59 5d 79 ee 4a 6a a4 6a 7d cb 00 2d 92 5d 5f 49 55 8c 39 33 c9 9b 40 41 73 5d e4 63 1d 06 da cb 9a b5 62 7b 2b 96 60 07 d1 b2 5e 0b 99 2e 07 f5 70 e2 5d f9 f8 ed fd 2d 73 30 da 43 41 1e 0d 0f a6 a8 38 d5 9a 54 af 1f 74 1f 17 e5 85 b4 4f 0e 38 c3 80 08 43 35 0c d5 2f Data Ascii: (pr&i-iS7;!7]zQ.EI[]-IFv~dmuq9nO[\$mC`ZcrkdrjWDJx/P ]P!JOY[jYj]]-_IU93<@As]cb{+`^p]-s0CA8Tt08C5/
2021-12-02 20:22:31 UTC	1341	IN	Data Raw: f3 39 20 58 f3 71 4b 39 9e af 7c a6 4a 9e 60 e0 6e 48 36 db d1 86 d5 9e 7d a9 7f 1d ef 8a 50 ef ab d9 17 d1 00 78 b8 f2 0e 56 5f e9 9e f6 13 11 da 83 dd 57 9b 1b 41 3a 45 b2 f6 31 cc 5b 21 c5 ce 00 e6 0a f5 52 2d a2 d3 17 c0 24 ec b7 4b 22 1b 0b e1 1b a3 1c 76 f6 c4 3a 1f d3 f8 e5 65 e9 f8 04 9f b1 52 6d e5 2e bf 85 e2 ab cf 58 58 8d bc af 4e ec b3 24 1f ab 6d 81 5c 52 f5 c2 8e c5 ef 5d 12 eb dc dc f2 33 56 16 ae 1b 26 5c 37 18 ae 61 f7 45 a0 c3 dc e2 42 8f 3b b0 e1 8d 91 8c 6b 8b 1c 77 0f ee 34 d2 74 3d 31 2e 4f 25 3d 6c 06 55 85 28 4f d4 d9 41 c7 9a 8b 5d 9f dc 76 62 50 14 c0 a8 a1 be 57 e8 26 94 be b1 08 92 ce a2 5c af 5b e6 46 91 df 90 d6 cb cb 82 ad 0f c4 29 5a 26 33 96 52 90 9d 84 e4 54 2b 05 37 2f 8d fe 2e 23 9d 20 76 b6 b7 87 51 97 e9 Data Ascii: 9 XqK9j]`nH6jwPxv_WA:E1[!R-\$K"v:eRm.XXN\$m\R]3V&!7aEB;kw4!=1.O%=IU(OMDA]vbPW&[F]Z&3RT+7!/#vQ
2021-12-02 20:22:31 UTC	1342	IN	Data Raw: 67 84 a1 2c 54 10 41 a2 3b 29 86 aa 3e 4e ec b2 70 28 a5 f1 50 5f 3a d3 6e f6 30 f4 42 11 46 30 3a 37 12 ec c2 62 7b 3c a4 50 1e 48 28 85 14 88 aa 3b d0 ce 8c 31 11 48 e8 aa 8f 87 b1 95 a7 bb 84 a3 93 3e 59 7e b2 f3 3f 42 a7 29 e4 4c cb 3a eb f1 c4 ff a1 5f c2 3a 4c 65 08 0d b4 ea e6 cd 41 e1 85 e7 9f d2 25 91 a4 20 97 4a 4c 3d fe 31 2d 1d 85 d9 1c 32 1f a6 e0 a3 b6 90 1a e0 43 9c c1 60 4c ea f1 ed f5 07 de 5e fa 01 4c be 82 b3 64 49 93 37 d5 5d ce 18 0a 55 2f 76 aa 98 3f b9 b4 8a b9 93 be 70 8b da 6d 16 4b 21 60 d6 67 e7 e7 30 6b 7e 45 b3 0e a0 f1 cb 43 fc 7e 4b e3 6e 03 43 09 86 9d 20 69 76 62 3c 4a c5 88 8a 55 2b 27 63 a0 5a 7b ad 50 b5 41 f1 c6 16 53 24 2b bd 1b 3c a1 f4 77 dc 43 c7 cf 21 b6 5b cd 28 c4 01 3d ea f1 af 8e e7 7c 07 6a 3f 12 92 24 3d 16 Data Ascii: g,TA;)>Np(P_~n0BF0:7b(<PH(1H~Y~?B)L:_LeA% JL=1-2C`L^Ld7!v?pmK!`g0k-EC-KnC ivb<JU+`cZ[PAS\$+<wC![(=]]?=\$=
2021-12-02 20:22:31 UTC	1343	IN	Data Raw: be 42 01 d7 e7 b3 0d 53 47 36 4a ab 20 c5 f4 0a c6 1e c2 66 b5 d1 3a b6 81 f3 6f 50 33 35 38 05 56 60 a1 e7 9b 7b d7 26 c7 6d d0 3b 29 55 47 f8 8e 14 d7 4f 4e e9 41 a6 81 be e9 ef 08 39 c1 30 a1 ca 92 ac 02 c7 6e 64 c7 29 17 80 72 eb 60 29 51 b3 59 b3 78 e5 29 16 6f 21 8f c7 9b b9 d2 2b 6d 3a 28 a8 fe 9e 85 71 a2 d3 72 d8 1a 05 5c 77 e4 16 08 1f 62 03 e7 f3 17 f8 85 23 2f d4 74 ac 03 56 8e de df d5 0e d8 fb a8 ba c5 aa cd b0 bc 97 a4 59 8d 05 e5 6a 90 9e 84 68 b8 d9 47 76 cb b5 50 15 84 d7 e5 7f 6c 50 3c 0e 74 74 3e 63 20 91 04 da 53 43 c5 d1 78 24 f3 7f 4c ab 98 c0 fa e3 a3 d0 b3 26 c5 a1 0d e1 01 30 3c 8f 01 93 8f 26 96 d4 fa a8 ed 32 2d ce 8a 20 7b ae 76 03 5b dc 13 71 05 28 e8 a7 9c 8c 08 33 7e 1b 2a 2b 7b 35 d7 09 7e b0 57 6b ad 0d b7 e0 d6 bd 2a fa Data Ascii: BSG6J f:oP358V {&m;]UGONA90ndr`)QYx)ol+m:(qrlwb#tVYjhGvPIp<tt<c SCx\$&L0&&2- {v[q(3~*+{5-Wk*`
2021-12-02 20:22:31 UTC	1345	IN	Data Raw: e9 a5 98 d1 07 21 86 88 2f 0b 5f 7c e7 38 88 62 94 1d ba d4 73 30 89 69 cb aa ba 05 da 1d db b0 6a 87 54 e4 91 bb 8a 45 a0 07 54 8c 9c db 20 8b a8 81 f9 98 ac b1 55 37 db dd 23 01 a4 98 a6 4c 7c 3c 4b 31 05 6f f2 e7 c6 f8 02 b4 81 34 d9 81 8b fa 72 2c 48 cf e7 8f f5 c9 ed 32 6f fb 50 e1 b7 cd 4e cc 8f 9c 93 c4 6c ed 1c d4 47 6f 0e e1 7f d2 9b a8 9c a4 7e 41 d6 ef c1 f9 d3 fc 3a a5 25 9d 33 4f 3f 17 0e f4 28 a1 4f e4 c7 1e 18 28 d2 83 83 a1 f9 7a 70 7d 3d b8 76 f7 81 82 cf e6 8e e9 db ff c0 98 a0 2b b1 40 3e 20 f2 61 8c 56 f9 bb ba 5a 69 49 89 c6 0c 88 60 09 24 c1 62 dc be 39 13 c3 b9 f1 c4 1e a7 af 36 86 8d 41 cc e1 f1 6a 4a 7e 23 05 44 46 e8 1e 77 30 54 2b 70 04 23 27 e1 61 50 a8 96 90 2d 91 ba d6 b2 d2 c7 2e f0 03 c0 2c 3c 65 8b 7b 85 aa 4f 3a 06 83 a9 Data Ascii: !/_J8bs0jTET U7#L<K1o4r,H2oPNmIGon-A:%3O?(O(zp)=v+@> avZi!\$b96AjJ-#DFw0T+p#`aP_-,<e{O:

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1346	IN	Data Raw: 7c 56 98 70 bd a1 1d ac 96 d7 b6 91 9a 48 ec cd 3e 56 b4 b5 c6 a3 a4 1f 95 19 68 de ab e2 b4 d7 ba d0 90 27 5f 38 77 5f ed 39 56 15 08 9c 8c 2f cf c6 a3 1e 5a 8b 89 1c 3a b1 61 3f c6 cc 6b 69 eb 83 60 79 79 8c cf d9 a7 9f 81 74 24 4c 3d 75 e0 14 29 48 35 7e d8 5b 9b 28 5e 49 1b 8b df cd 34 80 b8 93 9f 0f dd 16 ea 51 95 f4 99 ac 53 94 3b 5c a3 6a 62 6c 71 a5 54 8e b4 d1 04 85 10 ac 90 df ba 4f 26 28 28 cd ff e9 13 61 19 cb 60 cb 63 23 ad df c7 c5 66 80 1a 28 72 30 32 95 bf d0 8a 49 7a 94 d3 d2 40 92 cf 18 4e 06 b8 24 52 87 d2 6c b1 b6 90 1a d4 f7 1c 55 0e 19 f9 f2 17 6b 73 99 6b e1 4e d2 53 3a 72 67 1d ef 71 a6 64 ce b1 f9 4e 06 9b 00 44 73 4f cb 93 66 56 3d 29 1f a2 59 a4 1a 6f 4f b5 2d a7 00 95 0b 99 81 fc 98 a2 a3 94 ae 19 ff cd 3c 92 d2 e3 39 d0 53 e2 Data Ascii: VpH>Vh'_8w_9V/Z:a?ki'yyt\$L=u)H5-[(^!4QS;\jblqTO&((a#c#f(r02Iz@N\$RIUkSkNS:rgqdNDsOFv=)YoO-<9S
2021-12-02 20:22:31 UTC	1347	IN	Data Raw: 51 19 14 9c 63 f8 ca 97 e6 1b 68 7a b5 fc 37 35 84 1b 83 f5 4e a8 1e b5 c5 f5 d1 1a 49 2d 9a 72 cb 0b f0 7a 62 92 18 ad 69 27 e2 09 eb 7a 37 bd 45 34 83 fc 4b f8 54 6a 00 b3 ff 7c 3e 0e 9f 72 79 fc 12 d1 2a f9 b6 20 de 0a 40 1c 4d 7e 35 50 0b 53 f3 55 22 1e 77 48 6c f7 74 a6 4e 49 f0 4b 09 b5 95 71 3b ab de 5f fe 44 7c ce 1d 03 29 fa 4c 0d 00 dd 35 a3 82 80 2d 09 a2 ef 51 35 ca 76 24 fc 6a 59 34 ab d1 04 65 5c 49 a9 d4 f0 a0 cc aa 2c 84 20 7c ef db 5a f7 b2 52 04 f8 7f e8 ac 1e 75 1a 68 16 fc 04 24 4b 3e 61 13 a9 f8 07 40 af 88 b6 13 af 86 b5 d2 fb 46 f2 be 03 ab 02 69 22 58 71 8e ed 06 10 b7 62 ed 5d e1 cf 36 50 f1 18 9b d0 af db df 3c 94 4d 17 9b 05 d1 f4 e1 d7 29 5e c3 d5 9f 2a b1 16 3a 71 de 9a 05 b8 66 67 53 37 b1 6b 1c 5f 84 c4 c8 3c 8d 6e ea 34 2e Data Ascii: Qchz75NI-rzbi'z7E4KTj]>ry* @M~5PSU"WHltnIKq;_Dj)L5-Q5v\$Jy4eI, Z\$u\$K>a@Fi"Xqb)6P<M)**: qfgS7k_<n4.
2021-12-02 20:22:31 UTC	1348	IN	Data Raw: 77 65 9f 9c 86 22 45 22 fe b1 db 70 62 e5 ae d9 7f 83 bb e6 c7 d0 1b 8c fc e2 b9 3b 1c 02 b3 79 4c ba 11 09 61 14 69 8f 66 2d d5 a1 2a 6a 05 12 1f df 49 4a f1 7d 36 19 fb e1 41 3f fc bd 42 a4 7e 4f 5e 45 17 5b 72 28 a8 da 49 a2 5d f9 90 cf f2 ec ef 33 25 ea 09 b3 a9 bd 69 14 2f 3d 5b e1 c2 b8 38 42 5a dd 5b 5d 8e 11 b4 18 df f1 44 32 52 e5 f7 20 1b a6 01 ef a3 ef e4 cb 22 aa 5b 72 d1 ac aa b5 e3 23 ab 4e e6 23 63 9b d4 03 b1 c5 3a 6f 1f bb d5 3f 54 97 c4 8f 94 ab 8e c5 d1 c0 ed 0c 9b a4 fe 32 4a 68 05 f8 cf d4 22 d0 cc 53 13 1f 4f 4f 9c 39 8d 66 c7 d6 2c 07 6f df 8a 9c 65 bd 0c 1c 64 e1 4f 86 10 1e 67 57 ce 76 b7 a1 f5 23 24 e4 ed a1 ba 8a 6d 4e a6 f5 b7 f4 a2 d7 e0 59 b5 de 2b 07 14 75 db 80 0b 6e 10 17 0b 66 ab 56 c3 ea e9 f5 72 e5 7a 15 aa c9 3a 33 b5 Data Ascii: we"E"pb;YLaif-A*jIj]6A?B~O^E[r(lj3%w=[8BZ[RD2R "[r#N#c:o?T2Jh]"SOO9f,oedOgWw#\$mNy+unfVrz:3
2021-12-02 20:22:31 UTC	1350	IN	Data Raw: e5 ce b7 f3 03 0b 2e fa 12 10 a6 ac e7 8f 75 e0 d6 b5 88 f4 d8 5a ac 56 c9 bf 28 de ee 1d 45 f2 dd e2 23 9d 67 de d8 70 64 d1 c2 c8 d4 83 7f 42 53 8c 89 70 b7 67 46 bf 64 24 d0 68 4a cd 81 b6 43 86 db a2 ef f8 3e 39 a5 84 b3 06 08 bd b1 bc bc b0 14 d5 62 f8 3b 20 71 36 ab d8 c2 08 96 d8 e8 c5 6f 8d 83 70 48 0c 3b 26 18 d1 26 07 8a 4e 8b b8 0f 0a f8 89 f0 ca 67 34 59 8f 1d e7 e2 1c 8f f6 6f c4 42 e2 d0 31 d6 a6 d6 5e 5e 6e 13 8b 71 e8 fc ae 5b 7b 57 c7 97 7f 5d ee 5e 9d 03 05 fc 75 ef fc 2f fc 4c 0a 33 8a 3c 73 8c 62 00 41 87 f5 9b df c5 5d d8 ac db ea 4e 1a d8 7f 27 fe 78 7f bb c5 c3 c0 74 7d 0c 43 4d 13 74 c9 46 8e 85 f5 ce 12 87 e2 0c 0f 05 d0 b0 7a 67 6a b0 48 51 1d 52 f0 30 c3 41 06 68 a2 4f fc d9 ed b4 9e ac 2a 6a 64 cb 7c 4a 50 bd c8 43 3a 80 3b 38 Data Ascii: .uZV(E#gpdBSpgF\$d\$hJC>9b; q6opH;&A&Ng4YoB1^nnq[({W^u/L3<sbA)N'xt)CMTfZgjHQR0AhO*jdjJPC;:8
2021-12-02 20:22:31 UTC	1351	IN	Data Raw: 68 34 a3 f1 00 df 34 aa 4b 25 11 76 c6 e8 49 46 7e c1 45 5c 35 0f 4d fa 41 48 8a 97 27 e2 f0 5f b5 13 67 db 41 a5 6c 6d 7b db 26 71 a0 52 7e 42 2b 4c 58 b8 cd 77 f8 10 07 bf a5 39 f4 4e d8 1b 5e a0 74 96 b5 04 53 fe 27 13 01 a8 97 b9 f8 e2 d1 a8 57 f1 fd eb af c7 c7 c7 62 33 1c 35 8a dd 41 f4 57 33 f8 2b 18 b8 8d 41 6a dc b8 d1 6a dc 07 6d 58 d8 d5 04 a1 3c 36 83 10 b0 ca 2a dc 76 61 67 48 d2 61 04 12 3d dc 80 87 9b 72 e7 95 eb 61 d0 2f 39 7c a8 55 82 22 3c d3 08 9f 4c 2d a0 73 c1 a8 38 ec 01 71 c2 34 ae 50 cf ea 22 1b 97 49 28 97 2d 81 89 e9 bc 49 b2 84 a1 e4 4a 0d 27 d5 33 46 45 96 47 88 a4 e0 5c a7 06 86 e4 00 51 70 2c e4 0a 6f e1 9a 49 3e 8a 8f 77 28 e4 41 01 56 60 0a b0 d8 ff 93 af fd 57 93 b4 8f 7d d4 98 40 db 00 a0 0d 6f 0b e9 a3 96 58 6e fb db b9 ef Data Ascii: h44K%vlf~E!5MAH'_gAlm[&qR~B+LXw9N^tS'Wb35AW3+jmWmX<6*vagHa=ra/9U"<L-s8q4P"(I-J3FEG)Qp ,ol>w(AV"WJ}@oXn
2021-12-02 20:22:31 UTC	1352	IN	Data Raw: 94 12 a8 18 34 40 89 93 8b 68 58 e0 4b f6 12 a4 6d 1f f8 0a 1a 3d 28 6d c1 19 54 81 11 ad 53 66 e9 fd 21 bf 43 6c 75 97 29 96 90 0a e9 f4 14 01 90 ce 42 ad 23 9f 67 2a 15 e2 08 ed b8 8d f2 05 15 22 c8 bb 03 c3 cc 1d 28 6f 2a 46 30 a4 20 a2 ef 14 72 7e a3 dc 70 00 82 ae 69 cb 3b e3 5e 1b 4e b9 bf d6 dc b1 9d dc 6f 8e d3 28 ea 7b ef e5 25 79 f5 49 65 14 50 b0 25 5f 75 07 92 a4 b8 87 b6 c9 8b 36 fc 35 63 96 a3 20 52 de 4b 83 10 8e a1 1f d2 48 f1 bd 9f af a2 f1 d4 aa f0 bc 71 0a bc c6 7a ce c9 33 7d ce a4 df 32 e5 44 f4 a9 07 45 a3 27 fb c3 dc 61 d2 41 00 a6 fa 6e 3b 47 f9 67 d1 55 b4 93 ec b0 9e 4d b0 0b d5 05 94 1b 3f 34 f3 94 87 54 7d 49 c4 d5 dd 0c 4d 47 f2 83 d4 19 19 4f a9 8e a1 13 24 05 e0 05 e3 37 5a 3e ec 5f da 66 2e 13 af 4c 8f de 23 0d a7 34 ed e2 e2 Data Ascii: 4@hXKm=(mT\$!Clu)B#g""(o^FO r~pi;"No({%yleP%_u65c RKHzq3)2DE!aAn;GgUM?4Tj)MGO\$Z7>_f.L#4
2021-12-02 20:22:31 UTC	1354	IN	Data Raw: 4d 04 04 9c 82 c7 2f 78 89 65 48 39 7c 8d c7 37 97 4f 01 dd 71 9d 06 ed b9 a0 0a ac 37 1a a2 c8 09 9f c7 20 13 0d 50 c2 42 75 b8 cd 41 0b 16 46 88 3a 6b c6 e0 da db f4 bc 27 b6 e4 c8 b6 5d a3 01 96 09 a7 5e 4a bd 31 ad 49 b6 23 46 b6 a3 5d 10 63 52 3b 4c 3c a3 31 ef 81 26 e6 e8 23 8d 63 2e 12 61 5b c4 b7 ea b8 00 1b 40 fb 34 cc 5e 44 4b f4 18 22 45 d4 ec 6a c7 65 c7 ba 07 ac ff 68 50 d8 07 b9 92 62 c4 47 dd 6d dc 9a 7c 62 87 1e 56 49 e7 87 84 e9 8e 52 cc c7 17 49 54 a3 d8 89 96 97 97 f4 b3 ab a1 fc 50 e0 94 cb a3 13 7c ee d4 01 36 66 97 3c 38 da c3 9f 06 81 24 1a ae 55 ad 5f dc c5 a8 37 37 21 fa 2c e9 6d 23 d7 48 ff de 8a 18 13 cb e9 c4 5a 83 45 8c 4d 54 74 92 de aa 30 20 d4 45 30 f5 1d 6b ac 5d 91 1a 9b 1c 15 76 56 00 d0 5d c8 31 1c 47 a3 0d a9 d2 Data Ascii: M/xeH9j7Oq7 PBuAF:k'X^J1l#Fj]cR;L<1&#c.a[(@4^DK"EjehPbGm bVIRITP 6f<8\$U_77l,m#HEZMTt0 E0k jvVj]1G
2021-12-02 20:22:31 UTC	1355	IN	Data Raw: 42 1f 9b 26 d0 ac d9 8a b7 2c b2 55 6d a7 83 fc b7 29 56 96 f4 74 3b 25 5e ae a9 4f b8 90 51 00 86 76 cc 4a e1 ca c1 9e 34 57 57 5f 08 56 56 aa 9a df 33 b3 96 97 c3 95 15 34 6f 2e 20 44 44 7c 85 e3 c2 fb 08 11 85 6a a4 0e 5a c4 af 57 e2 47 96 04 76 53 44 90 dd 1c 1e f9 a8 0e 85 02 25 92 18 11 b0 3e 4c db 85 4a fe 51 68 8f 81 62 20 c6 64 3a 7f 98 b7 e7 67 0a 92 cf 10 49 68 a0 fc d1 64 6f d3 74 1c 43 e7 79 22 89 95 b0 48 e3 b9 ea ca e7 5e 12 c1 a2 33 82 6c 06 49 61 c9 39 37 be 5f 37 e8 56 2a 46 c0 69 34 a6 e5 f2 c0 47 78 35 74 26 08 4c 0b c6 5e 45 a1 e5 c9 e9 6b af 4a 03 f6 aa 94 24 15 d0 34 9c df 02 c6 24 c2 ed 85 81 f9 72 8f 2e 0f 92 a7 fb e5 e5 c4 74 33 9d 03 1b bb 03 df 69 91 bf 48 f6 7a 87 9e f6 eb f1 ea aa b1 cb 9c b8 bc bc d0 5e 5d e5 b1 fe 06 fc f5 Data Ascii: B&,Um)Vt;%^OQvJ4WW_~V34o. DDj]ZWGVsD%>LJQhb d:ghdotCy"H^3lla97_7V^Fi4Gx5tL^EkJ\$4\$r.t3iHz^]
2021-12-02 20:22:31 UTC	1356	IN	Data Raw: fa 8d fa 52 09 03 5c 64 5f 15 f0 60 63 3c 99 4a 05 c5 49 28 55 9e 6b b2 6b 8a e7 c4 73 76 01 5f b3 bc 8d 4c cb db b4 bb 91 4f 81 f4 45 da 69 90 ed 2d 9e cd 8d f4 7a ba ce 3e 87 67 9a 0a d6 a9 82 da b9 ea 57 cd 82 a5 f2 ef 11 d1 eb 90 64 94 c2 21 76 fd 7b 59 11 8d b2 1d 73 dd 77 d5 b2 73 d4 1d 0a ef bb 2d e8 83 c7 d4 ba 73 13 c1 06 b3 63 7f 21 ae bb 95 ef a1 53 68 f3 cd 1a 2c ac f6 bc ab ac 17 b4 0e 4b 4b e9 c3 dc 39 1d c4 63 4a f7 c4 23 8a 5f de ee ad cb e1 f7 75 f2 0c 69 aa aa dc 29 ff ae ca d6 ce 03 84 8b 8e 8f 73 3d f4 ef 3a 70 61 77 e4 59 6e c3 a0 87 f6 64 35 c1 ea e1 18 c7 6d 0f c5 22 90 01 51 13 4d 8a d4 71 ee 2a 6a 18 a5 c0 33 aa 2d 8e 7b 64 6b a9 ea f4 ef 66 bb dd 08 8a bf a3 1a f2 01 6d 58 2e 94 a3 48 4b 5e d2 `c 37 0c bc bf 79 7b a9 2c 62 53 Data Ascii: R!d_`c<Jl(Ukksv_LOEI-z>gWdlv{Ysww-sc!Sh,KK9cJ#_ui)s=pawYVwd5m"QMq*j3-[dkfmX.HK^j7y{,bS
2021-12-02 20:22:31 UTC	1357	IN	Data Raw: 04 c9 86 fa 11 15 f8 21 c1 e1 05 7b 71 ca 05 a1 52 1a 9c b2 96 a4 44 9c b2 41 3e e0 a0 bb 1d 7c 96 20 5e ef 22 74 f1 9c 13 c5 66 75 68 7b 51 a0 89 38 00 58 6c 2e 7d d4 01 0a 89 28 43 de 02 f7 d7 cb 4b 73 78 ea 9e da b3 f2 0b 05 df 39 4f 6d 82 af 21 6b ba b4 a3 c3 b5 1c cd a2 35 0f b7 15 7b 36 fe 0c 39 a7 9f 25 05 96 30 82 8a 4f f4 15 9f 98 8a c0 06 b7 f1 a4 76 94 b2 a2 25 26 2c 57 61 88 1b e0 47 32 6e 35 79 5e b3 c6 1d 4b 19 79 e3 e5 ec 16 ea 7e 5d f9 94 91 16 49 e4 33 df 02 de b5 0a 7f da 56 d5 4b bc ce a0 39 08 64 ff be 93 ee 5e 04 95 30 7c 68 b2 03 fc 8c 2c 03 99 98 5c 89 85 2b 4d 3d b1 d2 a7 3c 13 a1 9c 2d d5 7b 57 a8 af 96 ab 40 e0 ef e4 e0 16 98 53 1e 34 b8 a1 bf 87 6f b0 11 a0 84 03 12 83 02 9e 90 2f c7 0a 22 66 97 29 bc bc 9c 62 80 9e 72 45 cc 2d Data Ascii: !{qRDA> ^"tfuh[Q8Xl.](CKsx9OmIk5{69%0Ov%&,WaG2n5y^Ky~]l3VK9d^0 h,)+M=<-[W@S4o"fbE-

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1359	IN	Data Raw: 70 5b c3 90 dc 47 e6 e1 4a e9 b0 bb 98 c5 85 2b 5e 71 0a 11 56 8d b6 14 66 56 f5 65 1c b8 1a 7b a5 30 bd a3 04 30 26 40 d7 55 b8 39 d4 be d0 1a 45 f8 ce 9d bb 46 67 db e6 02 2d 78 37 81 dc 86 00 57 0a 16 e1 78 96 f8 d0 95 e1 e8 a5 b3 4a 96 12 73 50 1c f4 3f 84 3a 56 66 1c 9b 93 b4 28 4d 3e f6 68 d7 2c ab e5 94 63 15 f9 68 14 a7 9e 81 ba ea 35 08 4d e1 4e 5e 11 3c 4e 87 2f 7b 96 f7 47 75 b5 0c 97 0c fe 3b bc c7 7f bb f8 7b 62 0a b6 9d e4 8e 5f 5e 9e 4e f4 f2 12 fd bc 44 76 d6 e0 fe 2d dd 67 4a 4d 0e 7f 95 a7 23 fa 89 0b 9f 80 d3 c8 e2 5d 4e 77 5c 6f 57 db 2b fd 5a 5c dc bb 73 4a ef db 75 83 6c 28 97 4a 7f f6 ff 6a 17 60 e4 b5 92 7a bc a4 e0 97 2e 37 14 89 b6 e3 f1 cf 5d 11 17 e5 d4 b3 cd 6c ff d9 fe ab 5f a8 96 0a 93 b4 97 9f 5d 25 fb ed 2a d9 6f db 09 26 Data Ascii: p[GJ+~qVfVe{00&@U9EFg-x7WxJsP?:Vf(M>h,ch5MN~<N/{Gu;{bk_~NDv-gJM#}NwIoW+ZIsJUl(J,j.z.7)]_}%o&
2021-12-02 20:22:31 UTC	1360	IN	Data Raw: 1e 9a f7 be 57 0a 87 68 e2 03 e3 c4 75 44 ed 9d 53 e0 b4 53 07 cb 23 57 14 b1 83 b6 64 17 79 8a b0 d2 bd d3 b4 3b 40 8a ad 74 b9 6d fb 09 c5 c5 e1 e6 fd 94 4e e3 92 87 ef 2a 89 ce a3 91 cb 66 9b 0b 19 ff df 67 b9 16 6d f3 22 be 25 a1 02 99 da 64 af 7d 35 5f 27 64 1f 69 35 0d 4a 04 28 ff f4 f1 a7 1d 38 3d e4 22 8e c8 e9 75 b9 84 a6 6e 1f 2b 18 d8 c0 93 e1 d5 fc 74 2c 38 f1 65 da a6 30 77 84 48 2d d3 b8 30 c0 1a 91 84 e8 ad 08 6d 75 50 fd 3c 09 9d 97 7e 92 b4 0a 89 8b db 40 ad 81 40 07 d2 e7 77 e8 c0 ca 09 b5 32 7a 83 95 d1 93 24 a8 e9 34 a4 cb 0f ae 67 e5 72 34 d4 ec 23 9a 72 a4 d0 00 a3 82 60 d4 1c 15 30 40 0b 7b 72 c6 50 8d 7e b2 28 e9 25 c6 15 aa 29 a3 04 5f 9a 2f 72 cc bc 9b 5b ed a4 1a 8d 86 c9 48 30 60 57 36 17 77 19 27 5a 4a 51 eb 99 fe 09 83 fe 90 Data Ascii: WhuDSS#Wdy;@tmN*fgm"%d}5_-di5J(8="un+t,8e0wH-0muP<~@~@w2z\$4r4#r'0@{rP~(}%{r[H0'W6wZJQ
2021-12-02 20:22:31 UTC	1361	IN	Data Raw: af 34 4e 97 cb 74 eb 3a 59 59 ae cc bc 98 de 82 97 10 c5 33 8b 3e e3 9e e0 cc b7 5c 4b b2 e4 1b 3a 9c 41 46 64 b3 df 72 3d fd 93 cb 57 12 7b 33 7a 95 b9 aa d3 9c 3d 9b 2a 9a df 67 d6 6e 36 e9 2f 9b a3 ae 97 92 c8 c9 7b ad 6d b5 6b 0b 39 ad a7 36 0d c0 2f 2f f3 7f e9 4a 9f b3 d7 a9 fc 37 5d ed 6f dd 6b be b0 e6 74 9d 2e f0 b6 6b fe 0d 9d 7f e9 e5 f7 99 a4 cf bf 0a 5f e9 62 c6 75 b8 f0 af ee c3 7f 61 b0 ac 6e de 9c 75 ca 33 d1 6a 44 f1 33 6d 60 75 56 bd c4 59 1c f1 d1 81 82 3b 14 3b a3 24 f8 18 25 3e 9b a4 5f f2 55 c9 7a f2 0c c8 0b ca a8 3b 29 36 db 8a bc a0 ec bd 59 a0 b4 89 62 51 d2 30 91 b1 81 e9 95 0d 2a 75 78 cb 8f 3a 8d 2e f2 66 df be 2a ad c8 d1 ff d7 dc 97 37 b7 ad 2b 7b fe ef 4f 21 f3 a9 3c e4 35 a3 48 5e 62 4b 0a 8f ca f1 1e af f1 9a d8 c7 2f Data Ascii: 4Nt:YY3> K:AFdr=W{3z=~gn6{/mk96//J7}omt.k_buanu3o&izOdrT;;\$%>_Uz;)6YbQ0*ux:.*f*+{O <5H*bK/
2021-12-02 20:22:31 UTC	1362	IN	Data Raw: 58 33 c4 9a ad 58 1e 6c fd 35 d7 c4 ec a6 0d d1 a9 20 11 51 12 7e 88 ac 8f 66 eb 43 13 53 18 7c 88 a8 bf e5 69 2d fd 01 53 fb 7b 9e f8 81 87 1c e2 2e 0d 33 31 27 1f 12 48 70 d2 c1 0b e6 28 c3 18 45 62 d6 a0 ca 91 4f c2 13 66 0b cd 2f 70 78 e3 29 40 07 b6 ba af fb 22 36 63 5f 44 df 5e b6 cb 6c 75 59 91 17 c2 c1 b0 29 1f 35 e5 a3 26 3f 3a 37 43 7b 1d 85 79 bc a8 a2 03 fb 31 5c 48 37 d8 50 38 c9 ee ef 98 98 cf 9e dd fa be e2 8f 32 3f 5e 56 05 3f a9 2b fe b0 65 4e 20 21 a9 35 7f 3e 74 7e b4 5b b0 41 b3 Data Ascii: X3XI5 Q~fCSj ~S{.31*Hp(EbOf/px)@~6c_D^luY)5&?:7C{y1H7P82?~V?+eN i5>~-[A
2021-12-02 20:22:31 UTC	1363	IN	Data Raw: 1d 30 ed ee c7 be 91 40 fc 21 ac 3f ec 98 19 89 b2 11 7a 9a c1 dd 08 7b 99 ed 37 75 ab f5 e0 8a b8 b1 44 97 e7 60 31 7b 49 cb 7a bc 98 bb da ca c5 ef 20 a7 89 b8 02 1e 8f 66 15 5e d1 0a 0b 44 f1 33 6d 60 75 56 bd c4 59 1c f1 d4 ba 96 6a 47 73 12 98 55 bd 5a d6 de 9b ef 51 3b b3 6a 85 ab d2 21 94 dc 33 27 40 7b 2c 73 cd 57 2c 8b e7 1c 81 01 d1 81 03 29 01 5d f5 d0 55 24 ac e6 9e 25 dd 52 7b 80 ae 55 ed 81 e6 dc 6a e3 9e 8a b2 22 3e c1 bf cc ad 71 e7 42 c7 4d 9f ce 3f 81 70 45 8a 5d a3 6a 86 d5 c0 f3 ae 0f e7 dd 9a b1 18 d4 e0 02 ff f2 46 46 a9 51 d8 39 a4 fd e0 de ba 25 5f f7 6a c5 d7 4a 07 58 74 0d b9 a7 22 14 99 e5 f7 3b 70 78 75 4b 2a 5d 85 2a 3b b5 1f 84 84 7b a5 23 42 b7 49 dc 0d 94 44 1d cc 5a ab f3 cd 2a 49 09 bc 54 23 fc 01 bd 61 52 50 12 1b 9e 27 Data Ascii: 0@!~2{7uD`1{lz f^D3=~uVYjGsUZQ; 3~@{,sW.))U\$%R{Uj}~>BQM?pEj}FFQ9%_jJXi";pxuK~*~{#BID3*IT#arP'
2021-12-02 20:22:31 UTC	1364	IN	Data Raw: 9f 83 1a b4 c1 25 a0 e9 6a 42 3f 9b bb d5 a5 e2 89 90 3d 06 92 3d 8a c6 98 bb fe 43 2b 19 26 ab 5a 71 35 51 25 c9 d1 92 2d 2c e3 59 05 d3 0f cd 34 cb 26 39 63 8e 56 24 68 ea b2 46 3c 0f 99 81 b4 31 24 b0 ed 30 01 6b ea 7e 1c f7 08 eb 7b 8b b2 28 6e c1 d9 cf d3 e0 ac c4 69 ba 4c b5 17 85 b1 42 68 98 52 60 50 f8 7e 0f 71 a0 ca 22 24 61 c9 9e fb 50 c1 a9 fd 91 54 d5 4b 83 17 ba a6 d8 68 7b 74 4b 0f e1 2b 19 b9 fe 9c 11 2a 4e 07 e5 dd 06 77 c2 60 18 28 c3 c2 73 29 95 57 0c 6d 29 bd 19 2c 5b c4 5f c4 7a d7 10 35 af 14 e8 6a 49 c3 25 ae 28 f2 7e 4a 45 65 d4 a5 07 91 5c 21 96 28 25 42 2e 6c 71 bf fa 49 3e 48 44 67 d8 f3 e2 79 65 79 1d b5 e9 f1 62 67 f0 b5 ed 1d 8a ff 7d c2 3f b7 65 54 91 da 66 88 39 23 30 5c 24 c0 1a bc 74 d0 54 09 d3 72 a2 1e 58 d2 b7 0f 53 79 Data Ascii: %jB?==C+&Zq5Q%-_Y4&9cV\$hF<1\$0k~{(niLBhR'P~q"\$aPTKh{tK+~Nw(s)Wm)_[_z5j]%(~JEeU(%B.lql>H Dgyeybgj?eTf9#0\$!TrXSy
2021-12-02 20:22:31 UTC	1365	IN	Data Raw: 0d 72 7d 0a a7 67 23 c9 26 98 3f 18 27 e3 16 48 3d f5 af 20 d3 c1 8f 41 38 74 8d da 01 fd a0 28 81 5e 38 2e 6c bf 0c 3a 7d 4c 5d 5d 6b 35 f1 c1 4e 1b fe fb fe 8b 51 f3 42 20 91 20 fa 68 58 78 7b b3 85 e9 5a 27 dd 0f 1e 01 3e c1 83 d0 a8 75 b1 06 ce 4b 23 f5 1c f6 68 ba 01 65 7a 8c 59 6b 9c bb 4d 77 d8 8e 73 87 b9 53 7b 50 4d 71 36 a6 ec 51 55 b2 f5 51 b5 2e 98 a9 fb d4 8e 5c a0 c3 d2 a0 33 89 da bd 91 ed b1 5b 24 92 af 8b 7b 84 ea a0 e1 74 6b a7 80 f9 e9 48 dc 9b 73 6f bd 3b f2 b4 8f db 74 e6 a5 e4 46 3f 2a 53 24 c7 9c c1 eb f3 e0 9d d3 78 31 0f 07 e1 e3 0c 7f a2 68 71 8a db 35 41 8b 72 02 2f 17 44 d5 30 ba ae 0f df 0e ff 7e 18 0c e0 aa fc d9 b9 09 e2 62 9b c3 93 73 1e 4e 7f d8 87 b6 2e 42 1e 9b 4e bb 37 79 49 0c cd b8 9a ef 49 d5 cd 26 56 93 fc 7c d9 f4 Data Ascii: r}g##?~H= A8t(^8.I:.) k5NQB hXx[Z~>uK~hezYkMwsS{PMq6QUQ_!3{\$_@tkHso;f?~\$S*x1hq5Ar/D0~b sN.BN7yII&V
2021-12-02 20:22:31 UTC	1366	IN	Data Raw: cb 1c 04 b7 77 20 dc 65 19 f1 16 af 4c 90 11 ea cf 3a 73 1c 61 2e 70 7d 8a 70 4c 76 d5 19 37 5d b8 3f 48 97 35 55 de 10 99 6c b9 3d 12 93 68 5a b6 36 1c e2 47 17 c1 2d 05 bf db 9b 1d 1a e8 32 f0 e7 3c 1a b9 fe 42 08 ce 1d 8b d6 00 67 c4 06 81 d3 72 9d 33 1c f4 52 07 87 9d e2 02 51 7f b2 89 81 49 79 f0 a3 c9 88 26 2d 4e 30 d6 1d aa 38 41 5d 77 88 3e 3c ac 93 4b 05 31 99 39 21 76 ac a2 0f d3 90 a4 a1 c0 3a c3 98 c1 94 f9 ab de cc cb f1 c1 11 80 f7 1a 6e e9 bd c2 d2 b5 cb 7f 39 91 04 0d 96 98 a4 f7 71 e4 1f 79 a1 23 4e 42 ec 17 8e 36 0b 05 45 6a d9 49 03 6f a0 61 8e 5a 53 17 23 c8 4d e1 bb 03 27 7c 7a 86 62 ea fe 9f e7 6a a9 5c a6 69 9a 50 77 26 4e 60 e3 6c dc 37 ce 89 7e 31 76 06 5a 45 39 6d ee 68 86 51 8c 47 6c 1e 8d bf a0 d6 cd 58 f5 db c4 88 23 11 74 69 Data Ascii: w eL:sa.p)jPlv7?H5UI=hZ6G-2<Bgr3RQly&-N08A]w><K19!v:n-9qy~NB6EjloaZS#M{jzb}iPw&N'I'7~1vZ E9mhQGI@X#ti
2021-12-02 20:22:31 UTC	1368	IN	Data Raw: 93 80 46 59 4e 27 32 55 01 e3 7c f3 6c ff f4 c2 c0 78 d7 b7 7e bf 16 da 37 91 74 13 b1 79 85 9f ff 32 4f 1f 5c 90 ae a5 08 de 75 24 43 14 5d 68 a8 ab da ea fe 32 0c 10 a6 6c 6b c5 8e 04 c4 20 e1 a9 a9 f1 92 0d 18 6a 02 30 80 79 a0 40 d9 2f 55 b3 62 1b a2 64 01 8e ef 7e 0b 53 b5 f4 87 85 4e df 0d d8 e2 30 6c 0f c6 05 63 91 a2 2a bb d0 e5 d2 4d e4 b4 80 3d 80 14 8c 85 1c bc 20 1d 3f a2 e0 84 3e 79 cd ea 0c 2c 2c d1 53 d4 00 60 c2 4a ac 13 06 48 62 c9 fb 7e 1f fd 84 c7 61 ea 09 f0 75 ea 35 9c 40 87 78 bc 81 23 82 1d 95 a4 bd 80 36 0c c4 d8 8d 9d 20 55 99 93 fd 5c 84 ee d7 3e b8 6c 0b 6d da 73 ab dd 09 b3 1f 3a 87 5f 5a 47 c2 77 c7 30 7f de 64 8c c8 9f 6f d3 fa 91 0f c7 c4 b7 31 25 51 40 fd e1 c7 7b f7 c9 e5 6a 86 0d df 0d ec 73 5c 33 2e 2f 76 3e ac a3 7a aa Data Ascii: FYN'2U lx~7ty20u\$C]h2lk jOy@/Ubd~SN0lc*M=~?>y,,S`JHb~au5@x#6L U>lms:_ZGw0do1%Q@{js3./v>z
2021-12-02 20:22:31 UTC	1369	IN	Data Raw: 11 a5 24 d8 16 ee 91 41 a9 d7 a6 73 1f 16 f8 be 96 38 46 86 a5 9e ef 44 f5 2d 3c 11 4e ed b7 1f 8f b5 a0 74 1f d9 3b 13 f8 bb 09 ac 87 85 cc 0b 0c ad e5 f7 dc c0 58 f3 d5 77 38 69 b7 06 68 47 bf 0f 29 6e 03 c4 08 89 ef cb 25 a0 69 6c 8d 7f 8c dd 77 58 7b 4f c3 70 88 be 02 c3 3e 48 56 4a 98 18 84 6c 7d 8c b3 a9 e3 e7 8b 51 14 1d ea 27 e2 67 db d5 8d 9a be 92 21 be f2 2e ee 0b 17 de 2d 21 6a fb 89 fa ec d8 f8 33 fb 01 41 7b 2f ec 7c 51 da 55 06 c3 ef 0b 0b f1 4d 2c 7c b5 c6 bf be 23 74 17 5d 7d 63 cc b3 d7 aa 56 5d 3c 10 8d 9c fa 49 39 67 83 e5 2d 60 48 93 08 53 87 57 b6 57 c4 7c bb 6c b3 a2 1f 07 9e 23 4d c0 2f ae 53 d1 4d b3 aa a5 be f6 31 bf 3c f4 31 90 88 ad ea 76 e4 26 ab bc 7a c9 df 0f a9 ce 1d 0a e9 c7 15 9d 3c d5 87 77 8b 1b 3b 0f c7 a2 71 2f f9 fb Data Ascii: \$As8FD<Nt;Xw8ihG)n\$oilwX{Op>HVJl]Q'g!~.l}3A{/ QUM, #t]cV <I9g~`HSWW]#M/SM1<1vz<w;q/

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1370	IN	Data Raw: 07 7a 35 ef 5a d2 1b b9 95 39 03 0a 9f 4d 4f 21 6a 1b 35 a1 78 3b c5 cd 03 e3 39 b6 42 b6 25 a0 03 27 b0 fe db f2 5d 12 59 db a8 cd 2a fd 48 46 6b 84 1c ca 00 57 18 4b 06 da fc f1 fb a7 49 a4 ee 60 76 7b d7 fa db a5 5f e8 b6 67 2a 97 6c 3a 29 15 c8 12 c2 12 52 2c e5 9c e6 4b 39 c0 12 a4 2f 7f ea 6d ca 99 5f b8 fb c3 87 ce 83 24 78 a0 62 7f 5a 78 90 b3 e9 8e d8 ba df 3b 0a 3a d7 65 0a f0 e5 f4 c3 60 04 74 9a dd 63 41 49 52 85 12 74 d0 8e 53 49 10 08 9c 53 ba c1 e7 36 7a 1f 74 a5 5c 73 92 10 34 e7 34 cf 3e 68 d1 c6 44 0a 07 ae 8d 7e 22 44 67 be 73 4a 2f 93 f8 ce 64 d7 6b a9 38 07 0f cd a8 c8 7d e0 44 0d f4 81 78 8e 59 ee 5a cb e1 ad 6c 9d 96 f6 9e d8 d7 1b 24 59 e1 3d 2e a5 59 0c 17 d1 74 08 c4 76 d1 f0 e7 8e 46 7d bf 8d 7e 35 62 7b c0 6d 8c fa d5 72 d0 Data Ascii: z5Z9MOlj5x;9B%]Y*HFkWkI'v[_g!:)R,K9/m_\$xbZx;;e'tcAlRtSIS6zts44>hD~"DgsJ/dk8}DxYzI\$Y=.YtvF]-5b{mr
2021-12-02 20:22:31 UTC	1372	IN	Data Raw: 4d e4 70 a4 33 69 29 ff 17 21 03 06 b1 68 22 e4 40 0a 6b 46 4d aa f0 d8 e2 bd 80 5e b6 5c 4b 10 fc 3b 9b 1d 4d 7c 3f 0c 03 81 f3 27 01 7b b2 92 11 3a 42 da 73 f7 d7 39 ce 63 29 e9 52 30 79 5f 63 f2 cc a8 81 99 3f 65 7b 60 a0 b4 b9 cb 71 6e 22 a6 cc 2d 5d 49 51 a3 82 c7 e9 5d ff f7 ef 16 87 02 ba 68 54 41 33 d3 93 c9 52 d1 c2 42 d0 b8 aa d6 18 94 b0 dd c3 70 34 18 e5 0d 4c 13 96 e0 65 57 b6 31 6e fb 0f c8 cc 9e 10 02 99 76 4c 7a e5 54 bd c3 2d 1d 92 9e f8 50 be e2 aa 9a e2 88 87 71 2b 63 9a ce 43 d9 8a 94 93 37 dd 4e 87 35 61 22 69 5f 38 3e 4c 8d 25 7c f1 a3 4b c8 80 ba b0 fc 8d 69 2a 45 51 7e 86 a2 d8 d5 c4 43 82 f2 e3 cd 6e e6 cb 0a 7d b4 5c e4 9e 22 80 7a bf b1 34 60 7b 92 84 de db 9e 4e 36 73 3e ba bb 13 81 7c bf ca 48 da f2 a4 2b d8 3f 99 e5 93 56 a2 Data Ascii: Mp3i)lh"@kFM^K;M]?{Bs9c}ROy_c?e[qn"-JlQ]hTA3RBp4LeW1nvLzT-Pq+cC7N5a{__8>L% Ki*EQ~Cn}\'z4'{N6s> H+?v
2021-12-02 20:22:31 UTC	1373	IN	Data Raw: b8 3d c1 2d 3d 0d fd 09 bf 1d 3e 44 3b 12 68 86 be 02 a3 2f c0 3a 09 72 8a 90 5d 36 2e 22 57 b4 5f a4 56 39 41 4b 8e 5f e4 26 7c d9 7e 4e 4f ac b7 49 27 c7 8a 4e dc d5 ff 8b e2 fc a8 0b 20 e8 1b 0a 4d b8 b0 5c 59 2d 1b 8c c6 8d 4d 3b 98 92 91 1d 78 0f f2 d5 cc a8 63 f7 f0 c8 9e 32 41 e5 b0 58 42 73 f3 7d d3 55 9e 16 33 0c 6e 85 20 ed 69 21 5b f7 ea c4 91 e6 0c 09 60 21 06 96 11 ec fa bd 0f 4f ed e1 78 82 b2 fd 68 e8 17 c8 8e f1 dc 0a 41 ac ef 75 5e 0b fa b3 51 61 d4 22 ae e6 85 85 09 22 29 c6 07 6c d4 7e 12 00 27 1c dc e9 cb fe d0 cd 88 7b 4f c5 e1 e8 0b 9a 4b e8 f7 5a 0b d1 25 50 6f de 7e be 4e 6f 96 d9 99 b2 de 34 12 51 50 d2 05 03 37 c4 2b 75 44 87 b6 d2 e2 2d e9 d9 ea 02 fd af 74 08 f4 41 0b ec 05 97 c0 21 36 b9 b4 56 5e 46 76 71 ea 3a 1b 4f fa 0b Data Ascii: ==>D;h/rj6."W_V9AK_& -NOI'N MIY-M;xc2AXBs}U3n il['!OxhAu^Qa'") ~-{Gt6#%Po~No4QP7+uD-tA!6V^Fvq;O
2021-12-02 20:22:31 UTC	1374	IN	Data Raw: a4 6c 4b dc 2d 82 ad 63 6d 2f ab 19 28 72 13 1d e4 f0 af 10 95 ea 08 18 1c 90 ae 59 78 50 b5 f4 27 74 72 73 f3 38 26 6a 4a 25 cf 3c 42 da 6c a2 23 02 0c c2 51 5e 44 67 0b d3 8c 1d b0 92 a5 8b 1b 9f 00 25 a1 3d 5f 4c 9a 72 15 f3 94 fa c4 b3 10 7f c5 f6 f5 81 f7 e2 81 f7 70 e0 2d ab 46 cf 61 0a ec 87 d4 86 a5 0b 01 9e 08 33 da 8c 71 a0 3d 21 b4 b6 8b 78 78 54 e2 9d 87 f2 47 05 0e 35 76 25 bb e1 f4 c3 d4 3e c6 be c3 c2 22 d3 26 a8 bf 76 31 c1 cf bd e9 ad cf f7 e7 f3 1d 52 68 38 66 7a ab dc 17 19 cf f1 3e dd de 26 ea d3 0d 66 2c c6 8c a6 e5 71 6e a9 bc ba 1a 4b d0 70 90 5b e1 2d 16 da bd 49 1f e0 3c 84 92 8e 15 c4 5c 65 63 4d 46 d7 a0 ba 19 66 b0 dd 44 71 a6 e7 d1 c1 fc 3e b3 04 34 17 53 9c 67 0e 93 3a ee 93 74 ca 49 a1 46 05 18 5e d4 04 11 57 f4 52 b1 28 ca Data Ascii: lK-cm/(rYxP'trs8&j9%<Bl#Q^Dg%=_Lrp-Fa3q=lxxtG5v%>~&v1Rh8fz>&,fnKp[<-l<cmFFdQ>4Sg:tlfWR{
2021-12-02 20:22:31 UTC	1375	IN	Data Raw: 44 22 c5 af ac d7 17 f5 3c 28 c7 a1 8e a3 c9 00 8d 16 21 3b 96 53 b4 63 61 28 4d b7 fd 1e 7a 90 20 36 92 72 77 9e 4e eb 3f ae f4 b0 93 b0 17 64 57 5b 44 f7 51 39 96 2c dd 1e 9d e4 7a d9 1b 38 b2 86 38 96 46 7a b4 4b 7d 2e d1 40 bf b7 39 c3 cd 9e a9 13 48 88 57 4c 3f b9 62 ae ff 44 fc ef de e7 15 4a 1d 79 67 a4 76 fd 48 42 a2 c4 9b f1 bd f3 72 96 d8 9b 12 bb bb be 43 b9 24 ec 25 72 b2 07 20 f4 a1 1a 67 6b bc b0 b0 8f 48 66 e8 51 49 94 df 2f da d7 56 bd 3f 7b 6f 1f 08 be 5a bf fe 87 5d 78 90 1c a5 4d ce b2 14 2b 53 ec af 62 c7 43 1a 28 6c 26 63 1f 18 0a 6a 60 46 09 71 c0 87 12 fb 19 8e 39 28 c6 98 7c 38 30 3f ae cc ef 57 b8 ff ea 88 5e 88 78 f0 d6 1f 62 ce 9f 00 73 75 74 dd 97 b3 90 ac 6c dd f6 78 54 43 9f 0f 18 bf 2e e2 97 66 01 89 b1 d5 5f 0f 66 40 eb 49 Data Ascii: D"<(!;Sca(Mz 6rwN?dW[DAQ9,z88FzK}.@9HWL?bDJygvHBrC\$%r gkHfQl/V?{oZ}xM+SbC(l&c'Fq9{(l80?W^x bsutlxTC.f_f@l
2021-12-02 20:22:31 UTC	1377	IN	Data Raw: 51 96 c4 5f c6 41 5b 67 e3 c1 5e 88 48 eb 5b 93 ee 40 42 94 d3 87 e9 b8 82 1e 5a 94 11 90 9c 2b 09 2b b2 0b 13 e0 f8 8d b8 49 05 66 35 ab 6d 5a 0e d9 86 47 85 16 95 2b 04 58 50 2e d8 b6 f4 f9 63 b7 1a ed cd 35 34 74 66 53 f7 c2 b8 9d 2f 53 ee e1 1c e1 52 f6 f1 ec e2 34 f1 36 15 8e 37 a3 6f 79 1f ed 27 c1 8a b1 f1 03 99 02 74 24 52 80 a6 df f3 8e d6 17 8d 12 03 61 23 4e 49 28 33 f0 d6 d9 39 29 ac a3 f6 00 be bc d3 30 a3 f2 15 5c 45 7c dd 70 3c 48 bc 4e 78 ae 14 10 9f bb 53 40 c0 71 e0 2c d7 a1 07 87 62 c9 43 0b 2d 97 c4 e2 e1 58 c2 a2 75 66 e9 30 3a d7 82 7e a6 34 f8 f4 b9 7f a2 1f 74 8b 16 ef 94 2f 03 11 1c 99 ad e0 71 30 18 98 65 01 0f bf 40 a7 17 19 79 29 69 52 0e f4 09 3c c7 1e 8b 24 ab f8 35 20 a0 23 7e 9c 78 4d 76 98 0d 9b b6 15 fa 45 01 6c 7b 31 d2 Data Ascii: Q_A[g^H{(@BZ++Hf5mZG+XP.c54tfS/SR467oyt\$Ra#NI(39)0lE p<HNxS@q,bC-Xuf0:~4t/q0e@y)iR<\$5 #~xMvEl{1
2021-12-02 20:22:31 UTC	1378	IN	Data Raw: 54 56 d0 80 40 07 34 94 c2 3c f6 72 53 39 2a 7c a9 64 8a 2d fe 7d 27 c4 cd 92 af 11 2d 38 63 76 8a 58 72 e0 34 ad e7 bb 98 c5 11 2e 46 bb f5 63 b3 6b af 61 6a f3 73 b3 05 17 5d d8 6f 40 0e 95 3b 6e 4b 05 ab 7c 9f 99 5d e4 bb 2c 91 70 83 8a c8 a5 8d 9d 8f 1e 63 07 1e f9 6c 20 9f 0d b3 cf 1e e5 b3 51 f6 d9 50 3e 1b d7 9f 8d e4 b3 49 f6 d9 44 7b ce 3e 7b 92 cf 9e b2 cf d0 e2 cb c9 4b 5e 26 d2 ff d1 31 f6 8f f7 2f f6 37 0e 8d 5c 85 de 6e f2 e7 5e 22 23 1b d3 61 22 ed 8a 9e 82 e4 4a 9a 00 82 ec fc 09 5a 6c 42 a1 88 8d cc 2f 45 fb e6 9c a9 ed 21 ad 01 13 f8 01 ca 25 de 41 6f aa 74 9e 6a 62 85 59 77 3c 9f aa 6c 39 7e ec d7 3d 3c c3 46 70 f7 c0 30 7a 78 fb 4b c2 85 a8 3b cb da 7f 48 d6 fe 44 e1 c7 3c 08 3f fe fa 54 49 01 bd 32 d3 95 a0 93 2a ff 3c b3 1b 5d f6 Data Ascii: TV@4<rS9*[d-}'-8cvXr4.Fckajs]o@;:nK],p! QP>glD>{>[K^&1/7l^n""#a"JZlB/E!%AotjbYw<I~<=Fp0zxK;HD<?Tl 2*<]
2021-12-02 20:22:31 UTC	1379	IN	Data Raw: b7 93 53 73 4c 98 ce 96 5d 29 57 ac 92 07 0c 23 ea f7 a3 4e f8 01 5d 27 05 be f5 9d 88 b7 16 f0 cf 01 a2 3f 63 f4 fa cd 29 f0 ec 2b f8 c7 92 1e 88 68 c3 f1 9c a7 6f 94 76 14 23 9e 61 1f a0 7d 92 58 28 46 8b 3c ba e8 6e 79 7b 57 47 c6 43 08 20 8f 08 a0 12 fb c1 66 b8 90 c6 79 42 c5 73 10 1f 12 77 de 90 42 53 64 32 3d 7c 9f 23 be fc 86 1b a6 38 77 57 1d 0d 84 40 45 08 42 98 ce 4a 1a f3 b3 90 1f 14 f4 ba 03 1b 7b e9 97 ab a7 a5 79 89 59 4b 7d 2e b1 75 0c f2 dc 77 b0 28 9a 49 be 84 14 5a 4c 92 c5 4f ec ea 4f 81 3a 00 83 c9 b1 a3 c2 83 14 13 ae a0 33 9a 7c 1f 42 7b cb 7c 7f 57 7a ca 3f 9a b2 80 d2 fc 79 7a 7c 3d 67 01 c4 f7 49 2f 41 0a b8 c8 b3 77 13 b8 34 1c e8 28 c0 47 d3 fa 22 98 34 6d 0a bb 3c d6 a8 ac 4d 40 59 66 9c 2b 5d 6d 67 98 67 a4 3c a9 d0 8c db 94 Data Ascii: SsLj]W#Nj?c)<hov#a)X(F<y{WGC fyBswBSd2= #8ww@EBJ{yYK}.uw{lZLOO:3 B [Wz?yz]=gl/Aw4(G"4m<M@Yf+}mgg<
2021-12-02 20:22:31 UTC	1380	IN	Data Raw: e7 02 d6 6c 37 f1 22 02 5a 8f 3e 4b 60 9f 7a b4 b8 68 31 b7 69 f7 60 bf c6 2c 75 b7 d1 1d c1 bc 37 4c 7f 71 11 6a 07 bf 7f cf 77 02 f3 05 24 17 7c c4 48 62 96 55 33 08 03 3a 53 0d b6 8b 10 ea 35 9d 66 7e 3d f4 66 77 ca 9f 31 a4 be 03 7f 31 ce 2b a0 d4 87 f7 75 ae 83 c8 f8 a8 20 fc fd bb c9 8e 04 4a 2d b7 4a 2b 43 61 eb ac b0 34 28 7e 7d d2 68 15 95 30 7b 49 25 4c 2b b1 d8 a0 1d 5a 60 f3 31 de 44 bf aa 98 94 ed 49 f3 ad 1f 9b 6f 7d bb 62 c7 2e f8 68 c7 f5 ce 35 ca 60 e1 6c 3d 10 88 31 de 59 8f 0d 39 31 e6 80 b0 84 3d 94 fc 64 3e 3a 01 4b cd 87 f3 88 53 d4 12 c8 40 35 66 59 5b f8 8a 2d 5d 65 54 27 6d d8 5e 2b 4e 62 42 dd 47 e7 07 98 66 2e 46 0a d1 00 fe bd 80 f3 6a cb 9a f2 07 bd 90 9c 61 fb f6 89 c6 91 85 46 03 f7 12 42 d9 b8 91 cf 26 5a 26 c4 d4 a7 3c 94 Data Ascii: l7"Z>K'zh1i",u7Lqjw\$ HbU3:S5f~=-fw11+u J-J+Ca4(-)h0{!%L+Z' o1Dlo}b.h5'l=1Y91=d>:KS@5fY[-je T'm^+NbBGf.FjaFB&Z&<

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1382	IN	Data Raw: 10 d8 42 10 24 1d 80 75 d6 52 ae 87 f1 07 c3 69 cb 92 8f 9a c4 51 3c 78 fb 1d 4c 15 26 d4 e2 42 1f 2a f5 f2 67 27 aa 47 1f 3e 48 07 d5 26 32 1e ff b6 75 87 d0 c9 fc a6 16 ea 8e c4 95 35 c5 38 1a 44 63 0d 4d 1a b9 40 4f 8b fe 72 90 fa 08 e0 60 b4 98 50 6f 1e 5b 60 b4 63 68 dd ff 8c 2c 46 f4 19 4e 96 96 ac 12 dd fa 77 e8 87 91 67 b8 39 4e ea 59 dd 20 f5 5a 09 f2 21 50 c0 6e dd 3b b8 0b ff a6 6a 46 59 5f 6f 26 cf c5 c5 58 1c dc 43 7a bb 74 cd 1b 71 f2 da e1 35 62 d5 57 ca 15 0c 4b 36 b7 d4 9a 3d 8a 99 01 f9 ad f7 dc c9 b8 05 42 fe 2f 4a c2 79 56 94 e6 09 21 d4 2a e1 c5 aa ad 54 ca d4 d6 b9 28 03 d2 f8 85 58 d2 56 6d f9 b3 88 4c d7 df b5 21 52 be 08 8f 20 21 30 a1 cb bf e4 45 cc 29 2c 5b b6 59 d1 db d4 5a 42 c8 a0 d7 77 b5 44 7f 77 05 82 21 9c 0c ec f5 32 8d Data Ascii: B\$uRiQ<xL&B*g>H&2u58DcM@Or'Po['ch,FNwg9NY Z!Pn;]FY_o&XCztg5bWK6=B/JyV!T(XVmlLR !0E),[YZBwDw!2
2021-12-02 20:22:31 UTC	1383	IN	Data Raw: 21 ba 01 19 fc a2 a8 cb 8b ff aa 58 ef de 9b 46 77 58 ea b6 09 25 4d 8d 5b ba 9e 0d 55 78 8a ae ff d0 c9 6e 18 e2 81 61 24 95 8f 9b 42 a1 3f 36 af b9 c3 d7 ff d8 e1 23 d1 44 dc e1 44 9d 19 2b ef a7 7a 33 7f e0 f7 a4 48 a1 f2 dc 71 9a 3b fa f6 fd 25 53 4d cb c9 01 2c c2 31 de d8 84 23 c9 45 d3 35 b3 12 8b 97 20 43 ac b6 01 07 c6 8b fe 03 4c 22 5d 7b 4b 37 1a a7 7a fd cd 4b 74 67 06 9f 8e 96 cd ef e2 14 85 e9 d4 d1 28 9b 63 16 56 9e ff df 70 43 a2 d3 5c e2 5d 49 39 ea 4 32 f9 28 1d 78 eb 3a f2 8d 52 cc 52 d4 2d 26 c0 7c 3a 22 17 77 3a 30 08 b2 b9 9e 49 36 e9 d9 b3 5b 48 36 73 ff 1b 50 4b 07 08 94 8d 3c d4 71 08 03 00 52 5d 09 00 50 4b 03 04 14 00 08 08 08 00 29 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 13 00 00 00 6d 69 72 72 6f 72 69 6e 67 5f 77 65 62 72 Data Ascii: !XFwX%M[Uxna\$B?6#DD+z3Hq;%SM,1#E5 CL"2{K7zKtg(cVpC)]92(x:RR-&[!~w:0l6[H6sPK<qR]PK)Qmiring_webr
2021-12-02 20:22:31 UTC	1384	IN	Data Raw: 74 61 64 61 74 61 2f 76 65 72 69 66 69 65 64 5f 63 6f 6e 74 65 6e 74 73 2e 6a 73 6f 6e 95 59 5d 73 a3 38 d6 fe 2b 5b 7d bd 53 85 c0 38 ed bd 8b 0d 02 13 23 07 a1 0f d0 d6 56 17 20 62 0c 02 13 1b c7 c0 d4 fc f7 55 7a e7 e2 dd e9 6e af df 8b 54 ca 36 20 ce a3 73 9e 0f f8 e7 ef 5f 64 79 29 ce c7 7e 38 9e ba 2f ff f8 32 9c cb b2 ca 2e d5 df fa f2 fc b7 b7 a3 2a bf fc fd cb e5 78 e8 4a f9 ad 38 75 43 d9 0d 5f fe f1 fb 97 3e 9b d4 29 93 fa f8 72 0a ea dc b4 0d c1 6d 23 31 ab aa 30 2b 55 4c db 25 b7 2e c7 b4 1d 3f 52 73 78 2b 4c b5 14 f1 76 89 9c 67 1b 1d 6f 47 e1 a9 4e 2a c8 d8 6a d7 a3 3e 8e 0a 6b 6a 6e 3f bf 6f d5 45 24 e1 71 af 86 a7 6d b7 ae a4 77 38 ee 8f c1 5b ee ad ea 94 8f fa ba ab 24 8f 57 83 3e 77 4e b9 d4 9f ed f7 c2 5c 5d 3f cf 2d da d5 87 84 ab 53 Data Ascii: tadata/verified_contents.jsonY[s8+[]S8#V bUznT6 s_dy)~8/2.*x8uC_>)rm#10+UL%?.?Rsx+LvgoGN\$>kjn? oE\$gmw8[*W>wN)]?-S
2021-12-02 20:22:31 UTC	1386	IN	Data Raw: 8d d5 b8 77 ab 1e f9 fd 3b 85 a8 8f 3d 10 a6 bc 5f a7 ec eb 2d 35 c6 1b aa 05 2c 3b 11 c9 5a 41 de 60 40 7d 6c 44 f4 eb dd b9 cb 1e e6 bc 40 84 6e b0 0d cd 60 a3 fd 14 8a 5d ad 3b ad 60 68 8e 00 4d 54 af 7b bf c7 5c 78 61 c2 96 a1 39 10 cc c4 89 98 41 58 b8 77 b1 ef e5 f4 a0 c7 25 12 84 cd b8 d3 35 ee 78 b2 1d 32 2a 68 d1 08 9e 83 fe 43 b6 ab 29 d2 76 af 30 d9 7e cf 01 8c e9 68 a6 16 fc 28 0c 85 ee fb ac fe 51 9f 05 50 a2 71 21 e2 45 78 81 d1 5b 68 1d d5 30 c8 79 bf 4f 09 bb e6 04 5e 23 a5 1c 62 29 a1 fb 11 15 d0 d5 fc 88 dd b0 66 ec 2e f6 e6 e2 d1 be 77 e5 5c d1 94 06 15 82 ab 44 76 ea 35 aa 55 20 4d 91 c5 47 b0 c4 00 3a 29 0f 7c c6 45 9f ce 87 45 de 55 9b b2 b1 d7 92 d2 7b d8 9f f3 07 b1 8f 2c 76 94 dc 00 d8 0c ed b0 45 2e 6f 82 ad f4 4e 37 ca a5 9d 1a Data Ascii: w;= _-5,;ZA"@]D@n";'hMT[!xa9AXw%5x2*hC)v0~h(QPq!Ex[h0yO*#b).f.w!Dv5U MG:)]EEU[,vE.on7
2021-12-02 20:22:31 UTC	1387	IN	Data Raw: 96 42 1a e8 25 e4 bd c9 e9 a8 bd 36 e6 7b 58 18 d2 d3 07 df c1 be 6c 0f 0f 66 2b b8 29 dd f1 84 d4 69 48 2d 76 2e a8 3d 69 7f 41 11 ac b6 74 0e 2e 05 c7 22 56 18 84 b5 6a 33 4b 56 b1 c9 52 62 9d cc 18 de f5 f7 cb 0c ae 28 7b 34 5f f1 40 73 6b df 0a 4f 6e 50 17 6c 18 0c 7a c6 18 c8 3d 65 f3 0e c6 92 04 bb 90 e1 25 51 eb 17 4a 82 58 fb 11 77 17 6b 6c ff 8a 7f 0b af c2 62 97 34 d9 ea 7a c3 9f 61 fd 41 67 d6 d0 4e 86 fa 5a b7 bc 0e 04 33 d4 db de 03 33 03 b2 17 e6 e5 a6 7d 05 4f eb 6a 51 74 6a 4a cc 68 11 53 f9 2a 1a f8 03 bf a7 2d ac 33 53 4e b9 c5 ae 5a bf 67 cd d7 7d e1 47 bf 58 77 6b 50 17 9f 45 63 6b cd 3c d8 69 0b 74 9e 5c 5d 33 8e db c8 40 16 d3 e7 96 b5 1a c3 b9 59 c4 ce 5a df 14 c6 e1 5c cd da fb fe b8 ae 09 67 8d dd 2c b8 dd 88 5f d7 69 11 4b d7 00 Data Ascii: B%6{Xlf+)}iH-v.=iAt:"Vj3KVRb({[4_@skOnPlz=e%QJXwklb4zaAgNZ33}OjQtjJhS*-3SNZg)GXwkPEck<itl] 3@YZlg,_iK
2021-12-02 20:22:31 UTC	1388	IN	Data Raw: 0a cf 35 db 92 22 69 16 c1 61 31 ed d4 6b fe 7c 68 5e 9e 16 9d 7c 56 d0 eb 99 78 96 d3 37 8c ac a7 7c bf 5f d4 65 74 58 b4 b7 14 bd ec 3f d6 d7 af f5 38 5c b7 51 6b 7e db f5 56 e9 bd 39 57 26 f2 ab b7 ee 30 2c a1 b6 18 6d 7d fb ba 09 9e 67 cd 97 87 db 8b f9 da 6c 97 df fc cd 33 e8 e5 c9 ca 9f 36 4f 31 a6 61 75 3e de 1c ef f6 5b fd 04 62 1c 3a d7 0b 82 6b 0c 37 3d a9 cf 24 1b 6f eb 2e f9 70 6e ee b0 78 a2 c6 66 2a 2a 36 7a 46 63 90 6f 2c b0 40 9f 2d 00 f7 b2 8b ad 9c af 1f f5 b7 e6 f0 bc 30 5e 2b ce d2 97 f7 de ba 0e e4 f0 7e e1 6f db 0f 39 de be fc f1 af 3f fe f8 d7 bf 01 50 4b 07 08 16 b7 56 d0 ec 0f 00 00 a9 22 00 00 50 4b 01 02 14 03 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 09 00 00 00 00 00 00 00 00 10 00 ed 01 00 00 00 00 Data Ascii: 5"ia1k h"Vx7l_etX?8lQk~V9W&0,m)gl36O1au>[b:k7=\$o.pnx!*6zFco,~0-@+~o9?PKV"PK*Q
2021-12-02 20:22:31 UTC	1389	IN	Data Raw: 08 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 10 00 ed 01 a5 89 00 00 5f 6c 6f 63 61 6c 65 73 2f 65 6c 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 32 77 9f 34 08 13 00 00 f4 5f 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 e1 89 00 00 5f 6c 6f 63 61 6c 65 73 2f 65 6c 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 ed 01 30 9d 00 00 5f 6c 6f 63 61 6c 65 73 2f 65 6e 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 7a 25 be a9 78 0e 00 00 be 2d 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 6c 9d 00 00 5f 6c 6f 63 61 6c 65 73 2f 65 6e 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 Data Ascii: *Q_locales/el/PK)Q2w4__locales/el/messages.jsonPK*Q0_locales/en/PK)Qz%~!_locales/en/messages.jsonPK
2021-12-02 20:22:31 UTC	1391	IN	Data Raw: 02 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 10 00 ed 01 4d 32 01 00 5f 6c 6f 63 61 6c 65 73 2f 68 72 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 58 3d ee 03 7a 0f 00 00 65 31 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 89 32 01 00 5f 6c 6f 63 61 6c 65 73 2f 68 72 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 ed 01 4a 42 01 00 5f 6c 6f 63 61 6c 65 73 2f 68 75 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 5d 1c 7c 4f 11 10 00 00 16 36 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 86 42 01 00 5f 6c 6f 63 61 6c 65 73 2f 68 75 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 00 2a 8c 04 51 00 Data Ascii: M2_locales/hr/PK)QX=ze12_locales/hr/messages.jsonPK*QJB_locales/hu/PK)Q]]O6B_locales/hu/messages.j sonPK*Q
2021-12-02 20:22:31 UTC	1392	IN	Data Raw: 00 00 00 00 10 00 ed 01 f8 d7 01 00 5f 6c 6f 63 61 6c 65 73 2f 6d 6c 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 a8 68 87 8a 8d 12 00 00 0d 65 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 34 d8 01 00 5f 6c 6f 63 61 6c 65 73 2f 6d 6c 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 ed 01 08 eb 01 00 5f 6c 6f 63 61 6c 65 73 2f 6d 72 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 b9 ab d8 b2 b5 11 00 00 16 5a 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 44 eb 01 00 5f 6c 6f 63 61 6c 65 73 2f 6d 72 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 00 0c 00 00 Data Ascii: _locales/ml/PK)Qhe4_locales/ml/messages.jsonPK*Q_locales/mr/PK)QZD_locales/mr/messages.jsonPK*Q

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:31 UTC	1393	IN	Data Raw: 6f 63 61 6c 65 73 2f 73 6c 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 e5 6b e8 ea 60 0f 00 00 d8 31 00 00 19 00 00 00 00 00 00 00 00 00 00 a4 01 11 80 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 6c 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 00 00 10 00 ed 01 b8 8f 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 72 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 04 04 ee a1 ba 11 00 00 94 5d 00 00 19 00 00 00 00 00 00 00 00 00 00 a4 01 f4 8f 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 72 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 00 0c 00 00 00 00 00 00 00 00 00 10 00 ed 01 f5 a1 02 Data Ascii: ocales/sl/PK)Qk*_1_locales/sl/messages.jsonPK*_Q_locales/sr/PK)Q_locales/sr/messages.jsonPK*_Q
2021-12-02 20:22:31 UTC	1394	IN	Data Raw: 14 03 14 00 08 08 08 00 29 8c 04 51 5c 3f f4 81 9e 0f 00 00 d0 35 00 00 19 00 00 00 00 00 00 00 00 00 00 00 a4 01 f4 2a 03 00 5f 6c 6f 63 61 6c 65 73 2f 7a 68 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 10 00 ed 01 d9 3a 03 00 5f 6c 6f 63 61 6c 65 73 2f 7a 68 5f 54 57 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 80 77 20 c9 0c 10 00 00 f7 36 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 Data Ascii:)Q!/?*_locales/zh/messages.jsonPK*_Q:_locales/zh_TW/PK)Qw 6
2021-12-02 20:22:31 UTC	1395	IN	Data Raw: a4 01 18 3b 03 00 5f 6c 6f 63 61 6c 65 73 2f 7a 68 5f 54 57 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 4f 99 ea ee 33 b2 02 00 aa 44 09 00 0a 00 00 00 00 00 00 00 00 00 00 a4 01 6e 4b 03 00 61 6e 67 75 6c 61 72 2e 6a 73 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 ed c9 b8 eb cb 03 00 00 28 08 00 00 14 00 00 00 00 00 00 00 00 00 a4 01 d9 fd 05 00 62 61 63 6b 67 72 6f 75 6e 64 5f 73 63 72 69 70 74 2e 6a 73 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 ae 1a bc c5 0d 37 00 00 15 c4 00 00 0e 00 00 00 00 00 00 00 00 00 00 00 a4 01 e6 01 06 00 63 61 73 74 5f 73 65 6e 64 65 72 2e 6a 73 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 f1 1c 2d 6c 9b 34 00 00 d3 94 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: :_locales/zh_TW/messages.jsonPK)QO3DnKangular.jsPK)Q(background_script.jsPK)Q7cast_sender.jsPK)Q-l4

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	36	IN	Data Raw: 72 67 69 6e 2d 6c 65 66 74 3a 39 35 2e 38 33 33 33 33 25 7d 2e 63 6f 6c 2d 78 6c 2d 6f 66 66 73 65 74 2d 32 34 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 31 30 30 25 7d 7d 66 69 65 6c 64 73 65 74 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 62 6f 72 64 65 72 3a 30 3b 6d 69 6e 2d 77 69 64 74 68 3a 30 7d 6c 65 67 65 6e 64 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 77 69 64 74 68 3a 31 30 30 25 3b 70 61 64 64 69 6e 67 3a 30 3b 62 6f 72 64 65 72 3a 30 7d 6c 61 62 65 6c 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 6d 61 78 2d 77 69 64 74 68 3a 3 1 30 30 25 7d 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 65 61 72 63 68 22 5d 7b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 Data Ascii: rgin-left:95.833333%}.col-xl-offset-24{margin-left:100%}}fieldset(padding:0;margin:0;border:0;min-width:0)leg end{display:block;width:100%;padding:0;border:0}label{display:inline-block;max-width:100%}input[type="search"]{-webkit-b ox-sizing:border-box;-moz-b
2021-12-02 20:22:23 UTC	52	IN	Data Raw: 66 6c 6f Data Ascii: flo
2021-12-02 20:22:23 UTC	52	IN	Data Raw: 77 2d 78 3a 61 75 74 6f 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 2e 30 31 25 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 35 33 39 70 78 29 7b 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 35 70 78 3b 6f 76 65 72 66 6c 6f 77 2d 79 3a 68 69 64 64 65 6e 3b 2d 6d 73 2d 6f 76 65 72 66 6c 6f 77 2d 73 74 79 6c 65 3a 2d 6d 73 2d 61 75 74 6f 68 69 64 69 6e 67 2d 73 63 72 6f 6c 6c 62 61 72 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 74 61 62 6c 65 2d 72 65 73 70 6f 6e 73 69 76 65 3e 2e 74 61 62 6c 65 65 3e 74 68 65 61 64 3e 74 72 3e 74 68 2c 2e 74 61 62 6c 65 Data Ascii: w-x:auto;min-height:.01%}@media screen and (max-width:539px){.table-responsive{width:100%;margin-b ottom:15px;overflow-y:hidden;-ms-overflow-style:-ms-autohiding-scrollbar}.table-responsive>.table{margin-bottom:0}.table-responsive>.table>thead>tr>th,.table
2021-12-02 20:22:23 UTC	68	IN	Data Raw: 2c 22 54 75 6e 67 61 22 2c 22 4c 61 6f 20 55 49 22 2c 22 52 61 61 76 69 22 2c 22 49 73 6b 6f 6f 6c 61 20 50 6f 74 61 22 2c 22 4c 61 74 68 61 22 2c 22 4c 65 65 6c 61 77 61 64 65 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 20 55 49 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4a 68 65 6e 67 48 65 69 20 55 49 22 2c 22 4d 61 6c 67 75 6e 20 47 6f 74 68 69 63 22 2c 22 45 73 74 72 61 6e 67 65 6c 6f 20 45 64 65 73 73 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 48 69 6d 61 6c 61 79 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 4e 65 77 20 54 61 69 20 4c 75 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 50 68 61 67 73 50 61 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 54 61 69 20 4c 65 22 2c 22 4d 69 63 72 6f 73 6f 66 74 20 59 69 20 42 61 69 74 69 22 2c 22 4d 6f 6e 67 6f 6c Data Ascii: ", "Tunga", "Lao UI", "Raavi", "Iskoola Pota", "Latha", "Leelawadee", "Microsoft YaHei UI", "Microsoft JhengHei UI", " Malgun Gothic", "Estrangelo Edessa", "Microsoft Himalaya", "Microsoft New Tai Lue", "Microsoft PhagsPa", "Microsoft Tai Le", "Microsoft Yi Baiti", "Mongol
2021-12-02 20:22:23 UTC	84	IN	Data Raw: 69 6e 70 75 74 5b 74 79 70 65 3d 22 62 75 74 74 6f 6e 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 73 75 62 6d 69 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 2c 69 6e 70 75 74 5b 74 79 70 65 3d 22 72 65 73 65 74 22 5d 2e 62 74 6e 2d 70 72 69 6d 61 72 79 3a 61 63 74 69 76 65 7b 6f 75 74 6c 69 6e 65 3a 6e 6f 6e 65 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 2d 6d 73 2d 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 3b 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 7 2 6d 3a 73 63 61 6c 65 28 2e 39 38 29 3b 74 72 61 6e 73 66 6f 72 6d 3a 73 63 61 6c 65 28 2e 39 38 29 7d 2e 62 75 74 74 6f 6e 2e 73 65 63 6f 6e 64 61 72 79 7b 64 69 73 70 6c 61 79 3a 69 Data Ascii: input[type="button"].btn-primary:active,input[type="submit"].btn-primary:active,input[type="reset"].btn-prim ary:active{outline:none;text-decoration:none;-ms-transform:scale(.98);-webkit-transform:scale(.98);transform:scale(.98)} .button.secondary{display:i
2021-12-02 20:22:23 UTC	102	IN	Data Raw: 2e 64 72 6f 70 64 6f 77 6e 2d 74 6f 67 67 6c 65 2e 6d 65 6d 62 65 72 6e 61 6d 65 50 72 65 66 69 6c 6c 53 65 6c 65 63 74 2e 68 61 73 2d 65 72 72 6f 72 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 77 69 64 74 68 3a 31 70 78 3b 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 23 65 38 31 31 32 33 7d 2e 6f 75 74 6c 6f 6f 6b 45 6d 61 69 6c 4c 61 62 65 6c 7b 62 6f 72 64 65 72 2d 6c 65 66 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 6e 6f 6e 65 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 30 7d 2e 73 75 62 74 69 74 6c 65 7b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 31 Data Ascii: .dropdown-toggle.membernamePrefillSelect.has-error,.dropdown-toggle.membernamePrefillSelect.has-er ror: hover{border-width:1px;border-color:#e81123}.outlookEmailLabel{border-left:none;border-right:none;border-t op:none;padding-right:0}.subtitle{font-size:.81

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49760	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	1	OUT	GET /service/update2/crx?os=win&arch=x64&os_arch=x86_64&nacl_arch=x86-64&prod=chromecrx&prodchannel=&prodversion=85.0.4183.121&lang=en-GB&acceptformat=crx3&x=id%3Dnmmhkkegcagdldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelpbcmbmeomcjbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1 HTTP/1.1 Host: clients2.google.com Connection: keep-alive X-Goog-Update-Interactivity: fg X-Goog-Update-AppId: nmmhkkegcagdldgiimedpiccmgmieda,pkedcjkdefgpdelpbcmbmeomcjbeemfm X-Goog-Update-Updater: chromecrx-85.0.4183.121 Sec-Fetch-Site: none Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:23 UTC	100	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-E5kg+y4OSLZfp6hixyqn/Q' 'unsafe-inline' 'strict-dynamic' https: http://object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/clientupdate-aus/1 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 02 Dec 2021 20:22:23 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5449 X-Daystart: 44543 X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; m a=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-12-02 20:22:23 UTC	101	IN	Data Raw: 35 31 65 0d 0a 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 3f 3e 3c 67 75 70 64 61 74 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 75 70 64 61 74 65 32 2f 72 65 73 70 6f 6e 73 65 22 20 70 72 6f 74 6f 63 6f 6c 3d 22 32 2e 30 22 20 73 65 72 76 65 72 3d 22 70 72 6f 64 22 3e 3c 64 61 79 73 74 61 72 74 20 65 6c 61 70 73 65 64 5f 64 61 79 73 3d 22 35 34 34 39 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 34 35 34 33 22 2f 3e 3c 61 70 70 20 61 70 70 69 64 3d 22 6e 6d 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 22 20 63 6f 68 6f 72 74 3d 22 31 3a 3a 22 20 63 6f 68 6f 72 74 6e 61 6d 65 3d 22 22 Data Ascii: 51e<?xml version="1.0" encoding="UTF-8"?><gupdate xmlns="http://www.google.com/update2/response" p rotocol="2.0" server="prod"><daystart elapsed_days="5449" elapsed_seconds="44543"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2021-12-02 20:22:23 UTC	101	IN	Data Raw: 6d 68 6b 6b 65 67 63 63 61 67 64 6c 64 67 69 69 6d 65 64 70 69 63 63 6d 67 6d 69 65 64 61 2e 63 72 78 22 20 66 70 3d 22 31 2e 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 68 61 73 68 5f 73 68 61 32 35 36 3d 22 38 31 65 33 61 34 64 34 33 61 37 33 36 39 39 65 31 62 37 37 38 31 37 32 33 66 35 36 62 38 37 31 37 31 37 35 63 35 33 36 36 38 35 63 35 34 35 30 31 32 32 62 33 30 37 38 39 34 36 34 61 64 38 32 22 20 70 72 6f 74 65 63 74 65 64 3d 22 30 22 20 73 69 7a 65 3d 22 32 34 38 35 33 31 22 20 73 74 61 74 75 73 3d 22 6f 6b 22 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 2e 30 2e 36 22 2f 3e 3c 2f 61 70 70 3e 3c 61 70 Data Ascii: mhhkkgccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7781723f56b8717175c536685c54 50122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotected="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2021-12-02 20:22:23 UTC	102	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49773	104.18.10.207	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	114	OUT	GET /bootstrap/3.3.7/js/bootstrap.min.js HTTP/1.1 Host: maxcdn.bootstrapcdn.com Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	115	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 20:22:24 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding CDN-PullZone: 252412 CDN-Uid: b1941f61-b576-4f40-80de-5677acb38f74 CDN-RequestCountryCode: DE CDN-EdgeStorageId: 722 CDN-EdgeStorageId: 617 CDN-EdgeStorageId: 617 Last-Modified: Mon, 25 Jan 2021 22:04:00 GMT CDN-CachedAt: 2021-04-23 06:58:04 CDN-RequestPullSuccess: True CDN-RequestPullCode: 200 Cache-Control: public, max-age=31919000 timing-allow-origin: * cross-origin-resource-policy: cross-origin access-control-allow-origin: * x-content-type-options: nosniff CDN-RequestId: 74e57e8ba56ee256a776921149ca10e2 CDN-Cache: HIT CF-Cache-Status: HIT Age: 19321339 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Server: cloudflare CF-RAY: 6b774464f9e45be9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-12-02 20:22:24 UTC	116	IN	Data Raw: 37 62 64 31 0d 0a 2f 2a 21 0a 20 2a 20 42 6f 6f 74 73 74 72 61 70 20 76 33 2e 33 2e 37 20 28 68 74 7a 70 3a 2f 2f 67 65 74 62 6f 6f 74 73 74 72 61 70 2e 63 6f 6d 29 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 31 2d 32 30 31 36 20 54 77 69 74 74 65 72 2c 20 49 6e 63 2e 0a 20 2a 20 4c 69 63 65 6e 73 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 6c 69 63 65 6e 73 65 0a 20 2a 2f 0a 69 66 28 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 6a 51 75 65 72 79 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 6a 51 75 65 72 79 22 29 3b 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 62 3d 61 2e 66 6e Data Ascii: 7bd1/*! * Bootstrap v3.3.7 (http://getbootstrap.com) * Copyright 2011-2016 Twitter, Inc. * Licensed under the MIT license */if(("undefined"==typeof jQuery)throw new Error("Bootstrap's JavaScript requires jQuery");+function(a){function use strict";var b=a.fn
2021-12-02 20:22:24 UTC	117	IN	Data Raw: 22 2e 22 29 3b 69 66 28 62 5b 30 5d 3c 32 26 26 62 5b 31 5d 3c 39 7c 7c 31 3d 3d 62 5b 30 5d 26 26 39 3d 3d 62 5b 31 5d 26 26 62 5b 32 5d 3c 31 7c 7c 62 5b 30 5d 3e 33 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 42 6f 6f 74 73 74 72 61 70 27 73 20 4a 61 76 61 53 63 72 69 70 74 20 72 65 71 75 69 72 65 73 20 6a 51 75 65 72 79 20 76 65 72 73 69 6f 6e 20 31 2e 39 2e 31 20 6f 72 20 68 69 67 68 65 72 2c 20 62 75 74 20 6c 6f 77 65 72 20 74 68 61 6e 20 76 65 72 73 69 6f 6e 20 34 22 29 7d 28 6a 51 75 65 72 79 29 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 29 7b 76 61 72 20 61 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 6 5 45 6c 65 6d 65 6e 74 28 22 62 6f 6f 74 73 74 72 61 70 22 29 2c Data Ascii: ".");if(b[0]<2&&b[1]<9 1==b[0]&&9==b[1]&&b[2]<1 b[0]>3)throw new Error("Bootstrap's JavaScript requires jQuery version 1.9.1 or higher, but lower than version 4"))(jQuery),+function(a){function use strict";function b(){var a=document. createElement("bootstrap"),
2021-12-02 20:22:24 UTC	118	IN	Data Raw: 66 3d 66 26 26 66 2e 72 65 70 6c 61 63 65 28 2f 2e 2a 28 3f 3d 23 5b 5e 5c 73 5d 2a 24 29 2f 2c 22 22 29 29 3b 76 61 72 20 67 3d 61 28 22 23 2d 3d 3d 3d 66 3f 5b 5d 3a 66 29 3b 62 26 26 62 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 67 2e 6c 65 6e 67 74 68 7c 7c 28 67 3d 65 2e 63 6c 6f 73 65 73 74 28 22 2e 61 6c 65 72 74 22 29 29 2c 67 2e 74 72 69 67 67 65 72 28 62 3d 61 2e 45 76 65 6e 74 28 22 63 6c 6f 73 65 2e 62 73 2e 61 6c 65 72 74 22 29 29 2c 62 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 7c 7c 28 67 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 2 2 69 6e 22 29 2c 61 2e 73 75 70 70 6f 72 74 2e 74 72 61 6e 73 69 74 69 6f 6e 26 26 67 2e 68 61 73 43 6c 61 73 73 28 22 66 61 64 65 22 29 3f 67 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 Data Ascii: f=f&&f.replace(/.*(?=#[^\s]*\$)/,"");var g=a("#"===f?f:f);b&&b.preventDefault().g.length (g=g.closest(".alert")),g.t rigger(b=a.Event("close.bs.alert")),b.isDefaultPrevented() (g.removeClass("in"),a.support.transition&&g.hasClass("fade"? g.one("bsTransi
2021-12-02 20:22:24 UTC	119	IN	Data Raw: 24 65 6c 65 6d 65 6e 74 2e 66 69 6e 64 28 22 69 6e 70 75 74 22 29 3b 22 72 61 64 69 6f 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 3f 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 26 26 28 61 3d 21 31 29 2c 62 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 22 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 61 64 64 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 3a 22 63 68 65 63 6b 62 6f 78 22 3d 3d 63 2e 70 72 6f 70 28 22 74 79 70 65 22 29 26 26 28 63 2e 70 72 6f 70 28 22 63 68 65 63 6b 65 64 22 29 21 3d 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 61 73 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 26 26 28 61 3 d 21 31 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 74 6f 67 Data Ascii: \$element.find("input");"radio"==c.prop("type")?(c.prop("checked")&&(a=!1),b.find(".active").removeClass("act ive"),this.\$element.addClass("active")):"checkbox"==c.prop("type")&&(c.prop("checked")!=this.\$element.hasClass("active")&&(a=!1),this.\$element.tog
2021-12-02 20:22:24 UTC	121	IN	Data Raw: 75 73 65 28 29 2e 63 79 63 6c 65 28 29 7d 29 7d 76 61 72 20 63 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 3d 61 28 62 29 2c 74 68 69 73 2e 24 69 6e 64 69 63 61 74 6f 72 73 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 66 69 6e 64 28 22 2e 63 61 72 6f 75 73 65 6c 2d 69 6e 64 69 63 61 74 6f 72 73 22 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 63 2c 74 68 69 73 2e 70 61 75 73 65 64 3d 6e 75 6c 6c 2c 74 68 69 73 2e 73 6c 69 64 69 6e 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 69 6e 74 65 72 76 61 6c 3d 6e 75 6c 6c 2c 74 68 69 73 2e 24 61 63 74 69 76 65 3d 6e 75 6c 6c 2c 74 68 69 73 2e 24 69 74 65 6d 73 3d 6e 75 6c 6c 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6b 65 79 62 6f 61 72 64 26 26 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 Data Ascii: use().cycle()))var c=function(b,c){this.\$element=a(b),this.\$indicators=this.\$element.find(".carousel-indica tors"),this.options=c,this.paused=null,this.sliding=null,this.interval=null,this.\$active=null,this.\$items=null,this.options.keyboar d&&this.\$element

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	122	IN	Data Raw: 63 2e 70 72 6f 74 6f 74 79 70 65 2e 74 6f 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 74 68 69 73 2c 63 3d 74 68 69 73 2e 67 65 74 49 74 65 6d 49 6e 64 65 78 28 74 68 69 73 2e 24 61 63 74 69 76 65 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 66 69 6e 64 28 22 2e 69 74 65 6d 2e 61 63 74 69 76 65 22 29 29 3b 69 66 28 21 28 61 3e 74 68 69 73 2e 24 69 74 65 6d 73 2e 6c 65 6e 67 74 68 2d 31 7c 7c 61 3c 30 29 29 72 65 74 75 72 6e 20 74 68 69 73 2e 7 3 6c 69 64 69 6e 67 3f 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 6f 6e 65 28 22 73 6c 69 64 2e 62 73 2e 63 61 72 6f 75 7 3 65 6c 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 62 2e 74 6f 28 61 29 7d 29 3a 63 3d 3d 61 3f 74 68 69 73 2e 70 61 75 73 6 5 28 29 2e 63 79 63 6c 65 28 29 3a 74 68 69 73 2e 73 6c 69 64 65 Data Ascii: c.prototype.to=function(a){var b=this,c=this.getItemIndex(this.\$active=this.\$element.find(".").item.active));if(! (a>this.\$items.length-1 a<0))return this.sliding?this.\$element.one("slid.bs.carousel",function(){b.to(a)}):c==a?this.pause().cycle():this.slide
2021-12-02 20:22:24 UTC	123	IN	Data Raw: 28 68 29 2c 66 2e 61 64 64 43 6c 61 73 73 28 68 29 2c 65 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 66 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5b 62 2c 68 5d 2e 6a 6f 69 6e 28 22 20 22 29 29 2e 61 64 64 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 2c 65 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 5b 22 61 63 74 69 76 65 22 2c 68 5d 2e 6a 6f 69 6e 28 22 20 22 29 29 2c 69 2e 73 6c 69 64 69 6e 67 3d 21 31 2c 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 69 2e 24 65 6c 65 6d 65 6e 74 2e 74 72 69 67 67 65 7 2 28 6d 29 7d 2c 30 29 7d 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 63 2e 54 52 41 4e 53 49 54 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 29 3a 28 65 2e 72 65 6d Data Ascii: (h),f.addClass(h),e.one("bsTransitionEnd",function(){f.removeClass([b,h].join(" ")).addClass("active"),e.removeClass(["active",h].join(" ")),i.sliding=1,setTimeout(function(){i.\$element.trigger(m),0})).emulateTransitionEnd(c.TRANSITION_DURATION));(e.rem
2021-12-02 20:22:24 UTC	125	IN	Data Raw: 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 62 26 26 65 5b 62 5d 28 29 7d 29 7d 76 61 72 20 64 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 3d 61 28 62 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 64 2e 44 45 46 41 55 4c 53 2c 63 29 2c 74 68 69 73 2e 24 74 72 69 67 67 65 72 3d 61 28 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 63 6f 6c 6c 61 70 73 65 22 5d 5b 68 72 65 66 3d 22 23 27 2b 62 2e 69 64 2b 27 22 5d 2c 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 63 6f 6c 6c 61 70 73 65 22 5d 5b 64 61 74 61 2d 74 61 72 67 65 74 3d 22 23 27 2b 62 2e 69 64 2b 27 22 5d 27 29 2c 74 68 69 73 2e 74 72 61 6e 73 69 74 69 6f 6e 69 6e 67 3d 6e 75 6c 6c 2c 74 68 69 73 2e 6f 70 74 69 Data Ascii:)), "string"==typeof b&&e[b]()))var d=function(b,c){this.\$element=a(b),this.options=a.extend({},d.DEFAULTS,c),this.\$trigger=a("[data-toggle='collapse'"][href="#"+"b.id+""],[data-toggle='collapse'][data-target="#"+"b.id+""]),this.transitioning=null,this.opti
2021-12-02 20:22:24 UTC	126	IN	Data Raw: 28 22 2d 22 29 29 3b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 61 2e 70 72 6f 78 79 28 68 2c 74 68 69 73 29 29 2e 65 6d 75 6c 61 74 65 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 28 64 2e 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 5b 67 5d 28 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 5b 69 5d 29 7d 7d 7d 2c 64 2e 70 72 6f 74 6f 74 79 70 65 2e 68 69 64 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 21 74 68 69 73 2e 74 72 61 6e 73 69 74 69 6f 6e 69 6e 67 2b 64 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 61 73 43 6c 61 73 73 28 22 69 6e 22 29 29 7b 76 61 72 20 62 3d 61 2e 45 76 65 6e 74 28 22 68 69 64 65 2e 62 73 2e 63 6f 6c 6c 61 70 73 65 22 29 3b 69 66 28 74 68 69 73 Data Ascii: ("");this.\$element.one("bsTransitionEnd",a.proxy(h,this)).emulateTransitionEnd(d.TRANSITION_DURATION)[g](this.\$element[0][i]{}));d.prototype.hide=function(){if(!this.transitioning&&this.\$element.hasClass("in")){var b=a.Event("hide.bs.collapse");if(this
2021-12-02 20:22:24 UTC	127	IN	Data Raw: 65 2e 6e 6f 43 6f 6e 66 6c 69 63 74 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 2e 66 6e 2e 63 6f 6c 6c 61 70 73 65 3d 65 2c 74 68 69 73 7d 2c 61 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 63 6f 6c 6c 61 70 73 65 2e 64 61 74 61 2d 61 70 69 22 2c 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 63 6f 6c 6c 61 70 73 65 22 5d 27 2c 66 75 6e 63 74 69 6f 6e 28 64 29 7b 76 61 72 20 65 3d 61 28 74 68 69 73 29 3b 65 2e 61 74 74 72 28 22 64 61 74 61 2d 74 61 72 67 65 74 22 29 7c 7c 64 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 3b 76 61 72 20 66 3d 62 28 65 29 2c 67 3d 66 2e 64 61 74 61 28 22 62 73 2e 63 6f 6c 6c 61 70 73 65 22 29 2c 68 3d 67 3f 22 74 6f 67 67 6c 65 22 3a 65 2e 64 61 74 61 28 29 3b 63 2e 63 61 6c 6c Data Ascii: e.noConflict=function(){return a.fn.collapse=e,this},a(document).on("click.bs.collapse.data-api", "[data-toggle='collapse']",function(d){var e=a(this);e.attr("data-target") d.preventDefault();var f=b(e),g=f.data("bs.collapse"),h=g?"toggle":e.data();c.call
2021-12-02 20:22:24 UTC	129	IN	Data Raw: 29 2e 61 64 64 43 6c 61 73 73 28 22 64 72 6f 70 64 6f 77 6e 2d 62 61 63 6b 64 72 6f 70 22 29 2e 69 6e 73 65 72 74 41 66 74 65 72 28 61 28 74 68 69 73 29 29 2e 6f 6e 28 22 63 6c 69 63 6b 22 2c 63 29 3b 76 61 72 20 68 3d 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 74 68 69 73 7d 3b 69 66 28 66 2e 74 72 69 67 67 65 72 28 64 3d 61 2e 45 76 65 6e 74 28 22 73 68 6f 77 2e 62 73 2e 64 72 6f 70 64 6f 77 6e 22 2c 68 29 29 2c 64 2e 69 73 44 65 66 61 75 6c 74 50 72 65 76 65 6e 74 65 64 28 29 29 72 65 74 75 72 6e 3b 65 2e 74 72 69 67 67 65 72 22 66 6f 63 75 73 22 29 2e 61 74 74 72 2 8 22 61 72 69 61 2d 65 78 70 61 6e 64 65 64 22 2c 22 74 72 75 65 22 29 2c 66 2e 74 6f 67 67 6c 65 43 6c 61 73 73 28 22 6f 70 65 6e 22 29 2e 74 72 69 67 67 65 72 28 61 2e 45 76 65 6e 74 Data Ascii:).addClass("dropdown-backdrop").insertAfter(a(this)).on("click",c);var h={relatedTarget:this};if(f.trigger(d)=a.Event("show.bs.dropdown",h)),d.isDefaultPrevented())return;e.trigger("focus").attr("aria-expanded","true"),f.toggleClass("open"),trigger(a.Event
2021-12-02 20:22:24 UTC	130	IN	Data Raw: 29 2c 67 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 63 2e 44 45 46 41 55 4c 54 53 2c 65 2e 64 61 74 61 28 29 2c 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 62 26 26 62 29 3b 66 7c 7c 65 2e 64 61 74 61 28 22 62 73 2e 6d 6f 64 61 6c 22 2c 66 3d 6e 65 77 20 63 28 74 68 69 73 2c 67 29 29 2c 22 73 74 72 69 6e 67 22 3d 3d 74 79 70 65 6f 66 20 62 3f 66 5b 62 5d 28 64 29 3a 67 2e 73 68 6f 77 26 26 66 2e 73 68 6f 77 28 64 29 7d 29 7d 76 61 72 20 63 3d 66 75 6e 63 74 69 6f 6e 28 62 2c 63 29 7b 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 63 2c 74 68 69 73 2e 24 62 6f 64 79 3d 61 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 3d 61 28 62 29 2c 74 68 69 73 2e 24 64 69 61 6c 6f 67 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 66 69 Data Ascii:),g=a.extend({},c.DEFAULTS,e.data()),"object"==typeof b&&b?f e.data("bs.modal",f=new c(this,g)), "string"==typeof b?f[b](d):g.show&&f.show(d)))var c=function(b,c){this.options=c,this.\$body=a(document.body),this.\$element=a(b),this.\$dialog=this.\$element.fi
2021-12-02 20:22:24 UTC	131	IN	Data Raw: 74 28 29 2e 6c 65 6e 67 74 68 7c 7c 64 2e 24 65 6c 65 6d 65 6e 74 2e 61 70 70 65 6e 64 54 6f 28 64 2e 24 62 6f 64 79 29 2c 64 2e 24 65 6c 65 6d 65 6e 74 2e 73 68 6f 77 28 29 2e 73 63 72 6f 6c 6c 54 6f 70 28 30 29 2c 64 2e 61 64 6a 75 73 74 44 69 61 6c 6f 67 28 29 2c 65 26 26 64 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 2e 6f 66 66 73 65 74 57 69 64 74 68 2c 64 2e 24 65 6c 65 6d 65 6e 74 2e 61 64 64 43 6c 61 73 73 28 22 69 6e 22 29 2c 64 2e 65 6e 66 6f 72 63 65 46 6f 63 75 73 28 29 3b 76 61 72 20 66 3d 61 2e 45 76 65 6e 74 28 22 73 68 6f 77 6e 2e 62 73 2e 6d 6f 64 61 6c 22 2c 7b 72 65 6c 61 74 65 64 54 61 72 67 65 74 3a 62 7d 29 3b 65 3f 64 2e 24 64 69 61 6c 6f 67 2e 6f 6e 65 28 22 62 73 54 72 61 6e 73 69 74 69 6f 6e 45 6e 64 22 2c 66 75 6e 63 74 69 6f 6e 28 29 Data Ascii: t().length d.\$element.appendTo(d.\$body),d.\$element.show().scrollTop(0),d.adjustDialog(),e&&d.\$element[0].offsetWidth,d.\$element.addClass("in"),d.enforceFocus();var f=a.Event("shown.bs.modal",{relatedTarget:b});e?d.\$dialog.one("bsTransitionEnd",function()

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	133	IN	Data Raw: 64 6f 77 6e 2e 64 69 73 6d 69 73 73 2e 62 73 2e 6d 6f 64 61 6c 22 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 72 65 73 69 7a 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 69 73 53 68 6f 77 6e 3f 61 28 77 69 6e 64 6f 77 29 2e 6f 6e 28 22 72 65 73 69 7a 65 2e 62 73 2e 6d 6f 64 61 6c 22 2c 61 2e 70 72 6f 78 79 28 74 68 69 73 2e 68 61 6e 64 6c 65 55 70 64 61 74 65 2c 74 68 69 73 29 29 3a 61 28 77 69 6e 64 6f 77 29 2e 6f 66 66 28 22 72 65 73 69 7a 65 2e 62 73 2e 6d 6f 64 61 6c 22 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 68 69 64 65 4d 6f 64 61 6c 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 74 68 69 73 3b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 69 64 65 28 29 2c 74 68 69 73 2e 62 61 63 6b 64 72 6f 70 28 66 75 6e 63 74 69 6f 6e 28 29 Data Ascii: down.dismiss.bs.modal"));c.prototype.resize=function(){this.isShown?a(window).on("resize.bs.modal",a.proxy(t his.handleUpdate,this)):a(window).off("resize.bs.modal"));c.prototype.hideModal=function(){var a=this;this.\$element.hide (),this.backdrop(function()
2021-12-02 20:22:24 UTC	134	IN	Data Raw: 6e 64 28 63 2e 42 41 43 4b 44 52 4f 50 5f 54 52 41 4e 53 49 54 49 4f 4e 5f 44 55 52 41 54 49 4f 4e 29 3a 67 28 29 7d 65 6c 73 65 20 62 26 62 28 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 6e 64 6c 65 55 70 64 61 74 65 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 74 68 69 73 2e 61 64 6a 75 73 74 44 69 61 6c 6f 67 28 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 61 64 6a 75 73 74 44 69 61 6c 6f 67 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 61 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 2e 73 63 72 6f 6c 6c 48 65 69 67 68 74 3e 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e 63 6c 69 65 6e 74 48 65 69 67 68 74 3b 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 63 73 73 28 7b 70 61 64 64 69 6e 67 4c 65 66 74 3a 21 74 68 69 73 Data Ascii: nd(c.BACKDROP_TRANSITION_DURATION):g()})else b&b&)),c.prototype.handleUpdate=function(){this.adjustDialog(),c.prototype.adjustDialog=function(){var a=this.\$element[0].scrollHeight>document.documentElement.clientHeight ;this.\$element.css({paddingLeft:!this
2021-12-02 20:22:24 UTC	135	IN	Data Raw: 62 73 2e 6d 6f 64 61 6c 2e 64 61 74 61 2d 61 70 69 22 2c 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 6d 6f 64 61 6c 22 5d 27 2c 66 75 6e 63 74 69 6f 6e 28 63 29 7b 76 61 72 20 64 3d 61 28 74 68 69 73 29 2c 65 3d 64 2e 61 74 74 72 28 22 68 72 65 66 22 29 2c 66 3d 61 28 64 2e 61 74 74 72 28 22 64 61 74 61 2d 74 61 72 67 65 74 22 29 7c 7c 65 26 26 65 2e 72 65 70 6c 61 63 65 28 2f 2e 2a 28 3f 3d 23 5b 5e 5c 73 5d 2b 24 29 2f 2c 22 22 29 29 2c 67 3d 66 2e 64 61 74 61 28 22 62 73 2e 6d 6f 64 61 6c 22 29 3f 22 74 6f 67 67 6c 65 22 3a 61 2e 65 78 74 65 6e 64 28 7b 72 65 6d 6f 74 65 3a 21 2f 23 2f 2e 74 65 73 74 28 65 29 26 26 65 7d 2c 66 2e 64 61 74 61 28 29 2c 64 2e 64 61 74 61 28 29 3b 64 2e 69 73 28 22 61 22 29 26 26 63 2e 70 72 65 76 65 6e 74 44 65 66 61 Data Ascii: bs.modal.data-api",[data-toggle="modal"],function(c){var d=a(this),e=d.attr("href"),f=a(d.attr("data-target")) e&&e.replace(/.*(?=#[^\s]+\$)/,""),g=f.data("bs.modal")?"toggle":a.extend({remote:!/#.test(e)&&e},f.data(),d.data());d.is("a")&&c.preventDefault
2021-12-02 20:22:24 UTC	137	IN	Data Raw: 6c 65 6d 65 6e 74 29 3a 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 76 69 65 77 70 6f 72 74 2e 73 65 6c 65 63 74 6f 72 7c 7c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 76 69 65 77 70 6f 72 74 29 2c 74 68 69 73 2e 69 6e 53 74 61 74 65 3d 7b 63 6c 69 63 6b 3a 21 31 2c 68 6f 76 65 72 3a 21 31 2c 66 6f 63 75 73 3a 21 31 7d 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 69 6e 73 74 61 6e 63 65 6f 66 20 64 6f 63 75 6d 65 6e 74 2e 63 6f 6e 73 74 72 75 63 74 6f 72 26 26 21 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 73 65 6c 65 63 74 6f 72 29 74 68 72 6f 77 20 45 72 72 6f 72 28 22 60 73 65 6c 65 63 74 6f 72 60 20 6f 70 74 69 6f 6e 20 6d 75 73 74 20 62 65 20 73 70 65 63 69 66 69 65 64 20 77 68 65 6e 20 69 6e 69 74 69 61 6c 69 7a 69 6e 67 20 22 2b 74 68 69 73 2e Data Ascii: lement):this.options.viewport.selector this.options.viewport),this.inState={click:!1,hover:!1,focus:!1},this.\$element[0]instanceof document.constructor&&this.options.selector)throw new Error("'selector' option must be specified when initializing "+this.
2021-12-02 20:22:24 UTC	138	IN	Data Raw: 61 72 67 65 74 2c 74 68 69 73 2e 67 65 74 44 65 6c 65 67 61 74 65 4f 70 74 69 6f 6e 73 28 29 29 2c 61 28 62 2e 63 75 72 72 65 6e 74 54 61 72 67 65 74 29 2e 64 61 74 61 28 22 62 73 2e 22 2b 74 68 69 73 2e 74 79 70 65 2c 63 29 29 2c 62 20 69 6e 73 74 61 6e 63 65 6f 66 20 61 2e 45 76 65 6e 74 26 26 28 63 2e 69 6e 53 74 61 74 65 5b 22 66 6f 63 75 73 69 6e 22 3d 3d 62 2e 74 79 70 65 3f 22 66 6f 63 75 73 22 3a 22 68 6f 76 65 72 22 5d 3d 21 30 29 2c 63 2e 74 69 70 28 29 2e 68 61 73 43 6c 61 73 73 28 22 69 6e 22 29 7c 7c 22 69 6e 22 3d 3d 63 2e 68 6f 76 65 72 53 74 61 74 65 3f 76 6f 69 64 28 63 2e 68 6f 76 65 72 53 74 61 74 65 3d 22 69 6e 22 29 3a 28 63 6c 65 61 72 54 69 6d 65 6f 75 74 28 63 2e 74 69 6d 65 6f 75 74 29 2c 63 2e 68 6f 76 65 72 53 74 61 74 65 3d 22 Data Ascii: arget,this.getDelegateOptions()),a(b.currentTarget).data("bs."+this.type,c)),b instanceof a.Event&&(c.inState f["focusin"]==b.type?"focus":"hover"]=0),c.tip().hasClass("in") "in"==c.hoverState?void(c.hoverState="in):(clearTimeou t(c.timeout),c.hoverState="
2021-12-02 20:22:24 UTC	139	IN	Data Raw: 2c 67 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 61 6e 69 6d 61 74 69 6f 6e 26 26 66 2e 61 64 64 43 6c 61 73 73 28 22 66 61 64 65 22 29 3b 76 61 72 20 68 3d 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6c 61 63 65 6d 65 6e 74 3f 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6c 61 63 65 6d 65 6e 74 2e 63 61 6c 6c 28 74 68 69 73 2c 66 5b 30 5d 2c 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 5b 30 5d 29 3a 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6c 61 63 65 6d 65 6e 74 2c 69 3d 2f 5c 73 3f 61 75 74 6f 3f 5c 73 3f 2f 69 2c 6a 3d 69 2e 74 65 73 74 28 68 29 3b 6a 26 26 28 68 3d 68 2e 72 65 70 6c 61 63 65 28 69 2c 22 22 29 7c 7c 22 74 6f 70 22 29 2c 66 2e 64 65 74 61 63 68 28 29 2e 63 73 28 7b 74 6f 70 3a 30 2c Data Ascii: .g),this.options.animation&&f.addClass("fade");var h="function"==typeof this.options.placement?this.options.placement.call(this,f[0],this.\$element[0]):this.options.placement,i=/s?auto?s?/i,j=i.test(h);j&&(h=h.replace(i,"") "top"),f.detach().css({top:0,
2021-12-02 20:22:24 UTC	141	IN	Data Raw: 65 66 74 29 7d 29 7d 7d 2c 62 29 2c 30 29 2c 64 2e 61 64 64 43 6c 61 73 73 28 22 69 6e 22 29 3b 76 61 72 20 69 3d 64 5b 30 5d 2e 6f 66 66 73 65 74 57 69 64 74 68 2c 6a 3d 64 5b 30 5d 2e 6f 66 66 73 65 74 48 65 69 67 68 74 3b 22 74 6f 70 22 3d 3d 63 26 26 6a 21 3d 66 26 26 28 62 2e 74 6f 70 3d 62 2e 74 6f 70 2b 66 2d 6a 29 3b 76 61 72 20 6b 3d 74 68 69 73 2e 67 65 74 56 69 65 77 70 6f 72 74 41 64 6a 75 73 74 65 64 44 65 6c 74 61 28 63 2c 62 2c 69 2c 6a 29 3b 6b 2e 6c 65 66 74 3f 62 2e 6c 65 66 74 2b 3d 6b 2e 6c 65 66 74 3a 62 2e 74 6f 70 2b 3d 6b 2e 74 6f 70 3b 76 61 72 20 6c 3d 2f 74 6f 70 7c 62 6f 74 6f 6d 2f 2e 74 65 73 74 28 63 29 2c 6d 3d 6c 3f 32 2a 6b 2e 6c 65 66 74 2d 65 2b 69 3a 32 2a 6b 2e 74 6f 70 2d 66 2b 6a 2c 6e 3d 6c 3f 22 6f 66 66 73 65 Data Ascii: eft))))),b),0),d.addClass("in");var i=d[0].offsetWidth,j=d[0].offsetHeight;"top"==c&&f.f&&(b.top=b.top+f-j);var k=this.getViewportAdjustedDelta(c,b,i,j);k.left?b.left+=k.left:b.top+=k.top;var l=/top bottom/.test(c),m=l?"k.left-e+i:2*k.top-f+j,n=l?"o"offse
2021-12-02 20:22:24 UTC	142	IN	Data Raw: 22 42 4f 44 59 22 3d 3d 63 2e 74 61 67 4e 61 6d 65 2c 65 3d 63 2e 67 65 74 42 6f 75 6e 64 69 6e 67 43 6c 69 65 6e 74 52 65 63 74 28 29 3b 6e 75 6c 6c 3d 3d 65 2e 77 69 64 74 68 26 26 28 65 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 65 2c 7b 77 69 64 74 68 3a 65 2e 72 69 67 68 74 2d 65 2e 6c 65 66 74 2c 68 65 69 67 68 74 3a 65 2e 62 6f 74 74 6f 6d 2d 65 2e 74 6f 70 7d 29 29 3b 76 61 72 20 66 3d 77 69 6e 64 6f 77 2e 53 56 47 45 6c 65 6d 65 6e 74 2c 67 3d 64 3f 74 6f 70 3a 30 2c 6c 65 66 74 3a 30 7d 3a 66 3f 6e 75 6c 6c 3a 62 2e 6f 66 66 73 65 74 28 29 2c 68 3d 7b 73 63 72 6f 6c 6c 3a 64 3f 64 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2e Data Ascii: "BODY"==c.tagName,e=c.getBoundingClientRect();null==e.width&&(e=a.extend({},e,{width:e.right-e.left,height:e.bottom-e.top}));var f=window.SVGElement&&c instanceof window.SVGElement,g=d?(top:0,left:0):f?null:b .offset(),h={scroll:d?document.documentElement.

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	143	IN	Data Raw: 70 72 6f 74 6f 74 79 70 65 2e 74 69 70 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 21 74 68 69 73 2e 24 74 69 70 26 26 28 74 68 69 73 2e 24 74 69 70 3d 61 28 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 74 65 6d 70 6c 61 74 65 29 2c 31 21 3d 74 68 69 73 2e 24 74 69 70 2e 6c 65 6e 67 74 68 29 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 74 68 69 73 2e 74 79 70 65 2b 22 20 60 74 65 6d 70 6c 61 74 65 60 20 6f 70 74 69 6f 6e 20 6d 75 73 74 20 63 6f 6e 73 69 73 74 20 6f 66 20 65 78 61 63 74 6c 79 20 31 20 74 6f 70 2d 6c 65 76 65 6c 20 65 6c 65 6d 65 6e 74 21 22 29 3b 72 65 74 75 72 6e 20 74 68 69 73 2e 24 74 69 70 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 61 72 72 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 2e 24 61 72 72 6f 77 Data Ascii: prototype.tip=function(){}if(!this.\$tip&&(this.\$tip=a(this.options.template),1)!=this.\$tip.length))throw new Error(this.type+" `template` option must consist of exactly 1 top-level element");return this.\$tip;}.c.prototype.arrow=function(){return this.\$arrow
2021-12-02 20:22:24 UTC	145	IN	Data Raw: 26 65 5b 62 5d 28 29 29 7d 29 7d 76 61 72 20 63 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 74 68 69 73 2e 69 6e 69 74 28 22 70 6f 70 6f 76 65 72 22 2c 61 2c 62 29 7d 3b 69 66 28 21 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 50 6f 70 6f 76 65 72 20 72 65 71 75 69 72 65 73 20 74 6f 6f 6c 74 69 70 2e 6a 73 22 29 3b 63 2e 56 45 52 53 49 4f 4e 3d 22 33 2e 33 2e 37 22 2c 63 2e 44 45 46 41 55 4c 54 53 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 61 2e 66 6e 2e 74 6f 6f 6c 74 69 70 2e 43 6f 6e 73 74 72 75 63 74 6f 72 2e 44 45 46 41 55 4c 54 53 2c 7b 70 6c 61 63 65 6d 65 6e 74 3a 22 72 69 67 68 74 22 2c 74 72 69 67 67 65 72 3a 22 63 6c 69 63 6b 22 2c 63 6f 6e 74 65 6e 74 3a 22 22 2c 74 65 6d 70 6c 61 74 65 3a 27 3c 64 69 Data Ascii: &e[b]())}}var c=function(a,b){this.init("popover",a,b)};if(!a.fn.tooltip)throw new Error("Popover requires tooltip.js");c.VERSION="3.3.7";c.DEFAULTS=a.extend({},a.fn.tooltip.Constructor.DEFAULTS,{placement:"right",trigger:"click",content:"",template:'<di
2021-12-02 20:22:24 UTC	146	IN	Data Raw: 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 63 2c 64 29 7b 74 68 69 73 2e 24 62 6f 64 79 3d 61 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 2c 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 61 28 61 28 63 29 2e 69 73 28 64 6f 63 75 6d 65 6e 74 2e 62 6f 64 79 29 3f 77 69 6e 64 6f 77 3a 63 29 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 3d 61 2e 65 78 74 65 6e 64 28 7b 7d 2c 62 2e 44 45 46 41 55 4c 54 53 2c 64 29 2c 74 68 69 73 2e 73 65 6c 65 63 74 6f 72 3d 28 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 74 61 72 67 65 74 7c 7c 22 22 29 2b 22 20 2e 6e 61 76 20 6c 69 20 3e 20 61 22 2c 74 68 69 73 2e 6f 66 66 73 65 74 73 3d 5b 5d 2c 74 68 69 73 2e 74 61 72 67 65 74 73 3d 5b 5d 2c 74 68 69 Data Ascii: ,+function(a){["use strict";function b(c,d){this.\$body=a(document.body),this.\$scrollElement=a(a(c).is(document.t.body)?window:c),this.options=a.extend({},b.DEFAULTS,d),this.selector=(this.options.target "")+" .nav li > a",this.offsets=[],this.targets=[],this
2021-12-02 20:22:24 UTC	147	IN	Data Raw: 31 34 65 34 0d 0a 6f 6e 28 29 7b 76 61 72 20 61 2c 62 3d 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 73 63 72 6f 6c 6c 54 6f 70 28 29 2b 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 66 66 73 65 74 2c 63 3d 74 68 69 73 2e 67 65 74 53 63 72 6f 6c 6c 48 65 69 67 68 74 28 29 2c 64 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6f 66 66 73 65 74 2b 63 2d 74 68 69 73 2e 24 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 2e 68 65 69 67 68 74 28 29 2c 65 3d 74 68 69 73 2e 6f 66 66 73 65 74 73 2c 66 3d 74 68 69 73 2e 74 61 72 67 65 74 73 2c 67 65 74 73 2e 61 63 74 69 76 65 54 61 72 67 65 74 3b 69 66 28 74 68 69 73 2e 73 63 72 6f 6c 6c 48 65 69 67 68 74 21 3d 63 26 26 74 68 69 73 2e 72 65 66 72 6 5 73 68 28 29 2c 62 3e 3d 64 29 72 65 74 75 72 6e 20 67 21 3d 28 Data Ascii: 14e4on(){var a,b=this.\$scrollElement.scrollTop()+this.options.offset,c=this.getScrollHeight(),d=this.options.offset+c-this.\$scrollElement.height(),e=this.offsets,f=this.targets,g=this.activeTarget;if(this.scrollHeight!=c&&this.refresh(),b>=d)return gl=(
2021-12-02 20:22:24 UTC	149	IN	Data Raw: 2e 70 72 6f 74 6f 74 79 70 65 2e 73 68 6f 77 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 3d 74 68 69 73 2e 65 6c 65 6d 65 6e 74 2c 63 3d 62 2e 63 6c 6f 73 65 73 74 28 22 75 6c 3a 6e 6f 74 28 2e 64 72 6f 70 64 6f 77 6e 2d 6d 65 6e 75 29 22 29 2c 64 3d 62 2e 64 61 74 61 28 22 74 61 72 67 65 74 22 29 3b 69 66 28 64 7c 7c 28 64 3d 62 2e 61 74 74 72 28 22 68 72 65 66 22 29 2c 64 3d 64 26 26 64 2e 72 65 70 6c 61 63 65 28 2f 2e 2a 28 3f 3d 23 5b 5e 5c 73 5d 2a 24 29 2f 2c 22 22 29 29 2c 21 62 2e 70 61 72 65 6e 74 28 22 6c 69 22 29 2e 68 61 73 43 6c 61 73 73 28 22 61 63 74 69 76 65 22 29 29 7b 76 61 72 20 65 3d 63 2e 66 69 6e 64 28 22 2e 61 63 74 69 76 65 3a 6c 61 73 74 20 61 22 29 2c 66 3d 61 2e 45 76 65 6e 74 28 22 68 69 64 65 2e 62 73 2e 74 61 62 22 2c Data Ascii: .prototype.show=function(){var b=this.element,c=b.closest("ul:not(.dropdown-menu)"),d=b.data("target");if(d (d=b.attr("href"),d=d&&d.replace(/.*(?:#\s*\$)/,""),!b.parent("li").hasClass("active")){var e=c.find(".active:last a"),f=a.Event("hide.bs.tab",
2021-12-02 20:22:24 UTC	150	IN	Data Raw: 20 61 2e 66 6e 2e 74 61 62 3d 64 2c 74 68 69 73 7d 3b 76 61 72 20 65 3d 66 75 6e 63 74 69 6f 6e 28 63 29 7b 63 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 2c 62 2e 63 61 6c 6c 28 61 28 74 68 69 73 29 2c 22 73 68 6f 77 22 29 7d 3b 61 28 64 6f 63 75 6d 65 6e 74 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 74 61 62 2e 64 61 74 61 2d 61 70 69 22 2c 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 74 61 62 22 5d 27 2c 65 29 2e 6f 6e 28 22 63 6c 69 63 6b 2e 62 73 2e 74 61 62 2e 64 61 74 61 2d 61 70 69 22 2c 27 5b 64 61 74 61 2d 74 6f 67 67 6c 65 3d 22 70 69 6c 6e 22 5d 27 2c 65 29 7d 28 6a 51 75 65 72 79 29 2c 2b 66 75 6e 63 74 69 6f 6e 28 61 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 66 75 6e 63 74 69 6f 6e 20 62 28 62 29 7b 72 65 74 75 72 6e 20 74 68 69 Data Ascii: a.fn.tab=d,this};var e=function(c){c.preventDefault(),b.call(a(this),"show");a(document).on("click.bs.tab.data-api",[data-toggle="tab"],e).on("click.bs.tab.data-api",[data-toggle="pill"],e)}(jQuery),+function(a){["use strict";function b(b){return thi
2021-12-02 20:22:24 UTC	151	IN	Data Raw: 6c 65 6d 65 6e 74 2e 6f 66 66 73 65 74 28 29 3b 72 65 74 75 72 6e 20 74 68 69 73 2e 70 69 6e 6e 65 64 4f 66 66 73 65 74 3d 62 2e 74 6f 70 2d 61 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 63 68 65 63 6b 50 6f 73 69 74 69 6f 6e 57 69 74 68 45 76 65 6e 74 4c 6f 70 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 73 65 74 54 69 6d 65 6f 75 74 28 61 2e 70 72 6f 78 79 28 74 68 69 73 2e 63 68 65 63 6b 50 6f 73 69 74 69 6f 6e 2c 74 68 69 73 29 2c 31 29 7d 2c 63 2e 70 72 6f 74 6f 74 79 70 65 2e 63 68 65 63 6b 50 6f 73 69 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 69 73 28 22 3a 76 69 73 69 62 6c 65 22 29 29 7b 76 61 72 20 62 3d 74 68 69 73 2e 24 65 6c 65 6d 65 6e 74 2e 68 65 69 67 68 74 28 29 2c 64 3d 74 68 69 73 2e 6f Data Ascii: lement.offset();return this.pinnedOffset=b.top-a},c.prototype.checkPositionWithEventLoop=function(){setTimeout(a.proxy(this.checkPosition,this),1)},c.prototype.checkPosition=function(){if(this.\$element.is(":visible")){var b=this
2021-12-02 20:22:24 UTC	153	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49772	104.16.19.94	443	C:\Program Files\Google\Chrome\Application\chrome.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	115	OUT	GET /ajax/libs/popper.js/1.14.0/umd/popper.min.js HTTP/1.1 Host: cdnjs.cloudflare.com Connection: keep-alive Origin: null User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Intervention: <https://www.chromestatus.com/feature/5718547946799104>; level="warning" Accept: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:24 UTC	153	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 20:22:24 GMT Content-Type: application/javascript; charset=utf-8 Transfer-Encoding: chunked Connection: close Access-Control-Allow-Origin: * Cache-Control: public, max-age=30672000 ETag: W/"5eb03fa9-500f" Last-Modified: Mon, 04 May 2020 16:15:37 GMT cf-cdnjs-via: cfworker/kv Cross-Origin-Resource-Policy: cross-origin Timing-Allow-Origin: * X-Content-Type-Options: nosniff Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" CF-Cache-Status: HIT Age: 3033447 Expires: Tue, 22 Nov 2022 20:22:24 GMT Report-To: {"endpoints":[{"url":"https://V/a.nel.cloudflare.com/vreport/v3?s=PPAx7m9PtByQOkx38ZYFV01NMc3I5ClaWRcUwwXhY%2BzhVzBNfI0Hj1hbfb1e%2FjMvJT71A509hoPnQgQ1xwX%2FgsRXQyV7F%2FHwQjJeh%2FNyC9U4Tn6scxloHYaaPx27xaT4tNJQizsj"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800} Strict-Transport-Security: max-age=15780000 Server: cloudflare CF-RAY: 6b774464f9a5697b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-12-02 20:22:24 UTC	154	IN	Data Raw: 35 30 30 66 0d 0a 2f 2a 0a 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 46 65 64 65 72 69 63 6f 20 5a 69 76 6f 6c 6f 20 32 30 31 38 0a 20 44 69 73 74 72 69 62 75 74 65 64 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 4c 69 63 65 6e 73 65 20 28 6c 69 63 65 6e 73 65 20 74 65 72 6d 73 20 61 72 65 20 61 74 20 68 74 74 70 3a 2f 2f 6f 70 65 6e 73 6f 75 72 63 65 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 4d 49 54 29 2e 0a 20 2a 2f 28 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 27 6f 62 6a 65 63 74 27 3d 3d 74 79 70 65 6f 66 20 65 78 70 6f 72 74 73 26 26 27 75 6e 64 65 66 69 6e 65 64 27 21 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 74 28 29 3a 27 66 75 6e 63 Data Ascii: 500f* Copyright (C) Federico Zivolo 2018 Distributed under the MIT License (license terms are at http://opensource.org/licenses/MIT). */((function(e,t){'object'===typeof exports&&'undefined'!==typeof module?module.exports=t():'func
2021-12-02 20:22:24 UTC	154	IN	Data Raw: 74 69 6f 6e 27 3d 3d 74 79 70 65 6f 66 20 64 65 66 69 6e 65 26 26 64 65 66 69 6e 65 2e 61 6d 64 3f 64 65 66 69 6e 65 28 74 29 3a 65 2e 50 6f 70 70 65 72 3d 74 28 29 7d 29 28 74 68 69 73 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 27 75 73 65 20 73 74 72 69 63 74 27 3b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 72 65 74 75 72 6e 20 65 26 27 5b 6f 62 6a 65 63 74 20 46 75 6e 63 74 69 6f 6e 5d 27 3d 3d 3d 7b 7d 2e 74 6f 53 74 72 69 6e 67 2e 63 61 6c 6c 28 65 29 7d 66 75 6e 63 74 69 6f 6e 20 74 28 65 2c 74 29 7b 69 66 28 31 21 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 29 72 65 74 75 72 6e 5b 5d 3b 76 61 72 20 6f 3d 67 65 74 43 6f 6d 70 75 74 65 64 53 74 79 6c 65 28 65 2c 6e 75 6c 6c 29 3b 72 65 74 75 72 6e 20 74 3f 6f 5b 74 5d 3a 6f 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 65 Data Ascii: tion'===typeof define&&define.amd?define(t):e.Popper=t())(this,function(){'use strict';function e(e){return e&&[object Function]==={}?toString.call(e)}function t(e,t){if(!1===e.nodeType)return[];var o=getComputedStyle(e,null);return t?o[t]:o}function o(e
2021-12-02 20:22:24 UTC	155	IN	Data Raw: 72 20 66 3d 73 28 65 29 3b 72 65 74 75 72 6e 20 66 2e 68 6f 73 74 3f 64 28 66 2e 68 6f 73 74 2c 74 29 3a 64 28 65 2c 73 28 74 29 2e 68 6f 73 74 29 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 76 61 72 20 74 3d 31 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 31 5d 3f 61 72 67 75 6d 65 6e 74 73 5b 31 5d 3a 27 74 6f 70 27 2c 6f 3d 27 74 6f 70 27 3d 3d 3d 74 3f 27 73 63 72 6f 6c 6c 54 6f 70 27 3a 27 73 63 72 6f 6c 6c 4c 65 66 74 27 2c 6e 3d 65 2e 6e 6f 64 65 4e 61 6d 65 3b 69 66 28 27 42 4f 44 59 27 3d 3d 3d 6e 7c 7c 27 48 54 4d 4c 27 3d 3d 3d 6e 29 7b 76 61 72 20 69 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 72 3d 65 2e 6f 77 6e 65 72 Data Ascii: r f=s(e);return f.host?d(f.host,t):d(e,s(t).host)}function a(e){var t=1<arguments.length&&void 0!==(arguments[1]?arguments[1]:'top',o='top'===t?'scrollTop':'scrollLeft',n=e.nodeName;if('BODY'===n 'HTML'===n){var i=e.ownerDocument.t.documentElement,r=e.owner
2021-12-02 20:22:24 UTC	157	IN	Data Raw: 68 7c 7c 72 2e 72 69 67 68 74 2d 72 2e 6c 65 66 74 2c 64 3d 70 2e 68 65 69 67 68 74 7c 7c 65 2e 63 6c 69 65 6e 74 48 65 69 67 68 74 7c 7c 72 2e 62 6f 74 74 6f 6d 2d 72 2e 74 6f 70 2c 6c 3d 65 2e 6f 66 66 73 65 74 57 69 64 74 68 2d 73 2c 6d 3d 65 2e 6f 66 66 73 65 74 48 65 69 67 68 74 2d 64 3b 69 66 28 6c 7c 7c 6d 29 7b 76 61 72 20 67 3d 74 28 65 29 3b 6c 2d 3d 66 28 67 2c 27 78 27 29 2c 6d 2d 3d 66 28 67 2c 27 79 27 29 2c 72 2e 77 69 64 74 68 2d 3d 6c 2c 72 2e 68 65 69 67 68 74 2d 3d 6d 7d 72 65 74 75 72 6e 20 63 28 72 29 7d 66 75 6e 63 74 69 6f 6e 20 75 28 65 2c 6f 29 7b 7 6 61 72 20 69 3d 32 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 32 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 32 5d 2c Data Ascii: h r.right-r.left,d=p.height e.clientHeight r.bottom-r.top,l=e.offsetWidth-s,m=e.offsetHeight-d;if(!l){var g=t(e);l=f(g,'x'),m=f(g,'y'),r.width=l,r.height=m}return c(r)}function u(e,o){var i=2<arguments.length&&void 0!==(arguments[2]&&arguments[2],

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	158	IN	Data Raw: 6e 74 7d 66 75 6e 63 74 69 6f 6e 20 45 28 65 2c 74 2c 69 2c 72 29 7b 76 61 72 20 70 3d 34 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 34 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 34 5d 2c 73 3d 7b 74 6f 70 3a 30 2c 6c 65 66 74 3a 30 7d 2c 61 3d 70 3f 77 28 65 29 3a 64 28 65 2c 74 29 3b 69 66 28 27 76 69 65 77 70 6f 72 74 27 3d 3d 3d 72 29 73 3d 62 28 61 2c 70 29 3b 65 6c 73 65 7b 76 61 72 20 6c 3b 27 73 63 72 6f 6c 6c 50 61 72 65 6e 74 27 3d 3d 3d 72 3f 28 6c 3d 6e 28 6f 28 74 29 29 2c 27 42 4f 44 59 27 3d 3d 3d 6c 2e 6e 6f 64 65 4e 61 6d 65 26 26 28 6c 3d 65 2e 6f 77 6e 65 72 44 6f 63 75 6d 65 6e 74 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 29 29 3a 27 77 69 6e 64 6f 77 27 3d 3d 3d Data Ascii: nt}function E(e,t,i,r){var p=4<arguments.length&&void 0!==(arguments[4]&&arguments[4],s={top:0,left:0},a=p?w(e):d(e,t),if('viewport'===r)s=b(a,p);else{var l;'scrollParent'===r?(l=n(o(t)),'BODY'===l.nodeName&&(l=e.ownerDocument.documentElement)):'window'===
2021-12-02 20:22:24 UTC	159	IN	Data Raw: 74 74 6f 6d 29 2c 6e 3d 70 61 72 73 65 46 6c 6f 61 74 28 74 2e 6d 61 72 67 69 6e 4c 65 66 74 29 2b 70 61 72 73 65 46 6c 6f 61 74 28 74 2e 6d 61 72 67 69 6e 52 69 67 68 74 29 2c 69 3d 7b 77 69 64 74 68 3a 65 2e 6f 66 66 73 65 74 57 69 64 74 68 2b 6e 2c 68 65 69 67 68 74 3a 65 2e 6f 66 66 73 65 74 48 65 69 67 68 74 2b 6f 7d 3b 72 65 74 75 72 6e 20 69 7d 66 75 6e 63 74 69 6f 6e 20 53 28 65 29 7b 76 61 72 20 74 3d 7b 6c 65 66 74 3a 27 72 69 67 68 74 27 2c 72 6 9 67 68 74 3a 27 6c 65 66 74 27 2c 62 6f 74 74 6f 6d 3a 27 74 6f 70 27 2c 74 6f 70 3a 27 62 6f 74 74 6f 6d 27 7d 3b 72 65 74 75 72 6e 20 65 2e 72 65 70 6c 61 63 65 28 2f 6c 65 66 74 7c 72 69 67 68 74 7c 62 6f 74 74 6f 6d 7c 74 6f 70 2f 67 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 74 5b Data Ascii: ttom),n=parseFloat(t.marginLeft)+parseFloat(t.marginRight),i={width:e.offsetWidth+n,height:e.offsetHeight+o};return i}function S(e){var t={left:'right',right:'left',bottom:'top',top:'bottom'};return e.replace(/(left right bottom top)/g,function(e){return t[
2021-12-02 20:22:24 UTC	161	IN	Data Raw: 72 73 2e 66 6c 69 70 2e 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 6d 6f 64 69 66 69 65 72 73 2e 66 6c 69 70 2e 70 61 64 64 69 6e 67 29 2c 65 2e 6f 72 69 67 69 6e 61 6c 50 6c 61 63 65 6d 65 6e 74 3d 65 2e 70 6c 61 63 65 6d 65 6e 74 2c 65 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 54 28 74 68 69 73 2e 70 6f 70 70 65 72 2c 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2e 70 6f 73 69 74 69 6f 6e 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 70 6f 73 69 74 69 6f 6e 46 69 78 65 64 3f Data Ascii: rs.flip.boundariesElement,this.options.modifiers.flip.padding),e.originalPlacement=e.placement,e.positionFixed=this.options.positionFixed,e.offsets.popper=T(this.popper,e.offsets.reference,e.placement),e.offsets.popper.position=this.options.positionFixed?
2021-12-02 20:22:24 UTC	162	IN	Data Raw: 74 65 42 6f 75 6e 64 3d 69 2c 48 28 65 29 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 27 72 65 73 69 7a 65 27 2c 6f 2e 75 70 64 61 74 65 42 6f 75 6e 64 2c 7b 70 61 73 73 69 76 65 3a 21 30 7d 29 3b 76 61 72 20 72 3d 6e 28 65 29 3b 72 65 74 75 72 6e 20 41 28 72 2c 27 73 63 72 6f 6c 6c 27 2c 6f 2e 75 70 64 61 74 65 42 6f 75 6e 64 2c 6f 2e 73 63 72 6f 6c 6c 50 61 72 65 6e 74 73 29 2c 6f 2e 73 63 72 6f 6c 6c 45 6c 65 6d 65 6e 74 3d 72 2c 6f 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 21 30 2c 6f 7d 66 75 6e 63 74 69 6f 6e 20 4d 28 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 7c 7c 28 74 68 69 73 2e 73 74 61 74 65 3d 49 28 74 68 69 73 2e 72 65 66 65 72 65 6e 63 65 2c 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2c 74 68 69 73 Data Ascii: teBound=i,H(e).addEventListener('resize',o.updateBound,{passive:!0});var r=n(e);return A(r,'scroll',o.updateBound,o.scrollParents),o.scrollElement=r,o.eventsEnabled=!0,o}function M(){this.state.eventsEnabled (this.state=I(this.reference,this.options,this
2021-12-02 20:22:24 UTC	163	IN	Data Raw: 6c 65 6e 67 74 68 26 26 76 6f 69 64 20 30 21 3d 3d 61 72 67 75 6d 65 6e 74 73 5b 31 5d 26 26 61 72 67 75 6d 65 6e 74 73 5b 31 5d 2c 6f 3d 6c 65 2e 69 6e 64 65 78 4f 66 28 65 29 2c 6e 3d 6c 65 2e 73 6c 69 63 65 28 6f 2b 31 29 2e 63 6f 6e 63 61 74 28 6c 65 2e 73 6c 69 63 65 28 30 2c 6f 29 69 63 65 28 30 2c 6f 29 3b 72 65 74 75 72 6e 20 74 3f 6e 2e 72 65 76 65 72 73 65 28 29 3a 6e 7d 66 75 6e 63 74 69 6f 6e 20 7a 28 65 2c 74 2c 6f 2c 6e 29 7b 76 61 72 20 69 3d 65 2e 6d 61 74 63 68 28 2f 28 28 3f 3a 5c 2d 7c 5c 2b 29 3f 5c 64 2a 5c 2e 3f 5c 64 2a 29 28 2e 2a 29 2f 29 2c 72 3d 2b 69 5b 31 5d 2c 70 3d 69 5b 32 5d 3b 69 66 28 21 72 29 72 65 74 75 72 6e 20 65 3b 69 66 28 30 3d 3d 3d 70 2e 69 6e 64 65 78 4f 66 28 27 25 27 29 29 7b 76 61 72 20 73 3b 73 77 69 74 63 68 28 70 29 7b 63 61 Data Ascii: length&&void 0!==(arguments[1]&&arguments[1],o=le.indexOf(e),n=le.slice(o+1).concat(le.slice(0,o));return t?t.n.reverse():n}function z(e,t,o,n){var i=e.match(/((?!\- \+)?d*\.\?d*\.(.*)/),r=i[1],p=i[2];if(!r)return e;if(0===p.indexOf('%')){var s;switch(p){ca
2021-12-02 20:22:24 UTC	165	IN	Data Raw: 63 65 2c 64 3d 69 2e 73 70 6c 69 74 28 27 2d 27 29 5b 30 5d 3b 72 65 74 75 72 6e 20 6f 3d 55 28 2b 6e 29 3f 5b 2b 6e 2c 30 5d 3a 47 28 6e 2c 70 2c 73 2c 64 29 2c 27 6c 65 66 74 27 3d 3d 3d 64 3f 28 70 2e 74 6f 70 2b 3d 6f 5b 30 5d 2c 70 2e 6c 65 66 74 2d 3d 6f 5b 31 5d 29 3a 27 72 69 67 68 74 27 3d 3d 3d 64 3f 28 70 2e 74 6f 70 2b 3d 6f 5b 30 5d 2c 70 2e 6c 65 66 74 2b 3d 6f 5b 31 5d 29 3a 27 74 6f 70 27 3d 3d 3d 64 3f 28 70 2e 6c 65 66 74 2b 3d 6f 5b 30 5d 2c 70 2e 74 6f 70 2d 3d 6f 5b 31 5d 29 3a 27 62 6f 74 74 6f 6d 27 3d 3d 3d 64 26 26 28 70 2e 6c 65 66 74 2b 3d 6f 5b 30 5d 2c 70 2e 74 6f 70 2b 3d 6f 5b 31 5d 29 2c 65 2e 70 6f 70 70 65 72 3d 70 2c 65 7d 66 6f 72 28 76 61 72 20 58 3d 4d 61 74 68 2e 6d 69 6e 2c 4a 3d 4d 61 74 68 2e 66 6c 6f 6f 72 2c 51 Data Ascii: ce,d=i.split('-')[0];return o=U(+n)?[+n,0]:G(n,p,s,d),'left'===d?(p.top+=o[0],p.left=-o[1]):'right'===d?(p.top+=o[0],p.left+=o[1]):'top'===d?(p.left+=o[0],p.top=-o[1]):'bottom'===d&&(p.left+=o[0],p.top+=o[1]),e.popper=p,e}for(var X=Math.min,J=Math.floor,Q
2021-12-02 20:22:24 UTC	166	IN	Data Raw: 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 74 2c 6f 2c 6e 29 7b 72 65 74 75 72 6e 20 6f 26 26 65 28 74 2e 70 72 6f 74 6f 74 79 70 65 2c 6f 29 2c 6e 26 26 65 28 74 2c 6e 29 2c 74 7d 7d 28 29 2c 73 65 3d 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6f 29 7b 72 65 74 75 72 6e 20 74 20 69 6e 20 65 3f 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 74 2c 7b 76 61 6c 75 65 3a 6f 2c 65 6e 75 6d 65 72 61 62 6c 65 3a 21 30 2c 63 6f 6e 66 69 67 75 72 61 62 6c 65 3a 21 30 2c 77 72 69 74 61 62 6c 65 3a 21 30 7d 29 3a 65 5b 74 5d 3d 6f 2c 65 7d 2c 64 65 3d 4f 62 6a 65 63 74 2e 61 73 73 69 67 6e 7c 7c 66 75 6e 63 74 69 6f 6e 28 65 7b 66 6f 72 28 76 61 72 20 74 2c 6f 3d 31 3b 6f 3c 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 3b 6f 2b 2b 29 66 6f Data Ascii: turn function(t,o,n){return o&&e(t.prototype,o),n&&e(t,n),t}},se=function(e,t,o){return t in e?Object.defineProperty(e,t,{value:o,enumerable:!0,configurable:!0,writable:!0}):e[t]=o,e},de=Object.assign function(e){for(var t,o=1;o<arguments.length;o++)fo
2021-12-02 20:22:24 UTC	167	IN	Data Raw: 65 64 26 26 65 28 74 2e 6f 6e 4c 6f 61 64 29 26 26 74 2e 6f 6e 4c 6f 61 64 28 69 2e 72 65 66 65 72 65 6e 63 65 2c 69 2e 70 6f 70 70 65 72 2c 69 2e 6f 70 74 69 6f 6e 73 2c 74 2c 69 2e 73 74 61 74 65 29 7d 29 2c 74 68 69 73 2e 75 70 64 61 74 65 28 29 3b 76 61 72 20 70 3d 74 68 69 73 2e 6f 70 74 69 6f 6e 73 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3b 70 26 26 74 68 69 73 2e 65 6e 61 62 6c 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 73 28 29 2c 74 68 69 73 2e 73 74 61 74 65 2e 65 76 65 6e 74 73 45 6e 61 62 6c 65 64 3d 70 7d 72 65 74 75 72 6e 20 70 65 28 74 2c 5b 7b 6b 65 79 3a 2 7 75 70 64 61 74 65 27 2c 76 61 6c 75 65 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6b 2e 63 61 6c 6c 28 74 68 69 73 29 7d 7d 2c 7b 6b 65 79 3a 27 64 65 73 74 72 6f 79 27 Data Ascii: ed&&e(t.onLoad)&&t.onLoad(i.reference,i.popper,i.options,t.i.state))),this.update();var p=this.options.eventsEnabled;p&&this.enableEventListeners(),this.state.eventsEnabled=p)return pe(t,[[key:'update',value:function(){return k.call(this)}}],[key:'destroy'

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:24 UTC	169	IN	Data Raw: 5d 2c 6e 5b 65 5d 29 29 2c 73 65 28 7b 7d 2c 65 2c 6f 29 7d 2c 73 65 63 6f 6e 64 61 72 79 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 6f 3d 27 72 69 67 68 74 27 3d 3d 3d 65 3f 27 6c 65 66 74 27 3a 27 74 6f 70 27 2c 69 3d 70 5b 6f 5d 3b 72 65 74 75 72 6e 20 70 5b 65 5d 3e 6e 5b 65 5d 26 26 21 74 2e 65 73 63 61 70 65 57 69 74 68 52 65 66 65 72 65 6e 63 65 26 26 28 69 3d 58 28 70 5b 6f 5d 2c 6e 5b 65 5d 2d 28 27 72 69 67 68 74 27 3d 3d 3d 65 3f 70 2e 77 69 64 74 68 3a 70 2e 68 65 69 67 68 74 29 29 29 2c 73 65 28 7b 7d 2c 6f 2c 69 29 7d 7d 3b 72 65 74 75 72 6e 20 69 2e 6 6 6f 72 45 61 63 68 28 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 2d 31 3d 3d 3d 5b 27 6c 65 66 74 27 2c 27 74 6f 70 27 5d 2e 69 6e 64 65 78 4f 66 28 65 29 3f 27 73 65 63 6f Data Ascii:],n[e]],se({},e,o)),secondary:function(e){var o='right'===e?'left':'top',i=p[o];return p[e]>n[e]&&it.escapeWithReference&&(i=X[p[o],n[e]]-'right'===e?p.width:p.height)),se({},o,i));return i.forEach(function(e){var t=-1===['left','top'].indexOf(e)?'seco
2021-12-02 20:22:24 UTC	170	IN	Data Raw: 70 65 72 3d 63 28 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 29 3b 76 61 72 20 62 3d 64 5b 6d 5d 2b 64 5b 6c 5d 2f 32 2d 75 2f 32 2c 79 3d 74 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 29 2c 77 3d 70 61 72 73 65 46 6c 6f 61 74 28 79 5b 27 6d 61 72 67 69 6e 27 2b 66 5d 2c 31 30 29 2c 45 3d 70 61 72 73 65 46 6c 6f 61 74 28 79 5b 27 62 6f 72 64 65 72 27 2b 66 2b 27 57 69 64 74 68 27 5d 2c 31 30 29 2c 76 3d 62 2d 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 5b 6d 5d 2d 77 2d 45 3b 72 65 74 75 72 6e 20 76 3d 51 28 58 28 73 5b 6c 5d 2d 75 2c 76 29 2c 30 29 2c 65 2e 61 72 72 6f 77 45 6c 65 6d 65 6e 74 3d 69 2c 65 2e 6f 66 66 73 65 74 73 2e 61 72 72 6f 77 3d 28 6e 3d 7b 7d 2c 73 65 28 6e 2c 6d 2c 4d 61 74 68 2e 72 6f 75 6e 64 28 76 29 29 2c 73 Data Ascii: per=c(e.offsets.popper);var b=d[m]+d[l]/2-u/2,y=t(e.instance.popper),w=parseFloat(y['margin'+f],10),E=parseFloat(y['border'+f+'Width'],10),v=b-e.offsets.popper[m]-w-E;return v=Q(X[s[l]-u,v],0),e.arrowElement=i,e.offsets.arrow=(n={},se(n,m,Math.round(v)),s
2021-12-02 20:22:24 UTC	171	IN	Data Raw: 28 72 29 29 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 3d 6e 2b 28 72 3f 27 2d 27 2b 72 3a 27 27 29 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 3d 64 65 28 7b 7d 2c 65 2e 6f 66 66 73 65 74 73 2e 70 6f 70 70 65 72 2c 54 28 65 2e 69 6e 73 74 61 6e 63 65 2e 70 6f 70 70 65 72 2c 65 2e 6f 66 66 73 65 74 73 2e 72 65 66 65 72 65 6e 63 65 2c 65 2e 70 6c 61 63 65 6d 65 6e 74 29 29 2c 65 3d 4e 28 65 2e 69 6e 73 74 61 6e 63 65 2e 6d 6f 64 69 66 69 65 72 73 2c 65 2c 27 66 6c 69 70 27 29 29 7d 29 2c 65 7d 2c 62 65 68 61 76 69 6f 72 3a 27 66 6c 69 70 27 2c 70 61 64 64 69 6e 67 3a 35 2c 62 6f 75 6e 64 61 72 69 65 73 45 6c 65 6d 65 6e 74 3a 27 76 69 65 77 70 6f 72 74 27 7d 2c 69 6e 6e 65 72 3a 7b 6f 72 64 65 72 3a 37 30 30 2c 65 6e 61 62 6c 65 64 3a 21 31 2c 66 6e 3a 66 Data Ascii: (r)),e.placement=n+(r?'-':'r.'),e.offsets.popper=de({},e.offsets.popper,T(e.instance.popper,e.offsets.reference,e.placement)),e=N(e.instance.modifiers,e,'flip'))),e),behavior:'flip',padding:5,boundariesElement:'viewport'),inner:{order:700,enabled:!1,fn:f
2021-12-02 20:22:24 UTC	173	IN	Data Raw: 68 3d 7b 6c 65 66 74 3a 4a 28 69 2e 6c 65 66 74 29 2c 74 6f 70 3a 4a 28 69 2e 74 6f 70 29 2c 62 6f 74 74 6f 6d 3a 4a 28 69 2e 62 6f 74 74 6f 6d 29 2c 72 69 67 68 74 3a 4a 28 69 2e 72 69 67 68 74 29 7d 2c 63 3d 27 62 6f 74 74 6f 6d 27 3d 3d 3d 3d 6f 3f 27 74 6f 70 27 3a 27 62 6f 74 74 6f 6d 27 2c 75 3d 27 72 69 67 68 74 27 3d 3d 3d 6e 3f 27 6c 65 66 74 27 3a 27 72 69 67 68 74 27 2c 62 3d 57 28 27 74 72 61 6e 73 66 6f 72 6d 27 29 3b 69 66 28 64 3d 27 62 6f 74 74 6f 6d 27 3d 3d 63 3f 2d 66 2e 68 65 69 67 68 74 2b 68 2e 62 6f 74 74 6f 6d 3a 68 2e 74 6f 70 2c 73 3d 27 72 69 67 68 74 27 3d 3d 75 3f 2d 66 2e 77 69 64 74 68 2b 68 2e 72 69 67 68 74 3a 68 2e 6c 65 66 74 2c 61 26 26 62 29 6d 5b 62 5d 3d 27 74 72 61 6e 73 6c 61 74 65 33 64 28 27 2b 73 2b 27 70 78 2c 20 Data Ascii: h={left:J(i.left),top:J(i.top),bottom:J(i.bottom),right:J(i.right)},c='bottom'===o?'top':'bottom',u='right'===n?'left':'right',b=W('transform');if(d='bottom'===c?'-f.height'+h.bottom:h.top,s='right'===u?'-f.width'+h.right:h.left,a&&b)m[b]='translate3d('+s+'px,
2021-12-02 20:22:24 UTC	174	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49778	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	174	OUT	GET /shared/1.0/content/images/backgrounds/2-small_e58aafc980614a9cd7796bea7b5ea8f0.jpg HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	177	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 569695 Cache-Control: public, max-age=31536000 Content-MD5: 5YqvYBhSpzXeWvqe16o8A== Content-Type: image/jpeg Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D7B007295267C8 Last-Modified: Wed, 12 Feb 2020 22:01:50 GMT Server: ECAcc (frc/8F9C) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 1b3e17ef-601e-001b-1f8b-e2b5e2000000 x-ms-version: 2009-09-19 Content-Length: 987 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	175	OUT	GET /shared/1.0/content/images/work_account_1963c6b1926b773986f53f844ce4c32e.png HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	199	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Type,Cache-Control,Last-Modified,ETag,Content-MD5,x-ms-lease-status,x-ms-blob-type,Content-Length,Date,Transfer-Encoding Age: 12830721 Cache-Control: public, max-age=31536000 Content-MD5: GWPGsZJrdzmG9T+ETOTDLg== Content-Type: image/png Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D79A1BA1ED720E Last-Modified: Thu, 16 Jan 2020 00:32:56 GMT Server: ECAcc (frc/8FDA) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 6725e28a-f01e-0057-3408-7385c3000000 x-ms-version: 2009-09-19 Content-Length: 1487 Connection: close
2021-12-02 20:22:25 UTC	201	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 33 00 00 00 33 08 06 00 00 00 3a a1 30 2a 00 00 00 09 70 48 59 73 00 00 0b 13 00 00 0b 13 01 00 9a 9c 18 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 05 5c 49 44 41 54 78 da d4 5a 4f 68 14 57 18 7f 89 0b 89 58 9a c4 83 58 4b d9 ad 56 b0 18 d8 15 5a b4 05 cd 78 e9 a9 25 0b 3d e8 2d 23 3d 88 bd b8 16 7b 2c d9 1c 7a 6a 69 37 08 d5 8 b 64 bd b5 27 37 d8 53 7b e8 ac 82 87 da c2 a6 44 ac a0 74 83 18 25 87 b8 51 24 91 56 d2 ef 37 fb de f0 76 76 e6 cd 9b 9 9 b7 2e f9 60 98 fd 33 7f de ef 7d df f7 fb fe bc 37 b0 b9 b9 c9 4c ca c0 f9 9b 16 9d 0a 74 8c d2 61 05 5c d2 a0 a3 45 87 83 cf 9b df 7e d8 32 f6 ee b4 60 68 f0 18 b4 4d 47 91 8e 89 dc Data Ascii: PNGIHDR33:0*pHYstEXtSoftwareAdobe ImageReadyqe<\DATxZOHWXXKVZx%=-#{,zji7d'7S{Dt%Q\$V7vv`3}7Lta E~2'hMG

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49779	152.199.23.37	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	175	OUT	GET /ests/2.1/content/images/microsoft_logo.png HTTP/1.1 Host: aadcdn.msftauth.net Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: application/signed-exchange;v=b3;q=0.9,*/*;q=0.8 Purpose: prefetch Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: empty Referer: https://login.microsoftonline.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
2021-12-02 20:22:25 UTC	179	IN	HTTP/1.1 200 OK Accept-Ranges: bytes Access-Control-Allow-Origin: * Access-Control-Expose-Headers: x-ms-request-id,Server,x-ms-version,Content-Length,Date,Transfer-Encoding Age: 499341 Cache-Control: public, max-age=604800 Content-MD5: 7ZyesNzhfXUr7eprWs2m2Q== Content-Type: image/png Date: Thu, 02 Dec 2021 20:22:25 GMT Etag: 0x8D641014F7D2A46 Last-Modified: Fri, 02 Nov 2018 20:25:20 GMT Server: ECAcc (frc/8F55) X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: be489eec-e01e-005b-242f-e34940000000 x-ms-version: 2009-09-19 Content-Length: 1057 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 20:22:25 UTC	179	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 6c 00 00 00 18 08 06 00 00 00 1f d5 18 1a 00 00 00 09 70 48 59 73 00 00 0b 12 00 00 0b 12 01 d2 dd 7e fc 00 00 03 d3 49 44 41 54 68 de ed 58 4d 4e db 50 10 fe 5c b1 45 f1 0d 92 f6 02 b8 27 20 2c da 2d e9 ba 8b 24 27 c0 48 b3 8f d9 8f 14 73 02 8c d4 ae 31 db 76 51 e7 06 c9 01 aa 9a 13 34 e9 05 d2 cd 0c 1a 06 1b 0c 2d c2 91 3c 92 17 ef f9 fd cc 7b df fc 7c f3 82 3f a3 77 5b 34 94 fd ab 9f 41 f2 3d 68 3c 3e f9 b0 0d d0 c9 7f 95 37 dd 15 74 80 75 f2 82 b2 d7 5d 41 7b 84 88 26 00 06 d2 2c 98 b9 68 05 60 44 34 00 30 31 5d 95 ca d5 1c 04 cc 9c 48 7f 26 fd c9 43 f3 77 00 a8 10 40 01 e0 c0 fd 2a da e2 61 03 00 33 d3 be 03 48 c5 61 52 00 3d cb 67 88 28 02 30 d6 36 80 e1 0e 3b 57 6c c0 da 00 58 02 58 cb f9 47 Data Ascii: PNGIHDRlPhYs-IDATHXMNPtE' ,-\$Hs1vQ4-<[?w[4A=h<>7tu]A{&,h`D401]H&Cw@*a3HaR=g(06;WlXXG

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6464 Parent PID: 980

General	
Start time:	21:22:17
Start date:	02/12/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "C:\Users\user\Desktop\PaymentReceipt.html
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: chrome.exe PID: 6636 Parent PID: 6464

General	
Start time:	21:22:19
Start date:	02/12/2021
Path:	C:\Program Files\Google\Chrome\Application\chrome.exe

Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1552,6213295624667690040,7919256905441255605,131072 --lang=en-GB --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1956 /prefetch:8
Imagebase:	0x7ff609c80000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

[File Activities](#)

Show Windows behavior

Disassembly

Code Analysis