

JOeSandbox Cloud BASIC



ID: 532715

Cookbook: browseurl.jbs

Time: 16:36:33

Date: 02/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Overview	3
Dropped Files	3
Sigma Overview	3
Jbx Signature Overview	3
AV Detection:	4
Phishing:	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	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted URLs	8
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
Private	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	40
No static file info	40
Network Behavior	41
Network Port Distribution	41
TCP Packets	41
UDP Packets	41
DNS Queries	41
DNS Answers	41
HTTP Request Dependency Graph	42
HTTPS Proxied Packets	43
Code Manipulations	139
Statistics	139
Behavior	139
System Behavior	139
Analysis Process: chrome.exe PID: 2948 Parent PID: 384	139
General	140
File Activities	140
Registry Activities	140
Analysis Process: chrome.exe PID: 4580 Parent PID: 2948	140
General	140
File Activities	140
Registry Activities	140
Disassembly	140
Code Analysis	140

Windows Analysis Report https://pickup.acepickapart.c...

Overview

General Information

Sample URL:

http://https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com

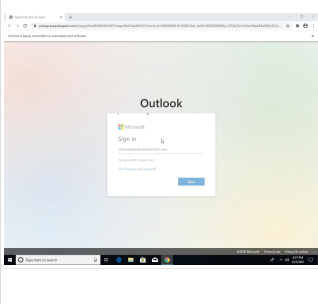
Analysis ID:

532715

Infos:



Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

HTMLPhisher

Score:

72

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus / Scanner detection for sub...

Phishing site detected (based on fav...

Yara detected HtmlPhish10

Phishing site detected (based on log...

Phishing site detected (based on im...

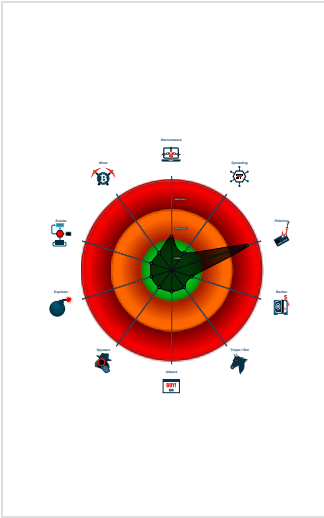
URL contains potential PII (phishing...

No HTML title found

HTML body contains low number of ...

Submit button contains javascript call

Classification



Process Tree

- System is w10x64
- chrome.exe (PID: 2948 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --enable-automation "https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com MD5: C139654B5C1438A95B321BB01AD63EF6")
 - chrome.exe (PID: 4580 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1560,8371606130546468176,16739999905795240130,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Antivirus / Scanner detection for submitted sample

Phishing:



Phishing site detected (based on favicon image match)

Yara detected HtmlPhish10

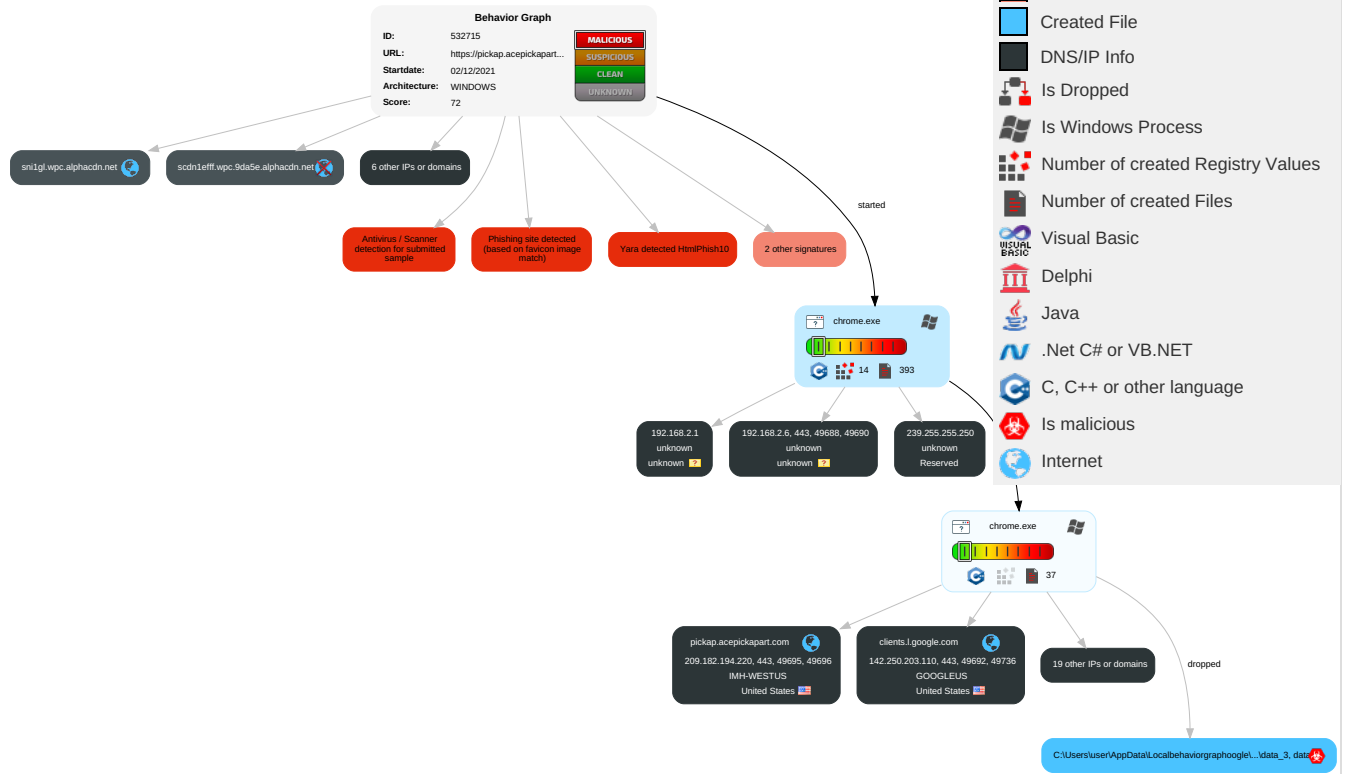
Phishing site detected (based on logo template match)

Phishing site detected (based on image similarity)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Masquerading 3	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	Modify System Partition
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	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Scripting 1	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	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Carrier Billing Fraud

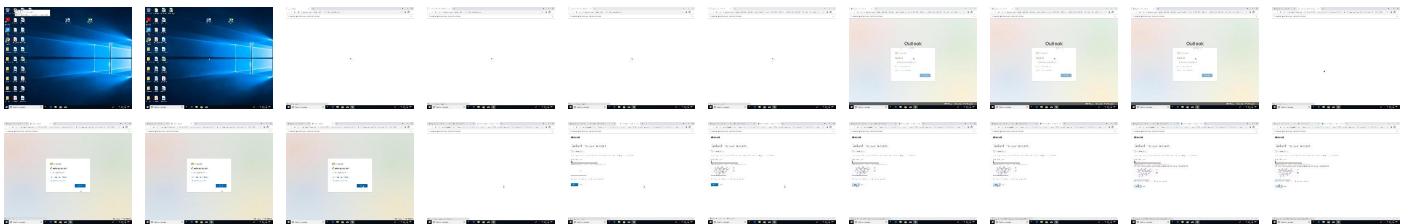
Behavior Graph

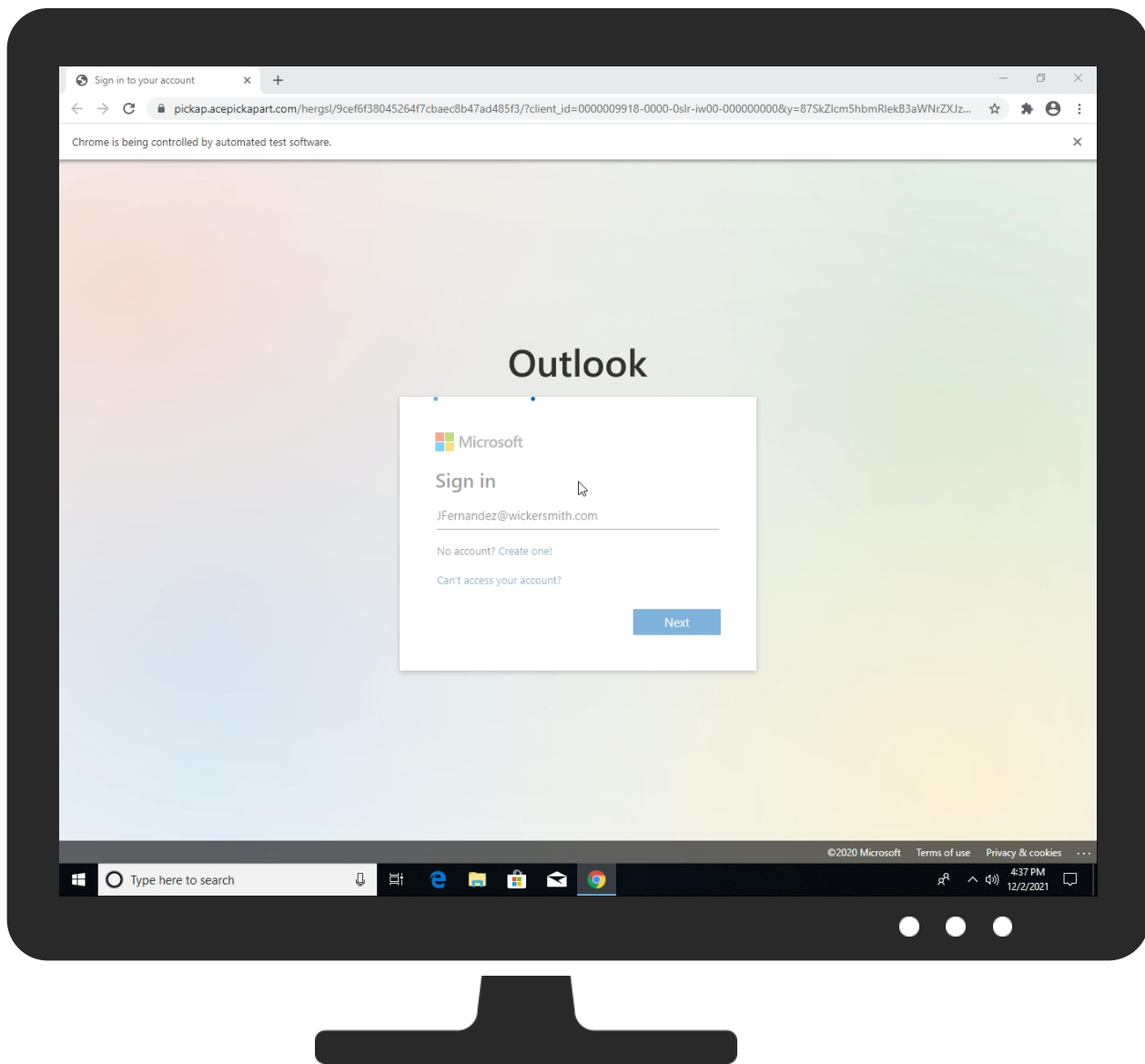


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com	0%	Virustotal		Browse
http://https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com	0%	Avira URL Cloud	safe	
http://https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com	100%	SlashNext	Fake Login Page type: Phishing & Social usering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/Mic_BG.jpg	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/lightweightsignuppackage_XHlZmGIS3q-Ac0QYFxaGDg2.js?v=1	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/0-small_138bcee6	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/rcopy.phpSign	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/microsoft_logo_e	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/rcopy.php2	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/oned5_EMWt_IK9fDTY6ZqY6xYrUA2.js?v=1	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_grey_2b	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/0-small_138bcee624fa04ef9b75e86211a9fe0d.jpg	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/favicon_a_eupa_yf	0%	Avira URL Cloud	safe	
https://pki.goog/repo/certs/gtsr1.der04	0%	URL Reputation	safe	
https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VuuqFA2.js?v=1	0%	URL Reputation	safe	
https://pickup.acepickapart.com/hergsl/rcopy.php	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/jqueryshim_tGLkJ9mWEbN2n0ToVG2gvQ2.js?v=1	0%	URL Reputation	safe	
https://acctcdn.msauth.net/images/2_vD0yppaJX3jBnfbHF1hqXQ2.svgZ	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/images/dropdown_caret_KXSZjGsyLLZaoTf0sl9X-A2.svg	0%	URL Reputation	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/mp.js	0%	Avira URL Cloud	safe	
https://dns.google	0%	URL Reputation	safe	
https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js	0%	URL Reputation	safe	
https://acctcdn.msauth.net/images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg	0%	URL Reputation	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/css.cssM	0%	Avira URL Cloud	safe	
https://www.google.com ;	0%	Avira URL Cloud	safe	
https://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	URL Reputation	safe	
https://pki.goog/repository/0	0%	URL Reputation	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/	0%	URL Reputation	safe	
https://aadcdn.msauth.net/ests/2.1/content/images/ellipsis_grey_5bc252567ef56db648207d9c36a9d004.png	0%	Avira URL Cloud	safe	
https://aadcdn.msauth.net/ests/2.1/content/images/ellipsis_white_0ad43084800fd8b50a2576b5173746fe.png	0%	Avira URL Cloud	safe	
https://crl.pki.goog/gsr1/gsr1.crl0 ;	0%	URL Reputation	safe	
https://acctcdn.msauth.net/lightweightsignuppackage_XHlZmGIS3q-Ac0QYFxaGDg2.js?v=1a	0%	Avira URL Cloud	safe	
https://crls.pki.goog/gts1c3/moVDfSia2k.crl0	0%	URL Reputation	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2824ef3517b6c416dcf8ff7d410.svg	0%	Avira URL Cloud	safe	
https://acctcdn.msauth.net/converged_ux_v2_kGcCYmU0rW3A6Zc7U1O8nw2.css?v=1	0%	URL Reputation	safe	
https://aadcdn.msauth.net/ests/2.1/content/images/ellipsis_white_5ac590ee72bfe06a7cecf75b588ad73.sv	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/45_sgsjshsdggdjx	0%	Avira URL Cloud	safe	
https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_white_5	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pickap.acepickapart.com	209.182.194.220	true	false		unknown
accounts.google.com	172.217.168.45	true	false		high
sni1gl.wpc.alphacdn.net	152.199.21.175	true	false		unknown
clients.l.google.com	142.250.203.110	true	false		high
googlehosted.l.googleusercontent.com	142.250.203.97	true	false		high
passwordreset.microsoftonline.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
signup.live.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
fpt.live.com	unknown	unknown	false		high
acctcdn.msauth.net	unknown	unknown	false		unknown
ajax.aspnetcdn.com	unknown	unknown	false		high
acctcdn.msftauth.net	unknown	unknown	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/Mic_BG.jpg	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/lightweightsignuppackage_XHIZmGIS3q-Ac0QYFXaGDg2.js?v=1	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/oned5_EMWt_IK9fDTY6ZqY6xYrUA2.js?v=1	false	Avira URL Cloud: safe	unknown
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/0-small_138bce624fa04ef9b75e86211a9fe0d.jpg	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/knockout_3.3.0_X1BYS2jZMbi7hfUj8VvuqFA2.js?v=1	false	URL Reputation: safe	unknown
http://https://pickap.acepickapart.com/hergsl/rcopy.php	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/jqueryshim_tGLkJ9mWEbN2n0ToVG2gvQ2.js?v=1	false	URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/images/dropdown_caret_KXSZjGsyLLZaoTf0sl9X-A2.svg	false	URL Reputation: safe	unknown
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/mp.js	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/datarequestpackage_h-_7C7UzwdexFJT9njDBTQ2.js	false	URL Reputation: safe	unknown
http://https://acctcdn.msauth.net/images/microsoft_logo_7lynN7YkjJOP0NwZNw6QvQ2.svg	false	URL Reputation: safe	unknown
http://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-US&acceptformat=crx3&x=id%3Dnmhmhkegccagldgiimedpiccmgmieda%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgdpelpbcmbmeomcjbbeemfm%26v%3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1	false		high
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_grey_2b5d393db04a5e6e1f739cb266e5b4c.svg	false	Avira URL Cloud: safe	unknown
http://https://passwordreset.microsoftonline.com/?ru=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2fprocess%3fctx%3drQIIAXWR02_TUABG47xoqwgqFhgrxARyYvv6GalDXIfYTWzXivPHWVSLHdhqb2NdJbuomv4CBoawdWUAdECAqEAXsDJ06s7AijSAGBhfwDLN53h0zkPcmSZrN6nAc043FDABYcFOC2QBO7QFIsDBrCAikPlcDs9tb2p1Kxkn12ob552mKwf1_f08fujBFK5tVKJU3TmhyNAtcvuzCqfMCwKwz7jmFn2YIf493OeXbOAlagOE7gKZIBgKYFpmyHNUaL2IHfqiM1PAzsDkFolsq0LGVpWwZSV26qhV2JfqrUHSmpbmqmJrVdZvVSQFtVJdc3r0tGqZU5C7ZpvGlxGtSf2SiFv63D8NXtLry3QmLoeOAtW_q_s5gjOokEC5-gs9wLTeZ9WvD0Yx76LyteYH6PAdVAA44MZTPwZCvz5bqfbH_U8nCGGEXcwTCIOYKV204tXAI95BhzARU8UepJ4TO7z01g0nB5oLk4oRkc1x18YU_548lhUeqow1UGDE-UTMwFHliuDrqk29Qe4drSSPwmJzteMNQHmilbfN1T-D2bXaJu722uuYawfygd3N9Kg68nWQGR8HEv8pjP_IIIIfd2NjatzN7GT-5LHnhXWtb-9eFd63vjQ_X7wbsbf_ez1wWKjDRZFOUOlawiCnbjPkJ1QhCuAIS6aV2ZQrFef0hkN1UoXe5KnlaxE6LxZ9F7MmNzMfN_7X-Bw2&mkt=en-US&hosted=0&device_platform=Windows+10	false		high
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true	true		unknown
http://https://pickap.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg	false	Avira URL Cloud: safe	unknown
http://https://acctcdn.msauth.net/converged_ux_v2_kGcCYmU0rW3A6Zc7U1O8nw2.css?v=1	false	URL Reputation: safe	unknown
http://https://clients2.googleusercontent.com/crx/blobs/Acy1k0bLljHsvnKaKN_oRpVaYYvFs25d7GKYF1WXrT6yizCMksBO0c_ggE0B6tx6HPRHe6q1GOEe3_NclbSiGG8kXeLMUY0sAKVvC6R89zvKM13s5VqoAMZSmuUgjQL5vlygJuArQghXXE_qTL7NIQ/extension_8520_615_0_5.crx	false		high
http://https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.182.194.220	pickap.acepickapart.com	United States		22611	IMH-WESTUS	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
239.255.255.250	unknown	Reserved		unknown	unknown	false
152.199.21.175	sni1gl.wpc.alphacdn.net	United States		15133	EDGECASTUS	false

Private

IP

192.168.2.1
192.168.2.6
192.168.2.22
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532715
Start date:	02.12.2021
Start time:	16:36:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com
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:	4
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.win@30/239@13/10
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 • Browse: <a ?ru="https%3a%2f%2flogin.microsoftonline.com%2fcommon%2fprocess%3fctc%3drQIIAXWRO2_TUABG47xoqwgqFhgrxARyYvv6GalDXIfYTWzXiVPHWSLHdhqb2NdJbuomv4CBoawdWUAdECAqEAsDJ06s7AiJsSAGBhlfwDLN53h0zkPcmSZrN6nAc043FDABYcFOC2QBO7QFIsDBrCAikiPlcDs9tb2p1Kxkn12ob552mKWf1_fO8fujBFK5tVKJU3TMhyNAtcvuzCqfMCwKwz7jmFn2YIf493OeXbOAlagOE7gKZlBgKYFpmyHNUaL2lHfqiM1PAzsDkFolsq0LGVpWwZSV26qhv2JFrqUHSmpbqmkJrVDzVSQFtVJdc3r0tGqZU5C7ZpvGlxGtSf2SiFV63D8NxtLry3QmLoeOAtW_q_s5gjOokEC5-gs9wLTEz9WvD0Yx76LyteYH6PAdVAA44MZTPwZCvz5bqfbh_U8nCGGEXcwtCI0YKV204tXAi95BhzARU8UepJ4TO7z01g0nB5oLk4oRkc1x18YU_548lhUeqow1UGDE-UTMwFHliuDrqkc29Qe4drSSPwmJzteMNQHmilbfN1T-D2bXaJu722uuNYawfgyd3N9Kg68nWQGR8HEv8pjP_illifd2NjatzN7GT-5LHnhXWtb-9eFd63vjQ_X7wsbf_" ez1wwkjdrzfouolawcnbjpkj1qhcuals6avz2qrfef0hkn1uoxe5knlaxe6lxz9f7mmnzmfn_7x-bw2&mkt="en-US&hosted=0&device_platform=Windows+10</a" href="https://login.live.com/oauth20_authorize.srf?response_type=code&client_id=51483342-085c-4d86-bf88-cf50c7252078&scope=openid+profile+email+offline_access&response_mode=form_post&redirect_uri=https%3a%2f%2flogin.microsoftonline.com%2fcommon%2ffederation%2foauth2&state=rQIIAXVSPW_TUADMS9rQVAiqCgkWRAfEgOT42S-240gVavPROk3s5tNxIshxnMRx_OzYr7HsjY2xE0gZGGBA6sgELOydOvcXICbUCSSQSNIZbri74XR3z1NMlik8zaEcpwtDkRj1HIE5kYGUnmN5CnGIRyxkRhxE_u72zpP56_nv9GP5Tevl5-DrnxcrcBnMraWZNVznAjycEulFBZoOwzDrjseW8U-gPwFwBcA3AFbJTRNTndZFMuARL7lCQqKQzwI5huHZrKxWLKXUteV2mcglA8kRhFrctGrTCac5daLNunZ_1rS1ulzkkhT1VS2qtxuh7Kz97JqzIFSO6lytPbe1WZ3lR41YjitTWW3O-qUOvE7eVw7OyJS9Bde3YvMmmRm7vjPw3lCsUh-A4plYGHVdjE2DZG9tJiaWoRPLxae-65k-scxgv1sblnS1s_D5PF8kRWPYOUN5Esc2Wlg-XjJzL6ZqC7w8VYxpjl6lw2V1MfHqZ4l9HWgN2zxWqlK8mGHKODNweOJo1ajnTxpmxPtlUIJqnZHI-64q2oBqjUbJyE6jQ4HXfZAHBUIVP6pQH1Ppda2Oiy9T99ahsDXa83x3bM3Nqw3wfeMuTBW2trZ3Eo8Se4mfG-Dd5nq5VP3X4Fm8W35v47c3sZC43KTbeUGhXaZChx5L94YLL2BYWirrejevdnhabQei5AiBaArifbbAnKfBeTr9lw1e3UI8yfxv6-vtB-u_iBTkKMjvMbAA-QLi-n8B0&estsfed=1&uid=6c966c1f06fc4e1d975381b973bffd3f&signup=1&lw=1&fl=ea si2&fci=4345a7b9-9a63-4910-a426-35363201d503&mkt=en-US• Browse:
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files	
C:\Program Files\Google\Chrome\Application\Dictionaryslen-US-9.0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603

C:\Program Files\Google\Chrome\Application\Dictionary\en-US-9-0.bdic	
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBIESBw4p6:NfOCzvRKhGvwJ
MD5:	A78AD14E77147E7DE3647E61964C0335
SHA1:	CECC3DD41F4CEA0192B24300C71E1911BD4FCE45
SHA-256:	0D6803758FF8F87081FAFD62E90F0950DFB2DD7991E9607FE76A8F92D0E893FA
SHA-512:	DDE24D5AD50D68FC91E9E325D31E66EF8F624B6BB3A07D14FFED1104D3AB5F4EF1D7969A5CDE0DFBB19CB31C506F7DE97AF67C2F244F7E7E8E10648EA832101
Malicious:	false
Reputation:	low
Preview:	BDic.....6....".Z..4g....6.2...{/...3...5...AF 1363.AF nm.AF pt.AF n1.AF p.AF tc.AF SM.AF M.AF S.AF MS.AF MNR.AF GDS.AF MNT.AF MH.AF MR.AF SZMR.AF MJ.AF MT.AF MY.AF MRZ.AF MN.AF MG.AF RM.AF N.AF MV.AF XM.AF DSM.AF SD.AF G.AF R.AF MNX.AF MRS.AF MD.AF MNRB.AF B.AF ZSMR.AF PM.AF SMNGJ.AF SMN.AF ZMR.AF SMGB.AF MZR.AF GM.AF SMR.AF SMDG.AF RMZ.AF ZM.AF MDG.AF MDT.AF SMNXT.AF SDY.AF LSDG.AF LGDS.AF GLDS.AF UY.AF U.AF DSGNX.AF GNDSX.AF DSG.AF Y.AF GS.AF IEMS.AF YP.AF ZGDRS.AF XGNVDS.AF UT.AF GNDS.AF GVDS.AF MYPS.AF XGNDS.AF TPRY.AF MDSG.AF ZGSDR.AF DYSG.AF PMYTNS.AF AGDS.AF DRZGS.AF PY.AF GSPMDY.AF EGVDS.AF SL.AF GNXDS.AF DSBG.AF IM.AF I.AF MDGS.AF SMY.AF DSGN.AF DSLG.AF GM DS.AF MDSBG.AF SGD.AF IY.AF P.AF DSMG.AF BLZGDRS.AF TR.AF AGSD.AF ZGBDRSL.AF PTRY.AF ASDGV.AF ASM.AF ICANGSD.AF ICAM.AF IKY.AF AMS.AF PMYTRS.AF BZGVDRS.AF SDRBZG.AF GVMS.AF PSM.AF DGLS.AF GNVXDS.AF AGDSL.AF DGS.AF XDSGNV.AF BZGDRS.AF AM.AF AS.AF A.AF LDSG.AF AGVDS.AF SDG.AF LDSMG.AF EDSMG.AF EY.AF DRSMZG.AF PRYT.AF LZ

C:\Users\user\AppData\Local\Google\Chrome\User Data\0895e2f3-90c4-4f24-8726-9cfb66b1c685.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.748576654032021
Encrypted:	false
SSDEEP:	384:FTk77p+0Ry1JVKAHmNHrkvZ3crNUH9wGonryNjbxkNJplrC/ma9O5Hr/EO1VzNn:RaadtShkkejvB9cPrOhKfp7Zn
MD5:	EC47B76295C2054F7959805FAA2CEC9E
SHA1:	A2D7D5CDCE22820EAB625E4AC99819D8A3BDBAD8
SHA-256:	BFFCEF75B663DD2DF52A5A125640BFB3255D686AFA9507E4516CCA07FF2C480F
SHA-512:	E5E1937804351B648326873CEDD4FA436F749517F8D39312D10E75823724B8468937797C6DAF151F37B95A750367EADABFA5EA3EC4D1CB9B6B9A25ACA1576351
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\0c2e9591-95f5-482f-bc5f-a48fa3596184.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):	399235
Entropy (8bit):	6.047665381809676
Encrypted:	false
SSDEEP:	6144:vMWT5jsSyAiP5i3a2G0OP1eVxR+v+F7EFpY4XB3iE7ZPXYGzLxinb:vMHSmc3a2GNPUZ+w7wJHyEtAWe
MD5:	09F910EFFCCA46BD22C3B59FBE9DD0CD
SHA1:	9300B1220405FFCC433F924E1C66C931F373176F
SHA-256:	BB5EA6B936F7DAD6E3C9E0D82D8AE049585A0D10CE7EB9E5A7275821F647E8DC
SHA-512:	32A6DF286C4C05CCBCED1F2F44E8FF98569A26769033DEA7277307C88C4A6426E16D956970DD4B90FF6D4DEFAC08BBA2FBC4B01378EB32DD69C42032FD07474
Malicious:	false
Reputation:	low
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user_r":{"background":{},"foreground":{}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.638491860068937e+12,"network":1.638459462e+12,"ticks":168047864.0,"uncertainty":4179482.0},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTihZGR/AW4M5AAAAAIAAAAAABmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAaAIAAAADeZr1ii2QiYPGPz0Jd0ZQIE5jKOKMTtbwwwADHJYDpEMAAAAACulP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAABYJv8rXU2wt9ZoSemiGI7Rv1MeHwgrJRvbYcUfMpiLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Google\Chrome\User Data\5d6dba8e-c562-4adc-b939-d268361dae01.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):	399235

C:\Users\user1\AppData\Local\Google\Chrome\User Data\5d6dba8e-c562-4adc-b939-d268361dae01.tmp	
Entropy (8bit):	6.047664940386291
Encrypted:	false
SSDEEP:	6144:gMWT5jsSyAiP5i3a2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinb:gMHSmc3a2GNPUZ+w7wJHyEtAWe
MD5:	51C283AD5C16D3668A5B6D0326C0A0EC
SHA1:	C1CDD84C3C0646A4E7C64CB4CB8355EE3A0E1064
SHA-256:	5AB0D1DCE119E5CD75398BA23FD85A47A37828654AE9F9950E960AAC0E3ABE14
SHA-512:	AC2B71B8F5AF0627F1CFB54809D86B393A054E9012E83628C48FC94E0DCC5A8D2D58E83C94A52CDA3FE98B5C46687CB948EC8A84DEBBC515A4B685593BC30CDB
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", "legacy": { "profile": { "name": "migrated": true } } }, "network_time": { "network_time_mapping": { "local": "1.638491860068937e+12", "network": "1.638459462e+12", "ticks": "168047864.0", "uncertainty": "4179482.0" }, "os_crypt": { "encrypted_key": "RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYzeObKMTihZGR/AW4M5AAAAAIAAAAAABBMAAAAAQAAIAAAACoSPhbyumSaNjLUAHEna2OU Dn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAGAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwwADHJYDpEMAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGI7Rv1MeHwgrJRvbYcUfMpiLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13245952488896803", "plugins": { "metadata": { "adobe-flash-player": { "disp

C:\Users\user1\AppData\Local\Google\Chrome\User Data\91720e0c-3641-4c73-805c-8e87ccd148af.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):	390768
Entropy (8bit):	6.027133715784902
Encrypted:	false
SSDEEP:	6144:ZMWT5jsSyAiP5i3a2G0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxinb:ZMHSmc3a2GNPUZ+w7wJHyEtAWe
MD5:	E7DDF019D4C642967AB65D7E6DC02A81
SHA1:	349FBC1D0415041EFD79720DD735AB95E03BEB26
SHA-256:	8CCF1627BE00377D74ACDB14AFDE9CF2300E96628DA3D6FB116B5CD7787C9FDB
SHA-512:	A09F5C2CDD32FEDFD281FB5D40C4E065FEF134B20394A2C22424719BFEDB1EEA2C1A6035B71538442BB13CAAA7A5C765A6293586D6355C535D9A57190B1546C7
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", "legacy": { "profile": { "name": "migrated": true } } }, "network_time": { "network_time_mapping": { "local": "1.638491860068937e+12", "network": "1.638459462e+12", "ticks": "168047864.0", "uncertainty": "4179482.0" }, "os_crypt": { "encrypted_key": "RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYzeObKMTihZGR/AW4M5AAAAAIAAAAAABBMAAAAAQAAIAAAACoSPhbyumSaNjLUAHEna2OU Dn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAGAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwwADHJYDpEMAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGI7Rv1MeHwgrJRvbYcUfMpiLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM", "password_manager": { "os_password_blank": true, "os_password_last_changed": "13245952488896803", "plugins": { "metadata": { "adobe-flash-player": { "disp

C:\Users\user1\AppData\Local\Google\Chrome\User Data\Crashpad\settings.dat	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	3.3041625260016576
Encrypted:	false
SSDEEP:	3:FkXEwozZHn:+EwozZHn
MD5:	BEBB369FF4A565B19D5E0BC83CD176AE
SHA1:	A6F07666F8DDDF61E5AACE533129BFB541A8A769
SHA-256:	8018F98553432706436A31FFD1E743018C3B7F1AA8D34B2FA18F494A4CFCEB19
SHA-512:	5D2F9F6E9502517AFF4673C3157D57046D4E38D70B5E228F468FB820363E559087D1A2F2E4006B4589BF3F175A4507F1FA3D7BE5FC34F9FA39EB17757DAEC17F
Malicious:	false
Reputation:	low
Preview:	sdPC.....y3..M.Y.NbD.

C:\Users\user1\AppData\Local\Google\Chrome\User Data\Default\2a8fa2fc-8ed0-47d8-966c-a3dc39ef2bf1.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):	5134
Entropy (8bit):	4.9780223898652
Encrypted:	false
SSDEEP:	96:nQ/XbueRqm9paAKI6xk0JCKL8Ykd1fqBOTQVuw:n2Xbu9m9p9A4K9kdBg
MD5:	E00D9AC1B9E964E4EC1E3E7FF85AB6DA

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3d66fa37-3c13-40de-805c-037b4ba5766d.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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMCHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1f/5vYGMgGQOGKJ03QshS
MD5:	95488A82D5073BDA AFC1480073FF801F
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{\"net\":{\"http_server_properties\":{\"broken_alternative_services\":{\"broken_count\":1,\"host\":\"accounts.google.com\",\"isolation\":[],\"port\":443,\"protocol_str\":\"quic\"},{\"broken_count\":1,\"host\":\"www.google.com\",\"isolation\":[],\"port\":443,\"protocol_str\":\"quic\"}},\"servers\":{\"alternative_service\":{\"advertised_versions\":[],\"expiration\":\"13248544952675493\",\"port\":443,\"protocol_str\":\"quic\"}},\"isolation\":[],\"network_stats\":{\"srtt\":32613,\"server\":\"https://dns.google\",\"supports_spdy\":true},{\"alternative_service\":{\"advertised_versions\":[],\"expiration\":\"13248544952813644\",\"port\":443,\"protocol_str\":\"quic\"}},\"isolation\":[],\"server\":\"https://ogs.google.com\",\"supports_spdy\":true},{\"alternative_service\":{\"advertised_versions\":[],\"expiration\":\"13248544952748754\",\"port\":443,\"protocol_str\":\"quic\"}},\"isolation\":[],\"server\":\"https://apis.google.com\",\"supports_spdy\":true},{\"alternative_service\":{\"advertised_versions\":[],\"expiration\":\"13248544952634896\",\"port\":443,\"protocol_str\":\"quic\"}},\"isolation\":[],\"server\"

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\48e812d0-ed15-4aa8-9844-efec8f1547f3.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):	5416
Entropy (8bit):	5.001415484449115
Encrypted:	false
SSDEEP:	96:nQ/XbqeQu9paAKl4xk0JCKL8Ykd1Skzhj3bOTQVuw:n2XbqA9pO4K9kdIkzBT
MD5:	BBB4C9468A2E7EF7F1F0B451FE093CE2
SHA1:	4C2B49B8BA8F6BFC45638A6494D2709EAAFEBA1F
SHA-256:	E62C683C3239050C31A81FBAFCFAF729CEE9A31B02D431AEA518B557F28A0A5A
SHA-512:	EAAC60916D018BADF7F27D2046A2B7972456A733912B2B4D5F644EF4AB905627C25B43F4809EFCEC5C50FCC6D97CE51E83C48F9B425D42A947E219FF4D2F73

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\73b1ce17-6756-4a70-aca1-7aea72f32ec6.tmp

Preview:	{ "extensions":{ "settings":{ "ahfgeienlihckogmohjhadllkjgocpleb":{ "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":"13282965457885873","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB"},"name":"Web Store","pe
----------	--

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\8dd7dfe2-be4f-4a23-9aec-3131f5aac8a4.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):	19181
Entropy (8bit):	5.570474814462528
Encrypted:	false
SSDEEP:	384:a/ytdLIXsXD1kXqKf/pUZNCgVLH2HfDDrUxHGn2KEaPZ4j;5LIOD1kXqKf/pUZNCgVLH2HfrUIGn2p
MD5:	4BDA4C93A676EF49E6E51CCA74D4EE32
SHA1:	958DAACFF85AF969305188076CDACB96C64E2EF7
SHA-256:	6082D797CEEF9043203C2EB97EDCB28109EF0A7F0EC7508E819CBA79746EF9B
SHA-512:	E00E3CEF1F48F933369A882CC8E7AD69D60460B6278F1AA371C058EB9D300DAE52251D92D3A09C99A078B0537949E2937F082C0715083A918B7E9EB643D07E3C
Malicious:	false
Reputation:	low
Preview:	{ "extensions":{ "settings":{ "ahfgeienlihckogmohjhadllkjgocpleb":{ "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":"13282965457885873","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB"},"name":"Web Store","pe

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):	337
Entropy (8bit):	5.222001316436423
Encrypted:	false
SSDEEP:	6:mNav+q2PN723iKKdK9RXXTZIFUtManHZZmwKae3VkwON723iKKdK9RXX5LJ:iZvVa5Kk7XT2FutM+Z/Kn5Oa5Kk7XVJ
MD5:	81FA792BC0B1126C6FF241347B8B1C09
SHA1:	20F26BE6F0E9D7A6CE8C1930438FF5D88DE87C8E
SHA-256:	CB36C6DCD3B05BF5CA041C0C439F557E01D5D5D08F9961631288F1C06E33D0E8
SHA-512:	12C64407E7B72A8841EE3AA1C2C3E68E2215D21EE328805D9CE7F3AFB6836D5485DF31FD3D02B45A810150CC1679D76AE7D82F9CA82D9A911F4675E7D28AE1C8
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:58.004 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/12/02-16:37:58.006 988 Recovering log #3.2021/12/02-16:37:58.012 988 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.old (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	337
Entropy (8bit):	5.222001316436423
Encrypted:	false
SSDEEP:	6:mNav+q2PN723iKKdK9RXXTZIFUtManHZZmwKae3VkwON723iKKdK9RXX5LJ:iZvVa5Kk7XT2FutM+Z/Kn5Oa5Kk7XVJ
MD5:	81FA792BC0B1126C6FF241347B8B1C09
SHA1:	20F26BE6F0E9D7A6CE8C1930438FF5D88DE87C8E
SHA-256:	CB36C6DCD3B05BF5CA041C0C439F557E01D5D5D08F9961631288F1C06E33D0E8
SHA-512:	12C64407E7B72A8841EE3AA1C2C3E68E2215D21EE328805D9CE7F3AFB6836D5485DF31FD3D02B45A810150CC1679D76AE7D82F9CA82D9A911F4675E7D28AE1C8
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:58.004 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\MANIFEST-000001.2021/12/02-16:37:58.006 988 Recovering log #3.2021/12/02-16:37:58.012 988 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.old (copy)

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):	321
Entropy (8bit):	5.234576093476529
Encrypted:	false
SSDEEP:	6:mNafp/+q2PN723iKKdKyDZIFUtMafIZmwKafEVkwON723iKKdKyJLJ:icsvVa5Kk02FUtMcl/KcE5Oa5KkWJ
MD5:	2B81315750C325E069BABEF42E72DDB3
SHA1:	EDA375AF80A8CB8CF34FB8E7114C31C1D5ACA566
SHA-256:	3402B374A0FE71040F47C80D2457DA4DFF84F3DF7D1CAD562CB8472E0CD82057
SHA-512:	678FACB2651CEE027DCECBEA32C25BD8A601920561817CB23C89204CC30E21DB15A788741671F1E138E80FE318A4C5E9EDA01056F3376512134BB30B2E07ADA
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.980 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/12/02-16:37:57.988 988 Recovering log #3.2021/12/02-16:37:57.989 988 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):	321
Entropy (8bit):	5.234576093476529
Encrypted:	false
SSDEEP:	6:mNafp/+q2PN723iKKdKyDZIFUtMafIZmwKafEVkwON723iKKdKyJLJ:icsvVa5Kk02FUtMcl/KcE5Oa5KkWJ
MD5:	2B81315750C325E069BABEF42E72DDB3
SHA1:	EDA375AF80A8CB8CF34FB8E7114C31C1D5ACA566
SHA-256:	3402B374A0FE71040F47C80D2457DA4DFF84F3DF7D1CAD562CB8472E0CD82057
SHA-512:	678FACB2651CEE027DCECBEA32C25BD8A601920561817CB23C89204CC30E21DB15A788741671F1E138E80FE318A4C5E9EDA01056F3376512134BB30B2E07ADA
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.980 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\MANIFEST-000001.2021/12/02-16:37:57.988 988 Recovering log #3.2021/12/02-16:37:57.989 988 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):	0.41219073361615666
Encrypted:	false
SSDEEP:	48:7Wwwp7V5xJmRy6DP8VkgFqZAT+unQ23CJkixktk:7RwBhD6DP8mqVTV3iB9
MD5:	D205C200594F6D8426B6AF1C4A9E0ADA
SHA1:	632B6E2454429838543D992C276327307627F225
SHA-256:	F1291397214F4155B4D00B7A037D3218CB8FE1AADEEDF1FD4618E1D094D42A3B
SHA-512:	A714C157B4CE2F159AB8604D7FE0C8F7457EB36AAC4F185D4B4989BBFD66E2FE0A3F20E32BDAA79F33DF0DF925C80D777C2A3CDCBA6C862F000411B9DBF86A
Malicious:	false
Reputation:	low
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

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

Category:	dropped
Size (bytes):	270336
Entropy (8bit):	0.6080106368359717
Encrypted:	false
SSDEEP:	192:Oai52as9oUVRfP5rgKp18xDfJRy2F+o0v98t3pX:CsoUVRfxD18xyol98t
MD5:	E2C7C5A0544BBD127E3842875C408298
SHA1:	195B434212F89A98055D8297BB9CE24BA81D9FE9
SHA-256:	A3E3CF3F944210E66BF238F500E5A4337CF4D33673507D580D46DF0953AFE930
SHA-512:	8E8D07A0BFB52162ADC3239DE2230DA631513D066C62CE3B39990AA9C25C6A810CCAF906D87B53B33E12CD1915ACD0A21CE301AE1437C834A2D1D741A57E042
Malicious:	false
Reputation:	low
Preview:	G.....

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):	1.642720884940711
Encrypted:	false
SSDEEP:	1536:fN1NQI/hN1NoTENTE1N1NsmdkUxnvoPc6h2:ylQdjxnvd02
MD5:	600198177D5D5C7EAC46BEFBF5645C19
SHA1:	0AF30452EB65CA684CFCF5EC11A0F030551C64A4
SHA-256:	1D81FE77C9A3B8609DCA88F58328ADAD541946164EF80EDB831E44857E48FAFC
SHA-512:	587166103BE0769CB298356544B2C786CA1EBAB51A26016F99E6D096CAD4CA3ADAF41B69C40263F37EB1E1FCFEDAE08E6ADEE04F5317CBB8A02EA62160C59A5
Malicious:	false
Reputation:	low
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):	0.6691595678414073
Encrypted:	false
SSDEEP:	1536:ps1nYzcmYchU9LeL60U3ew44i7l1rSVajJ8s0O8E9rL:psBYHyLeL60U3eH4i7l1rSXs0O8E9rL
MD5:	86D96513FE36CE8D8834EACC04D08493
SHA1:	DB55DBBB9D0FDE2626096D36C4B4635DA2F43E06
SHA-256:	61169FAEC3D37B427630F9E76A621C5B56704CC49ACFE680B499D2437B9326EA
SHA-512:	10195897D44639D92C3118E3DF0C552EEED006A48789E3173B3EE6E384327F0C9AA7DFCDBBF64FAE6B6895F41AF85FEA69AFA1C73E76A72738B74C8FF47EF2D
Malicious:	true
Yara Hits:	Rule: JoeSecurity_HtmlPhish_10, Description: Yara detected HtmlPhish_10, Source: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache\data_3, Author: Joe Security
Reputation:	low
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):	2.1980057019508275
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
SSDEEP:	96:tNwrsycslscyT2Js2sbwpssdMpes2sVGsQxiwFhhBf3a5p8xXwC4scDsc0sc1sg:tuXTOpOjGxiChhRlpzCxD
MD5:	FB39D39A203A3D9A6D3D93AC33C19610
SHA1:	BCF42EF341136B776BC6B711E4A84BC2BE579CAA
SHA-256:	6DC27C915A67221969CAED08E290E671C8C3DC63E165714A579BAFFF521B2595
SHA-512:	5AE7F083589E080D195740FDC7EFE7B87B6981189E9DD388CD2C5C3FEFF64726547FC60C0282B9CF41455CB802F566E6DA550175E668279E3EEA3F295396896C
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@C.....g...8.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23602
Entropy (8bit):	4.811545544311425
Encrypted:	false
SSDEEP:	384:MIRGmSvuDbDm5GmRvuDbabvuDPmNQUT3ZwUWH9:MvmSvEDmAmRvEgvQmNQupQ9
MD5:	9C49430176F5FB8A38B233DF07851D20
SHA1:	EE28D65C6878376DE5AB502557079E5A19944750
SHA-256:	E66841AF41DC1667E65C8ECDF26D7938C36180D9DB11BC1FDBC44F619A1222DB
SHA-512:	2062DCA0311427C15F1C7BB9A43B126B7F1813A7DB0EEA74C95E36D148B88A8BE91F373E7A45DF8AE7D12BC1CEA81BA4EA5913A6B7E89EC96C399C7FEB03A1B
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.....\$.7420bf79_ecdc_45cb_bc16_c3494e34f0ca.....~^.....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....L...https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com.....h.....`.....Λ3...Λ3...@.....X.....L...https://p.i.c.k.a.p... a.c.e.p.i.c.k.a.p.a.r.t...c.o.m./h.e.r.g.s.l/.k.u.t...g.x.s.?o.p.=J.F.e.r.n.a.n.d.e.z@.w.i.c.k.e.r.s.m.i.t.h...c.o.m.....8.....0.....8.....L...https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickers

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Tabs	
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:	884C0D3594390E2FC0AEB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	335
Entropy (8bit):	3.5297306448944714
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCT5z/t2qoEwhXeLKB:qWWWWWWWWWbopXeLKB
MD5:	4B02663C177BA8EA36FB2E49617CCC05
SHA1:	6E77145135116873842B1BEE6622B116CDA3CBB1
SHA-256:	0FD0B4ED1B18A8A1C73736E3C74168C6102092E5AFD431CD36F7F222E578A1C9
SHA-512:	6FAE4934BB9F7B840ECE19DC10FD522EB88497B97F47B76AC4DBC28146F73D23984322AFBF32DDBC3AC219277A7A6F899FAE59E5834DC2E28377A6306D9D6F3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Preview:	.f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....f.5.....i.Wd.....Sgdaefkejpgkiemlaofp almlakmbjdnl.declarative_rules.declarativeContent.onPageChanged.[].F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.212215520002592
Encrypted:	false
SSDEEP:	6:mNaopndL+q2PN723iKKdK8aPrqIFutMaorL1ZmwKao6N1LVkwON723iKKdK8amLJ:iRJv+vVa5Kkl3FutMRrL1/KR49V5Oa5G
MD5:	95D084A0F4260F09255F1FAC54EC6D1C
SHA1:	7C5849A3BBC69193276A4FC5FBB11EB8584F135
SHA-256:	30091BDB620970296B055E6D1BF21813BF6BD96C43C409FD5F8D199EBF1D2C7A
SHA-512:	5E46699EC3EA4F7874508E028ED4F72A3E20940727ABFF8D114F4DA490A610387762EA78BBEB632C41136BC10AA726B7638FFA2A267075B1943057036D2A6F12F
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.475 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\MANIFEST-000001.2021/12/02-16:37:38.477 87c Recovering log #3.2021/12/02-16:37:38.478 87c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.212215520002592
Encrypted:	false
SSDEEP:	6:mNaopndL+q2PN723iKKdK8aPrqIFutMaorL1ZmwKao6N1LVkwON723iKKdK8amLJ:iRJv+vVa5KkL3FutMRrL1/KR49V5Oa5G
MD5:	95D084A0F4260F09255F1FAC54EC6D1C
SHA1:	7C5849A3BBC69193276A4FC5FBFB11EB8584F135
SHA-256:	30091BDB620970296B055E6D1BF21813BF6BD96C43C409FD5F8D199EBF1D2C7A
SHA-512:	5E46699EC3EA4F7874508E028ED4F72A3E20940727ABFF8D114F4DA490A610387762EA78BEB632C41136BC10AA726B7638FFA2A267075B1943057036D2A6F12F
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.475 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\MANIFEST-000001.2021/12/02-16:37:38.477 87c Recovering log #3.2021/12/02-16:37:38.478 87c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log .

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.177605187107165

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Encrypted:	false
SSDEEP:	6:mNaU1jL+q2PN723iKKdK8NIFUtMa+1ZmwKabLVkwON723iKKdK8+eLJ:iB+vVa5KkpFUtMV1/K0V5Oa5KkqJ
MD5:	E5AC81DB113ABBAE3C94D3777F10CFBF
SHA1:	681E93F386640E9717243F0A047004A666119101
SHA-256:	15F2672D6015362CA483139F867261A4B96645A33E7C9DAF4F11F03ECBFAD0BA
SHA-512:	00BD99A028C156C6CB9217862BAF37C7A9D3A296FE901EC68FAA9FCF2AFB8C8FEB9E072C4D04FCB226798F596C40D0B02D0D253DA53CBFBEA89340EF34C3F73
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:41.314 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\MANIFEST-000001.2021/12/02-16:37:41.316 87c Recovering log #3.2021/12/02-16:37:41.320 87c 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\Extension State\LOG.old. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.177605187107165
Encrypted:	false
SSDEEP:	6:mNaU1jL+q2PN723iKKdK8NIFUtMa+1ZmwKabLVkwON723iKKdK8+eLJ:iB+vVa5KkpFUtMV1/K0V5Oa5KkqJ
MD5:	E5AC81DB113ABBAE3C94D3777F10CFBF
SHA1:	681E93F386640E9717243F0A047004A666119101
SHA-256:	15F2672D6015362CA483139F867261A4B96645A33E7C9DAF4F11F03ECBFAD0BA
SHA-512:	00BD99A028C156C6CB9217862BAF37C7A9D3A296FE901EC68FAA9FCF2AFB8C8FEB9E072C4D04FCB226798F596C40D0B02D0D253DA53CBFBEA89340EF34C3F73
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:41.314 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\MANIFEST-000001.2021/12/02-16:37:41.316 87c Recovering log #3.2021/12/02-16:37:41.320 87c 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\nmmhkkegcagdldgiimedpiccmgmieda\1.0.0.6_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:	D9CBFCDD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{ "file_hashes": { "block_hashes": ["A+1PYW3V6CJbBuQ7aqrqYhyH3bT8PKyBXp3hN2slpI0=", "WSOpQRKYTHjPSIG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=", "jDctR8lmG5KZrQKm4kDjUB7FokSJfjo/pmvFowRVlaY=", "LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=", "nZ9zLb2By96AkKXALRM+C0Eu11XUjPIMXEKjjiCPdtHE=", "wifibc1QfMBN2jrtUtlgsCefvuceTpAatmLvul11RJA=", "dHjWSilIdjj7MWqg3T8MG58RuugRXk32vqi/13JqEgA=", "zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=", "DpjXcO85FFY9KJFPkGNfUtdQIOsGwO5jUckiUwY14=", "gqid6l1+mk/6yWgUECRofl9lMipXgXh2jEN2+CxmPE0=", "prDB91X2Mmfg/MtxVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zfKEt3Cn2j0q2v9QOsthVFwn8EzCM=", "EPQ3jzdrLkAHyvf3920B5Y3aAkO1lJdn/UtbnaAmq6T0=", "+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWEvYCs40NI=", "3mBGNAiRITANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=", "1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=", "E3vWLQxzmj+e5QxYbUscIJ5n0lTpw5JBHV1Kph3/KM=", "i3l8ghdTf9c1ZXNB2mvsID+DV4gxBVN27rj9wsMtrpg=", "R8B8qYabnMSILPhrtu0hGyrHn3llsMHqBbi70gkljEE=", "rhizuEvv2KRAFmms896xFwkNgPrw6WvmgPn6xrBSa2Y=", "LAMXv6sRb0VZrY34aVXF3Ffts

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkdecjkdefgpdelpbcbmbmeomcjbbeemfm\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:	384:7dNc1NC6lcafusK4H1IIGRIhKikIALQWdynQh2RX4K6M1tVztzr7XSNyZ:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\computed_hashes.json	
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{ "file_hashes": [{ "block_hashes": ["DOZdV3jFvk12AM2JNDYKo3KZrIVRpmJ+sVGWkqQe4Q=", "rVEIW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFIhZ1U=", "X/3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=", "VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=", "EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq4whtE="], "block_size": 4096, "path": ".locales/iw/messages.json" }, { "block_hashes": ["xklkoZ7iSU1+7cd6DAteMUC5iPFd+EgcbnzxkOiFwk=", "3KbsvoxKY/3AwqgF2aAdVQRpMhsNVRkQ3rx2A6Z2Z+Y=", "o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=", "xV/K8xucyWJELVT8Cqn+ugFjobBV/mg8pnmACF+2PP4Y=", "p/mvJm2wuCl32Rx3it654MjKAsMe3S9IDeabc1A8mE=", "j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=", "nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc=", "eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=", "Wj7faqnspelXKMvnduxHn1XUBG8TEOqyns7/oUihekM=", "VtBwXoadl3EP336rAiL33Gz19KGqtN+RYdKnMKAxolw=", "iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=", "g+RfdfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVVMuHAtEj8=", "2oC4HcCuXu3VjF6wnKlzt9uqQNaebcuWpm/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
Size (bytes):	45056
Entropy (8bit):	3.925956806862218
Encrypted:	false
SSDEEP:	384:maPjGYHamHmcmmwmqGmbGmQGm4Gm6l9xrl6Gi:mkGY6mHmcmmwmdmqmDm7m62
MD5:	F3F7C4B1AE7C42EC0C9D35EE722CE32E
SHA1:	811CE528A53BF04AA2F78CF491AC56637972B277
SHA-256:	DBC260FE1E70F89F2B0AE4ECBBCAD19E24999FA6E0C7A61AD0D295BF92BB3802
SHA-512:	6925BAAF2069170C4E7F56DF63BE29CDB86F12F3946D0C050A8C75CD04E13ABB4A8549BEAC0973DEA4EE0639459C91F3DE61D7872E070F10BEFB2FB863CF7
Malicious:	false
Reputation:	low
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:	B643A8FA75EDA90C89AB98F79D4D022BB81F1F62F50ED4E5440F487F22D1163671EC3AE73C4742C11830214173FF2935C785018318F4A4CAD413AE4EEEF985DF
Malicious:	false
Reputation:	low
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):	375
Entropy (8bit):	5.258272622761373
Encrypted:	false
SSDEEP:	6:mNaf5Y+q2PN723iKKdK25+Xqx8chl+HfUitMafCXZmwKaf9v4VkwON723iKKdK25N:icPvVa5KkTXfchl3FUtMci/Kc1w5Oa5G
MD5:	186AABC016199BB0793292BD5653A981
SHA1:	A280918787F023A0D158067B1F31E118BDE6DD1B
SHA-256:	66583A0D97C57AF15BCDD451BC1600BBE37E75D562A658984BC6BB759CC40001
SHA-512:	F60A1A80941F56C936AF00BB14D40EEF59FE099221C97F2206CA60A07EA8772203FB3FF77C5BE9123EE589CFAB81A76733852F6A9EFB598B4A8EB1A662292A22
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG

Preview:	2021/12/02-16:37:57.828 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/12/02-16:37:57.859 988 Recovering log #3.2021/12/02-16:37:57.860 988 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):	375
Entropy (8bit):	5.258272622761373
Encrypted:	false
SSDEEP:	6:mNaf5Y+q2PN723iKKdK25+Xqx8chl+IFUtMafCXZmwKaf9v4VkwON723iKKdK25N:icPvVa5KkTXfchl3FUtMci/Kc1w5Oa5G
MD5:	186AABC016199BB0793292BD5653A981
SHA1:	A280918787F023A0D158067B1F31E118BDE6DD1B
SHA-256:	66583A0D97C57AF15BCDD451BC1600BBE37E75D562A658984BC6BB759CC40001
SHA-512:	F60A1A80941F56C936AF00BB14D40EEF59FE099221C97F2206CA60A07EA8772203FB3FF77C5BE9123EE589CFAB81A76733852F6A9EFB598B4A8EB1A662292A22
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.828 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\MANIFEST-000001.2021/12/02-16:37:57.859 988 Recovering log #3.2021/12/02-16:37:57.860 988 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):	361
Entropy (8bit):	5.210317553573027
Encrypted:	false
SSDEEP:	6:mNafL+q2PN723iKKdK25+XuolFutMafvXZmwKafO3VkwON723iKKdK25+XuxWLJ:icyvVa5KkTXFYUtMcv/KcS5Oa5KkTXHJ
MD5:	11A568440D5A58B82DC501AF1A49AE7B
SHA1:	B6FCD90F64CEFFF9D388F2285E7385B87AFDE3CC
SHA-256:	C48FB43B790473CE03482C7B28089531E741B87711B13F74284BE3C0A2F30409
SHA-512:	B6EAAE8C1F7848E48ADAFED1C9F23709B4F50318EE6B30FF2E7ED9C72A3F139A4252451341BD23CEB662D70A9DD580C4E5AAAD2DDD1A6DDF3244BAAB22F9A73A
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.739 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/12/02-16:37:57.810 988 Recovering log #3.2021/12/02-16:37:57.811 988 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):	361
Entropy (8bit):	5.210317553573027
Encrypted:	false
SSDEEP:	6:mNafL+q2PN723iKKdK25+XuolFutMafvXZmwKafO3VkwON723iKKdK25+XuxWLJ:icyvVa5KkTXFYUtMcv/KcS5Oa5KkTXHJ
MD5:	11A568440D5A58B82DC501AF1A49AE7B
SHA1:	B6FCD90F64CEFFF9D388F2285E7385B87AFDE3CC
SHA-256:	C48FB43B790473CE03482C7B28089531E741B87711B13F74284BE3C0A2F30409
SHA-512:	B6EAAE8C1F7848E48ADAFED1C9F23709B4F50318EE6B30FF2E7ED9C72A3F139A4252451341BD23CEB662D70A9DD580C4E5AAAD2DDD1A6DDF3244BAAB22F9A73A
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.739 988 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\MANIFEST-000001.2021/12/02-16:37:57.810 988 Recovering log #3.2021/12/02-16:37:57.811 988 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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Size (bytes):	333
Entropy (8bit):	5.187888436308406
Encrypted:	false
SSDEEP:	6:mNafrN+q2PN723iKKdKWT5g1ldqIFutMafbAWZmwKafVVkwON723iKKdKWT5g1lu:icrN+vVa5Kkg5gSRFUtMc8W/KcVV5Oaz
MD5:	A5D3718068E543F910DE8A3BDDBD280D
SHA1:	B3D41E1BEB8B2DED518735DAEF17961A993503CC
SHA-256:	40E3288C67F9D834D6DFF304CDF40A1365F228F4131057AC9D5C245F3B1F4931
SHA-512:	87E1429A6CAF4EE0C4A35CF533E37ACB665EE64C65D790E251DB86FE02E9BB87C3EF98A9498A475F5523B34683A22E3AE9A5D296207B4D6978C62EDFF6C1E44F
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.553 15c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/12/02-16:37:57.555 15c Recovering log #3.2021/12/02-16:37:57.557 15c 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	333
Entropy (8bit):	5.187888436308406
Encrypted:	false
SSDEEP:	6:mNafrN+q2PN723iKKdKWT5g1ldqIFutMafbAWZmwKafVVkwON723iKKdKWT5g1lu:icrN+vVa5Kkg5gSRFUtMc8W/KcVV5Oaz
MD5:	A5D3718068E543F910DE8A3BDDBD280D
SHA1:	B3D41E1BEB8B2DED518735DAEF17961A993503CC
SHA-256:	40E3288C67F9D834D6DFF304CDF40A1365F228F4131057AC9D5C245F3B1F4931
SHA-512:	87E1429A6CAF4EE0C4A35CF533E37ACB665EE64C65D790E251DB86FE02E9BB87C3EF98A9498A475F5523B34683A22E3AE9A5D296207B4D6978C62EDFF6C1E44F
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:57.553 15c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\MANIFEST-000001.2021/12/02-16:37:57.555 15c Recovering log #3.2021/12/02-16:37:57.557 15c 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):	147456
Entropy (8bit):	1.4019446044892985
Encrypted:	false
SSDEEP:	384:WfB4U3iVyBBE3uuMKom0mlm19Gm1Rmd3/QGmIXm87mL:WfmoiWBBjRbm0mlm10mzmhmtmemL
MD5:	094ABCD806C1FDE9557E4977EC421615
SHA1:	0B1986D74D92DF051C28FDB8CCDD99A8F5D4470E
SHA-256:	55B4C2034BC494D0A85D9510536651FCAEB4BFAEE8512588D8309B8DCD17166D
SHA-512:	BC480CBC67E9B5FF609A92486E46BA49304B3280855493FFD522DEBD5B1EE015374C8C95A08E8424526651A8FACF54FF9F2C55AB88689DF21713DB026101AEB1
Malicious:	false
Reputation:	low
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):	2909
Entropy (8bit):	5.963281306577294
Encrypted:	false
SSDEEP:	48:KYFjzR23XiE3p5Svo/P6clFJVl4BSfUqsH2dsjqBLlQaSF0uesL:H3RyyASvsrvC5WdcqDQa0e8
MD5:	1891B569A04826DA8350F6D5E753C6EF
SHA1:	A4EEB0D9B04D72FEA41B92A3347B9D30816E2DA6
SHA-256:	7ED4A8A3723BD4E2FCF7A07632CE52C1AA10FB85EE77AC815969515EE20B9C33
SHA-512:	60D8FB80508F8EF3E5EE4BC446DC81BC73CA198DF56117AE8C08D9E79406574A408316D82AB34C23897E20E18B974F42B1662D93EDC608DADB411501D544588

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Malicious:	false
Reputation:	low
Preview:	"....4..account..acepickapart..com..hergsl..https..in..php..pickup..rcopy..sign..to..your..0..0000..000000000..0000009918..0slr..45f4d5f9..4657..4816.%87skzlc m5hbmrlkb3awnrzjzbwl0ac5jb20..9528..9cef6f38045264f7cbaec8b47ad485f3..af3f59994174..client..code..form..id..iw00..mode..msafed..office..openid..outlook..owa.. post..protectedtoken..redirect..request..resource..response..scope..token..true..type..uri..y..gxs..jfernandez..kut..op..wickersmith*...4....0.....0000.....000000000... ...0000009918.....0slr.....45f4d5f9.....4657.....4816...).%87skzlc m5hbmrlkb3awnrzjzbwl0ac5jb20.....9528...\$. 9cef6f38045264f7cbaec8b47ad485f3.....account.....ace pickapart.....af3f59994174.....client.....code.....com.....form.....gxs./....hergsl.....https.....id.....in.....iw00.....jfernandez.0....kut.1....mode.....msafed.....office.....op.2....o penid.outlook!....owa."....php.....pickup.....post.#.....protectedtoken.\$.....rcopy.....redirect.%....request.&....resource

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):	0.3284214229143717
Encrypted:	false
SSDEEP:	6:KIW/fMt76Y4QZVTJXs99pG/2qR4EZY4QZv8fOgn:KgnMWQfy9LWBQZ8fOg
MD5:	EEF47A74FC5DD041DFBEC2DC62664EC7
SHA1:	20B5C2760C4D6110FE53ED09B90ED9AAC2809F28
SHA-256:	BF69239396BF46B7AE9311D908617734B972F07A63FD42D2A04C2D9137829546
SHA-512:	536ABDB076867D5B209D5455DAF8A37039AB5345BA8B837B5A3F9370C6D35FE5C5EB88A13CFB2C3DF911C452CD7151B69E5A0160899D4B01BAEE2B9559B23B74
Malicious:	false
Reputation:	low
Preview:	'....\$.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Session (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	23602
Entropy (8bit):	4.811545544311425
Encrypted:	false
SSDEEP:	384:MIRGmSvuDbDm5GmRvuDbabvuDPmNQUT3ZwUWH9:MvmSvEdmAmRvEgvQmNQupQ9
MD5:	9C49430176F5FB8A38B233DF07851D20
SHA1:	EE28D65C6878376DE5AB502557079E5A19944750
SHA-256:	E66841AF41DC1667E65C8ECDF26D7938C36180D9DB11BC1FDBC44F619A1222DB
SHA-512:	2062DCA0311427C15F1C7BB9A43B126B7F1813A7DB0EEA74C95E36D148B88A8BE91F373E7A45DF8AE7D12BC1CEA81BA4EA5913A6B7E89EC96C399C7FEB03A1B
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.....\$.7420bf79_ecdc_45cb_bc16_c3494e34f0ca.....~^.....5..0.....&...{68ADBCFB-ED3C-4AA1-B80C-ADD502B6FA85}.....L...https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFerna ndez@wickersmith.com.....h.....`.....\3...^3...@.....X.....L...h.t.t.p.s.:././p.i.c.k.a.p... a.c.e.p.i.c.k.a.p.a.r.t...c.o.m./h.e.r.g.s.l/.k.u.t..g.x.s.?o.p.=J.F.e.r.n.a.n.d.e.z.@.w.i.c.k.e.r.s.m.i.t.h...c.o.m.....8.....0.....8.....L...https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickers

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last Tabsnd (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:	884C0D3594390E2FC0AEB05460F0783815170C4B57DB749B8AD9CD10741A5604B7A0F979465C4171AD9C14ED56359A4508B4DE58E794550599AAA261120976C
Malicious:	false
Reputation:	low
Preview:	SNSS....

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):	335
Entropy (8bit):	5.1744006067359765
Encrypted:	false
SSDEEP:	6:mNato5dL+q2PN723iKkK8a2jMGIFUtMatoiZ1ZmwKatom1FILVkwON723iKkKdKw:ip5V+vVa5Kk8EFUtMpiZ1/Kp0NV5Oa5i
MD5:	1DE30E5EB5ED0727EC62525DA4364EB2
SHA1:	54B6121D6A349C01E1F2826E15B48AA4D8AF4B22
SHA-256:	7929BB1E7397F27D7C51698EBD0FB796E7A13639579AF76B07F32F26F9990AB4
SHA-512:	63E4E9BD67AA878176C514201CCD42DD5FB65307B6674182A1123DD9252BBF0A220EB019193AEA5C27710BC122553B6C584A5BCA7255B0310E5B2A10C44E1DC
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.906 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/12/02-16:37:37.909 87c Recovering log #3.2021/12/02-16:37:37.912 87c 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):	335
Entropy (8bit):	5.1744006067359765
Encrypted:	false
SSDEEP:	6:mNato5dL+q2PN723iKkK8a2jMGIFUtMatoiZ1ZmwKatom1FILVkwON723iKkKdKw:ip5V+vVa5Kk8EFUtMpiZ1/Kp0NV5Oa5i
MD5:	1DE30E5EB5ED0727EC62525DA4364EB2
SHA1:	54B6121D6A349C01E1F2826E15B48AA4D8AF4B22
SHA-256:	7929BB1E7397F27D7C51698EBD0FB796E7A13639579AF76B07F32F26F9990AB4
SHA-512:	63E4E9BD67AA878176C514201CCD42DD5FB65307B6674182A1123DD9252BBF0A220EB019193AEA5C27710BC122553B6C584A5BCA7255B0310E5B2A10C44E1DC
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.906 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\MANIFEST-000001.2021/12/02-16:37:37.909 87c Recovering log #3.2021/12/02-16:37:37.912 87c 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 Action Predictor	
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):	36864
Entropy (8bit):	0.6094297141107083
Encrypted:	false
SSDEEP:	96:/OqAuhjspnWOvcaWsBsgspsjmVXhsBsqs1+5DsM:3a9ah
MD5:	F69BFFD4FE3967F3CF6D76E980C32C0E
SHA1:	47A3FEC31EED417C3CD70A6DC96E41D07088C847
SHA-256:	6AB89CD9F7D22BDFDE9DE269606AB5E0D06D6085FB89D56B6EE28A84F458B293
SHA-512:	B912B86A43B4478350341B34997D5865D828A6F0FEA28DF05697B474A60A796394AB5A4F43ED55022E5AAEAECACBE5FE60B3506D7BCBEE2101869F17E3F6A17
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@C.....\t.+>.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\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):	2825
Entropy (8bit):	4.86435102445835
Encrypted:	false
SSDEEP:	48:YALtdpBeMsNMHK5sJDysACs37sHWsd5/sSYMHCKs/MHCzsSOMHwsSJtFsX3RLs9D:HQxGKWDS1i/5vYGmGqOGKJ03QshS
MD5:	95488A82D5073BDAAFC1480073FF801F

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent State (copy)	
SHA1:	E2E979B6D4A3EE16A815115C414D0A98E1DFA93F
SHA-256:	C091AE68AFCD5EC632B2C324B983D70F722463CB4D05A3CE8D52E07AA7E5A5D6
SHA-512:	D536466352320C5D394130A59B605617580050CDF325C4B3392D87D384C246E9D8C54FC16A247FF4B379F162536304E0D312D7781FFE245C643C5081B8BE08CD
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "broken_alternative_services": { "broken_count": 1, "host": "accounts.google.com", "isolation": [], "port": 443, "protocol_str": "quic" }, "broken_count": 1, "host": "www.google.com", "isolation": [], "port": 443, "protocol_str": "quic" }, "servers": { "alternative_service": { "advertised_versions": [], "expiration": "13248544952675493", "port": 443, "protocol_str": "quic" }, "isolation": [], "network_stats": { "srtt": 32613 }, "server": "https://dns.google", "supports_spdy": true }, "advertised_versions": [], "expiration": "13248544952813644", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "https://ogs.google.com", "supports_spdy": true }, "advertised_versions": [], "expiration": "13248544952748754", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "https://apis.google.com", "supports_spdy": true }, "alternative_service": { "advertised_versions": [], "expiration": "13248544952634896", "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
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.209626884629129
Encrypted:	false
SSDEEP:	6:mNaoQgSQL+q2PN723iKKdKgXz4rRIFUtMaoQMGKWZmwKaoQVpQLVkwON723iKKdA:iR93+vVa5KkgXiuFuTMR2KW/KRRV5OaR
MD5:	AF0DE78EBE629367D95F449570A4B911
SHA1:	0CB56C31F1D0D003388546344A8F92C0C0E7B485
SHA-256:	D1EE311A429C2E13E8D6270F4FDC8A6E48898EE223A3DD96708B112B1874B15F
SHA-512:	6447A3C313A7AA84A3A848BA3073E6993568DAAD0D690104F294F099FB377FF1B703A82FA71AA9261F1F77FAC969DD465BF172748046EE0DA958E4CD36E706FE
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.590 13ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\MANIFEST-000001.2021/12/02-16:37:38.593 13ec Recovering log #3.2021/12/02-16:37:38.594 13ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	340
Entropy (8bit):	5.209626884629129
Encrypted:	false
SSDEEP:	6:mNaoQgSQL+q2PN723iKKdKgXz4rRIFUtMaoQMGKWZmwKaoQVpQLVkwON723iKKdA:iR93+vVa5KkgXiuFuTMR2KW/KRRV5OaR
MD5:	AF0DE78EBE629367D95F449570A4B911
SHA1:	0CB56C31F1D0D003388546344A8F92C0C0E7B485
SHA-256:	D1EE311A429C2E13E8D6270F4FDC8A6E48898EE223A3DD96708B112B1874B15F
SHA-512:	6447A3C313A7AA84A3A848BA3073E6993568DAAD0D690104F294F099FB377FF1B703A82FA71AA9261F1F77FAC969DD465BF172748046EE0DA958E4CD36E706FE
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.590 13ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\MANIFEST-000001.2021/12/02-16:37:38.593 13ec Recovering log #3.2021/12/02-16:37:38.594 13ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (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):	5681
Entropy (8bit):	5.019474186276136
Encrypted:	false
SSDEEP:	96:nQ/XbqeMu9paAKI4xk0JCKL8AgsFkWuShlkd1SkzhjobOTQVuwn:n2Xbqm9p9O4KrkWZykdlkzBa
MD5:	83E2D065FDB1B982AE6EBDE1F372995F
SHA1:	BDB936F556E5A2C4FA2A66F8C38F641A062DC6C8
SHA-256:	74D6B5E7FA8A007904FBF9DBD0364EEEF3AC40DF9FE6C16A66A3235F87CDBAEE
SHA-512:	3BA230EF686338405842EE72001A577EC097A311815BA23C572AE8D6E1855704F3753345D8DEBA964F1E9DD81D4ACC746BA7CA239ADF38F7A702BA35C751D43
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Preview:	*...#.....version.1..namespace-..&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....&f.....x.....next-map-id.1.Ynamespace-67d58c94_d576_497d_aca7_95d903a0dda0-https://passwordrese t.microsoftonline.com/0...~.....map-0-BannerLogoUrl6i.m.a.g.e.s./h.e.a.d.e.r_.M.i.c.r.o.s.o.f.t..p.n.g...map-0-TenantBrandName.C.o.m.p.a.n.y..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.182491451790285
Encrypted:	false
SSDEEP:	6:mNaoWO1jL+q2PN723iKKdKrQMxIFUtMaoWQ1ZmwKaoWhdLVkwON723iKKdKrQMFd:iRWOV+vVa5KkCFUtMRWQ1/KRWfV5Oa5N
MD5:	A475C1BBD920F9C74AABAB14173E3CFE
SHA1:	72898B8218FF405B35C5DF5231ECBBD14B2002CA
SHA-256:	36D2660D8614388FCA1D3C9FA82C259EBAFA54531BD42F2C453EDD8D31241492
SHA-512:	5BD96F9C4D6668841EDEA99199A521428D5DEC6523482B254C0CE15192D06C14678376CC19A9F7E9B4F4662FA7ED52487D40523E5AACF57861AFA6D558D02D5
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.392 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000001.2021/12/02-16:37:38.394 87c Recovering log #3.2021/12/02-16:37:38.395 87c 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\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.182491451790285
Encrypted:	false
SSDEEP:	6:mNaoWO1jL+q2PN723iKKdKrQMxIFUtMaoWQ1ZmwKaoWhdLVkwON723iKKdKrQMFd:iRWOV+vVa5KkCFUtMRWQ1/KRWfV5Oa5N
MD5:	A475C1BBD920F9C74AABAB14173E3CFE
SHA1:	72898B8218FF405B35C5DF5231ECBBD14B2002CA
SHA-256:	36D2660D8614388FCA1D3C9FA82C259EBAFA54531BD42F2C453EDD8D31241492
SHA-512:	5BD96F9C4D6668841EDEA99199A521428D5DEC6523482B254C0CE15192D06C14678376CC19A9F7E9B4F4662FA7ED52487D40523E5AACF57861AFA6D558D02D5
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.392 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\MANIFEST-000001.2021/12/02-16:37:38.394 87c Recovering log #3.2021/12/02-16:37:38.395 87c 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):	354
Entropy (8bit):	5.177950309991291
Encrypted:	false
SSDEEP:	6:mNato/rHN+q2PN723iKKdK7Uh2ghZIFUtMatou9ZmwKatoIUWHNV/kwON723iKKF:ip8vVa5KklhHh2FUtMpu9Z/KppOz5Oal
MD5:	B81F95E8A12CBA0E4FC72A54284AC43E
SHA1:	A0910BEF3632A97BDB888BFE97763EDCE2472A82
SHA-256:	63E197926D8038596B4AD80A663BBD748F02771DC6735018C0950C0FD7CF8EF8
SHA-512:	EE898EA34CC208275E31DD8A63CFED65E308EA27AC8ECAD42999B773C3DF7E2FBF38A9E9B78428CA620236C60DA7B5B1770065444F8B2DCD9A658692667885E
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.900 15f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/12/02-16:37:37.905 15f8 Recovering log #3.2021/12/02-16:37:37.907 15f8 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.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	354

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Entropy (8bit):	5.177950309991291
Encrypted:	false
SSDEEP:	6:mNato/rHN+q2PN723iKkDk7Uh2ghZIFutMatou9ZZmwKatoIUWHNVkwON723iKKF:ip8vVa5KklhHh2FutMpu9Z/KppOz5Oal
MD5:	B81F95E8A12CBA0E4FC72A54284AC43E
SHA1:	A0910BEF3632A97BDB888BFE97763EDCE2472A82
SHA-256:	63E197926D8038596B4AD80A663BBD748F02771DC6735018C0950C0FD7CF8EF8
SHA-512:	EE898EA34CC208275E31DD8A63CFED65E308EA27AC8ECAD42999B773C3DF7E2FBF38A9E9B78428CA620236C60DA7B5B1770065444F8B2DCD9A6586926678851E
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.900 15f8 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\MANIFEST-000001.2021/12/02-16:37:37.905 15f8 Recovering log #3.2021/12/02-16:37:37.907 15f8 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\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:MsEIIllkEthXllkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898158
Malicious:	false
Reputation:	low
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):	433
Entropy (8bit):	5.276452081617288
Encrypted:	false
SSDEEP:	12:iRW+vVa5KkFFUtMRSPj1/KRSP9V5Oa5KkOJ:ipVa5KkfgMUgUVOa5Kkk
MD5:	2363BE00BF0E8498756369E8EFDE915B
SHA1:	7BD0FEB9C9F7CE099143B54A5C2A739AB7459D797
SHA-256:	FF860E24F053AEB3B7D5CE70B20F29A89D6660DCF99777F7F13B6619EB0D07DE
SHA-512:	8D6638330476F9E8043DDDCOE0A3FB4E7AD562136C4C650AAB5E182D5C05F356B8DFC5DAAB4FF557EF98F717E2EC918144A19AE9B5BB1E47D4A7C85218C125DEB
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.456 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\MANIFEST-000001.2021/12/02-16:37:38.458 87c Recovering log #3.2021/12/02-16:37:38.458 87c 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):	433
Entropy (8bit):	5.276452081617288
Encrypted:	false
SSDEEP:	12:iRW+vVa5KkFFUtMRSPj1/KRSP9V5Oa5KkOJ:ipVa5KkfgMUgUVOa5Kkk
MD5:	2363BE00BF0E8498756369E8EFDE915B
SHA1:	7BD0FEB9C9F7CE099143B54A5C2A739AB7459D797
SHA-256:	FF860E24F053AEB3B7D5CE70B20F29A89D6660DCF99777F7F13B6619EB0D07DE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\LOG.old (copy)	
SHA-512:	8D6638330476F9E8043DDDCCE0A3FB4E7AD562136C4C650AAB5E182D5C05F356B8DFC5DAAB4FF557EF98F717E2EC918144A19AE9B5BB1E47D4A7C85218C125CEB
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.456 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Local Storage\leveldb\MANIFEST-000001.2021/12/02-16:37:38.458 87c Recovering log #3.2021/12/02-16:37:38.458 87c 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):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [50], "expiration": "13248544897343531", "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\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):	4.957678621686452
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdSZsBdLJlyH7E4f3K3X
MD5:	93D2E0EFF548FC5E2DA9EC4E630D565B
SHA1:	3D0F4AF0C9516FB2FFE8690E7E932062BF2F147B
SHA-256:	D0044287A77347B99FB2FE2D4DE94B11EDE6659696A45D5874CA31312D2239FF
SHA-512:	3D9F2000B6F8B9DD108BFE62790E2A9E4D2742AFA0819464F7FB0C4E77B9A3DA860F326B985A6E37087141F5AA8DE959DC4218DD05EA3F6F90F1899B632CF13C
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [50], "expiration": "13248544897343531", "port": 443, "protocol_str": "quic" }], "isolation": [], "server": "https://dns.google", "supports_spdy": true }], "version": 5, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "3G" } } } }

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):	435
Entropy (8bit):	5.28078510478941
Encrypted:	false
SSDEEP:	12:iRlxvVa5KkmiuFuIMRoX/KRWz5Oa5Kkm2J:i69Va5KkSgMKyWoa5Kkr
MD5:	E2DD668C92AC32156555A152F28CF65A
SHA1:	18C1BAD45A87F3EF5FD930D640156A338FD52D02
SHA-256:	6C17382A744EBE66C821B4CA3FC9A37F979907FA3EF55D3242C463F7292654B5
SHA-512:	4AE8EC3A8A390CAD2DCC58B39755DDC929F9F81A2B5C2CB7DD7D3DEB46A9A8BD06722A3B1D065424D6F2EA73F5D48279EF35645FA51FE9EF863E59FB06D7F29
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.587 db0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\MANIFEST-000001.2021/12/02-16:37:38.591 db0 Recovering log #3.2021/12/02-16:37:38.593 db0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\def\Platform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\LOG.older (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	435
Entropy (8bit):	5.28078510478941
Encrypted:	false
SSDEEP:	12:iRlxvVa5KkmiuFutMRoX/KRWz5Oa5Kkm2J:i69Va5KkSgMKyWOa5Kkr
MD5:	E2DD668C92AC32156555A152F28CF65A
SHA1:	18C1BAD45A87F3EF5FD930D640156A338FD52D02
SHA-256:	6C17382A744EBE66C821B4CA3FC9A37F979907FA3EF55D3242C463F7292654B5
SHA-512:	4AE8EC3A8A390CAD2DCC58B39755DDC929F9F81A2B5C2CB7DD7D3DEB46A9A8BD06722A3B1D065424D6F2EA73F5D48279EF35645FA51FE9EF863E59FB06D7F29
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:38.587 db0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\MANIFEST-000001.2021/12/02-16:37:38.591 db0 Recovering log #3.2021/12/02-16:37:38.593 db0 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession 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+QUI1ASEGhTFijl:S85aEFjl
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.25632121755869
Encrypted:	false
SSDEEP:	6:mNadoHk+q2PN723iKKdKusNpZQMxiFUtMadoDoFZZmwKadoNkVkwON723iKKdKuG:ilk+vVa5KkMFUtMhE/K8V5Oa5KkTJ
MD5:	2DD10D20462EF927528F6EEC32546978
SHA1:	C0BC1E685F947DB322F18473B9D0445210CD39C8
SHA-256:	E01F05913B5E26EF7FD0B5DC699DE1D0232BBA788CF86AE555F6016B22AA59B0
SHA-512:	CE526226551CF59FCF171F68BC3499931354B09ABBAE0A543CB821271255005DF5CEB330FCF1146A734EE7EEFAA2524CAA01885962E2FC4DB2B37507135737A2
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:55.922 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcpahaombhbimeihdjnejgic\deflSession Storage\MANIFEST-000001.2021/12/02-16:37:55.926 6bc Recovering log #3.2021/12/02-16:37:55.928 6bc 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):	421
Entropy (8bit):	5.25632121755869
Encrypted:	false
SSDEEP:	6:mNadoHk+q2PN723iKKdKusNpZQMxiFUtMadoDoFZZmwKadoNkVkwON723iKKdKuG:ilk+vVa5KkMFUtMhE/K8V5Oa5KkTJ
MD5:	2DD10D20462EF927528F6EEC32546978
SHA1:	C0BC1E685F947DB322F18473B9D0445210CD39C8

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcbpahaomhbhimeihdjnejgic\deflSession Storage\LOG.old (copy)	
SHA-256:	E01F05913B5E26EF7FD0B5DC699DE1D0232BBA788CF86AE555F6016B22AA59B0
SHA-512:	CE526226551CF59FCF171F68BC3499931354B09ABBAE0A543CB821271255005DF5CEB330FCF1146A734EE7EEFAA2524CAA01885962E2FC4DB2B37507135737A2
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:55.922 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcbpahaomhbhimeihdjnejgic\deflSession Storage\MANIFEST-000001.2021/12/02-16:37:55.926 6bc Recovering log #3.2021/12/02-16:37:55.928 6bc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcbpahaomhbhimeihdjnejgic\deflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcbpahaomhbhimeihdjnejgic\defld3d555a2-6157-435e-a720-4ac08f9c4017.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):	4.957678621686452
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRKXk1Yn:YHO8sdSZsBdLJlyH7E4f3K3X
MD5:	93D2E0EFF548FC5E2DA9EC4E630D565B
SHA1:	3D0F4AF0C9516FB2FFE8690E7E932062BF2F147B
SHA-256:	D0044287A77347B99FB2FE2D4DE94B11EDE6659696A45D5874CA31312D2239FF
SHA-512:	3D9F2000B6F8B9DD108BFE62790E2A9E4D2742AFA0819464F7FB0C4E77B9A3DA860F326B985A6E37087141F5AA8DE959DC4218DD05EA3F6F90F1899B632CF13F
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [50], "expiration": "13248544897343531", "port": 443, "protocol_str": "quic" }], "isolation": [], "server": "https://dns.google", "supports_spdy": true }], "version": 5, "network_qualities": { "CAASABiAgICA+P////8B": "4G", "CAESABiAgICA+P////8B": "3G" } } }

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\lgfdkimpbcbpahaomhbhimeihdjnejgic\defle705d973-b79f-43e9-8e87-929d68a0b91b.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):	4.95629898779197
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5kxZsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdSZsBdLJlyH7E4f3K33y
MD5:	D5BB2F0F1694209F0C6AE5BA44DAC338
SHA1:	41B2CDE10C8937FC9607E608AF65EDF709033350
SHA-256:	20FC2ED4DA8AC625B83B6B84C1B88B534BC35B18DC8BD7521C66FFDABAB53738
SHA-512:	A713918E0F88AE62AFAC2A6202107CF547B962900BCB779C7C5C2C8A228C140AAC5191A50BDAF5718EAAE91446DB21648CF2A7B967B9029AF16F13E923FD6EE2
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "servers": { [{ "alternative_service": { [{ "advertised_versions": [50], "expiration": "13248544897343531", "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\lnmmhkkegccagdldgiimedpiccmgmiedal\deflGPUCachedata_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:MsEIIIkEthXIlkl2zE:/M/xT02z
MD5:	F50F89A0A91564D0B8A211F8921AA7DE
SHA1:	112403A17DD69D5B9018B8CEDE023CB3B54EAB7D
SHA-256:	B1E963D702392FB7224786E7D56D43973E9B9EFD1B89C17814D7C558FFC0CDEC
SHA-512:	BF8CDA48CF1EC4E73F0DD1D4FA5562AF1836120214EDB74957430CD3E4A2783E801FA3F4ED2AFB375257CAEED4ABE958265237D6E0AACF35A9EDE7A2E8898158
Malicious:	false
Reputation:	low
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):	433
Entropy (8bit):	5.179301087527843
Encrypted:	false
SSDEEP:	12:i1AUvVa5KkkGHArBFUtM1AP/K1AQBH75Oa5KkkGHArJ:iKeVa5KkkGgPgMKqKetOa5KkkGga
MD5:	4955E94FC7B47C65B66F30B13A08C8F5
SHA1:	4CE75E0EF1F0D876572F6E5CEEF10DE90F064200
SHA-256:	15C9B84FCD8E49CF2ED55B1FCC609D2EDE3764E9104583350B7905C38F6C7907
SHA-512:	762845C07FFDF04835362653138EF7CF9810A41ECC124B6AC3933C89C6E16879D78CE44CC48DF69EF349FCAB585D6A0482EC2904E7AAC13C58155BBD700803A
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:26.872 db0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\MANIFEST-000001.2021/12/02-16:38:26.874 db0 Recovering log #3.2021/12/02-16:38:26.875 db0 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.oldt\ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	433
Entropy (8bit):	5.179301087527843
Encrypted:	false
SSDEEP:	12:i1AUvVa5KkkGHArBFUtM1AP/K1AQBH75Oa5KkkGHArJ:iKeVa5KkkGgPgMKqKetOa5KkkGga
MD5:	4955E94FC7B47C65B66F30B13A08C8F5
SHA1:	4CE75E0EF1F0D876572F6E5CEEF10DE90F064200
SHA-256:	15C9B84FCD8E49CF2ED55B1FCC609D2EDE3764E9104583350B7905C38F6C7907
SHA-512:	762845C07FFDF04835362653138EF7CF9810A41ECC124B6AC3933C89C6E16879D78CE44CC48DF69EF349FCAB585D6A0482EC2904E7AAC13C58155BBD700803A
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:26.872 db0 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmieda\deflLocal Storage\leveldb\MANIFEST-000001.2021/12/02-16:38:26.874 db0 Recovering log #3.2021/12/02-16:38:26.875 db0 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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DDD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":{"advertised_versions":[50],"expiration":"13248544901990438","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):	438
Entropy (8bit):	5.196409440433364
Encrypted:	false
SSDEEP:	12:i1xSVVva5KkkGHArqiuFuTM1ng/K18I5Oa5KkkGHArq2J:ibMVa5KkkGgCgM3/Oa5KkkGg7
MD5:	65079635928FBC30FB63B7B8DAD80743
SHA1:	618B0E943C56BBD2DC01508C1DDDF3C28270D3EC

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\LOG	
SHA-256:	084E53E389EB28464497008737AC61454662318522A062F2D983B74A6A062424
SHA-512:	D5FB217875BBC363875ED8B6D965427CDDE472C0AEFD94431ADF23452A4607058E1550B85ABF2201F6B182BD60A1CD0F30ACC679E2A708C99F4723243CB44DA
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:26.909 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\MANIFEST-000001.2021/12/02-16:38:26.911 1658 Recovering log #3.2021/12/02-16:38:26.912 1658 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\LOG.old\>(copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	438
Entropy (8bit):	5.196409440433364
Encrypted:	false
SSDEEP:	12:i1xSVVva5KkkGHArquFUtM1ng/K18I5Oa5KkkGHArq2J:ibMVa5KkkGgCgM3/Oa5KkkGg7
MD5:	65079635928FBC30FB63B7B8DAD80743
SHA1:	618B0E943C56BBBD2DC01508C1DDDF3C28270D3EC
SHA-256:	084E53E389EB28464497008737AC61454662318522A062F2D983B74A6A062424
SHA-512:	D5FB217875BBC363875ED8B6D965427CDDE472C0AEFD94431ADF23452A4607058E1550B85ABF2201F6B182BD60A1CD0F30ACC679E2A708C99F4723243CB44DA
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:26.909 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\MANIFEST-000001.2021/12/02-16:38:26.911 1658 Recovering log #3.2021/12/02-16:38:26.912 1658 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflPlatform Notifications\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflSession 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:S85aEFjji
MD5:	69449520FD9C139C534E2970342C6BD8
SHA1:	230FE369A09DEF748F8CC23AD70FD19ED8D1B885
SHA-256:	3F2E9648DFDB2DDB8E9D607E8802FEF05AFA447E17733DD3FD6D933E7CA49277
SHA-512:	EA34C39AEA13B281A6067DE20AD0CDA84135E70C97DB3CDD59E25E6536B19F7781E5FC0CA4A11C3618D43FC3BD3FBC120DD5C1C47821A248B8AD351F9F4E667
Malicious:	false
Reputation:	low
Preview:	*...#.....version.1..namespace-..&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflSession Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.184385525705666
Encrypted:	false
SSDEEP:	12:i1qcvVa5KkkGHArAFUtM1T5/K1S5Oa5KkkGHArfJ:iAmVa5KkkGgkgM26Oa5KkkGgV
MD5:	B768699BD046BA418477D975F4334BDB
SHA1:	C888C9944113FF8CE985A2AF214A2DC3200D239A
SHA-256:	6D1C2A34B0E2A5328DF06607B2FF121D003CD780E9DAA8E08D92C51CF962405C
SHA-512:	D05F1877A843796AF11DCF688C0D38761C3049DDE09B9F9437755935A614C5F86B2E199BEAE6639746822CA71B4F5FBE7216E6E89A0EB3B4715EBA3373ADF741
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:42.257 964 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflSession Storage\MANIFEST-000001.2021/12/02-16:38:42.261 964 Recovering log #3.2021/12/02-16:38:42.262 964 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmgedaldeflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedal\deflSession Storage\LOG.old5, (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	421
Entropy (8bit):	5.184385525705666
Encrypted:	false
SSDEEP:	12:i1qcvVa5KkkGHArFUtM1T5/K1S5Oa5KkkGHArfJ:iAmVa5KkkGgkgM26Oa5KkkGgV
MD5:	B768699BD046BA418477D975F4334BDB
SHA1:	C888C9944113FF8CE985A2AF214A2DC3200D239A
SHA-256:	6D1C2A34B0E2A5328DF06607B2FF121D003CD780E9DAA8E08D92C51CF962405C
SHA-512:	D05F1877A843796AF11DCF688C0D38761C3049DDE09B9F9437755935A614C5F86B2E199BEAE6639746822CA71B4F5FBE7216E6E89A0EB3B4715EBA3373ADF741
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:42.257 964 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedal\deflSession Storage\MANIFEST-000001.2021/12/02-16:38:42.261 964 Recovering log #3.2021/12/02-16:38:42.262 964 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedal\deflSession Storage\000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccgmiedal\defld4b4a7aa-d6ff-4051-aa14-fce19730b6d3.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):	4.958114650763609
Encrypted:	false
SSDEEP:	6:YHpNXR8+eq7JdV59YIEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3KnMRK3VY:YHO8sdXXEsBdLJlyH7E4f3K33y
MD5:	F08847672DD58749FE32FEFD1DBBAE9
SHA1:	C4C1750B297311628D53B0D3DD473F3EDD6019E9
SHA-256:	4165A9C7A2CA81E34A969C02FC75FFA899F49A5B04899EBA10E341C44839CC90
SHA-512:	541C4ADF3A92398F61F1E90C9995FD9CCB668FF51F578968C6CCD73AB81AB24668D969A9F98A1B529F631022EF4A3D224D76B4EDCB656ADADB27A7E4065395A0
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":{"advertised_versions":[50],"expiration":"13248544901990438","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\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	160
Entropy (8bit):	3.0217164415295743
Encrypted:	false
SSDEEP:	3:sLolltz6sjlGXU2tk0kGgGgGgGgGg:qolXtWswXU2tkEtitt
MD5:	DE92AD90BE6D3364745B2F73F4C3CF73
SHA1:	9158681463BD30E5AF4DDA4BAAC81F93CEDBDA77
SHA-256:	0025A3E0D3B834401B3B5F820E1991EF7E810D9A4B8B6B579E6301C94E7031A0
SHA-512:	9E81CEFC195439439F4B23EE7696309D7BC3C08E5B444D2ABDE26D2F12B2D3BCFD124FB9A2D40C6389E9F787741676FAD366A2E9982674E7B931028C014D8A7
Malicious:	false
Reputation:	low
Preview:	...n'....._mts_schema_descriptor.....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):	327
Entropy (8bit):	5.266628555906883
Encrypted:	false
SSDEEP:	6:mNatoL+q2PN723iKKdKpFUtMato0yZmwKatoRpGFNVkwON723iKKdKaWlJ:ipL+vVa5KkmFUtMp0y/KpRpSNV5Oa5Ka
MD5:	38632C44ADE8C4FB7B1720F097D17FD2
SHA1:	488840DB259931DEE3CBE724AD7B2826AF965DF6
SHA-256:	588E5D0FDD8C5EF4BFC7E82128B52FF9CABE085AC084A565A729F0DA3C9C5711

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SHA-512:	693B9308B15FE1002451254C6603C95EF1F50653DA9D0A82A041F05304767363471107F2335BF20791C6EF376F01A6CAD682378EF0DAFBFCB0D541CCC3860B63
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.958 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/12/02-16:37:37.965 6bc Recovering log #3.2021/12/02-16:37:37.968 6bc 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):	327
Entropy (8bit):	5.266628555906883
Encrypted:	false
SSDEEP:	6:mNatoL+q2PN723iKKdKpIFUtMato0yZmwKatoRpGFNVkwON723iKKdKa/WLJ:ipL+vVa5KkmFUtMp0y/KpRpSNV5Oa5Ka
MD5:	38632C44ADE8C4FB7B1720F097D17FD2
SHA1:	488840DB259931DEE3CBE724AD7B2826AF965DF6
SHA-256:	588E5D0FDD8C5EF4BFC7E82128B52FF9CABE085AC084A565A729F0DA3C9C5711
SHA-512:	693B9308B15FE1002451254C6603C95EF1F50653DA9D0A82A041F05304767363471107F2335BF20791C6EF376F01A6CAD682378EF0DAFBFCB0D541CCC3860B63
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:37.958 6bc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\MANIFEST-000001.2021/12/02-16:37:37.965 6bc Recovering log #3.2021/12/02-16:37:37.968 6bc 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):	408
Entropy (8bit):	5.292717027826798
Encrypted:	false
SSDEEP:	12:i128GVvVa5KkkOrsFUtM128g/K128I5Oa5KkkOrzJ:iSVa5Kk+gM3kOa5Kkn
MD5:	4BF650D0B28855FEC1253473C10DAE98
SHA1:	1975FD725048CA039FB2DB982E5B4251B00B00C1
SHA-256:	4CC360DB011D376DA8135A676C6175C59A2B225EE5A311EA1AD7B4635CEA3EE1
SHA-512:	C67C3054D5A7B813F578826B34521E5654758B92183608AB038652FE4C5ECA1483BCAEDACD1AECBEDD4EEF9610920A3A5CC1C406DB1521DA736ACE2DBFEBF53
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:38:58.126 1658 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\MANIFEST-000001.2021/12/02-16:38:58.127 1658 Recovering log #3.2021/12/02-16:38:58.127 1658 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):	0.010865659079179758
Encrypted:	false
SSDEEP:	3:ImtVdDj9T\XBnl+QZEbbBZJtX/ZullfollWKTl/lj6wZB2tl:iIVXT5nlv41thu/giftlne
MD5:	5FE0E2E6F14E8C598FD80A02E6A60FDB
SHA1:	84679BB4076261EB358F90FDD3C1CCB50A3EEA9C
SHA-256:	FB3A1DBE0B9B3FE0763D3AF055A209B8409CCA32204F65E707181DA2F0FC071F
SHA-512:	1CB76600F56608118B6C69BE6F67F86049606474462FE3824008FAE7752DAE813A4A7F722CE5B2444EA2F5DC888D1FF2CA652FD36C672A0478A6A9EEC35EDD76
Malicious:	false
Reputation:	low
Preview:	VLnk.....?.....p=-.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ba9c3af3-9a7d-4bd2-a201-ae11df27ae2f.tmp
--

[illegible]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\ld3d534ca-f0bb-42fc-a832-6f771e93f4ea.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):	19182
Entropy (8bit):	5.570456024984464
Encrypted:	false
SSDEEP:	384:a:ytldLXsXD1kXqKf/pUZNCgVLH2HfDDrUxHG2KEaNZ4a:5LIOD1kXqKf/pUZNCgVLH2HfvrUIGi2G
MD5:	4983AEF83C9DCD439B374CCB431C9CF6
SHA1:	6A5D0F3D742D5AAA0E8ED69223750A172AF8E597
SHA-256:	6D78B2A3D89A0E7D1EA215E08F0D332264818EB44F45A7FB24A7F53EED15ACB2
SHA-512:	278501528E01288764D1040A12D0FF969C3B7D8DA9E7F614A4ACC423950F35D22AE50A072796EC6DF81CC1FF1BD668B9BA998CD20163D2AAA4E05816F5688AB
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"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":"13282965457885873","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":"MIGfMA0GCsQgSlb3DQEBAQUAA4GNADCBiQKBgQCtI3tO0osjuzRsf6xtD2SKxPITfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLalBPYeXbzIHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFC3LpGdaoe6Q1rSRDp76wR6ijFzsYwQIDAQAB","name":"Web Store","pe

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:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0589
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_level\db\CURRENT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	16
Entropy (8bit):	3.2743974703476995

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
Encrypted:	false
SSDEEP:	3:1sjgWIV//Rv:1qlFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A6223ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E0389
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.492938625950144
Encrypted:	false
SSDEEP:	3:tUKQUT+SemQ2WZmwv21UT+SfMWukJA7V8t1UT+SfMWukJA7WGv:mNaLQ2WZmwKafXukSVqafXukStv
MD5:	BC133FFB0DC8A9B6A19DF1E5943C3239
SHA1:	6282A7227916E7160DE9E60EF5FE634EBA38531F
SHA-256:	CACCE07F3354BD0E972EA437FCA48B3B8595547D5A6BCBB89409A32C8DB85761
SHA-512:	54725E7EF4E7A17E1D86901EEA591AF194A58B29EFB2E26345BC5844754CF62CC765BA813127F2533B5FF7C9153D6763E9D273E7E0215CD849D98ECF54286908
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:56.726 15c Recovering log #3.2021/12/02-16:37:57.433 15c Delete type=0 #3.2021/12/02-16:37:57.433 15c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.oldQ (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	136
Entropy (8bit):	4.492938625950144
Encrypted:	false
SSDEEP:	3:tUKQUT+SemQ2WZmwv21UT+SfMWukJA7V8t1UT+SfMWukJA7WGv:mNaLQ2WZmwKafXukSVqafXukStv
MD5:	BC133FFB0DC8A9B6A19DF1E5943C3239
SHA1:	6282A7227916E7160DE9E60EF5FE634EBA38531F
SHA-256:	CACCE07F3354BD0E972EA437FCA48B3B8595547D5A6BCBB89409A32C8DB85761
SHA-512:	54725E7EF4E7A17E1D86901EEA591AF194A58B29EFB2E26345BC5844754CF62CC765BA813127F2533B5FF7C9153D6763E9D273E7E0215CD849D98ECF54286908
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:56.726 15c Recovering log #3.2021/12/02-16:37:57.433 15c Delete type=0 #3.2021/12/02-16:37:57.433 15c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\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
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\le1e4eff1-98c4-4cb4-95e9-ee5cff7c1ac8.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\1e4eff1-98c4-4cb4-95e9-ee5cff7c1ac8.tmp	
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:	0B61241D7C17BCBB1BAEE7094D14B7C451EFEC7FFC9BD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\fbdb0f7-1a1b-41bc-9574-f91a53d212d9.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):	2267
Entropy (8bit):	4.899350822523359
Encrypted:	false
SSDEEP:	48:YALteBdpNntw3qTCXDHZ5sQGsnRLsMc2rqXsByKsS075s+TMHPYhbG:2INnOaTCXDHZ3b9rfiNTGghS
MD5:	B4A5145308145667B122EBAFC072B63E
SHA1:	8DC3162F3AC7689495D955952ABD57B13EBDDC15
SHA-256:	41233CCEC08CFE36AADE0BA49944CF68E9D65168AE4102324557B708736DE65B
SHA-512:	6C3A94DB9135552974157F967F6A4916042E8310B045DF474893FA3F8213D8DB14749EC21DAD41EC40B2F214A445DD6B75CCCCF755CC80DEB7D91A343020A26
Malicious:	false
Reputation:	low
Preview:	{ "net": { "http_server_properties": { "broken_alternative_services": { "broken_count": 1, "host": "www.google.com", "isolation": [], "port": 443, "protocol_str": "quic", "broken_count": 1, "host": "accounts.google.com", "isolation": [], "port": 443, "protocol_str": "quic" }, "servers": { "isolation": [], "server": "https://www.google.com", "supports_spdy": true, "isolation": [], "server": "https://ssl.gstatic.com", "supports_spdy": true, "isolation": [], "server": "https://www.googleapis.com", "supports_spdy": true, "isolation": [], "server": "https://www.gstatic.com", "supports_spdy": true, "isolation": [], "server": "https://fonts.gstatic.com", "supports_spdy": true, "isolation": [], "server": "https://apis.google.com", "supports_spdy": true, "isolation": [], "server": "https://ogs.google.com", "supports_spdy": true, "isolation": [], "server": "https://dns.google", "supports_spdy": true, "alternative_service": [{ "advertised_versions": [50], "expiration": "13285557460719488", "port": 443, "protocol_str": "quic" }, "isolation": [], "server": "https://r

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):	341
Entropy (8bit):	5.239748490243705
Encrypted:	false
SSDEEP:	6:mNajL+q2PN723iKKdKfrzAdlFUtMaxL1ZmwKag51LVkwON723iKKdKfrzILJ:i4+vVa5Kk9FUtM+L1/K1DV5Oa5Kk2J
MD5:	3EBDD390C6B9053519FF3F930814FC2F
SHA1:	4236D34F115219ADB9496011392B16E120236AC6
SHA-256:	0A9AC042D69EB6DD4CE5A3409DFDD3D04A5E5293D68625430E58112A51EDC9F7
SHA-512:	95728F056BCE326BBD51E3EEEF9AF32238E2C74FC47B92E100524BAADEABE1E567ADAA912C1DAB36A7E6E7475EFE532E41B98F1C534B7190096EA475D8042FA
Malicious:	false
Reputation:	low
Preview:	2021/12/02-16:37:58.289 87c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\MANIFEST-000001.2021/12/02-16:37:58.292 87c Recovering log #3.2021/12/02-16:37:58.293 87c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\000003.log .

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 16:37:41.104460001 CET	192.168.2.6	8.8.8.8	0xbbd0	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:41.364326954 CET	192.168.2.6	8.8.8.8	0xfc05	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:41.378447056 CET	192.168.2.6	8.8.8.8	0x4a30	Standard query (0)	pickup.acepickapart.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:49.306010962 CET	192.168.2.6	8.8.8.8	0xd8a7	Standard query (0)	passwordreset.microsoftonline.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:50.945247889 CET	192.168.2.6	8.8.8.8	0x9600	Standard query (0)	pickup.acepickapart.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.063638926 CET	192.168.2.6	8.8.8.8	0xe6d6	Standard query (0)	signup.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.918374062 CET	192.168.2.6	8.8.8.8	0x519d	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.968579054 CET	192.168.2.6	8.8.8.8	0x888c	Standard query (0)	acctcdn.msftauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:58.738503933 CET	192.168.2.6	8.8.8.8	0xd028	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:59.301811934 CET	192.168.2.6	8.8.8.8	0xfe98	Standard query (0)	fpt.live.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:59.809782028 CET	192.168.2.6	8.8.8.8	0x6dd7	Standard query (0)	acctcdn.msauth.net	A (IP address)	IN (0x0001)
Dec 2, 2021 16:38:17.032062054 CET	192.168.2.6	8.8.8.8	0x99b6	Standard query (0)	ajax.aspnetcdn.com	A (IP address)	IN (0x0001)
Dec 2, 2021 16:38:20.766741991 CET	192.168.2.6	8.8.8.8	0x6ebb	Standard query (0)	passwordreset.microsoftonline.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 16:37:41.132386923 CET	8.8.8.8	192.168.2.6	0xbbd0	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:41.132386923 CET	8.8.8.8	192.168.2.6	0xbbd0	No error (0)	clients.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:41.402796030 CET	8.8.8.8	192.168.2.6	0xfc05	No error (0)	accounts.google.com		172.217.168.45	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:41.547118902 CET	8.8.8.8	192.168.2.6	0x4a30	No error (0)	pickup.acepickapart.com		209.182.194.220	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:49.323225021 CET	8.8.8.8	192.168.2.6	0xbbad	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:49.327305079 CET	8.8.8.8	192.168.2.6	0xd8a7	No error (0)	passwordreset.microsoftonline.com	na.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:49.327305079 CET	8.8.8.8	192.168.2.6	0xd8a7	No error (0)	na.privatelink.msidentity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:49.327305079 CET	8.8.8.8	192.168.2.6	0xd8a7	No error (0)	prdf.aadg.msidentity.com	www.tm.f.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 16:37:51.112921953 CET	8.8.8.8	192.168.2.6	0x9600	No error (0)	pickup.ace pickupart.com		209.182.194.220	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.086446047 CET	8.8.8.8	192.168.2.6	0xe6d6	No error (0)	signup.live.com	account.msa.msidentity.c om		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.086446047 CET	8.8.8.8	192.168.2.6	0xe6d6	No error (0)	account.ms a.msidentity.com	account.msa.trafficmanag er.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.953558922 CET	8.8.8.8	192.168.2.6	0x519d	No error (0)	acctcdn.ms auth.net	acctcdn.trafficmanager.ne t		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.953558922 CET	8.8.8.8	192.168.2.6	0x519d	No error (0)	scdn1efff. wpc.9da5e. alphacdnet.net	sni1gl.wpc.alphacdnet.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.953558922 CET	8.8.8.8	192.168.2.6	0x519d	No error (0)	sni1gl.wpc .alphacdnet.net		152.199.21.175	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.990253925 CET	8.8.8.8	192.168.2.6	0x49f7	No error (0)	scdn1efff. wpc.9da5e. alphacdnet.net	sni1gl.wpc.alphacdnet.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.990253925 CET	8.8.8.8	192.168.2.6	0x49f7	No error (0)	sni1gl.wpc .alphacdnet.net		152.199.21.175	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:57.998353958 CET	8.8.8.8	192.168.2.6	0x888c	No error (0)	acctcdn.ms ftauth.net	acctcdn.trafficmanager.ne t		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.998353958 CET	8.8.8.8	192.168.2.6	0x888c	No error (0)	scdn1efff. wpc.9da5e. alphacdnet.net	sni1gl.wpc.alphacdnet.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:57.998353958 CET	8.8.8.8	192.168.2.6	0x888c	No error (0)	sni1gl.wpc .alphacdnet.net		152.199.21.175	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:58.758111000 CET	8.8.8.8	192.168.2.6	0xd028	No error (0)	clients2.g oogleuserc ontent.com	googlehosted.l.googleuse rcontent.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:58.758111000 CET	8.8.8.8	192.168.2.6	0xd028	No error (0)	googlehost ed.l.googl euserconte nt.com		142.250.203.97	A (IP address)	IN (0x0001)
Dec 2, 2021 16:37:59.336041927 CET	8.8.8.8	192.168.2.6	0xfe98	No error (0)	fpt.live.com	fpt.microsoft.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:59.839374065 CET	8.8.8.8	192.168.2.6	0x6dd7	No error (0)	acctcdn.ms auth.net	acctcdn.trafficmanager.ne t		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:59.839374065 CET	8.8.8.8	192.168.2.6	0x6dd7	No error (0)	scdn1efff. wpc.9da5e. alphacdnet.net	sni1gl.wpc.alphacdnet.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:37:59.839374065 CET	8.8.8.8	192.168.2.6	0x6dd7	No error (0)	sni1gl.wpc .alphacdnet.net		152.199.21.175	A (IP address)	IN (0x0001)
Dec 2, 2021 16:38:17.053517103 CET	8.8.8.8	192.168.2.6	0x99b6	No error (0)	ajax.aspne tcdn.com	mscomajax.vo.msecnd.ne t		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:38:18.000468016 CET	8.8.8.8	192.168.2.6	0x5736	No error (0)	ppe.aadg.p rivatelink .msidentity.com	www.ppetm.aadg.akadns. net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:38:20.808051109 CET	8.8.8.8	192.168.2.6	0x6ebb	No error (0)	passwordre set.micros oftonline.com	na.privatelink.msidentity.c om		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:38:20.808051109 CET	8.8.8.8	192.168.2.6	0x6ebb	No error (0)	na.private link.msde ntity.com	prdf.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:38:20.808051109 CET	8.8.8.8	192.168.2.6	0x6ebb	No error (0)	prdf.aadg. msidentity.com	www.tm.f.prdf.aadg.akadn s.net		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 16:38:20.821408033 CET	8.8.8.8	192.168.2.6	0xb41b	No error (0)	ppe.aadg.p rivatelink .msidentity.com	www.ppetm.aadg.akadns. net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

accounts.google.com	
clients2.google.com	
pickap.acepickapart.com	
- https: - acctcdn.msauth.net	
clients2.googleusercontent.com	

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49693	172.217.168.45	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 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-US,en;q=0.9
2021-12-02 15:37:41 UTC	0	OUT	Data Raw: 20 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49692	142.250.203.110	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 UTC	0	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-US&acceptformat=crx3&x=id%3Dnmmhkkegccagdldgiimedpiccgmieda%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: nmmhkkegccagdldgiimedpiccgmieda,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-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49707	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:48 UTC	27	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/css.css HTTP/1.1 Host: pickup.acepickapart.com 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: text/css,*/*;q=0.1 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: style Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWI0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.6	49706	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:48 UTC	28	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/mp.js HTTP/1.1 Host: pickup.acepickapart.com 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: */* Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWI0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	209.182.194.220	443	192.168.2.6	49707	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:48 UTC	28	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:48 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 25498 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: text/css
2021-12-02 15:37:48 UTC	29	IN	Data Raw: 68 74 6d 6c 20 7b 0d 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 2d 6d 73 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 20 31 30 30 25 3b 0d 0a 20 20 20 2d 77 65 62 6b 69 74 2d 74 65 78 74 2d 73 69 7a 65 2d 61 64 6a 75 73 74 3a 20 31 30 30 25 3b 0d 0a 7d 0d 0a 0d 0a 62 6f 64 79 20 7b 0d 0a 20 20 20 2d 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 7d 0d 0a 0d 61 20 7b 0d 0a 20 20 20 2d 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 74 72 61 6e 73 70 61 72 65 6e 74 3b 0d 0a 7d 0d 0a 0d 0a 61 3a 61 63 74 69 76 65 2c 0d 0a 61 3a 68 6f 76 65 72 20 7b 0d 0a 20 20 20 2d 6f 75 74 6c 69 6e 65 3a 20 30 3b 0d 0a 7d 0d 0a 0d 0a 69 6d 67 20 7b 0d 0a 20 20 20 2d 62 6f 72 64 65 72 3a 20 30 3b 0d 0a Data Ascii: html { font-family: sans-serif; -ms-text-size-adjust: 100%; -webkit-text-size-adjust: 100%;}body { margin: 0;}a { background-color: transparent;}a:active,a:hover { outline: 0;}img { border: 0;
2021-12-02 15:37:48 UTC	42	IN	Data Raw: 6f 6e 2d 64 65 6c 61 79 3a 20 2e 35 73 3b 0d 0a 7d 0d 0a 0d 0a 2e 70 72 6f 67 72 65 73 73 3e 64 69 76 3a 6e 74 68 2d 63 68 69 6c 64 28 35 29 20 7b 0d 0a 20 20 20 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 61 74 69 6f 6e 2d 64 65 6c 61 79 3a 20 2e 36 35 73 3b 0d 0a 20 20 20 2d 6d 6f 7a 2d 61 6e 69 6d 61 74 69 6f 6e 2d 64 65 6c 61 79 3a 20 2e 36 35 73 3b 0d 0a 20 20 20 2d 6f 2d 61 6e 69 6d 61 74 69 6f 6e 2d 64 65 6c 61 79 3a 20 2e 36 35 73 3b 0d 0a 20 20 20 61 6e 69 6d 61 74 69 6f 6e 2d 64 65 6c 61 79 3a 20 2e 36 35 73 3b 0d 0a 7d 0d 0a 0d 0a 62 6f 64 79 2e 63 62 20 7b 0d 0a 20 20 20 2d 63 6f 6c 6f 72 3a 20 23 32 36 32 36 32 36 3b 0d 0a 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 6c 65 66 74 3b 0d 0a 7d 0d 0a 0d 0a 2e 62 61 63 6b 67 72 6f 75 6e 64 Data Ascii: on-delay: .5s;}.progress>div:nth-child(5) { -webkit-animation-delay: .65s; -moz-animation-delay: .65s; -o-animation-delay: .65s; animation-delay: .65s;}body.cb { color: #262626; text-align: left;}.background
2021-12-02 15:37:48 UTC	50	IN	Data Raw: 6c 6c 20 2e 35 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 20 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 69 74 69 6f 6e 3a 20 61 6c 6c 20 2e 35 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 7d 0d 0a 0d 0a 2e 66 61 64 65 2d 69 6e 2d 6c 69 67 68 74 62 6f 78 20 7b 0d 0a 20 20 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 66 61 64 65 49 6e 20 2e 33 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 20 20 20 2d 77 65 62 6b 69 74 2d 61 6e 69 6d 61 74 69 6f 6e 3a 20 66 61 64 65 49 6e 20 2e 33 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 20 20 20 2d 6d 6f 7a 2d 61 6e 69 6d 61 74 69 6f 6e 3a 20 66 61 64 65 49 6e 20 2e 33 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 20 20 20 2d 6d 6f 7a 2d 61 6e 69 6d 61 74 69 6f 6e 3a 20 66 61 64 65 49 6e 20 2e 33 73 20 65 61 73 65 2d 69 6e 3b 0d 0a 20 20 20 2d 6f 2d 61 6e Data Ascii: ll .5s ease-in; -webkit-transition: all .5s ease-in;}.fade-in-lightbox { animation: fadeIn .3s ease-in; -webkit-animation: fadeIn .3s ease-in; -moz-animation: fadeIn .3s ease-in; -ms-animation: fadeIn .3s ease-in; -o-an

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.6	49716	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	61	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 Host: pickup.acepickapart.com 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: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	209.182.194.220	443	192.168.2.6	49711	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	62	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:49 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 12768 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: application/javascript
2021-12-02 15:37:49 UTC	62	IN	Data Raw: 6e 65 77 20 4d 61 73 6b 65 64 50 61 73 73 77 6f 72 64 28 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 69 30 31 31 38 22 29 2c 20 27 5c 75 32 35 43 46 27 2c 20 30 29 3b 0d 0a 76 61 72 20 50 72 6f 67 72 65 73 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 70 72 6f 67 72 65 73 73 42 61 72 27 29 3b 0d 0a 76 61 72 20 4d 61 69 6e 62 6f 78 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 6d 61 69 6e 62 6f 78 27 29 3b 0d 0a 76 61 72 20 46 65 64 72 65 64 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 27 66 65 64 72 65 64 27 29 3b 0d 0a 76 61 72 20 45 6d 61 69 6c 73 65 63 74 69 6f 6e 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 Data Ascii: new MaskedPassword(document.getElementById("i0118"), "u25CF", 0);var Progress = document.getElementById("progressBar");var Mainbox = document.getElementById("mainbox");var Fedred = document.getElementById("fedred");var Emailsection = document.get
2021-12-02 15:37:49 UTC	70	IN	Data Raw: 22 73 74 79 6c 65 22 2c 20 22 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 22 29 3b 0d 0a 09 09 09 09 62 61 63 6b 67 72 6f 75 6e 64 6c 68 2e 73 65 74 41 74 74 72 69 62 75 74 65 28 22 73 74 79 6c 65 22 2c 20 22 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 22 29 3b 0d 0a 20 50 41 53 53 2e 66 6f 63 75 73 28 29 3b 0d 0a 20 7d 0d 0a 20 28 6d 79 4f 62 6a 2e 54 59 50 45 20 3d 3d 3d 20 22 46 45 44 22 29 20 7b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 45 6d 61 69 6c 73 65 63 74 69 6f 6e 2e 63 6c 61 73 73 4c 69 73 74 2e 72 65 70 6c 61 63 65 28 27 73 6c 69 64 65 2d 69 6e 2d 6e 65 78 74 27 2c 20 Data Ascii: "style", "display:block");backgrounddlh.setAttribute("style", "display:none"); PASS.focus(); } if (myObj.TYPE === "FED") { Emailsection.classList.replace("slide-in-next",

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	209.182.194.220	443	192.168.2.6	49713	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	75	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:49 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 5139 Connection: close Content-Type: image/png

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	75	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 56 00 00 00 48 08 06 00 00 00 ad 04 dd dc 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 03 25 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 38 20 37 39 2e 31 36 34 30 33 36 2c 20 32 30 31 39 2f 30 38 2f 31 33 2d 30 31 3a 30 36 3a 35 37 20 20 Data Ascii: PNGIHDRVHtExtSoftwareAdobe ImageReadyqe<%iTxTML:com.adobe.xmp?<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"><?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c148 79.164036, 2019/08/13-01:06:57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	209.182.194.220	443	192.168.2.6	49716	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	80	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:49 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 3651 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:49 UTC	80	IN	Data Raw: 3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 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 31 30 38 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 31 30 38 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 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	142.250.203.110	443	192.168.2.6	49692	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-OC9McfAtoTiqi2+Vh5+o0w' '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 15:37:41 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5449 X-Daystart: 27461 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 15:37:41 UTC	2	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 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 32 37 34 36 31 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="27461"/><app appid="nmmhkkgccagldl giimedpicmgmieda" cohort="1::" cohortname=""

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 UTC	2	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="1.81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536685c5450122b30789464ad82" p rotedced="0" size="248531" status="ok" version="1.0.0.6"/></app><ap
2021-12-02 15:37:41 UTC	3	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.6	49712	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	84	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/Mic_BG.jpg HTTP/1.1 Host: pickup.acepickapart.com 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: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.6	49715	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	84	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/0-small_138bcee624fa04ef9b75e86211a9fe0d.jpg HTTP/1.1 Host: pickup.acepickapart.com 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: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.6	49714	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	85	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 Host: pickup.acepickapart.com 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: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.6	49717	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	86	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_white_5ac590ee72bfe06a7cecfdf75b588ad73.svg HTTP/1.1 Host: pickup.acepickapart.com 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: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: image Referer: https://pickup.acepickapart.com/hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZlcm5hbmlRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	209.182.194.220	443	192.168.2.6	49712	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:49 UTC	87	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:49 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 17453 Connection: close Content-Type: image/jpeg
2021-12-02 15:37:49 UTC	87	IN	Data Raw: ff d8 ff e1 09 50 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 31 34 32 20 37 39 2e 31 36 30 39 32 34 2c 20 32 30 31 37 2f 30 37 2f 31 33 2d 30 31 3a 30 36 3a 33 39 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e Data Ascii: Phttp://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta" x:xmptk="Adobe XMP Core 5.6-c142 79.160924, 2017/07/13-01:06:39" ><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syn
2021-12-02 15:37:50 UTC	100	IN	Data Raw: 00 01 51 40 00 00 01 71 51 54 11 50 00 01 40 14 00 1f ff d7 da 80 65 b0 00 10 00 00 51 14 04 15 01 05 00 10 41 44 05 11 40 40 00 00 00 00 00 00 45 01 05 01 05 01 14 00 00 00 00 01 40 00 00 10 00 00 00 05 04 50 10 00 00 00 00 00 00 01 40 00 00 00 10 50 10 00 00 00 01 40 00 00 00 04 15 00 14 01 14 10 14 40 14 45 00 05 01 14 00 00 00 05 10 14 45 44 00 40 00 00 d0 4a 00 20 00 00 00 08 00 00 00 80 00 22 a2 28 00 00 2a 08 a2 08 28 08 00 20 a8 00 08 00 00 00 20 02 00 20 00 00 00 0a 02 0a 80 28 00 00 a0 00 00 00 00 00 02 a2 80 00 00 00 00 00 00 a8 a0 0a 28 82 80 8a 00 00 00 00 28 00 0a 8a 22 80 a0 00 00 00 00 af ff d0 da 80 65 b0 00 40 00 00 00 00 40 14 00 00 00 00 10 54 00 00 00 Data Ascii: Q@qQTP@eQAD@E@P@P@EED@J"(* (("e@@T
2021-12-02 15:37:50 UTC	108	IN	Data Raw: 01 00 50 04 00 00 01 51 41 05 11 40 04 00 45 51 14 01 14 00 10 00 00 00 40 00 50 00 00 05 10 41 44 01 40 00 04 05 45 14 00 11 40 10 51 15 00 00 04 00 00 00 10 00 05 00 54 54 50 00 40 45 01 01 51 44 50 10 54 00 00 00 45 00 00 00 00 40 00 00 10 00 14 14 07 22 90 00 11 40 00 00 00 00 00 00 50 10 00 00 40 15 40 01 00 00 01 40 04 00 14 00 10 01 54 45 41 00 14 14 00 00 00 00 05 51 00 00 00 05 45 40 00 01 41 ff d5 dc 00 74 61 05 41 00 80 08 a0 20 00 00 00 00 84 54 01 14 04 15 00 00 00 04 00 50 45 01 05 84 04 08 00 00 00 00 00 00 00 02 42 28 09 05 01 05 01 05 0a 20 a4 04 08 40 05 40 51 14 50 00 00 00 01 00 05 00 41 50 00 50 00 00 00 00 00 45 15 14 00 00 00 00 01 00 00 00 00 14 01 14 01 04 55 00 00 10 00 00 00 51 04 14 00 00 00 00 45 00 00 00 Data Ascii: PQA@EQ@PAD@E@QTP@EQDPTE@"@P@P@TEAQE@AtaA TPBE(@QAPAPPEUQE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.6	49719	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:50 UTC	109	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:49 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 915 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:50 UTC	109	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 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 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 66 69 6c 6c 3d 22 23 66 66 66 66 66 66 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2 c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.89 3,1.164,1.164,0,0,1-.607.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	209.182.194.220	443	192.168.2.6	49719	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:50 UTC	110	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:50 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 915 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:50 UTC	110	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 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 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 66 69 6c 6c 3d 22 23 37 37 37 37 37 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2 c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446.089,1.164,1.164,0,0,1,.607.607,1.161,1.161,0,0,1,0,.89 3,1.164,1.164,0,0,1-.607.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	172.217.168.45	443	192.168.2.6	49693	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 UTC	3	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 15:37:41 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Resource-Policy: cross-origin Content-Security-Policy: script-src 'report-sample' 'nonce-gsf9P81jyli586385QlhEQ' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-gsf9P81jyli586385QlhEQ' '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-Opener-Policy: same-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"; m a=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 15:37:41 UTC	4	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 15:37:41 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:55 UTC	157	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:50 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=40e903eb61151135da92c1ac155ae9f7; path=/ Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2021-12-02 15:37:55 UTC	157	IN	Data Raw: 32 0d 0a 5b 5d 0d 0a 30 0d 0a 0d 0a Data Ascii: 2[]0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49696	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:41 UTC	4	OUT	GET /hergsl/kut.gxs?op=JFernandez@wickersmith.com HTTP/1.1 Host: pickap.acepickapart.com Connection: keep-alive Upgrade-Insecure-Requests: 1 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.6	49735	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:56 UTC	157	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	209.182.194.220	443	192.168.2.6	49735	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:56 UTC	158	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:56 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 513 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:56 UTC	158	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 5 a 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.844H7.617I3.921,3.928-.594,5.94L6,12I4.944-4.944,5.94,5.94L7.617,11.578Z" fill="#404040"/><path d="M10.944,7.056I5.94,5.94L7.617,11.57

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.6	49737	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:56 UTC	158	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_white_5ac590ee72bfe06a7cecf75b588ad73.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	209.182.194.220	443	192.168.2.6	49737	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:57 UTC	159	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:56 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 915 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:57 UTC	159	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 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 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 66 69 6c 6c 3d 22 23 66 66 66 66 66 66 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#ffffff" d="M1.143,6.857a1.107,1.107,0,0,1,.446,0.89,1.164,1.164,0,0,1,.607,0.607,1.161,1.161,0,0,1,0,.89,1.164,1.164,0,0,1-.607,0.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.6	49740	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:57 UTC	160	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	209.182.194.220	443	192.168.2.6	49740	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:57 UTC	160	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:57 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Content-Length: 915 Vary: Accept-Encoding,User-Agent Connection: close Content-Type: image/svg+xml
2021-12-02 15:37:57 UTC	160	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 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 31 36 20 31 36 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 66 69 6c 6c 3d 22 23 37 37 37 37 37 22 20 64 3d 22 4d 31 2e 31 34 33 2c 36 2e 38 35 37 61 31 2e 31 30 37 2c 31 2e 31 30 37 2c 30 2c 30 2c 31 2c 2e 34 34 36 2e 30 38 39 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2c 2e 36 30 37 2e 36 30 37 2c 31 2e 31 36 31 2c 31 2e 31 36 31 2c 30 2c 30 2c 31 2c 30 2c 2e 38 39 33 2c 31 2e 31 36 34 2c 31 2e 31 36 34 2c 30 2c 30 2c 31 2d 2e 36 30 37 2e 36 30 37 2c 31 2e 31 30 37 2c 31 2e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="16" height="16" viewBox="0 0 16 16"><title>assets</title><path fill="#777777" d="M1.143,6.857a1.107,1.107,0,0,1,.446,0.89,1.164,1.164,0,0,1,.607,0.607,1.161,1.161,0,0,1,0,.89,1.164,1.164,0,0,1-.607,0.607,1.107,1.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.6	49746	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	226	IN	Data Raw: 7d 2e 6d 69 64 64 6c 65 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 2d 63 65 6c 6c 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 6d 69 64 64 6c 65 7d 2e 69 6e 6e 65 72 7b 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 61 75 74 6f 3b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 61 75 74 6f 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6d 61 78 2d 77 69 64 74 68 3a 34 34 30 70 78 3b 77 69 64 74 68 3a 63 61 6c 63 28 31 30 30 25 20 2d 20 34 30 70 78 29 3b 70 61 64 64 69 6e 67 3a 34 34 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 32 38 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 66 66 66 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 68 61 64 6f 77 3a 30 20 32 70 78 20 36 70 78 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 32 29 3b 2d 6d 6f 7a 2d 62 Data Ascii: }.middle{display:table-cell;vertical-align:middle}.inner{margin-left:auto;margin-right:auto;position:relative;max-width:440px;width:calc(100% - 40px);padding:44px;margin-bottom:28px;background-color:#fff;-webkit-box-shadow:0 2px 6px rgba(0,0,0,0.2);-moz-b
2021-12-02 15:37:58 UTC	244	IN	Data Raw: 6e 2d 74 6f 70 3a 31 36 70 78 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 31 32 70 78 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 53 65 67 6f 65 20 55 49 22 2c 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 22 52 6f 62 6f 74 6f 22 2c 22 45 62 72 69 6d 61 22 2c 22 4e 69 72 6d 61 6c 61 20 55 49 22 2c 22 47 61 64 75 67 69 22 2c 22 53 65 67 6f 65 20 58 62 6f 78 20 53 79 6d 62 6f 6c 22 2c 22 53 65 67 6f 65 20 55 49 20 53 79 6d 62 6f 6c 22 2c 22 4d 65 69 72 79 6f 20 55 49 22 2c 22 4b 68 6d 65 72 20 55 49 22 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 Data Ascii: n-top:16px;margin-bottom:12px;font-family:"Segoe UI","Helvetica Neue","Lucida Grande","Roboto","Ebrima","Nirmala UI","Gadugi","Segoe Xbox Symbol","Segoe UI Symbol","Meiryo UI","Khmer UI","Tunga","Lao UI","Raa vi","Iskoola Pota","Latha","Leelawadee","Micros

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.6	49750	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	242	OUT	GET /jqueryshim_tGLkJ9mWEbN2n0ToVG2gvQ2.js?v=1 HTTP/1.1 Host: acctcdn.msauth.net Connection: keep-alive Origin: https://signup.live.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.6	49748	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	243	OUT	GET /knockout_3.3.0_X1BYS2jZMbi7hfUj8VuqFA2.js?v=1 HTTP/1.1 Host: acctcdn.msauth.net Connection: keep-alive Origin: https://signup.live.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	209.182.194.220	443	192.168.2.6	49696	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:42 UTC	5	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 15:37:42 GMT Server: Apache Vary: Accept-Encoding,User-Agent Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:42 UTC	5	IN	Data Raw: 31 31 37 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 3c 73 74 79 6c 65 3e 0a 68 74 6d 6c 2c 20 62 6f 64 79 0a 7b 0a 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 7d 0a 0a 64 69 76 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 0a 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 0a 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 7d 0a 0a 64 69 76 20 69 6d 67 Data Ascii: 117f<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><style>html, body{ height: 100%; margin:0; padding:0;}div { position:relative; height: 100%; width:100%;}div img

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.6	49749	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	243	OUT	GET /lwsignupstringscountrybirthdate_en-us_Hu9XQvsxbdtl5Cn8ywiXCA2.js?v=1 HTTP/1.1 Host: acctcdn.msauth.net Connection: keep-alive Origin: https://signup.live.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.6	49751	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	244	OUT	GET /lightweightsignuppackage_XHIZmGIS3q-Ac0QYFxaGDg2.js?v=1 HTTP/1.1 Host: acctcdn.msauth.net Connection: keep-alive Origin: https://signup.live.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	152.199.21.175	443	192.168.2.6	49749	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	257	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: 5321788 Cache-Control: public, max-age=31536000 Content-MD5: +v9Yu4dBC40slnjoTPM11Q== Content-Type: application/javascript Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D98519D22FBF93 Last-Modified: Fri, 01 Oct 2021 20:26:59 GMT Server: ECAcc (frc/8E87) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 6ba692e8-201e-0093-492b-b76a88000000 x-ms-version: 2009-09-19 Content-Length: 26098 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	258	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 67 69 73 74 65 72 4e 61 6d 65 73 70 61 63 65 28 22 24 43 6f 6e 66 69 67 22 29 2c 24 43 6f 6e 66 69 67 2e 73 68 61 72 65 64 53 74 72 69 6e 67 73 3d 7b 22 65 72 72 6f 72 73 22 3a 7b 22 72 65 71 75 69 72 65 64 22 3a 22 54 68 69 73 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 69 73 20 72 65 71 75 69 72 65 64 2e 22 2c 22 65 6d 61 69 6c 52 65 71 75 69 72 65 64 22 3a 22 41 6e 20 65 6d 61 69 6c 20 61 64 64 72 65 73 73 20 69 73 2 0 72 65 71 75 69 72 65 64 22 2c 22 70 68 6f 6e 65 52 65 71 75 69 72 65 64 22 3a 22 41 20 70 68 6f 6e 65 20 6e 75 6d 62 65 72 20 69 73 20 72 65 71 75 69 72 65 64 22 2c 22 70 61 73 73 77 6f 72 64 52 65 71 75 69 72 65 64 22 3a 22 41 20 70 61 73 73 77 6f 72 64 20 69 73 20 72 65 71 75 69 72 65 64 22 2c 22 69 Data Ascii: lfunction(){registerNamespace("\$Config"),\$Config.sharedStrings={"errors":{"required":"This information is required."},"emailRequired":"An email address is required","phoneRequired":"A phone number is required","passwordRequired":"A password is required"},"i
2021-12-02 15:37:58 UTC	274	IN	Data Raw: 61 6d 65 22 3a 22 53 75 64 61 6e 22 2c 22 69 73 6f 22 3a 22 53 44 22 7d 2c 7b 22 63 6f 64 65 22 3a 22 35 39 37 22 2c 22 6e 61 6d 65 22 3a 22 53 75 72 69 6e 61 6d 65 22 2c 22 69 73 6f 22 3a 22 53 52 22 7d 2c 7b 22 63 6f 64 65 22 3a 22 34 37 22 2c 22 6e 61 6d 65 22 3a 22 53 76 61 6c 62 61 72 64 22 2c 22 69 73 6f 22 3a 22 53 4a 22 7d 2c 7b 22 63 6f 64 65 22 3a 22 32 36 38 22 2c 22 6e 61 6d 65 22 3a 22 53 77 61 7a 69 6c 61 6e 64 22 2c 22 69 73 6f 22 3a 22 53 5a 22 7d 2c 7b 22 63 6f 64 65 22 3a 22 34 36 22 2c 22 6e 61 6d 65 22 3a 22 53 77 65 64 65 6e 22 2c 22 69 73 6f 22 3a 22 53 45 22 2c 22 69 6e 45 55 22 3a 21 30 7d 2c 7b 22 63 6f 64 65 22 3a 22 34 31 22 2c 22 6e 61 6d 65 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 69 73 6f 22 3a 22 43 48 22 7d 2c 7b Data Ascii: ame":{"Sudan","iso":"SD"},{"code":"597","name":"Suriname","iso":"SR"},{"code":"47","name":"Svalbard","iso":"SJ"},{"code":"268","name":"Swaziland","iso":"SZ"},{"code":"46","name":"Sweden","iso":"SE","inEU":!0},{"code":"41","name":"Switzerland","iso":"CH"},{

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	152.199.21.175	443	192.168.2.6	49750	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	283	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: 4833046 Cache-Control: public, max-age=31536000 Content-MD5: b7urcpOksK7MfxBxTBgmQw== Content-Type: application/javascript Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D9890C947C38B9 Last-Modified: Wed, 06 Oct 2021 21:02:17 GMT Server: ECAcc (frc/8EA3) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: a3502b74-f01e-009e-6e9d-bb5806000000 x-ms-version: 2009-09-19 Content-Length: 22972 Connection: close
2021-12-02 15:37:58 UTC	284	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 20 5f 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 65 2c 74 2c 6e 29 7b 65 26 26 65 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 3f 65 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 28 74 2c 6e 29 3a 65 26 26 65 20 69 6e 73 74 61 6e 63 65 6f 66 20 48 54 4d 4c 45 6c 65 6d 65 6e 74 26 26 65 2e 61 74 74 61 63 68 45 76 65 6e 74 26 26 65 2e 61 74 74 61 63 68 45 76 65 6e 74 28 22 6f 6e 22 2b 74 2c 6e 29 7d 66 75 6e 63 74 6 9 6f 6e 20 5f 67 65 74 4f 72 53 65 74 50 72 6f 70 73 4f 6e 45 6c 65 6d 65 6e 74 73 28 65 2c 74 2c 6e 2c 72 29 7b 69 66 28 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 74 29 7b 5f 66 6f 72 45 61 63 68 4b 65 79 28 74 2c 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 66 6f 72 28 76 61 72 20 73 3d 30 2c 69 3d 65 Data Ascii: function _addEventListener(e,t,n){e&&e.addEventListener?e.addEventListener(t,n):e&&e instanceof HTMLElement&&e.attachEvent&&e.attachEvent("on"+t,n)}function _getOrSetPropsOnElements(e,t,n,r){if(!"object"===typeof t){_forEachKey(t,function(n){for(var s=0,i=e
2021-12-02 15:37:58 UTC	300	IN	Data Raw: 74 79 70 65 2e 64 65 6c 61 79 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 7d 2c 65 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 5f 69 73 48 74 6d 6c 45 6c 65 6d 65 6e 74 4c 69 73 74 28 74 68 69 73 2e 65 6c 65 6d 73 29 29 7b 74 68 72 6f 77 22 55 6e 73 75 70 70 6f 72 74 65 64 22 7d 66 6f 72 28 76 61 72 20 65 3d 30 2c 74 3d 74 68 69 73 2e 65 6c 65 6d 73 3b 65 3c 74 2e 6c 65 6e 67 74 68 3b 65 2b 2b 29 7b 76 61 72 20 6e 3d 74 5b 65 5d 3b 5f 73 65 74 43 61 63 68 65 56 61 6c 75 65 28 6e 2c 63 5f 64 69 73 70 6c 61 79 2c 6e 2e 73 74 79 6c 65 2e 64 69 73 70 6c 61 79 29 2c 6e 2e 73 74 79 6c 65 2e 64 69 73 70 6c 61 79 3d 63 5f 6e 6f 6e 65 7d 72 65 74 75 72 6e 20 74 68 69 73 7d 2c 65 2e 70 72 6f Data Ascii: type.delay=function(){return this},e.prototype.hide=function(){if(!_isHtmlElementList(this.elems)){throw"Unsupported"}}for(var e=0,t=this.elems;e<t.length;e++){var n=t[e];_setCacheValue(n,c_display,n.style.display),n.style.display=c_none}return this},e.pro

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	152.199.21.175	443	192.168.2.6	49748	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	339	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: 1361702 Cache-Control: public, max-age=31536000 Content-MD5: mEyEiaw/euujjdOzfYEllw== Content-Type: application/javascript Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D9A884488F77AA Last-Modified: Mon, 15 Nov 2021 22:07:15 GMT Server: ECAcc (frc/8F10) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: d6360240-301e-0071-2c30-db1d53000000 x-ms-version: 2009-09-19 Content-Length: 194658 Connection: close
2021-12-02 15:37:58 UTC	340	IN	Data Raw: 66 75 6e 63 74 69 6f 6e 20 45 6e 63 72 79 70 74 28 65 2c 74 2c 6e 2c 61 29 7b 76 61 72 20 6f 3d 5b 5d 3b 73 77 69 74 63 68 28 6e 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 7b 63 61 73 65 22 63 68 67 73 71 73 61 22 3a 69 66 28 6e 75 6c 6c 3d 3d 65 7c 7c 6e 75 6c 6c 3d 3d 74 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 6f 3d 50 61 63 6b 61 67 65 53 41 44 61 74 61 28 65 2c 74 29 3b 62 72 65 61 6b 3b 63 61 73 65 22 63 68 67 70 77 64 22 3a 69 66 28 6e 75 6c 6c 3d 3d 65 7c 7c 6e 75 6c 6c 3d 3d 61 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 6f 3d 50 61 63 6b 61 67 65 4e 65 77 41 6e 64 4f 6c 64 50 77 64 28 65 2c 61 29 3b 62 72 65 61 6b 3b 63 61 73 65 22 70 77 64 22 3a 69 66 28 6e 75 6c 6c 3d 3d 65 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 6f 3d 50 61 63 6b 61 67 65 Data Ascii: function Encrypt(e,t,n,a){var o=[];switch(n.toLowerCase()){case"chgsqsa":if(null==e){return null}o=PackageSAData(e,t);break;case"chgpwd":if(null==e){return null}o=PackageNewAndOldPwd(e,a);break;case"p wd":if(null==e){return null}o=Package
2021-12-02 15:37:58 UTC	356	IN	Data Raw: 6e 67 22 29 29 2c 6e 3d 6e 7c 7c 24 66 2e 6c 6f 61 64 69 6e 67 54 79 70 65 2e 73 70 69 6e 6e 69 6e 67 2c 61 3d 61 7c 7c 22 32 30 70 78 22 2c 6f 3d 6f 7c 7c 61 2c 69 3d 69 7c 7c 22 33 70 78 22 2c 72 3d 72 26 26 72 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 7c 7c 22 23 36 36 36 22 2c 6c 3d 6c 7c 7c 22 22 3b 0a 76 61 72 20 75 2c 70 3d 22 63 5f 73 70 69 6e 6e 69 6e 67 44 6f 74 73 22 2c 6d 3d 28 24 43 6f 6e 66 69 67 2e 69 6d 67 73 42 61 73 65 7c 7c 22 2f 69 6d 61 67 65 73 22 29 2b 22 2f 63 6f 6d 6d 6f 6e 2f 22 3b 6e 3d 3d 24 66 2e 6c 6f 61 64 69 6e 67 54 79 70 65 2e 66 6c 79 69 6e 67 3f 28 70 3d 22 63 5f 66 6c 79 69 6e 67 44 6f 74 73 22 2c 75 3d 22 66 6c 79 69 6e 67 64 6f 74 73 2e 67 69 66 22 29 3a 28 75 3d 22 73 70 69 6e 6e 65 72 5f 22 2c 75 2b 3d 22 23 66 66 Data Ascii: ng"))),n=n \$f.loadingType.spinning,a=a "20px",o=o a,i=i "3px",r=r&r.toLowerCase() "#666",l=l "";var u,p="c_spinningDots",m=(\$Config.imgsBase "/images/")+"/common/";n=\$f.loadingType.flying?(p="c_flyingDots",u="flyingdots.gif):(u="spinner_",u+="#ff
2021-12-02 15:37:58 UTC	418	IN	Data Raw: 65 74 2e 70 61 67 65 54 69 74 6c 65 3f 7b 22 61 72 69 61 2d 6c 61 62 65 6c 22 3a 65 74 2e 70 61 67 65 54 69 74 6c 65 7d 3a 7b 22 61 72 69 61 2d 6c 61 62 65 6c 6c 65 64 62 79 22 3a 22 69 50 61 67 65 54 69 74 6c 65 20 44 69 61 6c 6f 67 55 73 65 72 54 69 74 6c 65 22 7d 3a 7b 7d 7d 66 75 6e 63 74 69 6f 6e 20 6a 28 29 7b 76 61 72 20 65 3d 24 50 61 67 65 48 65 6c 70 65 72 2e 67 65 74 28 65 74 2e 76 69 65 77 54 65 6d 70 6c 61 74 65 29 2e 63 6c 6f 6e 65 28 29 2c 74 3d 65 74 2e 76 69 65 77 43 6f 6e 74 65 78 74 54 6f 6b 65 6e 73 3b 69 66 28 74 26 26 74 2e 6c 65 6e 67 74 68 3e 30 29 7b 66 6f 72 28 76 61 72 20 6e 3d 65 2e 68 74 6d 6c 28 29 2c 61 3d 30 3b 61 3c 74 2e 6c 65 6e 67 74 68 3b 61 2b 2b 29 7b 76 61 72 20 6f 3d 74 5b 61 5d 2c 72 3d 57 28 6f 29 3b 76 6f 69 64 Data Ascii: et.pageTitle?{"aria-label":et.pageTitle};{"aria-labelledby":"IPageTitle DialogUserTitle"}:})();function j(){var e=\$PageHelper.get(et.viewTemplate).clone(),t=et.viewContextTokens;if(t&t.length>0){for(var n=e.html(),a=0;a<t.length;a++){var o=t[a],r=W(o);void
2021-12-02 15:37:58 UTC	434	IN	Data Raw: 64 69 76 20 63 6c 61 73 73 3d 22 72 6f 77 20 70 72 6f 67 72 65 73 73 2d 63 6f 6e 74 61 69 6e 65 72 22 3e 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 70 72 6f 67 72 65 73 73 22 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 75 62 6c 69 6e 65 20 69 6e 63 22 3e 3c 2f 64 69 76 3e 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 75 62 6c 69 6e 65 20 64 65 63 22 3e 3c 2f 64 69 76 3e 20 20 2 0 20 20 20 20 20 3c 2f 64 69 76 3e 20 20 20 20 3c 2f 64 69 76 3e 27 2c 77 3d 27 3c 64 69 76 20 64 61 74 61 2d 69 64 3d 22 6d 61 72 63 68 69 6e 67 41 6e 74 73 22 20 72 6f 6c 65 3d 22 70 72 6f 67 72 65 73 73 62 61 72 22 20 63 6c 61 73 73 3d 22 70 72 6f 67 72 65 73 73 2d 69 6e 64 69 63 61 74 6f 72 22 20 3e Data Ascii: div class="row progress-container"> <div class="progress"> <div class="subline inc"></div> <div class="subline dec"></div> </div>w=<div data-id="marchingAnts" role="progressbar" class="progress-indicator" >
2021-12-02 15:37:58 UTC	450	IN	Data Raw: 29 7d 29 29 2c 73 2e 6f 6e 28 22 72 65 73 69 7a 65 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 24 50 61 67 65 48 65 6c 70 65 72 2e 68 61 73 46 6f 63 75 73 28 72 29 26 26 64 2e 74 6f 6f 6c 74 69 70 26 26 28 64 2e 74 6f 6f 6c 74 69 70 28 22 68 69 64 65 22 29 2c 64 2e 74 6f 6f 6c 74 69 70 28 22 73 68 6f 77 22 29 29 7d 29 7d 65 6c 73 65 7b 72 2e 6f 6e 28 22 73 68 6f 77 2e 62 73 2e 74 6f 6f 6c 74 69 70 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 24 50 61 67 65 48 65 6c 70 65 72 2e 62 79 43 6c 61 73 73 4e 61 6d 65 28 22 74 6f 6f 6c 74 69 70 22 29 2e 6e 6f 74 28 74 68 69 73 29 2e 68 69 64 65 28 29 7d 29 3b 76 61 72 20 63 3d 7b 7d 3b 63 2e 61 6e 69 6d 61 74 69 6f 6e 3d 21 31 3b 76 61 72 73 2d 39 69 26 26 69 5b 74 5d 26 26 6e 5b 69 5b 74 5d 5d 3b 63 5b 74 5d 3d 75 7c 7c 6e Data Ascii:)))),s.on("resize",function(){\$PageHelper.hasFocus(r)&&d.tooltip("hide"),d.tooltip("show"))))));el se(r.on("show.bs.tooltip",function(){\$PageHelper.byClassName("tooltip").not(this).hide();var c={};c.animation=1;var u =i&&i[t]&&n[i[t]];c[t]=u n
2021-12-02 15:37:58 UTC	466	IN	Data Raw: 65 64 53 69 67 6e 49 6e 53 70 65 65 64 62 75 6d 70 22 3a 63 2c 22 62 61 63 6b 53 74 61 63 6b 22 3a 5b 48 2c 4d 5d 7d 7d 2c 22 65 76 69 63 74 69 6f 6e 53 70 65 65 64 62 75 6d 70 22 3a 7b 22 70 61 67 65 49 64 22 3a 46 2e 53 69 67 6e 75 70 5f 45 76 69 63 74 69 6f 6e 53 70 65 65 64 62 75 6d 70 50 61 67 65 5f 43 6c 69 65 6e 74 2c 22 73 65 63 74 69 6f 6e 49 64 22 3a 22 45 76 69 63 74 69 6f 6e 53 70 65 65 64 62 75 6d 70 22 2c 22 63 6f 6e 74 72 6f 6c 22 3a 7a 7c 7c 71 3f 22 53 69 67 6e 75 70 43 6f 6e 74 72 6f 6c 22 3a 22 53 69 67 6e 75 70 43 72 65 61 74 65 43 6f 6e 74 72 6f 6c 22 2c 22 6f 70 74 69 6f 6e 73 22 3a 7b 22 76 69 65 77 4d 6f 64 65 6c 22 3a 22 53 69 67 6e 75 70 56 69 65 77 4d 6f 64 65 6c 22 2c 22 76 69 65 77 4d 6f 64 65 6c 4f 70 74 69 6f 6e 73 22 3a 7b Data Ascii: edSignInSpeedbump":c,"backStack":[H,M]],"evictionSpeedbump":{"pageld":F.Signup_EvictionSpeedbumpPage_Client,"sectionId":"EvictionSpeedbump","control":z q?"SignupControl":"SignupCreateControl","options":{"viewModel":"SignupViewModel","viewModelOptions":{

[illegible]

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	152.199.21.175	443	192.168.2.6	49752	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	577	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: 11800248 Cache-Control: public, max-age=31536000 Content-MD5: nzaLxFgP7ZB3dfMcaybWzw== Content-Type: image/svg+xml Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D949CA9E99F66E Last-Modified: Sun, 18 Jul 2021 09:01:24 GMT Server: ECAcc (frc/8FED) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 53b4adb0-401e-0009-1d3f-7c07a7000000 x-ms-version: 2009-09-19 Content-Length: 3651 Connection: close
2021-12-02 15:37:58 UTC	577	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 31 30 38 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 31 30 38 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 34 34 2e 38 33 36 2c 34 2e 36 56 31 38 2e 34 68 2d 32 2e 34 56 37 2e 35 38 33 48 34 32 2e 34 4c 33 38 2e 31 31 39 2c 31 38 2e 34 48 33 36 2e 35 33 31 4c 33 32 2e 31 34 32 2c 37 2e 35 38 33 68 2d 2e 30 32 39 56 31 38 2e 34 48 32 39 2e 39 56 34 2e 36 68 33 2e 34 33 36 4c 33 37 2e 33 2c 31 34 2e 38 33 68 2e 30 35 38 4c 34 31 2e 35 34 35 2c 34 2e 36 5a 6d 32 2c 31 2e 30 34 39 61 31 2e 32 36 38 2c 31 2e 32 36 38 2c 30 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="108" height="24" viewBox="0 0 108 24"><title>assets</title><path d="M44.836,4.6V18.4h-2.4V7.583H42.4L38.119,18.4H36.531L32.142,7.583h-.029V18.4H29.9V4.6h3.436L37.3,14.83h.058L41.545,4.6Zm2,1.049a1.268,1.268,0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.6	49753	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	581	OUT	GET /images/dropdown_caret_KXSZjGsyILZaoTf0sI9X-A2.svg HTTP/1.1 Host: acctcdn.msauth.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 Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	152.199.21.175	443	192.168.2.6	49753	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	581	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: 5366395 Cache-Control: public, max-age=31536000 Content-MD5: 5h8LmH5/oEH5cNR2+nY3g== Content-Type: image/svg+xml Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D9846FFE07F84C Last-Modified: Fri, 01 Oct 2021 00:11:18 GMT Server: ECAcc (frc/8E8B) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 882c997f-901e-0047-44c3-b63aeb000000 x-ms-version: 2009-09-19 Content-Length: 224 Connection: close

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	582	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 33 36 22 20 68 65 69 67 68 74 3d 22 33 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 36 20 33 36 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 32 32 2e 34 38 34 6c 2d 38 2d 38 2c 2e 39 36 39 2d 2e 39 36 38 4c 31 38 2c 32 30 2e 35 34 37 6c 37 2e 30 33 31 2d 37 2e 30 33 31 2e 39 36 39 2e 39 36 38 2d 38 2c 38 5a 22 2f 3e 3c 72 65 63 74 20 77 69 64 74 68 3d 22 33 36 22 20 6 8 65 69 67 68 74 3d 22 33 36 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 2f 3e 3c 2f 73 76 67 3e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="36" height="36" viewBox="0 0 36 36"><title>assets</title><path d="M18,22.484l-8-8,.969-.968L18,20.547l7.031-7.031.969.968-8,8Z"/></rect width="36" height="36" fill="none"/></svg>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49695	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:42 UTC	9	OUT	POST /hergsl/rcopy.php HTTP/1.1 Host: pickup.acepickapart.com Connection: keep-alive Content-Length: 34 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: https://pickup.acepickapart.com Content-Type: application/x-www-form-urlencoded 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig ned-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Referer: https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-12-02 15:37:42 UTC	10	OUT	Data Raw: 74 6f 6b 65 6e 3d 4a 46 65 72 6e 61 6e 64 65 7a 25 34 30 77 69 63 6b 65 72 73 6d 69 74 68 2e 63 6f 6d Data Ascii: token=JFernandez%40wickersmith.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.6	49754	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	582	OUT	GET /images/favicon.ico?v=2 HTTP/1.1 Host: acctcdn.msauth.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 Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.6	49755	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	583	OUT	GET /oneds_EMWt_IK9fDTY6ZqY6xYrUA2.js?v=1 HTTP/1.1 Host: acctcdn.msauth.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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
------------	-----------	-------------	----------------	------------------	---------

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	617	IN	Data Raw: 56 6e 3d 22 69 73 49 6e 69 74 69 61 6c 69 7a 65 64 22 3b 66 75 6e 63 74 69 6f 6e 20 42 6e 28 6e 2c 74 29 7b 66 6f 72 28 76 61 72 20 65 3d 5b 5d 2c 72 3d 6e 75 6c 6c 2c 69 3d 6e 2e 67 65 74 4e 65 78 74 28 29 3b 69 3b 29 7b 76 61 72 20 6f 3d 69 2e 67 65 74 50 6c 75 67 69 6e 28 29 3b 6f 26 26 28 72 26 26 61 65 28 72 5b 55 6e 5d 29 26 26 61 65 28 6f 5b 44 6e 5d 29 26 26 72 5b 55 6e 5d 28 6f 29 2c 61 65 28 6f 5b 56 6e 5d 29 26 26 6f 5b 56 6e 5d 28 29 7c 7c 65 2e 70 75 73 68 28 6f 29 2c 72 3d 6f 2c 69 3d 69 2e 67 65 74 4e 65 78 74 28 29 29 7d 43 65 28 65 2c 66 75 6e 63 74 69 6f 6e 28 65 29 7b 65 2e 69 6e 69 74 69 61 6c 69 7a 65 28 6e 2e 67 65 74 43 66 67 28 29 2c 6e 2e 63 6f 72 65 28 29 2c 74 2c 6e 2e 67 65 74 4e 65 78 74 28 29 29 7d 29 7d 66 75 6e 63 74 69 6f Data Ascii: Vn="isInitalized";function Bn(n,t){for(var e=[],r=null,i=n.getNext();i;){var o=i.getPlugin();o&&(r&&ae(r[Un])&&ae(o[Dn])&&r[Un](o),ae(o[Vn])&&o[Vn]) e.push(o),r=o,i=i.getNext())}Ce(e,function(e){e.initialize(n.getCfg(),n.core(),t,n.getNext())})}function
2021-12-02 15:37:58 UTC	633	IN	Data Raw: 6b 7c Data Ascii: k]
2021-12-02 15:37:58 UTC	634	IN	Data Raw: 7c 7b 7d 2c 65 2e 73 64 6b 2e 76 65 72 3d 57 74 29 2c 61 2e 74 72 61 63 6b 28 6e 29 7d 7d 29 2c 65 7d 76 61 72 20 77 72 3d 28 6d 28 54 72 2c 62 72 3d 43 74 29 2c 54 72 29 2c 49 72 3d 61 65 3b 66 75 6e 63 74 69 6f 6e 20 50 72 28 6e 29 7b 76 61 72 20 61 3d 30 2c 75 3d 6e 75 6c 6c 2c 65 3d 5b 5d 3b 66 75 6e 63 74 69 6f 6e 20 69 28 74 2c 72 2c 69 2c 6f 29 7b 65 2e 70 75 73 68 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 65 3b 74 72 79 7b 28 65 3d 31 3d 3d 3d 61 3f 49 72 28 74 29 3f 74 28 75 29 3a 75 3a 49 72 28 72 29 3f 72 28 75 29 3a 75 29 69 6e 73 74 61 6e 63 65 6f 66 20 50 72 3f 65 2e 74 68 65 6e 28 69 2c 6f 29 3a 28 32 21 3d 3d 61 7c 7c 49 72 28 72 29 3f 69 3a 6f 29 28 65 29 7d 63 61 74 63 68 28 6e 29 7b 72 65 74 75 72 6e 20 76 6f 69 64 20 6f 28 6e 29 Data Ascii: {},e.sdk.ver=Wt(),a.track(n)})),e)}var wr=(m(Tr,br=Ct),Tr),lr=ae;function Pr(n){var a=0,u=null,e=[];function i(t,r,i,o){e.push(function(){var e;try{(e=1===a?lr(t)?t(u):u:lr(r)?r(u):u)instanceof Pr?e.then(i,o):(2!==a lr(r)?i:o)(e))catch(n){return void o(n)}}function
2021-12-02 15:37:58 UTC	650	IN	Data Raw: 3a 6e 75 6c 6c 7d 2e 70 72 6f 70 65 72 74 79 49 73 45 6e 75 6d 65 72 61 62 6c 65 28 27 74 6f 53 74 72 69 6e 67 22 29 2c 61 65 3d 5b 22 74 6f 53 74 72 69 6e 67 22 2c 22 74 6f 4c 6f 63 61 6c 65 53 74 72 69 6e 67 22 2c 22 76 61 6c 75 65 4f 66 22 2c 22 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 22 2c 22 69 73 50 72 6f 74 6f 74 79 70 65 4f 66 22 2c 22 70 72 6f 70 65 72 74 79 49 73 45 6e 75 6d 65 72 61 62 6c 65 22 2c 22 63 6f 6e 73 74 72 75 63 74 6f 72 22 5d 3b 66 75 6e 63 74 69 6f 6e 20 75 65 28 65 29 7b 76 61 72 20 6e 3d 74 79 70 65 6f 66 20 65 3b 6e 3d 3d 3d 61 7c 7c 6e 3d 3d 3d 7a 26 26 6e 75 6c 6c 21 3d 3d 65 7c 7c 63 28 22 6f 62 6a 4b 65 79 73 20 63 61 6c 6c 65 64 20 6f 6e 20 6e 6f 6e 2d 6f 62 6a 65 63 74 22 29 3b 76 61 72 20 74 2c 72 3d 5b 5d 3b 66 6f 72 Data Ascii: :null},propertyIsEnumerable("toString"),ae=["toString","toLocaleString","valueOf","hasOwnProperty","isPrototypeOf","propertyIsEnumerable","constructor"];function ue(e){var n=typeof e;n===a n===z&&null!==e c("objKeys called on non-object");var t,r=[];for
2021-12-02 15:37:58 UTC	666	IN	Data Raw: 2e 64 69 61 67 4c 6f 67 28 29 2e 77 61 72 6e 54 6f 43 6f 6e 73 6f 6c 65 28 22 46 61 69 6c 65 64 20 74 6f 20 73 65 6e 64 20 74 65 6c 65 6d 65 74 72 79 20 75 73 69 6e 67 20 73 65 6e 64 42 65 61 63 6f 6e 20 41 50 49 2e 20 45 78 3a 22 2b 75 29 2c 74 3d 30 7d 66 69 6e 61 6c 6c 79 7b 79 28 65 2c 74 2c 7b 7d 2c 22 22 29 7d 7d 66 75 6e 63 74 69 6f 6e 20 6d 28 65 29 7b 72 65 74 75 72 6e 20 32 3d 3d 3d 65 7c 7c 33 3d 3d 3d 65 7d 66 75 6e 63 74 69 6f 6e 20 72 28 65 29 7b 72 65 74 75 72 6e 20 71 26 26 6d 28 65 29 3f 32 3a 65 7d 66 75 6e 63 74 69 6f 6e 20 6f 28 29 7b 72 65 74 75 72 6e 21 46 26 26 4d 3c 65 7d 66 75 6e 63 74 69 6f 6e 20 74 28 29 7b 76 61 72 20 65 3d 4b 3b 72 65 74 75 72 6e 20 4b 3d 5b 5d 2 c 65 7d 66 75 6e 63 74 69 6f 6e 20 64 28 65 2c 6e 2c 74 29 7b 72 Data Ascii: .diagLog(),warnToConsole("Failed to send telemetry using sendBeacon API. Ex:="+u,t=0)finally{y(e,t,{},""))}}function m(e){return 2===e 3===e}function r(e){return q&&m(e)?2:e}function o(){return!F&&M<e}function t(){var e=K;return K=[],e}function d(e,n,t){r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.6	49759	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	633	OUT	GET /datarequestpackage_h-_7C7UzwdefXJT9njDBTQ2.js HTTP/1.1 Host: acctcdn.msauth.net Connection: keep-alive Origin: https://signup.live.com 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: */* Sec-Fetch-Site: cross-site Sec-Fetch-Mode: cors Sec-Fetch-Dest: script Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.6	49760	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	634	OUT	GET /images/2_vD0yppaJX3jBnfbHF1hqXQ2.svg HTTP/1.1 Host: acctcdn.msauth.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 Referer: https://signup.live.com/ Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
66	152.199.21.175	443	192.168.2.6	49759	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	680	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: 11713672 Cache-Control: public, max-age=31536000 Content-MD5: GpB463eVzCq5vobQLSGoUw== Content-Type: application/javascript Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D94AFF41500CE6 Last-Modified: Mon, 19 Jul 2021 21:50:42 GMT Server: ECAcc (frc/8F1B) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 5a741bc7-e01e-003f-7009-7d201f000000 x-ms-version: 2009-09-19 Content-Length: 8111 Connection: close
2021-12-02 15:37:58 UTC	681	IN	Data Raw: 21 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 65 29 7b 66 75 6e 63 74 69 6f 6e 20 74 28 65 29 7b 72 65 74 75 72 6e 20 65 26 26 65 2e 73 74 61 74 65 3d 3d 6c 26 26 28 65 2e 70 72 65 76 26 26 28 65 2e 70 72 65 76 2e 6e 65 78 74 3d 65 2e 6e 65 78 74 29 2c 65 2e 6e 65 78 74 26 26 28 65 2e 6e 65 78 74 2e 70 72 65 76 3d 65 2e 70 72 65 76 29 2c 44 3d 3d 65 26 26 28 44 3d 65 2e 6e 65 78 74 29 2c 24 3d 3d 65 26 26 28 24 3d 65 2e 70 72 65 76 29 2c 65 2e 73 74 61 74 65 3d 75 2c 65 2e 70 72 65 76 3d 65 2e 6e 65 78 74 3d 6e 75 6c 6c 2c 79 2d 2d 29 2c 65 7d 66 75 6e 63 74 69 6f 6e 20 61 28 65 29 7b 69 66 28 65 26 26 65 2e 73 74 61 74 65 3d 3d 75 29 7b 76 61 72 20 72 3d 24 3b 72 3f 28 72 2e 6e 65 78 74 3d 65 2c 65 2e 70 72 65 76 3d 72 29 3a 44 3d Data Ascii: !function(){function e(e){function t(e){return e&&e.state==l&&(e.prev&&(e.prev.next=e.next),e.next&&(e.next.prev=e.prev),D==e&&(D=e.next),\$==e&&(\$=e.prev),e.state=u,e.prev=e.next=null,y--),e}function a(e){if(e&&e.state==u){var r=\$;r?(r.next=e,e.prev=r):D=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
67	152.199.21.175	443	192.168.2.6	49760	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	689	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: 5059177 Cache-Control: public, max-age=31536000 Content-MD5: DhdiJYrICeaRJRG/y9mA== Content-Type: image/svg+xml Date: Thu, 02 Dec 2021 15:37:58 GMT Etag: 0x8D98583D2C8CF51 Last-Modified: Sat, 02 Oct 2021 09:05:47 GMT Server: ECAcc (frc/8F36) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: ddee09dd-a01e-003d-3f8f-b92d72000000 x-ms-version: 2009-09-19 Content-Length: 1864 Connection: close
2021-12-02 15:37:58 UTC	690	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 31 39 32 30 22 20 68 65 69 67 68 74 3d 22 31 30 38 30 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 3e 3c 67 20 6f 70 61 63 69 74 79 3d 22 2e 32 22 20 63 6c 69 70 2d 70 61 74 68 3d 22 75 72 6c 28 23 45 29 22 3e 3c 70 61 74 68 20 64 3d 22 4d 31 34 36 36 2e 34 20 31 37 39 35 2e 32 63 39 35 30 2e 33 37 20 30 20 31 37 32 30 2e 38 2d 36 32 37 2e 35 32 20 31 37 32 30 2e 38 2d 31 34 30 31 2e 36 53 32 34 31 36 2e 37 37 2d 31 30 30 38 20 31 34 36 36 2e 34 2d 31 30 30 38 2d 32 35 34 2e 34 2d 33 38 30 2e 34 38 32 2d 32 35 34 2e 34 20 33 39 33 2e 36 73 37 37 30 2e 34 32 38 20 31 34 30 31 2e 36 20 31 37 32 30 2e 38 20 31 34 30 31 2e 36 Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="1920" height="1080" fill="none"><g opacity=".2" clip-path="url(#E)"><path d="M1466.4 1795.2c950.37 0 1720.8-627.52 1720.8-1401.6S2416.77-1008 1466.4-1008-254.4-380.482-254.4 393.6s770.428 1401.6 1720.8 1401.6

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
68	192.168.2.6	49761	142.250.203.97	443	C:\Program Files\Google\Chrome\Application\chrome.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	692	OUT	GET /crx/blobs/Acy1k0bLljHsvnKaKN_oRpVaYyVFs25d7GKYF1WXrT6yizCMksBOOc_ggE0B6tx6HPRHe6q1GOEe3_NclbSiGG8kXeLMUY0sAKVvC6R89zvKM13s5VqoAMZSmuUgjQL5vlygJuArQghXXE_qTL7NIQ/extension_8520_615_0_5.crx HTTP/1.1 Host: clients2.googleusercontent.com Connection: keep-alive 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-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
69	142.250.203.97	443	192.168.2.6	49761	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	692	IN	HTTP/1.1 200 OK X-GUploader-UploadId: ADPycdsI6XF5sFh67FBM0DwnOVnu0_-zM0NniXmKXmMqe5hGEnEr7klJ0bzNCCrppxvYrff18vP9h3fm0endZdFzFj4 Date: Thu, 02 Dec 2021 13:59:38 GMT ETag: 730d2491_a246e948_e80d9c94_d8b3f142_86eb8dd2 Expires: Fri, 02 Dec 2022 13:59:38 GMT Last-Modified: Wed, 05 Aug 2020 01:15:29 GMT Content-Type: application/x-chrome-extension Accept-Ranges: bytes X-Goog-Hash: crc32c=DxAZGA== Content-Length: 768843 Server: UploadServer Age: 5900 Cache-Control: public, max-age=31536000 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" Connection: close
2021-12-02 15:37:58 UTC	693	IN	Data Raw: 43 72 32 34 03 00 00 00 18 04 00 00 12 ac 04 0a a6 02 30 82 01 22 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 8f fb bf 5c 37 63 94 3c b0 ee 01 c4 b5 a6 9a b1 9f 46 74 6f 16 38 a0 32 27 35 dd f0 71 6b 0e dc f6 25 cb b2 ed ea fb 32 d5 af 1e 03 43 03 46 f0 a7 39 db 23 96 1d 65 e5 78 51 f0 84 b0 0e 12 ac 0e 5b dc c9 d6 4c 7c 00 d5 b8 1b 88 33 3e 2f da eb aa f7 1a 75 c2 ae 3a 54 de 37 8f 10 d2 28 e6 84 79 4d 15 b4 f3 bd 3f 56 d3 3c 3f 18 ab fc 2e 05 c0 1e 08 31 b6 61 d0 fd 9f 4f 3f 64 0d 17 93 bc ad 41 c7 48 be 00 27 a8 4d 70 42 92 05 54 a6 6d b8 de 56 6e 20 49 70 ee 10 3e 6b d2 7c 31 bd 1b 6e a4 3c 46 62 9f 08 66 93 f9 2a 51 31 a8 db b5 9d bf 0f 73 e8 a0 09 32 01 e9 7b 2a 8a 36 a0 cf 17 b0 50 70 9d a2 f9 a4 6f 62 4d Data Ascii: Cr240"0"H0\7c~Fto82"5qk%2CF9#exQ[LJ3>/u:T7(yM?V<?.1aO?dAH'MpBTmVn Ip>k 1n<Fb*Q1s2[*6PpobM
2021-12-02 15:37:58 UTC	693	IN	Data Raw: 4d 62 68 3d 9f 5b 4f 7d b2 2b 1b ae 55 af 4b 48 46 28 6e 33 e8 5c 22 d7 dd d8 2c 67 d7 63 0e b5 8a 36 29 13 10 28 dd 45 ed ff 00 55 db fa ff 23 92 69 ad 61 03 e7 3a 04 98 9f 4e 89 fd 0a 1d 0e 50 88 1b a9 78 ef 4f a0 90 ea 28 6d 43 3b 7c eb 35 01 53 ac 7b 6d ea 61 45 78 8d bb 91 5b 7f 98 66 50 af 69 60 85 79 cc c2 35 b1 88 52 02 84 8b 90 76 7f 24 1a cf 2e b4 00 bd 6c 2d 6d ee b5 02 03 01 00 01 12 80 01 9a a3 91 dc 6d 10 04 8c cf 6e 69 83 be 14 60 f5 b7 57 06 05 84 19 a6 52 d1 70 e4 62 bd 2b 89 10 ce 8a 2b b9 5c 6b b6 52 24 65 7e dd 8b 4a 5c 9d 26 63 25 a7 64 ae 9d cf 4d c4 e8 6a a0 8b 56 bf 25 07 ad df 2b 31 46 b1 a4 03 be 44 03 85 83 96 58 5c 95 31 63 74 0b 3c 94 86 b1 c4 02 1c 96 fa 45 06 42 df 2b c1 69 40 01 eb fe 38 f4 9c 5e 9b b9 c5 26 59 52 ca e6 0a Data Ascii: Mbh=[O]+UKHF(n3l",gc6)(EU#a:NPxO(mC:[5S{maEx[fPi'y5Rv\$.l-mmn1"WRpb++kR\$~Jl&c%dMj)V%+1FDXl1ct<EB+i@8^&YR
2021-12-02 15:37:58 UTC	695	IN	Data Raw: 78 7e fb f1 fa df 70 f1 7f ee ae bf bc b8 bd bf bc f6 b4 fe 04 8b 3b 2e cb cd aa 58 57 a2 6a 15 40 46 b0 99 55 06 9e 99 69 25 32 27 d9 60 40 0f c3 54 2a 57 e8 61 24 24 d0 59 30 1d a0 d3 c5 2c ef b6 1e 00 31 f7 64 d3 b3 96 91 0f 99 4e 45 d3 31 4b 63 4d 47 0d f6 3b ea d5 06 08 c9 60 85 f7 ca 04 25 25 9f d1 eb e0 30 31 ee e2 c8 60 5c 26 20 9b 40 82 ca bc 08 da b0 e5 57 6c c7 37 d9 13 d3 66 94 a2 02 c8 10 01 4a 8a 75 0a 02 4f 27 45 fc eb 39 a8 70 74 38 02 1d ce 67 3f 7e f9 7c 7f 53 7c fe f1 fa f2 f2 b6 bc fb 49 0e 7e 16 5f 5f 17 57 1f ae ef ef be fd 2c bf 62 84 7f 9d 4c 4f 86 e3 d1 3f f2 e9 37 ac 64 e8 09 9b c1 f6 4e c5 df d9 64 7c 3d 90 58 af d6 98 13 78 29 d7 57 e5 43 62 fe 97 8a 29 d1 c9 7a 84 dd 7d 2c 6f 7e 3f 71 df 50 bb c6 40 f5 11 12 fc 4a 41 d6 77 82 Data Ascii: x~p;XWj@FU!%2"@T*Wa\$S\$Y0,1dNE1kCMG;`%0%01`& @WI7fJuO'E9pt8g?~ S ~__w,bLO?7dNd =Xx)WCb)z},o~?qP@JAw
2021-12-02 15:37:58 UTC	696	IN	Data Raw: 85 47 b6 62 5b 97 15 31 5f ec 34 e8 4b 82 df 3b dd f5 26 a3 7f 47 af 7c 4f 33 bc 69 98 32 ae b8 bf d7 fd c4 f6 f6 dd cd f5 fd ea 73 79 fb f1 fa fa 0e db dc 56 69 d7 74 4c 2d f0 51 c0 2e ca 67 19 00 85 20 ac 64 d1 02 96 dd 08 6b 75 1c 99 59 5b 6d c2 d8 10 64 d5 21 60 db 48 3b c1 17 9b 72 85 d9 7a 55 d3 94 b3 da 5b 88 6f ed 83 75 3a 28 eb d8 8e 03 44 7d 1d 23 9d 94 a5 77 f7 49 08 6d 8c f6 c4 ac 17 7b 72 0d 3c 7d f7 e9 f9 f1 27 92 21 1e b7 99 d9 71 66 8c c6 2c 6e 57 e2 42 8c 11 02 34 a3 9c 07 7d 66 c2 48 76 bb 52 52 ce b1 d1 ad 03 52 f6 f2 b8 bc 8f 6a 88 6d 14 4c 7f d8 f0 8d bb ba 11 3c ff 12 a7 07 13 0c 5e c3 bf 50 cc a5 08 3d 9b a9 55 ce fa 74 f5 a1 96 a3 d2 de 0c c5 64 d8 98 28 0a a2 fb 4d 81 fe 42 95 98 ec c9 ee e4 85 b6 50 d2 fa 13 3b 6f 4d a9 8a 6b 70 Data Ascii: Gb[1_4K;&G O3i2sVtL-Q.g dkuY[md]'H;rzU[ou:(D)}wlm[r<']qf,nWB4}fHvRRRjmL<^P=Utd(MBP,oMkp
2021-12-02 15:37:58 UTC	697	IN	Data Raw: 47 db bf 69 0a 4c a8 7a 35 e0 b4 32 78 98 5f f0 c0 fe bf 7b 6e 0d 7a 41 c1 15 1a 87 ac ed aa c2 65 ab 73 76 7b 28 59 ef 09 08 94 0f 15 ea ed f9 b8 9e b5 26 fe 56 14 e4 a7 82 b2 0f 86 9d 94 7e 3c 9c a1 0a eb 03 a7 f1 38 22 a2 f5 35 e6 21 34 3d a9 cb cd 69 05 ec 3e 56 a7 a1 33 e1 bd f6 0a a2 05 c2 86 ed a8 fd 8e 3b 8d 4f df ce 8d 00 86 c8 e0 4e 48 3d 79 a7 f6 2c 3f 1a 0d 97 d3 c9 62 9e 4f 97 c3 a3 a3 d1 7c 34 19 0f 4f 97 87 93 b3 b3 7c 3c 9f ed aa 81 3b 9d 9f ca 59 1c 8d 26 cb bf 2f 86 a7 a3 f9 fb 5d 09 5c fd 4b 24 1c 0e c7 87 f9 e9 f2 d5 62 3e 9f 8c 3f 39 a4 27 d9 53 09 93 f1 1c 16 00 b3 c8 67 d5 9a 76 85 70 7d f2 44 c8 d1 e8 68 39 9e cc 97 f3 69 b2 0c ae c5 92 8c 8f 3c fe f3 a3 57 c3 c3 37 cf fc 6c 38 3a 5d 1e 8f f2 d3 a3 5d 41 dc a9 d5 7e 41 c7 93 e9 d9 f2 Data Ascii: GiLz52x_{nzAesv{(Y&V~<8"5!4=>V3;ONH=y,?bOJ4O <;Y&/J K\$b>9'Sgvp)Dh9?W7!8:]]A~A

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	758	IN	Data Raw: f1 91 87 c4 b6 01 97 ba 81 34 9b 40 35 57 97 68 e1 2d 1d ae 7d 6a 4c dd b0 b4 e1 dd 90 9b a1 3c 74 03 5c 12 20 8e 81 e5 5a a6 14 f4 9f 9b 24 3b e3 02 d0 da df 05 bb 7c 57 27 c0 b8 ba 26 5a d1 68 45 b9 4d f3 a4 26 4d f9 3d f7 ee 83 62 74 dd b3 2c 0f ce 4d cb b2 cc 73 ef d3 26 15 43 0d dd 36 40 48 5e 00 5a 31 3c a0 fe f9 d0 31 a6 6c 4a 0e cb 16 aa c5 77 5d d3 f5 6d 43 b7 74 18 49 c3 a3 fc 58 a4 58 f0 f9 39 04 26 b9 c2 87 15 a0 7e 3c df 81 0f 03 81 b0 7b a0 5d 70 d4 01 24 2e 66 b7 40 9b 26 75 e4 05 58 41 a0 58 2c 83 00 3e d8 c6 21 30 0d ec cf 09 ac 80 e6 49 0a c2 c2 69 5a cf 8e 6d ea 36 fc 82 a5 75 cb c2 ea 24 cf 13 f0 a7 18 eb 42 7e 00 06 b1 16 17 11 0b 02 4b 8a ee 7b 36 d2 d6 41 8b 01 08 db 43 d8 c0 d9 ae 9c 87 70 8b e0 54 44 23 af f7 09 b8 eb bb 5d b2 69 Data Ascii: 4@5Wh-)jL<t\ Z\$; W&ZhEM&M=bt,Ms&C6@H^Z1<1Jw]mCtiXX9&-<[j]p\$.f@&uXAX,>!0i,iZm6u\$B-nK{6ACpTD#]j
2021-12-02 15:37:58 UTC	759	IN	Data Raw: c3 66 e0 c8 37 77 d0 03 c9 b6 95 21 14 f7 12 f6 87 87 f8 17 f8 89 26 82 a9 1e ee 30 a0 22 dd 31 90 46 10 0d 18 d6 96 ca f6 36 69 8e 49 5a b5 e3 51 dd 26 96 8e c3 e9 db a8 2a 43 8a cd 6f 60 e2 fc 32 61 39 2e 09 5f 5a d3 e1 30 d6 73 f0 04 bb 3a 8e 03 9a 24 48 fd 00 69 40 05 4b 93 8d 2f b9 d0 e1 7e e1 45 30 e5 c5 74 99 70 79 9f 12 7a 5e 58 b6 7e 83 f4 a2 df 77 75 90 0b 24 a0 d7 87 20 08 9f 5e bb b9 96 74 3c ff c4 eb 67 fa 19 2c 98 d4 45 2a 1a 21 d7 a6 97 ab a6 ed 40 b4 a0 a6 1c f9 3a e0 c4 cb 55 42 55 b3 c4 10 2d 4a d3 ea 27 f9 b6 2c f8 22 7f ff 7b 15 79 2b bf df b5 8a eb f8 4e 00 78 75 0d a0 17 0e 3a 40 ec 7c e6 9f 28 74 24 29 ab 2a 26 60 84 8a e6 fe ae 81 1e d4 0f 20 64 4c 48 4f 5d 91 c0 8e 9c 12 11 2f c9 7d 52 6e c5 4d 8d 1b 00 9d d1 d4 07 00 6a 54 a5 1f Data Ascii: f7w!&0"1F6ilZQ&*Co"2a9._Z0s:\$Hi@K/-EO^tpyz^X-wu\$ ^t<g,E"!@:UBU-J-,"{y+Nxu:@([t\$)& dLHOJ])RnMjT
2021-12-02 15:37:58 UTC	761	IN	Data Raw: ed c7 d3 1b 09 1e 15 ad 8b c2 78 b9 9a ad ef e2 45 fc 36 66 45 d6 9b 52 c5 fb 40 b2 b7 e9 68 f9 21 9c f7 57 be 8a df 24 2f ab c9 fb c9 f4 83 64 ab 6a 1b 25 db bb 78 18 f5 a3 bd 42 6b f4 78 58 dc 4e a7 cb 77 93 68 21 45 55 f5 1a 99 e4 e4 63 24 93 95 e2 9d 00 66 b7 b8 59 8f 00 c8 a8 de e5 14 5c b3 90 e0 4b f5 8c a9 b5 44 a4 80 36 c3 68 12 cb 88 b6 7a 5e f6 dc 6e 19 df 46 58 b0 74 f0 14 d7 7b ad e1 2d 63 b3 49 34 58 8a 55 4b f1 51 bc 20 d7 31 3e 21 24 e7 e5 70 30 88 66 cb f0 ed 58 3a 3b aa 0b d2 7e 3f 37 d3 a9 b4 12 95 0e ed f7 30 8b e6 23 ec 4a da 8e e2 2d bb 17 9c 4a a7 12 83 29 84 7a bf 83 d5 24 86 54 18 8f e3 9b 58 11 13 d5 73 38 95 af 61 bc 18 84 f3 21 cd d4 28 9e df 86 aa a3 a8 7a ae ab f2 35 8a 27 11 83 97 35 4e f6 44 41 3e aa 5b 31 95 23 e6 a3 87 e4 Data Ascii: xE6fER@h!W\$[dj]%xBkxXNwhl!EUc\$FYKD6hz^nFXt{<cl4XUKQ 1>!\$0fX;::~~?70#J-L)z\$TXS8a!(z5\$NDA>[1#
2021-12-02 15:37:58 UTC	762	IN	Data Raw: 1f df 2d 6f ef 6a 6e 34 cb ae ff b3 b8 f9 74 bf fc 74 5f b1 e6 49 56 33 b1 19 4c 7e 96 f5 cf 6b ce 90 07 14 7a 80 a5 a0 8f be 7d 4b c8 69 f6 f9 c3 a6 a8 fe 72 52 fe f7 db 2f 4b 21 c4 5f 4e ee 3e 97 9f 9a ff 94 9d 0f b7 cb d5 af 6f 8f 3e dc df 7f be 7b 7e 72 72 f7 e5 f3 e7 9b db fb e3 f7 b5 a0 8e 17 37 bf 9f 2c 1e d8 7f 52 7e ba fb e7 f2 f6 44 fa 3a ee bc 74 df 2a ed ba dc b7 ef 97 f7 30 7e 36 ff 58 7e fa 9f b7 47 0d e1 6a 92 ce e2 63 79 77 07 3f de 2e ff f7 cb 6f b7 cb 77 cf e2 8a 60 e0 a7 f7 cf ee 3e dc fc 13 7e fc d3 fd cd e7 e3 bb 2f ab d5 6f 8b df 60 73 67 cb e5 bb 79 b9 a8 48 d5 2c 00 ef 63 ac 91 1a e6 b4 4a 0a 9b 67 ac 7d 04 e1 97 16 d9 2c b6 15 ec f7 62 0c 59 6d 9a 7d f8 1c 7c 7e 0c 74 ea f9 c1 da c0 0a 2b db 25 4d 19 a5 c9 ec 96 95 26 96 e1 77 64 b5 f1 Data Ascii: -ojn4tt_IV3L-kz)KirR/K!_N>o>{-rr7,R-D:=0-6X-Gjcyw?.ow>-/o^sgyH,cJg),bYm)]-t+%M&wd
2021-12-02 15:37:58 UTC	763	IN	Data Raw: a3 29 3c 60 8d 2b d7 93 b7 5d 0b 7a e8 b1 e7 34 d8 d9 cf 3d 4a c1 63 24 51 d1 5e 8c 74 c2 79 48 bf eb 63 37 e3 12 b5 1d cc e5 16 26 3e 14 eb 1c 7c 6c d5 8c fe f7 3c b6 aa ca cc 4a 49 2f 95 f1 2e 37 5e 50 fe c5 8a 1c da 3d 53 87 6d f8 85 e2 42 e3 e5 d6 8a c1 39 41 82 ca d9 f2 ee 1f 64 1e 5d 62 34 60 9c 7a b5 22 1b c5 f3 3f 4e 02 1e 74 d7 2a ed ba dc d2 18 99 b1 e5 29 47 61 2c 03 91 03 45 5b 15 4a 41 98 06 fe 28 2b 40 b8 3f b4 38 f7 63 2d e6 bb f3 7d 7b 29 b1 ed bc 36 4a 89 1a 1c 8d b7 10 cf 72 6d bd 51 da f1 27 1a 3b 32 bf 24 6a 40 3a b7 5f 1c a9 17 65 44 a6 55 ae bd d0 46 68 61 95 e1 5d e0 8e 93 63 23 64 75 6a ed b4 32 b9 b7 42 e8 7c 67 19 8d 03 4c 87 ea 14 4e 4c 1e cc 2d 82 c3 53 ee a4 37 2e 1a 05 9d 38 c3 1f 4a 8c e7 a8 22 da d4 55 98 fc ae a5 14 49 47 Data Ascii: <-+jz4=Jc\$Q^tyHc7&> <Jl/.^?P=SmB9Ad]b4"t"?Nr^p)Ga,E[JA(+@?8c-)}6JrmQ;2\$@:_eDUFha]c#duj2B]gLNL-S7.8J"UIG
2021-12-02 15:37:58 UTC	764	IN	Data Raw: 6c b4 fc 47 95 a9 82 ee c7 8c 22 7a a9 e3 a7 1d 79 ac cf 5f fe 5f 0b 31 1c 77 0c 7c f5 4b dc a9 cd ad d4 12 52 77 65 b4 02 1c f8 98 23 5e 26 a2 ec ba 82 99 34 f6 7a 59 95 b7 ac 4e 5e 32 58 9f 94 ba 19 c9 a6 cc 49 b5 4f 83 19 aa fc 4e b8 2a 29 87 fc bc 2e 7c 0a ef f8 f4 7c 7b 8d 49 e0 54 6d ff 5b 06 0e 60 b8 f7 3e af eb 03 5a db 2c 11 76 d0 f9 12 2e ff cf 43 cd d6 a9 1a c0 3a e7 32 95 0b 6b 20 03 63 c1 2c 8a ad bb 1a 74 0f d8 08 e1 42 0a 9a 82 83 fe b9 59 0e c3 97 9f 97 e6 38 ad 54 05 27 9c ca 73 e5 bd f6 3c da 4f 15 5e 9c 36 da 6b ab 33 c8 aa ab da 82 4e b9 a0 56 39 03 cb 16 db ac 5a 8b 93 03 03 3b 6a ee fb f9 2c 5c b6 6d a8 87 ad 98 cc 64 da e9 0c 92 1f c8 80 2c 28 7c 3a bc b4 eb 3c 71 bc 12 2e 33 5e 09 2f 9d 84 8c 55 6e b9 9e 78 c0 e5 ec c3 ad 15 94 c9 Data Ascii: IG"zy_1w]KRwe#^&4zYN^2XION*). [fITm]">Z,v.C:2k.c,tBY8T's<O^6k3NV9Z;],md,(l:<q.3^/Unx
2021-12-02 15:37:58 UTC	766	IN	Data Raw: 00 68 aa 48 9b e1 98 d1 93 fe e4 a2 98 11 c3 60 5e 30 86 06 87 b4 10 52 96 08 18 4e bb 57 95 17 23 3b 60 3a 91 1f a8 00 44 25 ec 62 0e 58 9b e7 af ba d3 31 19 c0 bd 52 e8 61 c0 45 97 ba 2f e6 9d 50 cd f3 e3 a2 20 e1 99 ab 31 37 cf 4f 07 dc 16 b8 c3 b2 66 c4 f5 f0 62 7a 49 46 70 6f b2 fc f6 ed 5f 50 4b 07 08 5b 19 f5 c3 bf 11 00 00 ee 56 00 00 50 4b 03 04 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 68 69 2f 03 00 50 4b 07 08 00 00 00 02 00 00 00 00 00 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 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 68 69 2f 6d 65 73 73 61 6f 65 73 2e 6a 73 6f 6e cd 1c d9 72 1b 37 f2 57 b8 5a 3f 6c 52 b2 84 1b 18 6f b2 29 9a 1c c9 8c 25 Data Ascii: hH^"0RNW#::D%bX1RaE/P 17OfbzIFpo_PK[VPK*Q_locales/hi/PKPK)Q_locales/hi/messages.jsonr7WZ?IRo)%
2021-12-02 15:37:58 UTC	767	IN	Data Raw: e2 4c 32 80 45 42 09 94 ab cf c5 2f 5b 58 d2 67 16 e2 12 d1 26 c4 75 9d e4 0b 0e 2a 56 b2 82 83 83 83 80 8e 2c c0 22 59 a7 01 1d 0e 4c 57 64 d4 95 66 43 d4 d4 95 09 0d c1 bc d5 e0 25 24 03 60 ee 0e 6f 01 27 2e 32 34 a3 74 c6 af 57 60 e6 05 07 ca 6b 40 bd 92 6f 9a 5b 58 6c 50 0c d7 d0 5c 2b c1 14 e0 00 79 0a 93 12 8e 4b 62 91 35 de d5 0a 70 38 0e fe 09 03 8c 2f 0a 49 ae 47 e9 2b d7 f5 4a 55 a5 09 05 64 26 16 d8 0e c9 89 a1 a5 8d 79 05 42 a1 a5 14 9d 7f b5 d2 ec 15 2c 10 5e 20 2a 79 59 0b b1 c4 0f 4f 9a 3d 2b 92 73 0e d7 2b 3f 26 32 41 3d 62 a9 88 f2 d1 05 02 cd 70 f4 ca b0 08 71 8f 38 92 ba 26 81 bb 44 37 73 9c 74 e0 53 2c 11 df c2 ad 49 da 14 6f e8 f6 91 c4 49 04 8b b6 99 98 97 99 8c fe 21 4c cf 24 da 8d a5 f1 1b 73 8e e9 82 f4 0f 45 6c 4c 78 a3 84 11 ba Data Ascii: L2EB/[Xg&u^V,"YLVdfCM%\$'o'.24tW^k@q[XIP\+yKb5p8/Ig+JUd&yB,^*yYO=+s+?&2A=bpq8&D7stS,lo!L\$SsEILx
2021-12-02 15:37:58 UTC	768	IN	Data Raw: 6a 20 3c d5 fa 78 33 4e b9 b5 32 9a 49 65 40 d9 59 35 b8 a3 0c 99 72 6f 12 85 a8 e0 87 27 25 a2 9e c4 21 a2 a3 68 c1 fa cb be 74 15 d7 d8 77 22 76 4e 52 44 b0 b7 8d 8c 38 6d 04 e3 10 23 0a f8 b1 30 05 3d 63 ca 91 8c e2 64 9c 28 dc a7 81 e3 83 83 ff 17 c2 39 89 3b d7 24 a3 3f 78 5c 4d 01 62 2c 0b 0b 72 ed 98 66 90 b9 7d 1d 53 08 46 ec e8 d4 6f 61 21 09 02 8d a9 6a 2d c0 7d 51 68 92 ff 58 f0 c4 d5 e3 f4 27 42 56 19 3a 35 c6 24 8c 06 f8 ed 8b aa d9 ab 39 e8 2d 24 62 52 82 fa 92 c9 28 92 93 a6 98 1a d6 83 91 13 40 1f 70 58 4e 81 59 e3 34 37 ff be 25 8e 8d ad f5 f5 da bc 6d 71 a3 a6 96 61 e0 a8 38 f8 73 6e 0b 90 7c f0 01 09 b5 42 de 7b 97 c5 90 2a 69 a2 62 e5 67 d4 d4 b1 b9 47 32 1c 95 e3 52 e0 02 f5 bb 30 d9 70 fd 2e 30 b3 e9 23 24 d8 c4 a6 d0 40 d4 51 cd 35 Data Ascii: j <x3N2le@Y5ro%lhtw^vNRD8m#0=cd(9;\$?xIMb,rf)SFOajj-QhX^BV:5\$9-\$bR(@pXNY47%mq88nB]#^ibgG2R0p.O#\$@Q5

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	793	IN	Data Raw: d5 f5 bb cb cb 9b 30 b1 95 8c ab 76 28 28 b9 02 1b 2a 66 b4 06 3c 60 89 a4 48 46 81 de 81 b6 90 4f fb ce 45 aa 3a c4 bd 6c a8 68 29 dd f0 5f 5a 4b 5d d3 8c cd 4d f0 b3 83 c1 e3 c1 8b 71 43 c4 48 88 5c 6e ac 54 d0 db 4b 95 b6 de e7 a3 10 03 06 9b ed 07 40 07 56 33 83 57 ef 1f 1f bf f7 3f dc eb 1c ac dc 3f c4 49 93 57 73 2a 27 85 20 e0 16 9a 29 03 ca d2 44 50 f4 b8 ea 5e 69 e1 a1 09 a1 72 01 ce 5c c3 62 42 b1 08 c9 3b 1d 2a 34 7c 1f 2e 4b 52 80 2c d6 70 f8 2f 54 6d 4a 2c 2a 48 dc 63 e0 67 70 db f1 3a 3a 1e 08 e7 3d d2 d4 a4 8b b6 be dc d2 0b df 83 20 07 eb d2 56 28 25 09 17 0a 82 89 b8 13 10 a1 50 20 de cb 41 54 d7 ca 78 16 a0 a2 bf e3 5a d6 64 ea c1 72 76 3a 68 05 54 b2 c1 de d1 f0 e6 4e 5b 18 a9 18 a1 50 ce 99 85 62 a8 2c 7a d6 1b 1b 60 1d 25 ca 78 18 71 Data Ascii: 0v((*f<`HFOE:lh)_ZK]MqCHnTK@V3W??!Ws* )DP^ir!bB;*4].KR,p/TmJ,*Hcgpp:= V(%P ATxZdrv:hTN [Pb,z`%xq
2021-12-02 15:37:58 UTC	794	IN	Data Raw: e9 2c c7 f9 74 f5 fb 72 78 9a 2f 5e ef 53 c0 aa 61 42 61 34 9c 8c b2 d3 d5 f3 e5 62 31 9d a4 3c a4 97 5d 53 0a d3 c9 02 04 00 2e b2 b9 93 69 9f 08 36 4e 4c 88 8c f3 f1 6a 32 5d ac 16 b3 44 0c ac 43 4e d6 1f 67 d9 f8 f9 70 f4 72 95 9d 0d f3 d3 d5 71 9e 9d 8e f7 09 61 d7 dd fa 09 1d 4f 67 67 ab 71 36 1f cd f2 f3 54 2c e4 6c ab 9f da 8b 6c 38 ce 66 fb 34 b0 ce a9 9f c6 f9 6c 7a 76 be 48 d4 93 8e 6f fa 49 cc b2 df 97 f9 2c 4b 54 83 4d 8e fa a9 2c 5e 9f 67 07 cc 9d 0e f7 13 52 67 f9 6c 36 9d e5 93 93 d6 77 57 f3 e5 73 a7 23 f8 2a 71 63 04 48 25 04 27 d9 e2 d5 74 f6 12 fc e8 f8 38 9b 39 77 7c 95 1f e7 89 be 11 ac de 4b aa 4f 40 ec 9d a2 5e 22 f3 e1 59 86 b2 82 9d d3 f4 52 79 e5 6c b6 3a 1f 25 aa 49 f1 4d 4a 63 ba bf 0a bb 5a 9a 2c 3b 9f e5 17 c3 d1 eb d5 78 b8 Data Ascii: .trx/^SaBa4b1<]S.i6NLj2]DCNgrpqaOggq6sT,ll8f4lvzHol,KTM,*gRgl6wWss**qcH%t89w]KO@^^YRyl:~%IMJcZ,;x
2021-12-02 15:37:58 UTC	795	IN	Data Raw: 67 39 8e 47 8a 49 9e 6e 7d 8a 69 91 39 64 e2 78 dc 73 5c a0 b1 a0 8d f2 06 94 ad 80 0b 7a a9 0a a7 25 7b 59 74 cc 2b bb 56 a6 24 b0 e5 5a 3a 73 85 f4 6e ae b1 a0 37 b9 30 b3 71 0b 56 29 69 44 e1 b5 96 b0 11 a1 2d bf 85 fa 50 5e d5 54 a6 54 e0 44 1c d1 4a 66 2a 27 3f 2c 82 e3 d6 fa bf e9 72 93 d2 5a e3 ee df 4b 74 4a 2a d9 79 94 46 dc 26 b6 d3 48 bb b1 00 29 7e 12 ee f2 38 f1 c5 8a 20 80 31 c6 49 e1 95 0f d6 b3 ce c0 93 4d c7 5d 25 01 17 ba 28 7c e1 4c a5 5b 26 18 ed 8a 3c 77 e7 aa 69 3c d5 56 23 15 2f 40 39 95 33 85 f5 c1 58 27 1d eb 98 f0 f5 23 e3 13 95 e5 9a fa ca ba 13 5d 2b 74 70 56 80 ca 2b a1 84 f6 5b ce 18 9d dc ca 85 b4 1e 0d 4f ed c1 68 72 de ed bd 7c d4 3a bb be 7e f7 61 d1 7a 71 fd 47 74 18 be d8 bc fa 5a 18 2b b7 91 58 8f f6 99 94 65 f9 a8 ec Data Ascii: g9Gln!j9dxslz%{Yt+V\$Z:sn70qVj)D-P^TTD.Jf*?,rZKtJ*yF&H)-8 1IM)%{[L<~wi<V#/@93X'#]~tpV+{Ghr]:~azqGt Z+Xe
2021-12-02 15:37:58 UTC	796	IN	Data Raw: 99 6e ef ad a6 8f c2 7a c1 74 99 a9 4c 37 8f 38 5f b3 ef 50 30 b2 51 d5 cb d9 e8 3e 3a 78 b8 65 61 e6 53 ef da 54 c4 bd 4d 31 29 56 8a 04 0d 95 9b f2 92 cd 55 3c 93 b8 d2 41 71 d1 0a a7 79 38 f4 26 5f 8f ab b9 c0 87 38 f0 6a 53 64 3b 0d 98 97 64 3a 5f 9f aa 51 be 6b 14 56 91 48 9b 6c a2 55 38 89 44 8d 15 36 57 d1 4f 8b 8b ed c6 b0 77 09 ef 70 7d fd b9 4e ec 10 f5 8f 32 53 eb 9f 06 fb 78 3f c3 48 e5 d9 fa 78 14 cd 4f e9 3e b7 2b 66 23 64 a2 1e d4 5e 27 3e d8 85 65 1d 48 50 eb 43 06 2a ff 94 12 3d bc 34 11 77 a9 db 4c 9f 04 22 95 04 29 6a 0e 78 45 be d8 e1 36 9b 06 bc 79 a0 ed 8d af 79 03 bd c6 54 d1 48 e3 b5 10 02 92 5f 07 79 11 24 df 7c eb 33 0b b8 be 3f 23 6e 6c 34 2e 9b 6f 57 8c 39 52 7e 52 bb 6b a6 8a bf a5 53 16 1a f2 37 5d e5 60 42 59 0d 39 3e 7b 4a Data Ascii: nztL78_P0Q>:xeaSTM1)VU<Aqy8&_8jSd;d:_QkVHIU8D6W0wpN}N2Sx?HxO>+##d">eHPC*=4wL")jxE6yyTH_y \$j3?#nl4.oW9R~RkS7"}BY9>{J
2021-12-02 15:37:58 UTC	798	IN	Data Raw: 87 1c 98 b9 50 1c f9 49 51 ae 91 ab 2e 0e 1c e1 d8 91 16 61 5e 44 0a a7 78 80 a3 37 42 95 5c 5b f7 5b fb 23 39 d4 be 9a 47 f8 fe 33 ee 3f f4 95 f5 fc 0d 90 b1 df 3c ce 3e 35 b4 ac 8b c7 0d ab 46 ab 7c be 79 b9 1f dd 21 d9 31 e3 15 d0 24 1e 16 44 16 ed a5 16 08 20 74 57 08 25 ab fe 33 a4 73 06 60 33 eb 25 91 a7 a1 c8 ad d1 4a a4 9e d8 49 08 38 00 36 04 a4 de e0 8a 05 84 83 0c 4c bb 2f 1a e7 eb 23 91 f5 58 b1 b0 6e e0 5b 0b 56 19 30 cf b7 a6 1b fa 2e 81 22 8d 6a ea 23 4e 27 a9 67 4c 12 00 ee f8 a2 ea 43 55 15 3b 69 04 1d 02 c7 b5 53 74 c8 87 cc 26 37 ca 8a ff 42 79 e5 c0 54 6f a9 10 f6 2c ce ae 30 0e 18 91 86 6c d3 09 e7 aa 79 7c 78 c3 27 6b 18 af 46 fd 6c dc a0 17 69 b9 aa 46 6c 25 58 a4 91 06 f2 57 7a 07 03 ee 1e ef b0 95 ed d1 3b c9 06 c9 2c 15 0f b7 76 Data Ascii: PIQ.a^Dx7B\[[#9G3?<>5Fj]1\$D tW%3s'3%Jl86L/#Xn[V0.]"#N'gLCU;:St&7ByTg,0ly x'kFlFI%XWZ;,v
2021-12-02 15:37:58 UTC	799	IN	Data Raw: d2 ef 93 08 c6 54 d2 04 c6 bd 2e 40 85 f3 f3 ee 59 97 e1 09 77 5f 0e 47 ab d3 1e 9a b4 07 9d 4a 52 a7 dd c1 45 9b 33 45 ee 46 52 8e d6 69 b7 57 d6 ee 65 02 96 dd 63 82 0f d7 f1 e7 08 d5 34 32 41 9e a9 9b 72 24 7a 6d 0a bf e8 53 e5 b8 95 fd 97 d4 c5 d3 87 04 71 2b 07 65 e5 60 99 73 73 37 27 71 04 32 cb b9 27 58 e5 96 d7 a6 46 7c 29 93 a0 64 09 70 f1 81 9b d1 cc 12 18 8e c1 52 a9 37 e4 aa 15 1c 8d 1a 0f 3d 1f 9f 4d fa 83 49 59 01 1b aa 8e f4 8e df 2c a1 4a bf fb af 4a 0a 84 99 87 03 67 89 9c 9c ed d1 18 62 55 05 f8 4a c6 eb d2 5b a3 b2 a4 20 54 a0 5e 66 9b 75 a0 c0 52 6f a9 7d c0 4e 73 c1 8b 7b d0 1c 47 2e c6 af 2d 7e 95 b9 e3 21 4f e7 74 50 96 ff a0 c1 8c 7b 00 77 9e 08 e7 9c 99 47 f0 6d 21 30 00 59 d1 83 d0 5b 29 f2 24 fe 56 0e 5e 52 40 c0 d4 fb Data Ascii: T.@Yw_GJRE3EFRiWec42Ar\$zmSq+e'ss7'q2'XF)]dpR7=MIY,JJgbUJ[TPo]Ns[G.-!OtP[wGm!0Y)]\$V^R@
2021-12-02 15:37:58 UTC	800	IN	Data Raw: 7f cd 17 a2 f1 05 b1 56 d2 17 5d 0f cf 0f d5 1d 97 cc 69 66 ad 50 4e 74 d6 55 9d aa f6 71 ce 6d d9 c8 38 95 19 86 ec 44 76 1b cb 9c 54 a9 8c af 2b be ec dc 84 82 af cb 2c 22 42 54 20 1c c4 91 3c 99 d3 99 10 50 90 a0 c8 e7 4b d8 6d 32 9a c0 70 cb c5 93 8f ef 3f dd 15 ef 9f dc de dc dc d7 0f cf f8 e0 67 f6 39 14 3b 5f 52 b5 af 21 00 0e f9 e5 67 fe f9 f3 6c 7e 36 9c 4e fe 91 cf bf f8 97 57 c1 a5 37 e5 80 7a 5a a4 4f fb a5 62 47 03 de a2 4b 9f f0 ed c3 db fa ae 5f fe 8f 5f 93 ff 12 ed a0 14 2a 2b e3 70 3b f0 4b 67 8c 40 9e d2 da 4d 03 a6 4f 07 e3 ab 71 14 44 c0 30 0e c0 72 30 9f 93 99 14 94 07 58 5d 9d f8 32 6f 3c 5a 89 42 b5 c8 5a f1 4d c0 1f cd bc 87 6c a8 6a 96 57 de c3 da 86 42 67 6d 07 98 84 05 ae 31 66 a4 34 78 97 90 52 0a aa 94 b3 f6 69 ce 14 07 10 Data Ascii: VjifPNpNUqm8DvT+,"BT <PKm2p?g9;_R!gl-6NW7zZOoGK__*+p;Kg@MOQD0r0X]2o<ZBZMljWBgmn1f4xRi
2021-12-02 15:37:58 UTC	802	IN	Data Raw: 16 2d 8f 06 0a a0 5d a0 3a df 06 39 b7 a3 d7 2e 63 da 55 a2 48 36 63 7b cb 23 75 8c f8 ad b9 da 61 79 0c f6 3d a4 cb 58 52 6f 0f eb 61 b3 d6 4c 33 a9 d0 06 82 bf 08 ff 13 c5 5c 74 68 42 75 a0 67 e0 5d 36 ac c6 2f b6 16 ec 64 35 3f ef 90 c2 43 b8 f5 c9 3a 88 2d 8a ff 20 db 9f 2c 36 6b 40 73 87 c6 0a 85 1f db 46 4f ea a8 b9 7b d8 f1 3e af d9 f6 2b 07 68 e0 ed f9 27 ff 89 0d 3e 2a f4 8f f1 3d 99 83 3b a4 33 f0 8f 65 9a 81 3f 7c 3d 07 10 c9 a7 17 51 dc 00 d5 e1 55 cf ee 60 28 e1 34 49 f2 1c 8b a5 38 c0 91 f2 1b ad 8a d8 c9 42 33 ba 67 cd 11 1d e0 06 e0 5c 8a c8 a4 c6 38 ac cd 3e 9f 74 02 2b 46 08 5a 85 28 e6 84 6d fa f9 59 c3 f8 65 a7 c4 22 7e fd 04 28 8c 04 b6 48 ca 37 df 86 a1 61 4d 19 43 26 73 14 30 6e 1c bc 85 c4 22 d6 44 91 9c 0e 6a c4 60 ff 9d fd 4c 43 Data Ascii: -]:9.cUH6c{#uay=XRoal3thBugj6/d5?C:- ,6k@sFO{>+h'>*=:;3e?}=QU'(4l8B3gl8>t+FZ(mYe)"-(H7aMC &sOn"Dj'LC
2021-12-02 15:37:58 UTC	803	IN	Data Raw: cf da d8 5d 2f 56 cf bd 8d f0 a7 24 8c 09 e6 90 28 9c e6 cb 57 b3 f9 4b c4 d1 e9 69 3e f7 e1 f8 6a 72 3a 49 ec 4d 90 cb 5e 55 7d 1b a4 ee d3 f6 2a 59 0c 2f 72 72 29 d4 00 b9 57 cb 2b ef b3 f5 e5 28 31 4d 0a ed a9 8e d9 a1 14 75 69 25 11 bb 9c 4f ae 86 a3 d7 eb f1 70 39 5c af 16 c3 b3 9c 48 a7 e4 e2 48 a2 66 e1 f9 16 5d 5c 28 3c a3 e5 cf 67 67 49 79 24 7a 47 42 78 b9 ba 5c 5f 4d 16 93 e7 93 10 64 bd 2e 25 ee a2 a6 da 66 a7 cb 57 c3 79 7f ea 4f 53 c8 9a 68 59 4d 5f 4e 67 af 12 59 aa 95 4f 64 af 26 e3 bc bf da 13 9c a8 47 c3 e2 62 36 5b be 98 e6 8b c4 aa d4 bd e8 44 c9 eb 3c 05 2b e2 be 59 90 5b 9c ad 4f 51 90 11 bd cb 19 b0 66 91 94 2f ea b8 bb 95 84 a5 50 6d c6 f9 74 92 56 2c ea 84 7f 5f 6e 39 b9 c8 b1 e0 24 f1 88 d1 73 2b 78 11 d0 6c 9a 8f 96 cd aa 13 fb 10 Data Ascii: J\V\$(WKi>jr:IM^UJ*y/r/r)W+(1Mui%Op9\HHfj)(<ggly\$zGBx\ _Md.%fWyShYm_NgYOd&Gb6[D<+Y[OQf/PmtV ,_n9\$S+xl

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	804	IN	Data Raw: 15 52 17 79 be 5c a7 da 07 88 36 62 6f a2 a4 d7 ac fd a1 95 1c 0f c3 e4 cd 77 fc 07 fe f1 08 96 6d d7 e4 36 fd 92 af 17 69 51 72 93 5a 31 fe e5 36 cf aa 34 ab 98 7d 6f 0c be 93 56 58 fa d9 e4 3f 3f 9b 28 2d b0 f6 16 28 35 d8 47 4f 4f 1d ce 9a 6d bf 1c fa eb fb 53 f2 ef cf 75 aa eb fa f7 a7 e5 96 64 ed 17 a2 7d 29 d2 bb f7 9f 8f be 54 d5 b6 7c 77 7a 5a d6 db 6d 5e 54 27 4b ee a1 93 db 7c 73 7a bb 73 f1 29 c9 ca 9f d3 e2 d4 0c 78 96 7f 3e d2 2a 52 2c d3 0a f2 b3 39 82 64 f5 f9 a8 55 cc 1e a2 dd ae 49 59 e2 c7 22 fd 6f 4d 8b 74 f1 56 58 04 c1 6c f9 b6 fc 92 ff 8c 1f ff 51 e5 db 93 b2 be bb a3 b7 14 9b eb a7 e9 62 4e 6e 99 2a ee 02 e4 82 e3 39 a6 8d 67 7a 96 a9 7b ae 21 47 1a 32 7d 8d 53 a7 da 0a 86 66 b0 89 d0 77 bf fb 18 95 5e 36 7e ed 18 4c 71 0c 0a 33 95 Data Ascii: RyI6bowm6iQrZ164)oVX??(-5GOOmSudj)T wzZm^TK szs)x>*R,9dUIy"oMTVXIqBNn*9gz{!G2}Sfw*6~Lq3
2021-12-02 15:37:58 UTC	805	IN	Data Raw: 2e 8d 4a 6f 5b ae 8d 46 d2 41 2f e9 59 8e ec f5 83 2e 32 4b 59 98 ac 88 88 ef 8a 4d 01 a8 d0 65 b2 3e d4 b7 51 7a c0 30 75 db 95 02 f3 8a cc 01 3a c0 73 86 36 9b f4 b0 97 df f7 c4 31 9e 54 6a f7 34 e5 d9 8d a7 ec 80 8d f9 ec 45 fb f7 5c 10 4e b4 1f 53 aa 15 00 19 2a b0 69 2e 70 1c 8c 59 88 02 b4 59 4c 92 07 3c 05 5f 50 59 d8 98 61 07 ae 04 4f 26 5b d8 01 dc 6e 22 e3 45 07 da ea bc 05 7d 2f d2 e7 76 f3 e4 8f b4 95 af f4 8d 6d 3f a2 70 ea eb 6d e1 ef ec 04 ab 22 af b1 6d f4 27 79 d5 74 84 8e 69 b9 6d 43 e2 80 fe 01 ee 4c df f3 00 50 81 ee 18 52 30 83 a1 d0 0d 3b 4e 21 e0 39 0e 9b 11 38 01 68 1b 18 80 cc c3 f8 3c a1 25 9d 1f 7a 42 0c 7c 0b cf f2 41 bd c0 43 c0 59 a4 d0 09 9b 7a 44 19 ab dc 6c 69 0d 6b d9 44 a9 73 7e f0 08 66 8b 48 bd af b3 25 70 82 c5 2c e2 Data Ascii: .Jo[FA/Y.2KYMe>Qz0u:s61Tj4EiNS'i.pYYL<_PYaO&[n"E]/vm?pm"mytimCLPR0;Nl98h<%zB ACYzDlikDs ~fH%p,
2021-12-02 15:37:58 UTC	807	IN	Data Raw: 82 48 88 d2 7d 33 4c 8e d9 4d e6 b6 b9 d6 4f 8b 07 44 03 0e bc 25 e4 a4 58 e4 62 9e 96 84 63 4d dc 26 8b 19 67 b0 f3 7f b6 dc 7f 9d 80 dd c2 79 ba ef 5b 3e 5a 02 36 fb 93 5b 8e dd 5c 6a e7 b7 ae 4d 7b d6 89 76 d3 78 94 b3 a3 d7 c7 4f d7 51 2f 0e 67 a3 c1 74 12 8d 66 61 af 17 4f e2 41 12 5e cd ce 07 d7 d7 51 32 19 1f da ad ba 62 95 f5 4c 7b f1 60 f6 d3 34 bc 8a 27 9f 0e 35 a8 d0 55 d2 70 1e 26 e7 d1 d5 ec 6c 3a 99 0c 12 d9 06 f9 0a 53 d6 30 48 26 d8 00 ac 88 c6 6c 4f 87 4a 54 fd ac a4 a4 17 f7 66 c9 60 32 9b 8c a4 6d a8 f8 b6 24 df 8f a2 de 59 78 7e 39 8b ae c3 f8 6a d6 8f a3 ab de a1 22 d5 bd 48 b7 a2 fe 60 74 3d eb 45 e3 f3 51 3c 54 6e 4b 31 20 eb d6 f6 21 0a 7b d1 e8 50 87 8a 50 76 eb 18 8e 06 d7 c3 89 e4 1e b9 7f eb 56 31 8a 7e 9a c6 a3 48 72 8d aa 73 Data Ascii: H}3LMOD%XbcM&gy >Z6 jM{vxOQ/gtfaOA^Q2bL{^4'5Up&L:SOH&IOJTf2m\$Yx~9j"H"=EQ<TnK1 !{PPvV1 ~Hrs
2021-12-02 15:37:58 UTC	808	IN	Data Raw: bb 54 ab a4 89 be e1 ff ac b5 6d b2 13 4f a0 4f 49 bc d5 e8 fe 91 6e 9e d3 a7 72 cb be 3d 27 f9 86 2e ea 7b 33 ba ce 8b 32 4b b5 a7 0a 6f 91 97 1c ce 58 ac 37 e5 6f 42 1d 28 e2 78 ae 63 39 c4 d4 7d e2 da 97 da 44 71 c6 65 96 71 8e d5 64 94 eb 46 77 94 03 58 86 67 c1 30 0e 64 3d dd 70 5c 53 bf 44 78 48 56 71 0a d5 e2 dd 96 ab 2e 00 17 02 c1 36 0c dd 22 8e 67 9a 3a 70 88 69 4b 08 83 38 39 ac e2 67 be ae 5c 4b 0e cf 71 b2 4a 0b 2d a7 0c 95 2d be bc d1 fa 7c 91 ab 43 79 ad 89 07 55 cf 31 93 5d 12 17 da b3 70 43 06 ac 1b f1 60 9b f8 04 4f b6 5c 98 87 79 d4 a8 86 42 db 93 d2 b0 67 0f 74 1c cf 71 2d 66 48 cb b7 4c d7 91 17 f0 4c 13 28 4a b7 62 cd 1e 81 d9 0d d7 72 6c cf b7 6c 57 77 a5 98 9a ac 2b 4b 9b cb 72 2b 1e e3 d9 c4 f4 5d 9b c0 51 06 31 88 e9 c9 ea Data Ascii: TmOOInr='.{32KxX7oB(xc9)DqeQdFwXg0d=plSDxHVq.6"q:piK89g KqJ~ CyU1 pC' OlwRtq-fHLL(Jbrl W w+Kr+ Q1
2021-12-02 15:37:58 UTC	809	IN	Data Raw: 98 fc 6e 99 9c 56 9d 5c db a7 f8 9a 08 ed b6 b5 81 56 07 f0 f3 a3 6d ae 1b 5e ca ba e6 5a 78 01 0e 62 2a 0b b6 09 1d 33 ad b1 6b 6d 47 6e c5 c6 40 4f 30 44 99 95 b5 08 4c b9 2a d7 f8 9d af 6f 4d 37 7b 3e 0e f0 c4 c0 c8 66 82 47 a0 5a a1 8f 23 39 4c 89 66 33 ca 5c 97 7c 84 4b 35 e3 e0 f2 a9 ee bf 09 2c 07 f3 89 6d b2 4c 25 86 6d a2 f4 49 83 1b 0f 4a 31 87 70 a6 6f 19 e8 13 18 6d 2c d7 43 ab 70 2c dd 93 72 f3 58 d8 f6 59 7c 10 0c 8d 0f 2f 22 b4 61 b2 d7 46 f3 26 0d 58 a8 c1 6c 48 56 9a 88 44 2d f2 f3 09 a8 3c 3c e2 1a 1b 7c 10 5e 3f 34 0e 59 36 9a 87 79 d4 a8 86 42 db 93 d2 b0 67 0f 8c b5 dd d9 3c 76 fe e0 1a b8 19 58 7f ec d9 ae 8d 4a ee 1b a6 8d d6 62 fb 44 7e fe 79 2f cf b1 78 e6 1f b8 1a da 3c d3 ac 4e 7b 36 a2 26 79 22 12 b6 38 d7 ad ae 4e 0b 5a Data Ascii: nVVm^Zxb*3kmGn@O0DL*oM7{>fGZ#9Lf3 K5,mL%mlJ1pom,Cp,rXY /"a)F&XlHVD-<< '^4Y6yBRg<vXJbD~ y <xN{6&y"8NZ
2021-12-02 15:37:58 UTC	810	IN	Data Raw: 11 a0 3d a5 6c 13 b4 76 79 9d 44 a0 e6 eb 26 1f 84 d3 31 c2 7a c4 d4 1d 03 bd 0a f3 bb 2b 13 8b 1f 61 7b 2b ca 3d 2c 12 1b c9 ab 22 7d f8 f9 27 ac a3 3e 2d a4 db 6b cd b8 b6 f8 4d 77 ef 0f ec 11 76 f3 ed e7 5a 41 d7 71 0d cb 00 fb 01 93 33 51 c8 db 46 ee 4a c5 46 af 4a 13 d0 ab cb c8 e3 9d 8d 25 12 9b cf 74 c0 1b 06 18 af 21 11 93 28 6e f7 a7 47 3c c6 66 40 6c 2a aa 4d 7c 4f 12 0f 2a 5a a8 d8 7e f6 d0 98 7c df 77 2a 5e 34 0e 59 36 9a 87 79 d4 a8 86 42 db 93 d2 b0 67 0f 9e 07 7a e6 10 17 d3 a5 54 0b ba 17 f5 f9 b2 f4 55 c5 a1 65 8f f0 4c e5 e4 cf ed da 8a a5 fd 79 6d 1b 6c dd 64 55 da 33 1d 10 38 df f2 a5 56 79 c2 c2 3d d0 62 10 71 4b 07 e3 62 3c cf 52 a7 0d 66 72 36 0b 51 04 22 02 bf 09 28 74 d8 6b 6d 81 22 dd 9e 51 bf 37 34 79 e0 c0 ba e5 59 3a ba 3b 5a bc Data Ascii: =lvyD&1z+a{+=",}>-kMwvZAq3QFJFJ%t!(nG<f@!^M O^Z~ w^*dY).R=zTUElyrmdU38Vy,=bqKb<Rfr6Q"(t km"Q74yY::Z
2021-12-02 15:37:58 UTC	812	IN	Data Raw: 90 9e 46 d3 7e 38 97 12 43 f1 9a fa 89 30 1f 0b 31 b2 08 c2 d0 09 46 ac 8a 49 2b 50 bc 7f d0 a0 80 a2 4a e6 52 1c 31 d4 f7 8f 82 d9 44 12 50 bd aa db 08 f4 03 b9 7c 29 5e 64 ae ef 9f 84 a1 d4 9e 55 3b 7f f5 fd b3 81 6a 09 aa 5d f5 5a e2 61 d8 9f dd 4b 12 aa ff e4 f3 f2 f2 7f 50 4b 07 08 98 9c 1d 6c 39 10 00 51 36 00 50 4b 03 04 14 00 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 6d 6c 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 00 00 00 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 19 00 00 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 dd 5d 5b 6f 1b 3b 92 fe 2b 5a 4f 1e f6 0c 1c 9b f7 4b 76 ce 1e 28 56 db d1 c4 96 3c ba 38 c8 20 Data Ascii: F~8C01FH+PJR1DPI)^dU; jZaKPKl9Q6PK*Q_locales/ml/PKPK)Q_locales/ml/messages.json [o;+ZOKv(V<8
2021-12-02 15:37:58 UTC	813	IN	Data Raw: 05 2d 76 44 4f 48 73 20 02 7a fc 43 8c 46 02 9c 4e c8 b5 a1 22 0e f9 02 4e 45 be 3c 10 8a d0 44 38 00 d0 8c 59 29 2d cc 57 48 09 fa 9e c7 f2 a9 27 bf 8c 54 38 53 1c 90 b8 f5 00 77 b9 05 90 47 2e 04 9e 4e 58 0e 1b 04 01 21 56 81 10 2b 56 ed 68 e0 24 58 38 67 8c 30 4e 71 26 19 74 48 77 55 31 16 23 ff 16 3a 43 e6 2f 1b 4d 31 14 86 a6 08 7f f3 d8 09 00 f7 de 5e 1c bb f4 60 3e ad d3 30 76 0e a2 a6 1e 80 03 b3 c1 64 5c a3 24 64 6a ad 37 ac af b1 60 bf e1 d3 03 0b 7d 6e a5 72 ba 4e e8 64 90 af 40 5d 81 7f 13 1c a4 41 7b e9 4b ed 24 a5 09 47 f0 b6 c5 f8 e6 59 22 4f 54 1b 20 c4 97 60 5f d2 c9 b6 65 45 2b c1 14 4c 15 c2 45 26 25 70 9e 9c 6c c8 5b 10 4e af 6c 01 2e db c1 3f c2 80 54 7b 2f f3 31 40 b4 f4 57 55 4b c5 20 12 f1 10 fc 59 10 57 88 ff 4c 46 ad 50 9c 83 a5 Data Ascii: ~vDOHs zCFN^NE<D8Y)-WH^T8SwG.NX!V+Vh\$X8g0Nq&tHwU1#:(C/M1^">0vd sdj7")nrNd@ A K\$GY"OT `_eE +LE&%p [Nl.?T /1@WUK YWLFP
2021-12-02 15:37:58 UTC	814	IN	Data Raw: 57 1f 9e 1e 7e 78 d4 fa e0 15 45 3b 3d d8 5d 2d f6 5b 97 71 0f 93 52 8a 31 e0 99 30 0e d6 ca 32 c5 e9 c2 df 16 af f1 de 5e a7 4e e2 c4 0d 15 89 7d 87 11 26 8a c5 1f 98 50 d9 ac 40 5a 2b 60 95 77 12 fe 05 e0 cd 99 a7 f9 e4 92 b0 3e dd ca ca 71 8b 28 3c 6f 95 7a e0 97 e8 ad bc bc 5d ae b3 ac b2 e1 35 51 37 fd 93 82 29 42 82 6b f8 16 79 6d 34 93 ca 80 05 63 65 65 a6 32 6b 8f 41 64 d7 7b eb 29 f1 fc 8e ee 25 53 a1 55 4e 2b 27 78 c6 ee 33 b1 3f 9f 1c 27 b9 4f 02 d2 b2 2e b9 54 bc 96 48 a7 8d 60 1c 80 ba f0 00 35 8d 27 8f 70 44 c5 62 8d 4a b5 f7 84 37 da bc db 12 b1 d7 24 42 b1 43 74 f7 bc d1 89 16 02 c1 d8 b0 b3 5c 28 bf a2 bf 04 86 18 0f 9a 29 bd 05 55 75 4c 33 2d ba aa d2 1f cd f3 80 87 38 3c 09 03 b0 10 95 83 89 28 13 86 20 b5 c2 6b 52 6e 03 84 e3 1b 73 13 Data Ascii: W~xE;= ~qR102^N)&P@Z+`w>q<oz 5Q7)Bkym4cee2kAdf)%SUN+^x3?^O.TH^5pDbJ7\$BCt()UuL3~<(kRns

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	816	IN	Data Raw: 63 a3 00 e9 fb cf aa a4 29 c2 14 17 d6 c5 ff bd b3 d3 d1 6e a6 15 4e 54 b4 a0 60 e4 da 2e 4a d6 63 13 85 35 e9 7b 53 78 a3 fe 14 ef f0 bc 45 c2 75 d9 5d 29 b0 0a 5d 31 c7 eb 72 c7 dc 95 14 f1 8c 43 79 bf 8e 65 ce 49 27 c0 3e 83 a1 a6 f7 57 ff 4f 94 a8 62 73 4f 44 d5 0c cd be 75 13 e0 8f 2f 4e 3e 29 06 c3 fe 62 32 9e cf 8a c9 a2 3f 18 0c 67 c3 f1 a8 7f bc 38 18 9f 9c 14 a3 d9 74 95 e5 d4 45 53 29 9d f9 60 38 5e fc 6d de 3f 1e ce 5e af 52 a0 20 67 42 e1 a0 3f 3a 28 8e 17 cf e7 b3 d9 78 94 8e 21 bd 87 29 a5 30 1e cd 60 02 30 8a 62 5a ce 69 95 08 55 76 92 10 19 0c 07 8b d1 78 b6 98 4d 92 69 50 db 37 49 fb c3 a2 18 3c ef 1f bc 5c 14 27 fd e1 f1 e2 70 58 1c 0f 56 09 51 57 4d e4 09 1d 8e 27 27 8b 41 31 3d 98 0c 4f c9 69 11 55 bb 79 6a 2f 8a fe a0 98 ac d2 a0 32 Data Ascii: c)nNT".Jc5{SxEuJ})1rCyel'>WObsODu/N>)b2?g8tES)`8'm?*"R gB?:(x!)0'bZiUvxMiP7l<l'pXVQWm"A 1=OiUyj/2
2021-12-02 15:37:58 UTC	817	IN	Data Raw: 59 fd 55 fe e0 e1 b0 73 c0 05 97 85 b6 85 13 56 48 67 75 21 18 05 8b 9b 16 96 ac 61 29 d6 7e 16 8b fa 1b 57 3f a9 fd af 1d f4 9f cb 76 5b a1 fc e6 f5 cf cc b4 ab 03 d4 eb fa 9b 95 df ad 7e 48 38 bf a2 86 e7 7f f0 84 b1 76 81 df 87 2f 10 6c e9 d6 1f 92 18 19 b5 be 58 d5 e8 49 8b be 5f 75 e8 dd 02 25 e0 91 e8 b7 fe 6e 88 fb 25 b0 16 98 6a 9c 35 ca 30 c9 0b 66 35 79 4a bc 5e 8f 08 0b d8 16 e8 f4 ac a7 c8 e3 63 10 19 e1 10 95 70 0a 64 c1 c0 93 8e 0b 63 25 a7 b6 22 c0 af d6 51 e0 d2 9f cc 0a d1 e6 d0 d9 23 3a e5 d2 6f ae 85 e0 8a 19 27 25 07 14 98 d4 e4 e6 1e 56 74 98 18 1d 83 58 ca 34 12 02 d3 a2 10 1d 63 10 b0 eb 44 2e ed 11 16 3d d9 4a 58 2c 55 5e 56 38 42 2a 62 3b 7e e8 1a 51 be 5a 97 1e 42 0c e4 f2 28 70 46 03 31 c0 1a 65 39 73 c2 15 da e5 8f 25 1c 85 43 db Data Ascii: YUsVHgu!a)-W?v[-H8v!Xl_u%r%j50f5yJ'cpdc%"Q#::o%VtX4cD.=JX,U^V8B*;-QZB(pF1e9s%C
2021-12-02 15:37:58 UTC	818	IN	Data Raw: 96 36 94 cc aa a4 48 20 45 a2 20 02 d5 a2 02 75 e1 1c 0b c4 bf a0 c0 57 eb 6c 8f d4 55 e1 80 23 f0 fd 0a 41 0f 67 ee 1f f2 75 85 a8 40 b0 b7 77 8b cc 4a 14 64 b5 8f 06 31 c0 9e 69 0b f9 ff 92 ed a1 0e da 33 c7 b5 52 44 99 3d bc 0f d6 07 af a2 76 5d ae 72 88 35 b6 62 d9 12 d7 8c b4 bf 42 96 4c e5 0d 55 2c 1b cb 99 1e f6 e5 d3 c6 74 51 1e 0f 80 e2 82 e6 50 94 e9 45 aa 8d 74 be 41 36 51 d5 68 07 2c c5 3a 03 7b 27 b1 8f ab 78 98 de 2d 65 5b 96 b2 00 89 8a 20 fc 00 46 79 27 af 73 88 85 12 fb 0c c2 ef 59 84 a6 67 85 6b d1 8c bc 55 20 12 2d 48 9d a1 a8 91 23 21 8e 2b 9f a9 0d 64 eb f4 fa e3 8f 0d 5b 6a 68 58 22 7b 3e 1a fa a6 26 66 17 09 08 15 39 77 b8 af c8 fb af 44 64 24 71 8c 8a 43 e0 28 46 d9 d6 16 88 fe 0b e5 bc 9a 0b 69 68 8e f3 84 28 da ac 5d d8 69 53 Data Ascii: 6H E uWU#Agua@wJd13RD=vJr5bBLU,QtQPEtA6Qh,:[x-e' Fy'sYgkU -HA#:+d[jhX']>+f9wDdSqC(Fih[jiS
2021-12-02 15:37:58 UTC	819	IN	Data Raw: 12 c1 58 5a 32 21 c4 34 3b 58 65 0c 57 10 28 14 5c 58 e1 b4 64 84 ac 22 cd 45 eb 1f e1 60 10 22 99 54 39 4c 8b 99 02 42 7b 2b 65 01 51 3e 18 1f 57 30 5a c0 17 48 e2 50 c8 10 c6 93 3c 82 5f 67 34 71 f9 d1 b4 16 46 26 b3 22 4d 24 16 45 07 ad 1a 10 61 63 68 c5 e2 a6 d4 b6 18 80 50 ed ff f3 0b b3 d7 98 32 58 6d a8 4c ac 45 63 d9 c6 f4 34 0e 98 98 49 89 48 69 da 98 29 17 51 89 61 db bc d6 be 73 6b b8 bc b2 a9 e7 f7 b8 fa 3f 36 65 01 11 81 44 58 27 ea 15 f9 93 7c 89 6a 9f 09 b6 3d 26 22 70 41 7f 73 00 4f 14 df 02 0f 2f 91 94 24 53 50 cd 6e b9 ca 56 2e 68 21 fa 14 c8 a5 71 62 9e 8a 28 c7 43 4c 6c 0d 13 bc 6a 6a 42 12 a3 20 da dc 30 27 ba cb 2e 59 cb 67 39 18 7d 70 d5 0c 52 48 30 7d 0c 4c f2 fa 56 eb 35 d2 2d 65 40 1c 92 8b 48 16 2e 11 42 b1 d2 e3 73 8c 6e 1c ee Data Ascii: XZ2!4;XeW(XdE""T9LB{+eQ>W0ZHP<_g4qF&"M\$EachP2XmMEcO4IH)Qask?6eDXJ'>+pAsO/\$SPnV.h!qb (CLljjB 0'.Yg9)pRH0)LV5-e@H.Bsn
2021-12-02 15:37:58 UTC	821	IN	Data Raw: 61 d9 9b 06 ac 13 fe 10 2f 31 43 8b bf 5a 48 ef 97 bb bd 5e 79 31 ed 3e 3f 4b 74 87 9a 3b c9 c3 39 1d 8d 12 4c a8 84 2f 0f e1 a2 1c 9f 00 55 09 39 c4 bb bf 36 00 19 8d 12 0f 46 24 e5 79 00 b3 e1 00 42 85 b3 b3 c1 e9 80 e0 09 75 0b 80 82 d5 1f 4c 7a dd 71 bf 3a a9 93 c1 f8 bc 4b a9 22 75 e9 8c 82 75 32 18 96 b5 79 99 83 66 0f 09 e7 43 75 41 29 40 35 8c 8c 93 27 ca 80 14 88 61 37 0d bf d2 77 14 51 2b 47 2f 53 13 9f be aa 83 5a 39 2e 2b 03 4b d0 4d dd 90 a0 00 64 96 53 6f 7d c9 2d af 55 2d b1 a5 44 fa Data Ascii: a!1CZH"*y!>?Kt;9L/U96F\$yBuLzq;K"uu2yfCuA)@5'a7wQ+G/SZ9.+KMDsQ)-U-D
2021-12-02 15:37:58 UTC	821	IN	Data Raw: 91 05 40 f9 07 6a 54 2d 0b 60 32 03 4d 4d ad 21 55 45 a0 60 d4 f1 d0 f3 d9 e9 7c 34 9e 97 55 60 93 8a 63 7a 51 30 0b a8 92 ef d1 ab 32 0d 84 89 17 45 66 81 9c 94 dd e9 0c 7c 55 15 f0 95 84 d5 4d 6f 6b 64 41 81 ab 48 85 9a 7a c9 4d 16 02 04 ae 7f 02 eb 03 7a 9a 73 5e d4 bb 98 28 70 de 7f 6d b0 ab c4 10 76 1e ce c9 b8 2c ff 92 3a 33 ea bd a9 79 20 94 71 26 5e 6c b5 01 c0 18 ce 2a 25 24 1d dc ce 83 f8 53 39 7e 99 06 04 44 5d 3c 0f 22 83 72 d1 a8 4b 35 1b 80 10 1e 82 9a 1a cc 43 f0 a1 49 ea 76 75 f2 86 cc 0d 30 a6 10 6f a6 22 4b cd 4e e6 81 cc 86 af bb d3 de 0b 4a c8 a8 71 1d 0a d0 9b d1 0c 32 f4 e1 e4 35 a1 3e c4 8b a8 10 88 17 dd e1 29 84 2e f3 c1 b0 0b 6a f3 2a c1 80 ea 40 92 cb 5f 81 b6 a5 a1 13 71 35 92 58 1d 32 80 34 55 4c 07 11 89 d5 d3 c1 f4 ac 9c 27 8a Data Ascii: @JT-^2MM!UE'j4U'czQ02EFjUmokdAHzMzs^(pmv,:3y q&!*%\$S9-D]<?K5C!vu0o"KNJq25>).j"@_q5X24UL'
2021-12-02 15:37:58 UTC	822	IN	Data Raw: 5e 35 a3 74 89 c0 15 5a 5c 60 ba aa 3a 86 e1 40 89 6e 18 86 7e aa e5 23 2b 57 6a aa a9 a1 01 38 1e 40 5d 73 80 c3 a7 2b 3b d8 8e 58 6b 20 98 ae 6d eb b6 6b 6a aa a1 42 82 ae 85 63 16 1c 55 77 e8 66 cb 55 be 56 a6 00 c2 f4 f2 f2 b2 d4 60 78 08 ae e3 5a d0 a0 61 ab 26 81 d8 0f ec 89 6d cb fe 56 c8 18 e8 4d 48 07 fc ef e1 ce 9e c4 c2 36 2c bc 58 ed cd 34 91 9d ba 86 8d 59 9e e1 f1 08 90 cd 7f 88 2a e5 96 a9 ab 26 54 a3 ba 86 01 d4 c8 87 d1 a2 0b c5 36 9a 39 d0 0f f6 d8 70 95 e7 19 a7 8b 7b 77 62 a5 a9 a2 43 79 e8 93 0e 5c 86 56 69 53 ff 07 28 bd 95 f2 d3 36 e6 fd 23 f9 f9 6d 25 c7 b7 aa 69 aa a7 f3 8a d1 69 97 bb 07 8a c4 65 bb 39 57 fe 10 df d2 38 cd a2 b5 b2 85 f3 23 b8 6d 05 7e 70 0e 02 91 09 47 36 80 a2 e7 4a 9a b1 0c ab 90 6b db 5d 84 2f 90 c2 f2 c7 Data Ascii: ^5Zl':@n-~#Wj8@]s+;Xk mkjBcUwJUV'xZa&mVMH6,X4Y*+Tr69p[pwbCyViS(6#m%iiie9W8#m-pG6Kj/
2021-12-02 15:37:58 UTC	823	IN	Data Raw: 71 84 c2 89 6d 12 ff e8 d9 9a 1a fe e3 46 6b db 72 2d 0f 90 65 6b c0 07 d4 19 60 42 de 93 4b 42 52 08 d9 1a 66 1c d7 43 33 d7 c1 a6 54 49 74 ca 43 4a 11 66 4e 74 12 fc 2b 64 3d 40 1d c6 44 0f a8 87 1c 72 3d 95 84 c9 5f 8b 11 f3 42 e1 09 14 a1 22 05 65 da 71 f2 9c 3c 72 66 3e 63 5f 39 f9 fc 47 39 40 20 84 4f 00 02 0c 0d f3 a5 e0 7f 1c 0d 0a 76 cc 21 41 30 b9 3d 05 47 75 a5 98 65 3f 8b 99 f9 05 7f e1 10 bb 65 7c 12 a9 0a a2 20 1d 41 9d 63 25 f8 d9 1b 39 32 75 4f ff 7a 05 57 25 0f af ea f5 b4 06 41 f0 3b 6d 66 b2 17 52 eb 95 c8 c0 59 f2 46 d2 2b 0a 06 88 15 dd 08 7d a8 56 af e2 43 30 b8 a5 84 50 47 2b ba 54 af a2 a6 43 c8 1e fb be a2 44 d2 21 64 8f 70 ea 35 14 d4 84 b6 5d fa 1a eb 2b 3a 46 e0 9b 34 65 65 4f a4 ea 95 8c bb 0f fe a8 71 2b 4b 32 d9 b3 00 99 a2 8f bd 31 26 f4 ee f0 41 52 3e 92 77 b4 8e 54 dc fa dd 1b 50 97 49 d8 f5 51 36 f7 c4 02 d9 69 ae 54 fc 1e d5 46 a9 93 e4 5d 08 89 74 39 Data Ascii: 'q[uJ(y*QeLClO08H*(X1z' u3ZUh4e/jqA5/92uEzW%A;mfrYF+)]VC0@rTCD!dp5]+:F4eeOq+K21&AR>wTPIQ 6iTf]9
2021-12-02 15:37:58 UTC	826	IN	Data Raw: 72 03 cb 5b 4c 12 a4 51 01 e8 dd 94 5f f3 ac dc ec 93 74 5d 01 fb 97 79 a1 2d 93 0c 18 84 69 48 6e b8 cd 8b 85 74 e9 03 c7 75 dd b3 2c 0f 1e 4d cb b2 4c 02 a2 49 3d d2 d0 6d 03 af e0 05 00 73 c3 03 e0 12 98 db 22 e1 41 4d 62 bc 85 2d f5 5d d7 74 7d db d0 2d 1d 56 74 3c 67 ae 42 ab d6 e9 6d b2 61 0f 2c 5d 08 02 f8 fd 1e d3 3e 43 22 de b1 0f 59 fe 7b 91 6c 79 1c 4c b7 76 6b 05 d8 6e cf 77 e0 d6 40 40 6c 8a b6 7b 14 9b a4 3c 69 62 81 a7 4c ee c1 0b 30 9b 40 31 f3 10 7b 58 0f b6 91 b4 a6 81 c5 3a 81 15 f0 6d 22 01 99 80 56 9f f9 68 9b ec 4a 26 2d 1d db d4 6d 3c 04 1c a9 5b 16 e6 48 1e 33 60 eb 7a a8 0b 76 07 48 62 5e 2e 42 19 04 d6 f1 d0 e1 95 18 69 eb 20 ab 00 fc e9 21 9c a0 50 97 ee 4f 74 b6 cd cb 4a fb 0e db bd 5a 16 58 f4 f7 1f 1a 53 be 6a c3 d0 03 93 97 Data Ascii: rLQ_tjy-iHntu,MLI=ms"AMB->]j)-Vt<gBma,]>C"Y{yLvknw@&[f<ibL0@1[X:m"VhJ-&m<[H3'zvHb^:Bi !IPotJZXSj

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	827	IN	Data Raw: 78 48 93 55 23 33 ca 63 11 53 34 ee 7d 97 9f 2e 01 81 7d 7e 5c e3 5a a4 22 7e d0 f8 39 d1 2a 01 0a 36 71 72 6d 7e b0 66 da 0e f8 1d 1b ee d0 46 73 c2 9b 1e 21 85 88 08 ba ff f3 db 72 3a df 3f af 2b 77 1d df 09 80 58 ae 01 78 40 b9 01 25 68 0b 59 53 ed 42 66 80 b4 73 0d b4 42 7e 00 05 60 42 79 e9 8a 9d 89 90 4a 8b 3a 0f d1 a1 5a d0 5b 56 00 84 43 ce f8 81 4e 9b ff 05 d2 aa 7c 29 9a 2e 5b 12 48 e1 02 8a 0a a5 d8 08 2a 8e 49 bc 40 9e 55 d7 0b eb f5 eb 66 22 63 0b a1 f3 35 f4 10 7c 8f e5 6e 1d e2 42 51 43 86 e8 d4 b9 c4 28 d7 95 c8 87 67 91 7b ae 5d f0 53 ce fc 61 55 17 c1 6b 01 cc fb 66 a1 91 12 0e 2e 7c 42 7b de 05 ad 0e a5 b0 54 2e 98 0a 9f 43 9d ce 01 e4 08 f4 1e 57 a9 80 39 28 40 52 c0 37 1c d7 9a 20 7b 06 b2 01 35 a0 03 6a 11 65 1d 7b a5 a8 de 8a f7 3f Data Ascii: xHU#3cS4.}-\Z"--9*6qrm-fFs!r:~?wXx@%hYSBfsB~`ByJ:Z[VCNj].H*I@Uf#c5jnBQC(g{[SaUkf. B{T.CW9(@R7{5je{?
2021-12-02 15:37:58 UTC	828	IN	Data Raw: e9 84 e3 2e df a9 5e 3c be 0e 55 a5 a8 ba 79 53 f9 ea c5 83 48 c0 cb 1c 95 3d 50 90 8f ea 5c 47 e5 48 f8 68 21 79 45 ff a9 72 31 08 a9 fc a2 ef 88 a8 2c 87 57 14 e2 e9 7d bb ca 72 1c 71 80 55 ac 5b 75 89 a5 72 d0 62 ae 7a 17 a2 cd 5c 94 1a c1 52 85 2c 6f 75 a0 e2 07 d5 51 78 ab 83 c9 0c 95 4a d1 50 d5 14 fc 08 3d f4 71 76 31 1f 8e e7 11 17 36 34 1d e9 fd 6d ab 23 9e df c3 9b 88 0a 61 c5 3b 8c ad 4e 7a 51 38 9d 81 ab b8 e0 8b 14 a8 4b 6f 0e 5b 5d 81 2a 68 52 ab 5e 31 69 f5 00 e1 fa 0b d0 07 75 da 46 5e aa 17 7d 54 ee 24 7f bd 81 ab 8a eb ac 76 3f bd 71 14 fd 46 c9 4c f5 0e 6b bb 13 15 38 b2 5e 76 7a c3 c1 18 7b 45 17 42 6f d9 da 5d fc 12 8d af a8 20 50 9c 20 b5 bb 68 61 08 d5 15 f1 1b 4e 14 0c a1 ba d4 69 f7 20 a5 09 a5 5d fa e6 eb 1b 3e a6 d0 9b 34 65 Data Ascii: .^<UySH=PIGHhlyEr1,WjrqU[urbzIR,ouQxJP]=qv164m#a;NzQ8Ko[!hR^1iuF^)]T\$~?qFLk8+^vz[EBo] P hani]>4e
2021-12-02 15:37:58 UTC	830	IN	Data Raw: f3 56 55 99 57 fd 4c 95 08 e9 ce 99 b2 41 02 b3 2c 7d ca ca 25 cb 5f b3 fe 7b 6d 91 3e 3d 55 5b 32 4d 60 9a aa 21 57 3a 90 c7 56 05 9c be c8 d8 4c 39 51 66 0f 15 b2 e9 c8 ae aa 01 d6 3d 44 c0 33 6c 43 17 22 76 07 08 5d 44 0f 6c f5 18 25 71 c9 e2 92 c3 74 19 dd e3 74 cc ce ee b7 39 8b b6 f4 b1 f2 e7 02 e9 55 d5 31 0c 07 ee 74 c3 30 f4 43 7f 1f a2 7a a4 a6 9a 1a 68 c1 f1 80 f0 9a 03 14 16 92 3b 2f 36 2c a9 73 6b 20 b9 ae 6d eb b6 6b 6a aa a1 c2 4a 18 df 44 8f 52 94 58 55 fa 79 0b ec b0 6b 63 c3 43 92 1d d7 82 b1 86 3d 9b 02 c6 7e c8 b6 8f 88 66 f9 98 65 b7 17 ac dd 76 74 f2 78 98 d5 93 ad 30 e5 67 8d 8f 36 51 aa ba 86 5d 59 9e e1 51 22 84 9d f7 69 f4 7d ce 56 cd 96 2c 53 57 4d b8 07 4f aa 86 81 f5 09 13 f4 18 ab 87 da a0 73 e0 22 56 64 23 58 9e 67 08 Data Ascii: VUWLA,}%_ {m>=U[2M'!W:VL9Qf=D3lC~v]DI%qtt9U1t0Czh;/6,sk mkjJRXUykcC=-feyvtx0g6jYQY`i}V,SW MOs~Vd#Xg
2021-12-02 15:37:58 UTC	831	IN	Data Raw: 57 44 c5 55 2d 15 50 dc 5e 0e c8 ed f9 75 65 e6 00 5d 11 43 62 2a ec 4b f7 2c 61 67 97 11 68 bb 54 8a 6c 5d a9 4d 68 41 e8 4c 4b 43 f4 81 ca 60 1c 53 28 a3 61 c2 c0 1f f5 68 d4 9a 8e 55 e1 a8 b8 26 f2 ae 09 5b fe c0 b8 b8 42 dc a2 67 f4 22 54 e4 c9 b9 67 8d 32 ae 72 61 ab 28 42 e8 77 48 51 0f 11 44 1d 09 0e 29 ef 35 95 f3 c4 d7 14 51 90 4f 9e 6b e4 1e 78 ad 44 b5 00 7c a1 2a f6 18 be 99 d0 b5 e9 26 09 10 ea d2 4d 8c 6d 08 e5 ff 93 72 0b 5c 8b eb ab 30 db 4a 0b 33 dd b4 c0 c3 c8 b7 25 b6 8e 17 90 6e 5c cb bd 50 20 d9 e6 7b b7 d8 e2 4a bf 5f 8d 87 6f 93 72 0b 51 e0 da 97 1d 45 d9 e3 b2 99 af f3 b0 17 70 78 99 e0 64 f7 24 e4 23 bb da 91 39 e2 3e 5a 48 5e d2 72 ca 5c f4 7c 51 7e 89 af 7e c8 2c fb 1f 45 88 17 1f ad cb 2c 07 01 01 ac 64 df b2 a7 4d 32 07 2d e6 b2 17 1b da cc f9 51 13 b0 54 a2 c4 5b 1d c8 f8 41 76 23 de ea 60 38 c6 49 15 d1 50 d6 08 c9 7c 70 3d f4 7e 7c 31 e9 0f Data Ascii: '\$Hbr@F_~("KQx"5zAgTZ=BVw%Z~_XL4{:@8v^pu^ uat)SE2pxd#\$9>ZH^r Q~--,eDM2-QT[Av#`8IP p=-[1
2021-12-02 15:37:58 UTC	832	IN	Data Raw: 04 27 9f 02 91 ac 24 8f 48 b9 dd f0 62 72 0e 40 46 f5 8e fa e0 9a a1 00 5f b2 ab fd c6 12 91 02 da 74 83 5e 28 22 96 ec b1 c4 4b bb 51 78 1d 60 c1 c2 c1 93 cd 1b 35 86 d7 9c cd 7a 41 67 54 af 5a 88 8f e4 dd 9d 3d e3 1d 42 56 bc ec 77 3a c1 cd c8 7f 7f 25 9c 1d d9 a5 5a bb 9f 8b 7e 5f 58 89 4c 34 b6 7b b8 09 06 e7 d8 95 b0 1d c9 3b 40 af 38 e9 f7 05 06 93 08 e7 76 07 e3 5e 08 a9 70 75 15 5e 84 92 98 c8 9e 8c c8 7c 75 c3 61 c7 1f 74 29 53 e7 e1 e0 da 97 1d 45 d9 e3 b2 99 af f3 b0 17 70 78 99 e0 64 f7 24 e4 23 bb da 91 39 e2 3e 5a 48 5e d2 72 ca 5c f4 7c 51 7e 89 af 7e c8 2c fb 1f 45 88 17 1f ad cb 2c 07 01 01 ac 64 df b2 a7 4d 32 07 2d e6 b2 17 1b da cc f9 51 13 b0 54 a2 c4 5b 1d c8 f8 41 76 23 de ea 60 38 c6 49 15 d1 50 d6 08 c9 7c 70 3d f4 7e 7c 31 e9 0f Data Ascii: '\$Hbr@F_~("KQx"5zAgTZ=BVw%Z~_XL4{:@8v^pu^ uat)SE2pxd#\$9>ZH^r Q~--,eDM2-QT[Av#`8IP p=-[1
2021-12-02 15:37:58 UTC	834	IN	Data Raw: 36 d9 5c 64 f9 d3 53 34 8d b0 b8 ab 30 9c 3d b2 29 b9 2a 43 80 0a b1 1c 4b 37 f1 4c c7 d0 55 c7 d6 84 94 eb 24 33 b6 5d 26 bb bd b2 c4 44 63 cc a9 f8 f8 a7 77 51 1a 64 ed f7 76 41 af 76 41 32 4b e9 2e 1c c7 fe 7f 18 22 cb d3 0c d5 b3 54 d7 d5 4d 4f d7 34 01 47 5a 71 be ca 17 d5 68 cf b4 1d 15 05 89 2a 76 5c d5 33 4c 19 ea cc 12 e0 6b b1 e7 26 ba 07 03 d5 03 de 59 b6 ae c3 44 40 e6 6f 7d c4 28 68 07 08 d2 68 78 be 59 e5 29 5b 9d 27 4f 59 b8 fd a8 29 3f ad 07 3e b3 78 9e e4 db 97 9f b4 fa a3 82 5d fa d6 1b 5c b7 ba c1 6f fe e0 e5 e5 27 bd e1 17 25 52 16 61 56 00 d2 f0 df 59 5c c1 7a 92 25 1c 27 ac 97 a7 70 f7 fb a6 7f 2f 2d d8 3a 7a 59 b3 78 ff 67 c6 27 db e7 30 fd 23 06 51 1c 13 05 c1 6c ff f2 c2 23 67 9a 80 57 55 43 52 e8 40 40 5b 15 c8 a6 43 84 a0 7c Data Ascii: 6ldS40=)*CK7LU\$3]&DcwQdvAvA2K."TMO4GZqh^v\3Lk&YD@o)(hnxY)(`OOY)?>xj)o%RaVYIz%`p/-:zYxg' 0#Q #gWUCR@#@[C]
2021-12-02 15:37:58 UTC	835	IN	Data Raw: 96 b7 59 96 6e d8 b5 cc b7 a0 03 01 74 ba eb a0 5f 07 48 59 9a 90 c7 1d 82 95 6d 08 92 ab 32 c2 70 2c 8b 3a 70 cb 83 74 83 1c 10 55 58 89 ce c4 b8 db f8 20 43 3f 77 2a 6b 08 2f 3c d4 85 06 83 30 81 82 11 f2 e9 a6 d2 94 a8 de d7 0e 1c bbb b4 45 26 67 6c 4d 7f a3 70 1a 29 0f d1 8f 57 55 4e 9b a6 aa 62 50 86 58 83 03 61 29 48 d2 5f 48 38 20 ad 00 ff 05 5b e4 c7 ca f0 6d 76 64 c5 cf 95 4f 78 f5 5c a8 32 0b b0 04 f1 23 b8 ec 9f 24 95 52 a1 cf ae f2 7b 28 01 2e 4a a0 7a c0 3f 34 0e 45 bd 55 92 c7 03 ed 44 3b 22 68 e2 b6 fd fa cd e9 50 1c e5 17 d5 64 6c 74 e4 26 34 27 88 49 a7 4f 02 25 d1 02 95 35 36 2a ad f5 cc e5 78 70 5b 51 a5 a9 9f 94 c0 be 5e 24 34 24 b6 07 f0 05 6d 07 51 eb 09 4d d8 43 c5 b5 ab 68 71 ac 7d c2 c7 7c 9e f0 6a fb ae 80 84 99 62 09 df 73 9f Data Ascii: Ynt_HYm2p.:ptUX C?w*k<0E&glMp)WUNbRPXa)H_H8 [mvdOx12#\$R{.(Jz?4EUD;`hPldt&4!O%56*xP[Q\$ 4\$mQMChq]]jbs
2021-12-02 15:37:58 UTC	836	IN	Data Raw: 87 b4 a6 53 27 b2 96 4e 70 d2 09 3a 93 6e 6f 34 19 0d 84 65 c8 c4 a9 60 7f e5 fb 9d 4f ad f6 cd c4 bf 6b 05 b7 93 ab c0 bf ed 9c 3a 92 5d 11 34 3b ba ea 0d ee 26 1d 7f d8 1e 04 7d e9 b2 24 e7 45 cd de 3e fb ad 8e 3f 38 f5 21 13 6b cd 3e fa 83 de 5d 7f 24 84 47 ec 75 9a 5d 0c fc 5f c7 c1 c0 17 42 23 6b b1 9a bd 8c be fa fd 77 b6 5b 3c a2 10 5c dd 05 83 41 6f 10 74 af eb dc 9d 0c c7 9f 28 46 f8 27 21 8d 25 ec 29 38 ec fa a3 87 de e0 06 79 74 75 e0 28 1d 1f 82 ab 40 88 b7 44 12 35 ba 6a 5a a0 ec 4d 9b 46 27 c3 d6 9d 2f 9d 8a ec 78 a8 d1 cb 03 ed d9 a4 df 16 42 23 92 9d e8 a3 77 6a 25 bb 7f 13 cc fa 83 e0 be d5 fe 32 e9 b4 46 ad c9 78 d8 ba f6 25 e5 24 5c 97 09 8e 86 24 3d ea e0 22 e3 17 b9 fd 6d ef 5a 80 47 49 47 22 31 1e 8d fb 93 fb 60 18 7c 0a ca 24 6b Data Ascii: S'Np:no4e'Ok:];&]>?8!k>]\$GuJ_B#kw[<Aot(F!%)8ytu([@D5jZMF/xB#wj%2Fx%\$n\$~"mZGIG"1`)\$k
2021-12-02 15:37:58 UTC	837	IN	Data Raw: b4 64 f5 60 db b0 6d d7 76 4c 6e 20 d3 33 0d c7 3e 1d 3c 64 c5 92 a5 55 e3 2c 57 85 2d 75 c7 b4 2d d7 33 2d 47 73 88 6f 6f f3 f5 6e d3 48 77 2d d5 f0 1c 4b 85 dd 75 55 57 0d 97 a8 c2 f7 32 f7 14 18 ba ac ad 72 cf d6 0a cb b0 cf aa 48 0a 38 7c a7 f4 ee 8a 7c c3 e6 49 59 61 ab ca b3 f1 c4 1f 4d 66 d7 61 f4 fe 59 b2 dd 2a 57 79 be 5a 33 e5 1d 86 3c 0b a2 7e fd c3 9b 76 d8 78 e8 47 cf 7e 12 3f 88 c7 33 68 b5 5d 27 73 76 97 af 17 ac 28 85 3a ed 34 f1 07 5f 19 c6 e4 ba 3d d3 c4 2e da c9 e4 67 5d fc ac 8f 19 60 1c 0c 90 4a 30 cf 1e 1e 3a 0c 35 db de 9d da 3e 67 cb ea 4 1f 9f 77 4c 55 d5 9f 2f cb 6d 92 b5 7f 24 ca 5d c1 96 af 3f 9f dd 55 d5 b6 7c 75 79 59 ee b6 db cb a8 2e 56 c2 ea 17 f3 73 39 df 1b f1 32 c9 ca af ac b8 d4 3d 91 a4 9f cf 94 2a 29 56 ac c2 fc Data Ascii: d' mVln 3><dU,W-u-3-GsoonHw-KuUW2rH8 YamFaY*WyZ3<--vxG~?3h]`sv(4_-g])J0:5wLU/m\$?U uyY .V6[s92=*)V

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	839	IN	Data Raw: 58 16 c0 f8 54 83 30 e3 bd d7 3a 5d ed 57 ae 67 3a bc 94 42 69 0b ff 18 0e f0 8f 78 6d 6f 88 36 7e 4f fd 5f 9b 45 94 a1 bd 5e 07 05 08 e5 03 f0 8a a0 40 fd f6 2c c3 74 89 75 c6 5d 2e 6e 32 5b 88 41 35 37 0d db 44 77 64 a1 41 72 0c 8b 5a f9 a8 db b1 54 9d 37 50 ae 89 02 02 ea a4 9a 36 09 ae 31 db c9 20 a9 55 20 dd 70 22 2e 48 48 8b 3c 9b 63 e4 39 c0 ee 0b 65 c8 33 71 ef cd 47 d0 e2 18 71 02 f3 c8 f1 72 87 26 18 d2 0e 5b a2 1e e3 8d 93 80 69 9f af f6 d8 13 5d fc 37 bd cf 13 cd 4d cb 96 25 46 7a ba 77 f9 8b ed 0a 4a d2 0e 66 00 7b 06 78 8a b6 c5 d2 0d bb a5 cb 16 68 19 80 47 77 1d 74 bb 00 0e 4b 23 c1 e7 cf e1 d0 da 39 6d c8 22 4c 2d 8b f7 b1 96 07 26 85 5a 4d 69 11 9f b0 30 2a 14 1e e5 79 b2 ae 38 6f 5b a6 59 7a 14 5f 2f 1a 61 e0 45 50 03 9d b6 0d ee 00 92 Data Ascii: XT0:]Wg:Bixmo6--O_E^@,tu].n2[A57DwdArZT7P61 U p".HH<c9e3qGqr&[j]7M%FzwJf{xhGwtK#9m"L-&ZMi 0*y8o[Yz_/_aEP
2021-12-02 15:37:58 UTC	840	IN	Data Raw: 3e b8 1d 46 22 f4 51 52 d7 e2 a0 8d bf e6 5d f2 b7 7f 9d c3 2f 05 fb 9a ac c5 0f 65 be ac be 26 05 53 22 7f 8c 7a 59 22 8d e0 c9 ba 39 e0 37 2a 8e ea ba 86 0b 3a cc cf ac 28 09 7f e2 a4 e5 e9 f3 8b 83 43 15 c0 6c 5a f2 9b b5 45 c3 50 6f 82 7e e8 cf 46 f1 74 12 8c 66 7e bf 1f 4e c2 38 f2 af 67 bd f8 e6 26 88 26 e3 53 25 64 57 66 54 ce b4 1f c6 b3 0f 53 ff 3a 9c 7c 3a 95 20 43 34 22 a1 e7 47 bd e0 7a f6 76 3a 99 c4 11 d5 81 de 45 51 09 71 34 c1 06 a0 45 30 e6 7b 3a 15 22 6b f3 88 90 7e d8 9f 45 f1 64 36 19 91 6d c8 38 27 99 3f 08 82 fe 5b bf 7f 7e 16 dc f8 e1 f5 6c 10 06 d7 fd 53 41 b2 b3 fd 6e 41 83 78 74 33 eb 07 e3 de 28 1c 4a b7 25 39 1b ea 96 f6 2e f0 fb c1 e8 54 86 8c 71 75 cb 18 8e e2 9b e1 84 98 87 f6 2f dd 22 46 c1 87 69 38 0a 88 69 64 ed 53 b7 94 Data Ascii: >F"QR[e&S"zY"97*:(ClZEPo-Ftf-N8g&&S%dWfTS:]: C4"Gzv:EQq4E0[:"k-Ed6m8"?]-ISAnAxt3(J%9.Tq u/"Fi8idS
2021-12-02 15:37:58 UTC	841	IN	Data Raw: a2 6c 49 ac dc c6 29 55 72 8a 41 ba 76 4b 49 45 94 92 bc e6 33 61 0e db 75 6c d3 56 0d cd 53 1d eb 78 a2 21 74 65 3b 9a c7 39 25 98 b0 d8 65 5f e3 32 be a7 49 96 37 1a 4c dd b3 51 4b 1b c2 ae a6 db 8e a1 89 b6 26 71 49 4a c8 e7 74 dd 2e 34 56 ee e3 35 cd 56 49 bc ab 92 8a af db d2 75 cd 54 6d d7 30 34 68 54 0d 4b d4 95 a5 f4 4b 5c a5 50 96 56 4a f1 82 28 45 49 6e 63 4c 70 a6 40 b5 ba a2 e9 8a e6 2b d2 ac 35 66 2e 52 d2 ac 3a e3 fa 2d d5 53 31 81 e9 68 aa ab bb 9e e5 f6 ec 4a 12 a7 8d a1 8d 9c 6d d8 b6 6b 3b 26 73 95 e9 99 86 63 f7 c8 c1 51 1b 2a 7a f7 65 5d 15 1e d1 d3 d3 b6 5c cf b4 1c cd 11 22 e1 26 4b aa 2d 1f 6c a9 86 e7 58 2a 36 43 57 75 d5 70 05 03 07 1f f3 6c 4b 57 a4 28 ab 44 59 df 17 67 0a d9 b1 99 d9 e2 29 4d 95 67 b3 b9 3f 9d 2f af c2 e8 ed 33 Data Ascii: lI)UrAvKIE3aulVSxIte;9%e_2l7L5H&qIjLt.4V5ViuTm04hTKKlPVJ(EIncLp@+5f.R:-S1hJmk;&scQ*e])"K-&K- lX*6CWuplKW(DYg)Mg?/3
2021-12-02 15:37:58 UTC	842	IN	Data Raw: 91 2d 86 a4 4d 49 ab 36 92 5b a5 09 e9 d6 f4 9a eb b1 c1 d8 2d 83 65 b0 aa 5b 06 83 cd 23 3d 41 ce 9a 93 66 b4 0e 80 00 c7 37 1d 17 18 61 9b 9a 2b e4 e7 0c ae 5f c5 8c d4 90 da 4f 58 07 fd ca f6 0b 1f 37 08 30 74 12 c5 2e 4e b9 bf 10 9d 8d 3b 4a ba 2b 3b 2b 39 54 11 34 49 b4 51 d2 82 17 6b 10 0e 3b 03 d3 02 3c b8 e8 b3 f4 ba 23 b2 5c 11 71 a2 a6 dd d8 55 25 d0 b1 01 9d 92 fc 85 a6 83 71 24 d4 68 4f 37 2c 40 84 e5 a9 32 d5 75 9a 70 e8 ad 2b 4f ca d2 a4 99 0b b1 79 c7 6b 3f eb 72 50 ba e2 cd 23 ab c7 c8 83 1c db 5f 63 8f 3d 20 4b ba 63 98 9e 87 1e c8 b2 80 06 82 3d 94 7c 89 ef 62 74 56 8d 90 c3 70 1c d6 5b f8 63 38 28 ac c2 06 8f 3a 50 3b 32 be a9 57 67 ca 8c 3e 1a 47 f2 96 41 b4 b6 71 20 04 7e a1 7a 23 8a 40 21 3c cb 30 5d c1 59 fb a1 81 7a 7d 50 2d 1a Data Ascii: -Ml6[-e[=#=Af7a+_OX070t.N;J+;+9T4lQk;<#qU%6q\$hO7,@2up+Oyk?rP#_c= Kc=,btVp[c8(:P;2Wg>GAq ~z#@!<0]Yz]P-
2021-12-02 15:37:58 UTC	844	IN	Data Raw: 45 d6 64 bf 09 42 6f ce 4a ae eb 82 be d8 aa 83 2e 4a 72 2d c8 8a 64 dc f5 1e ab ce 84 bd d3 ae 1f 8b 75 12 ab 7f 1c d8 81 a2 1a ac 5e ba 86 0d 52 e3 99 9e 00 3e 72 7a e5 82 1c 82 81 9a 1a f8 08 a3 41 a6 2c ea 7f fb b7 b7 ac 1e 6e e2 fc 54 89 49 be 9f 07 3b ba d7 06 b8 60 7a 1a 9a 67 0d 80 08 54 74 10 09 3d f6 74 0d 2a 97 43 9b a4 59 9e 81 0e df 05 39 b6 75 f1 f2 a9 db e9 fa 02 b7 11 83 df 3d 64 ae ad 69 96 aa b2 58 13 ef 2d 9b 59 aa f2 e0 dc dc 75 54 9b 9d 45 8a ac 53 37 c1 11 4c c1 6f d7 55 d2 48 54 5b b4 cd bc 96 ec d1 2a 7e bc 50 ab f3 18 c7 c5 de 6b e8 33 f1 d1 05 b5 eb c1 85 4e 43 23 a7 e9 aa 87 dc b7 59 ed b1 d8 31 b4 c8 1d 62 25 6b 88 e5 1e c8 62 3b 77 ac 59 6f a1 0a 75 e6 66 12 9d b2 fa f0 e5 df a7 6c 9b eb 67 92 24 35 ce 57 a9 52 64 9b f2 33 73 Data Ascii: EdBoJ.Jr-dur">rZA,wnTI;`zgT=t*CY9u=diX-YuTES7LoUHT[*-Pk3NC#Y1b%kb;wYoufIq\$5WRd3s
2021-12-02 15:37:58 UTC	845	IN	Data Raw: 72 75 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 00 00 00 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 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 72 75 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e d5 5c 7b 6f 1b b9 11 ff 2a aa 9b 3f 2e 85 e3 f0 b9 4b a6 77 3d 28 d6 da 51 63 4b ae 1e 0e 52 18 10 64 59 4a 82 26 76 6a 3b 38 14 07 7f f7 ce ee 72 a3 a1 66 28 c9 8e 93 c3 21 80 22 6b 97 43 72 38 f3 9b e7 ee ef 3b 52 48 e7 9d b1 99 34 ce 59 25 ac cc 77 5e b4 7e df f9 34 bf b9 99 be 9b c3 f7 9d b3 2f c2 c8 bc fc d4 a2 fa 54 d5 a7 2b 3f 8d 44 bf 5f a0 df 17 3b 77 bb ad 1d a9 a4 f6 36 f7 4e e5 4a bb dc 7a 25 58 ea 53 44 a5 fe 3e af 3e 7d 6b 49 52 e7 2d 34 7b 75 af 11 e8 32 5a 83 51 88 86 6a ad 2e 4e 67 d5 a7 c5 17 30 25 89 46 9f d7 b7 Data Ascii: ru/PKPK)Q_locales/ru/messages.json{0*?.Kw=(QcKrDYJ&vj;8rf(!"kCr8;RH4Y%w^~4/T+?D_;w6NJz% XSD>>)kIR-4(u2ZQj.Ng0%F
2021-12-02 15:37:58 UTC	846	IN	Data Raw: d0 bd c3 bd e0 c7 38 f8 4f 65 20 49 de eb f4 a1 ca 69 35 c6 08 88 f0 3c c4 f6 39 48 04 84 f7 59 42 64 c5 12 bd 22 7c aa b5 c6 5c 2c 35 2c a8 fe 94 68 e4 1c b1 00 33 c2 93 78 ba d6 76 d3 c4 6a 3f a1 21 18 39 e5 52 a1 35 86 b9 b5 ee b0 9e 3f 7d d1 ec bc 14 14 29 85 57 a5 af a6 12 71 2e 76 bd 67 e8 8c 67 79 d0 a6 c1 20 bf 3d ce 7c 86 16 17 21 cf 2e ce 93 e0 ac 20 ce 3f 26 39 86 25 2b ac 0c 5d 08 5e 63 80 e3 dd 26 d6 0c 21 22 62 20 ca d2 04 9b a1 a8 a6 a5 94 1f 1f 79 70 56 71 a0 81 2f e3 19 6a d2 1e f1 e2 fe f1 c9 8b b3 cb b3 4b f9 b4 b5 3a c2 20 63 17 41 7c 14 4b 45 e8 4d 4e 66 bd ac 62 da 91 96 a3 fc 62 93 63 70 98 d5 78 3a 8d 0e 3a 5a 4c 48 10 fc bd dc 9e 7a 4a b2 b6 eb 33 0e 41 8a 9a 54 c0 59 65 7f f7 21 d2 ad c8 e9 88 5b 73 b4 02 0c b4 19 3e 4d 74 38 Data Ascii: 8Oe lI5<9HYBd"[\,5,h3xvj?l9R5?)Wq.vggyp = !. ?&9%+^]c&!"b ypVq/Jk: cA KEMnfbcbpx::ZLHz3JATYe !>M t8
2021-12-02 15:37:58 UTC	848	IN	Data Raw: 23 b1 4f 91 8a 4b 4e ff 84 48 a1 ba 64 64 8e b1 41 c5 0e 24 4d 3b 2e 9e d6 4c c8 3c e8 97 f6 39 28 9c 13 56 40 0c fe 98 80 7d 86 81 f5 e0 b8 9e 32 87 e0 15 54 bb cc de 80 e0 29 6f 79 d1 bb 40 5a 88 bd 4c ac 91 18 d1 b1 9f 43 8b 12 4c 1f ea f6 95 ed 40 ae 5e be 2f 6b e8 56 02 40 41 00 ae 35 e0 d4 9a 5a 2b 8e 9a 70 1c 1c 4c 59 69 c1 14 f0 1e 4c b6 03 97 5f 48 5e 04 99 fe ba b5 a9 e5 46 f2 23 e7 6d 43 fc 52 2b 45 26 c0 d8 49 f0 1a 64 ee 41 25 c0 72 f0 2b fa 86 84 e6 4a b0 f3 6a 7a f9 ee ea cb ed 0d ce 62 22 43 82 dd f7 14 56 c4 82 fd 67 c8 8b 87 40 a3 e1 b9 cb ca 07 26 20 7e 73 65 b7 7a a6 89 a7 f1 b7 6a 4f df d4 2a 50 4f 65 ca e7 84 94 b1 1a dc 01 9b d9 44 6f 28 11 ab b4 93 8b 6f 9a e2 8d 6e 65 ed 7f 6c 5f 2e dd fd 8f 6b cb cd ac b3 1e 1c d7 4c 82 1b 06 06 Data Ascii: #OKNHddA\$M;L<9(V@)2T)oy@ZLCL@^kv@A5Z+pLYiL_H^F#mCR+E&IdA%+Jjzb"CVg@& ~sezjO *POeDo(onel_ kL
2021-12-02 15:37:58 UTC	849	IN	Data Raw: 6c 64 77 32 1c bf 2c 79 04 3f 11 31 66 9c 76 42 b0 57 8c de f4 07 af 41 8e 0e 0e 8a 41 29 8e 6f ba 07 5d c2 6f 26 bc 4e 92 4a 6d 90 7b 13 5c 92 c8 b0 7d 5c b0 4b e1 da 69 92 54 de 94 67 36 39 d9 27 ac a1 9e 30 a5 d1 5f 1d c5 3d 85 4c 86 9d 0c ba a7 ed fd b7 93 4e 7b d4 9e 8c 87 ed c3 82 51 27 f2 90 2d 21 33 2c c3 16 1e 5c 38 7f 88 1f 7f d4 3f 24 f0 c8 e4 33 99 c1 a3 f1 c9 e4 b4 3b ec be ec 56 42 96 3c 52 e6 0d 53 94 5a ff 60 f4 a6 3d 48 4b 3e e7 63 11 2a e3 de eb 5e ff 0d 19 cb a5 a3 c9 d8 d3 6e a7 48 a3 3d e3 c4 27 28 0c 8f fb fd d1 ab 5e 31 24 5c e5 de 55 47 88 bc 2d a8 b1 62 de 8e 50 8d 1b 1e 4e 0e 00 90 41 7a 47 7d b0 35 43 02 5f dc 53 0e cd 48 e0 14 a0 4d a7 e8 75 29 62 71 4f 87 c4 e3 46 dd e3 02 16 4c 14 8f e9 31 68 06 1e 57 d6 ac 57 ec 8f c2 aa 09 Data Ascii: ldw2,y?1fvBWAA)o]o&NJm(f))KiTg69'0_ =LN{Q'-!3,8?;\$3;VB<RSZ'=HK>c^*nH=?(^1\$UG-bPNazG)5C_S HMu)bqOFL1hWW

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	850	IN	Data Raw: d2 ae d2 f4 4b 4c b5 6b 58 bc 0b 7b 1d fe cc 4f 9a b0 18 0d 5a bd 77 7f ab 7e a8 3e 9e 61 48 59 4c 66 74 91 c6 73 9a 17 d5 58 6a b3 ea 2f b3 34 29 69 52 b2 81 bd e3 13 af 8d a5 9f cd ea e7 c3 d0 a4 07 ac a3 07 94 08 f6 d9 cb 4b 83 97 a6 d9 e2 d4 51 7f 7f 4f fe f1 b0 a6 ba ae ff fd 7d 91 91 a4 fe 0b d1 16 39 7d fa f1 e1 6c 51 96 59 f1 e1 fd fb 62 9d 65 69 5e 5e 7c a9 7c 73 31 4b 57 ef 67 7b 9f be 27 49 f1 95 e6 ef cd a0 ca ea 87 33 ad 24 f9 17 5a c2 7e fa 18 93 64 f9 70 56 03 b3 97 68 33 2c 6a 81 1f 73 fa ef 75 94 d3 f9 0f 62 44 30 4c be fc 50 2c d2 af f8 f1 2f 65 9a 5d 14 eb a7 a7 68 16 61 72 97 94 ce 1f c9 8c 41 55 2e 40 d8 3b 9e 63 da 78 a7 67 99 ba e7 1a 52 d0 55 b9 4e 49 bc 4f ee 25 c6 9b f0 c4 37 72 fa e1 37 af a8 d2 e1 c6 2f ad 88 29 56 44 31 62 e5 Data Ascii: KLkX{OZw~>aHYLftsXj/4)iRKQO}9j}QYbei^ s1KWg{!3\$Z~dpVh3,jsubD0LP,/e]harAU.@:cxgRUNIO%#7r7j)VD1b
2021-12-02 15:37:58 UTC	851	IN	Data Raw: 62 38 ec 75 10 c9 79 1a af 31 e4 3a 31 77 87 14 2f de 18 0d f4 ab e9 59 76 10 a0 45 75 1c 70 95 34 1a ba c3 eb d6 ab 53 46 e0 f6 1e 93 22 98 86 83 3f 2c 0f ac 20 d3 0f 4f c8 88 36 66 e1 be 97 1e a4 cb 75 c1 a6 9a 66 64 b9 7e a6 35 69 83 68 c1 3b 08 30 48 a0 c0 b1 6c 5f 72 59 b5 c6 73 45 b0 f0 72 b6 ae 60 20 82 6c cb b5 d1 93 3b 68 cb 3d cb 91 5d af 6e ae 1d dd 64 fd bb 6f 83 6d 21 bf 75 db 7d 23 6e df 10 21 f5 d2 ac 10 64 2b 51 3e 8f 93 bd ce 3a 51 54 38 df 90 7d d4 b3 08 8e b4 e7 b5 36 ab 37 3d 56 94 39 6d 95 ce ea aa 95 8b bd 15 63 ff c4 69 d5 2f f6 70 88 57 48 51 31 a4 e7 79 45 c0 0f 52 43 8f 77 95 39 ab 68 78 4b 74 e8 e1 2f 7e 4f af fe 46 33 5e 77 76 0a 57 bf dd 6b ff c6 f6 1a 59 b2 7e 8c 29 3a bd b4 e4 6d b6 63 5a 6e dd da 39 10 c7 28 93 a6 ef 79 28 Data Ascii: b8uy1:1w/YvEup4SF"? , O6fufd~5ih;0Hl_rYsEr` l;h=]ndom!u]#n!d+Q>:QT8j67=V9mci/pWHQ1yERCw9h xKt/-OF3*vvWkY~):mcZn9(y(
2021-12-02 15:37:58 UTC	853	IN	Data Raw: 17 0c ec 21 7c a4 90 df 9f 95 08 0b 74 7d 86 13 58 7a 80 ee 13 5a c5 94 98 be 8e cc c3 7d 01 1f 2b 15 20 f7 5d c3 70 74 9d 05 a6 24 ca af 1f c4 b5 85 e3 33 0d df d3 5d b6 e3 a2 b3 4d 08 1b ba c4 96 1c fd c0 4f 5b d9 16 c8 8a dd 73 a8 b7 57 9b 75 1d af 48 01 d3 e3 08 1c 03 fd 33 3e fa d0 98 ea dd 98 87 5f dc dd e3 78 86 a9 07 a8 1d 2e 2b 70 0e 3b 33 90 af 44 c8 a7 5c a8 b2 cf a4 de e9 e6 94 99 d1 59 c4 fd cd f6 8f b3 c3 35 8a fb 41 ef 5c 2b 68 be a1 39 db a8 f8 cf f6 5c ab 57 26 59 6b 4f 88 e5 af 24 Data Ascii: !j!XzZ)+]pt\$3jMO[sWuH3>_x.+p;3DIY5A!+h9lW&YkO\$
2021-12-02 15:37:58 UTC	853	IN	Data Raw: 8e eb 0d ce f4 a9 14 ba 23 d7 7a ad 11 6f bf d8 01 ac a7 fb be e5 a3 b3 60 9b 9c 72 5b 33 7a 63 fb f5 f5 c6 5a 7a e4 1e f5 2e 1e 9e 16 db 69 76 ce bd 7e 17 76 ba ad e9 b0 3f 19 87 c3 69 ab d3 e9 8e bb fd 5e eb 76 da ee df dd 85 bd f1 e8 74 34 aa e3 76 19 67 d2 e9 f6 a7 ff 9a b4 6e bb e3 cf a7 08 aa 4a 2a 21 b4 5b bd 76 78 3b fd 38 19 8f fb 3d 79 0c f2 19 b6 8c d0 ef 8d 31 01 8c 22 1c b1 39 9d 82 a8 9a 6b 09 a4 d3 ed c4 7b fd f1 74 3c 94 a6 a1 52 e8 92 fd 65 18 6b 7e 30 b6 da 37 d3 f0 ae d5 bd 9d 5e 76 c3 db ce 29 90 ea 68 ab 19 e8 b2 3f bc 9b 76 c2 51 7b d8 1d 28 a7 a5 d8 ed 6b 46 bb 0e 5b 9d 70 78 8a a1 52 95 cd 18 83 61 ff 6e 30 96 dc 23 b7 7d cd 10 c3 f0 5f 93 ee 30 94 5c a3 ea 38 9b 51 c6 9f 07 e1 1b cb 2d ef 0c 49 50 77 dd e1 b0 3f ec f6 ae ea d8 9d 8e Data Ascii: #zo`r!3zcZz.iv~v?^vt4vgnJ*! vx;8=y1"9kL{t<Rev>7^v)h?vQ{[(kF[pXRan0#_0l8Q-IPw?
2021-12-02 15:37:58 UTC	854	IN	Data Raw: ba e7 1c 7b 1f 2e 56 59 5c b2 14 3e 53 b6 c9 58 59 db d9 a6 6f 63 01 2e 4c 7c c3 74 3d cb 38 36 9c f2 95 90 37 d3 17 5c bd 64 7c 51 b2 65 e5 a5 8c 17 5c 6c 44 9e f2 62 c5 6a 67 8e 69 1a b6 ee fa 96 65 c0 a5 6e 39 c4 d9 dd 0e 16 05 2b e3 82 97 da 46 94 7c c7 4a 04 14 6b db 7c c3 13 76 a6 8d 44 be da e6 f8 59 db a5 a2 64 67 8d 63 47 0f 74 78 b6 3d 43 f7 4d 3f 70 fc 37 a2 ac 4d 5c cb 75 7d d7 b3 65 56 ec c0 b6 3c 97 66 24 89 6b 93 54 d4 b7 fd f1 74 3c 94 a6 a1 52 e8 92 fd 65 18 6b 7e 30 b6 9e e1 91 2d bd 4c 58 9e 62 05 cd f5 8e 6e 05 9e a3 23 e5 a6 6e ea 96 4f c2 ea 25 b1 86 5c 9d 3f 65 62 cd 1f 58 5e 54 69 4b b5 52 7b 37 99 f6 c6 d3 f9 4d 34 b8 7e c7 36 49 bc 62 0f f1 32 d6 2e 85 78 4c b8 76 85 cb df 85 83 7e fd fb 2f ed d5 93 51 6f f0 ee ef d5 0f d5 c7 13 44 b1 49 d8 03 7f 12 Data Ascii: {.VY!>SXYoc.L t=867\dl Qe\lDbjgien9+F Jk vDYdgcGtx=CM?p7Mlu]eV<f\$kt6\$:-~;-LXbn#nO%)?ebX^T iKR{7M4~6lb2.xLv~/QoDI
2021-12-02 15:37:58 UTC	855	IN	Data Raw: 57 f6 04 10 90 e8 5a 81 ed 5e d0 63 d5 f7 71 52 a1 6e 86 14 a4 52 cf e3 77 ad 84 94 df 57 e7 5a 66 12 1a 5f ac 9b 7d d1 17 b8 f5 12 cb 49 39 fe d7 9a af f2 46 fb db 0e f0 da c7 b8 64 56 33 8e e3 53 e4 3f c0 e0 fd 28 21 3a 46 09 a9 89 00 8c 81 69 39 c0 69 27 d0 a9 bb 08 8a 0d 0b ab 79 8e ed 89 0e 9e b1 38 81 fe 7d dc cf 43 e8 f8 7a 03 50 88 b2 e0 10 49 c9 33 79 cb 78 2d 37 a2 59 2a 89 01 82 c8 f4 2c 3b 08 30 cd 38 0e 60 97 02 27 5c 6f d7 c9 32 2e 6b 7c b6 3d c9 95 08 d8 c1 3f 96 07 4c 23 7b f8 bb 78 e5 20 3f 77 2f bb c2 db 48 0f 79 07 8c 01 08 45 c9 80 b0 03 c7 b2 7d 92 a9 83 3a 68 3a bf 0e 16 54 6d 5b ae 8d 91 cd c1 d4 e6 59 0e 4d 32 19 be 1c dd 94 93 9d 6f 83 2c a0 e9 74 db 25 65 77 55 b2 a4 2e 3a 75 fb a2 78 ea 8e 05 3c 2c 25 30 bc ea c9 b5 38 44 da 33 Data Ascii: WZ~cqRnRwWZf_]i9FdV3S?(!:Fi9iy8)CzPi3yx-7Y*;;08"lo2.k]=?L#x {w/HyE]:h:Tm YM2o,t%ewU..ux<,%08D3
2021-12-02 15:37:58 UTC	857	IN	Data Raw: a8 06 52 b0 f2 58 b7 b9 18 93 81 e1 04 16 86 58 1f 12 d2 35 09 b3 ed 8b 8c 3e 64 f4 b1 0f 01 5a d3 35 0c 47 d7 65 ad 11 4d 18 e5 ab fd 79 ac ef e9 ae 1c b5 75 39 89 da e0 5f 9b 64 af 1a 2b 81 e6 18 d1 2a b5 2b cf 79 12 f5 79 4a 0d 10 81 14 87 28 03 03 c3 15 3e fa 50 4e 6f e1 b9 ca 51 ed c7 c0 80 8d 2e 77 25 ce 38 f2 a4 93 c4 26 4f 7c e2 35 ab 19 a7 39 69 78 21 ea 4d 75 5a 26 5e 3d 0f d6 ee 46 03 79 8c d8 7e 23 f7 78 93 89 ff fe 9f d3 86 36 31 bc 62 4a d5 76 f1 a2 a2 53 fc f6 98 31 8c 15 70 23 c1 52 68 83 de a4 d6 f9 f2 b1 8d a7 fb be e5 43 de ca 83 29 2a a0 47 1d 67 0c 87 ba a4 4a 68 75 3a f2 fa 30 04 3f 40 70 b7 49 bd 0d fb 51 6f 3e 1e ce a6 e1 78 de eb f7 a3 69 34 1c f4 6e e6 e7 c3 db db 70 30 9d 1c df 59 f5 0c 8e fa 99 f5 a3 e1 fc 5f b3 de 4d 34 fd 72 Data Ascii: RXX5>dZ5GeMyu9_d+*+yyJ(>PNoQ.w%8&Oj59ix!MuZ&^=Fy~#x61bJvS1p#RhC)*GgJhu:0?@p Qo >xi4npOY_M4r
2021-12-02 15:37:58 UTC	858	IN	Data Raw: dd be cd 05 b4 38 92 b9 96 48 2d 1f 32 bc 30 40 d0 d4 c8 36 ce b1 7c 92 8c 00 67 e8 bf 5f 0d a7 c7 ac 66 55 53 64 ac 28 bb 87 00 0a 4d 4e 57 77 bd 9f 3d df f6 a4 90 3e 78 63 9d 34 de 5b 25 ac 2c f6 9e 77 be ed fd 5a dd dc cc df 57 f0 79 ef ed 57 61 64 51 ff d5 a2 fe 6b f4 f2 af 5c fe 55 ab ef f5 f2 b3 0d cd 37 9d d5 43 da ee dd ed 77 f6 a4 92 3a d8 22 78 55 28 ed 0b 1b 94 60 b7 9a 2f d7 54 4b 60 1e 01 6b be d2 06 43 7e d7 c0 6f 7e 58 7d b6 cd f7 cb d5 c6 e2 d5 97 cb af dc ea e7 74 8b 8b 15 3a f1 07 89 4e d3 a0 46 e1 c5 8d ea 8a 3a 71 71 7c 74 b1 fc 41 a0 b3 ba e6 d1 5f 22 61 80 24 ce 17 ce 38 a1 65 10 85 65 e9 52 21 82 cf 11 44 bf 22 7e 3c f9 1c 6d 1e b9 85 36 b7 8a 20 29 9a 73 18 e5 0d 88 81 83 23 78 a9 5c a1 e5 06 06 61 ce 63 72 ab d5 4e 46 75 08 e6 97 Data Ascii: 8H-20@6 g_fUSd(MNww=>xc4[%wZWYwadQkU7Cw:"xU('TK<c~o~X)!:NF:qq tA_"a\$8eeR!D"~<m6)s#x \acrNFu
2021-12-02 15:37:58 UTC	859	IN	Data Raw: 9c 98 dd c7 53 a2 42 54 63 8d 13 43 95 4d ba a2 cc 61 4b 95 58 0a 7c ca fd 66 05 4a 28 9b ca 4f 34 7d 6d 51 0b 3b 20 5c 22 88 07 42 e2 fd 9d 54 4d 66 f7 b4 f9 d7 fe 2e 2b d7 a5 28 59 40 2c b9 c6 e6 a8 59 95 9c 1d d7 ab 70 71 63 91 9c 0c 5b 3c 54 6d c1 84 61 4a 20 80 25 e4 4d 09 8e b4 56 98 90 9d 30 a2 75 53 1d c4 fe 68 de 69 66 3f 47 ac 61 44 0b 5b 75 92 23 b3 c7 c7 6c b5 e8 29 5a 76 ba c8 e8 84 c5 07 c7 29 be c5 a4 d3 eb 3c 62 24 d2 e1 c3 e0 83 53 93 21 b2 ee 1e a5 7d 06 6f ba 45 c9 c0 e8 58 92 4a 0a 61 bb 3a c4 07 30 33 96 51 bd 8d 41 64 6a 72 12 aa fc 00 43 f2 d2 86 e3 43 5c 95 5e 30 52 95 54 83 24 fa 25 c5 ef 92 00 46 65 e8 44 0b b1 04 18 5c 4f c5 2a c2 d8 ee 86 b9 2a 71 0c 49 f5 6a b9 b0 c0 32 93 33 0d 09 e3 36 fb 04 bc 9a 5a d9 b4 96 b6 9f 10 09 1d Data Ascii: SBTcCMaX{fj(O4)mQ; !^BTmf.+(Y@,Ypqc<TmaJ %MV0uShif?GaD[u#]Zv)<b\$S!)oEXJa:03QAdjrCC^\0 RT\$%FeD\O**qjJ236Z

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	860	IN	Data Raw: a4 5a c3 4c cd c7 cd 1a c8 a6 be 6c a2 8c d5 10 23 40 46 9f 19 b9 fc 33 9a 8c 38 6e c2 4d 64 a6 3a 82 85 30 1a da c7 9e 9c a5 84 7c bc c1 59 67 bd 0d 10 fa 3a 09 61 1e 38 60 88 f6 ee 1b 76 4d 84 9d c9 74 73 a5 8d ea 00 89 7f 53 77 76 4e 02 17 7d 90 aa 50 de 6a c1 08 27 da 3d a9 cc de d3 8d 49 cd 72 36 53 6b 4e 11 20 36 2f b4 0e 10 a6 83 a1 f1 41 b0 92 ac 34 41 b5 e0 6d 17 b2 88 4b 47 84 d4 0b 1f 1e 19 13 a6 99 58 31 75 6f 3c 81 2d 70 20 eb b6 0a 23 f0 9c 02 52 ca f6 f8 ff f9 e3 01 49 1b 60 e0 14 26 73 ed 2c 6d cc 33 74 ca 32 39 17 fd d9 0e c4 7d 4f 89 96 27 66 86 b6 90 98 39 b9 24 b8 42 97 6b b8 e0 83 6e f1 3b 2d 19 53 58 46 3e 68 cb b2 03 62 70 32 ed 84 87 a9 ee a9 51 a7 9a 94 14 76 70 eb 1e 63 c3 94 b8 91 1b 6e 59 9f 29 ec a4 53 50 f8 08 4c 28 db 21 Data Ascii: ZLI#@F38nMd:0]Yg:a8`vMtsSwvN)Pj`=lr6SkN 6/A4AmKGX1uo<-p #Rl`&s,m3t29)O'f9\$Bkn';SXF>hbp2Q vpcnY)SPL(!
2021-12-02 15:37:58 UTC	862	IN	Data Raw: 8e f2 92 cf c5 69 04 ca 74 f0 6a 30 7c 4d d6 72 05 7d b2 f6 bc df 2b f3 d6 9e 49 79 32 10 c6 a7 c3 e1 e4 e5 a0 1c 13 aa 72 2f e9 23 40 de 94 d4 59 31 ef df 58 ae 1b 1f cf 8e c0 20 83 f4 4e 86 e0 6b c6 c4 7c 71 b7 47 da 95 40 29 b0 36 bd 72 d0 a7 16 8b bb 16 94 ae 9b f4 4f 4b 38 30 51 3c 66 68 a5 5d 78 ba f4 6f 83 c3 81 2d 70 4d e8 c3 bc df 0f 2d fe 6e 21 1b bf dc 3d 3c 2c cf 26 dd 17 27 44 77 b8 29 a3 3c 9c e3 e1 90 9c 84 cb 93 f3 10 ce ca d1 11 60 45 d0 61 de a7 b7 01 c8 70 48 3c 18 53 e7 c8 03 98 0e fa 10 2a 9c 9c f4 8f fb 0c 4d b8 6b 1e 1c ac 5e 7f 7c d8 1d f5 6a 4e 1d f5 47 a7 5d 4e 15 b9 ab 7c 1c ac a3 fe a0 5c 9a 97 19 68 f6 80 71 3e 5c ff 9d 03 b4 84 91 71 f2 4c 59 97 03 31 e8 d2 f0 8b be ed 8b 5b 39 7c 45 4d 3c 7d 57 09 b7 72 54 d6 06 96 c1 9b bb Data Ascii: itj0]Mrj+ly2rl#@[Y1X Nk]qG@)6rOK80Q<fh]xfpOM-n!!=<,&'Dw<`EapH<S*Mk^ljN]N[hq> qLY1[9]EM<`JWrT
2021-12-02 15:37:58 UTC	863	IN	Data Raw: cc a3 7f 6f e2 3c 9a 1d d5 16 41 30 5d 1c 15 0f d9 6f 78 f9 8f 32 5b 1f 17 9b f9 3c be 8f b1 b8 6e 14 cd ee c2 7b ae aa 72 01 22 db b4 4d cd c0 9c b6 ae 29 b6 a5 92 68 fa 5c 22 04 91 ef 61 1e b1 65 b6 5a 41 0b 1e f3 7f 7f 79 27 a5 8e 56 ff 68 27 b4 7a 27 24 96 4a 77 62 d7 ff ff 43 37 99 ae aa 2b ae a9 38 8e 66 b8 9a aa 12 0c f0 b6 77 f9 63 59 8f 76 0d cb 56 90 6f 48 52 db 51 5c dd 20 70 f5 b5 82 d3 1a 79 d6 cf 70 aa 69 2e 04 15 17 78 65 5a 9a 06 51 02 a7 df 06 f0 55 70 16 c0 59 e3 d1 e1 3a d9 e4 61 72 98 cd e7 45 54 be 57 d9 07 e5 db 45 98 2e b2 4d f9 f4 41 6d 1e d9 2a 9a b1 6f fd e1 b9 d7 0b 7e f5 87 4f 4f 1f b4 b6 57 2c bb 7f 60 6a 65 dc 53 56 3e 44 f9 9b 03 ff 29 06 3e 09 db 0d 03 50 a6 a8 d8 1e 0d 50 63 29 04 a4 4f f3 90 7d d9 68 8a aa b3 d9 76 26 84 Data Ascii: o<A0]ox2[<n(r"m)h\`aeZAY`Vh`z\$JwbC7+8fwcYvVoHRQ\ pypi.xeZQuPy:arETWE.MAM*o~OOW,`jeSV>D) >PPc)O]hv&
2021-12-02 15:37:58 UTC	864	IN	Data Raw: ac 32 91 ff 00 15 02 ad 4b 11 4a b3 d7 15 a3 02 32 26 f8 43 f2 75 33 3b ae 27 b3 d0 fb 19 a0 5d 28 08 1a 7f 92 95 02 6e 35 30 36 12 93 9a 88 58 01 e9 5b fe 2a 65 bf 45 77 77 35 d9 a9 66 01 3c 37 4b 01 9f c2 26 00 60 40 75 c0 ee 5c 42 f4 47 0d ac 3c 67 00 e7 2f 45 cd 42 7e c8 23 d1 8d 21 ee c3 e2 47 a1 d4 42 eb a8 a2 5f 85 9f 1c c5 54 80 ea ed 91 d3 04 41 f7 5a c8 da 40 69 b8 96 97 3c 2c 56 73 4d b2 cd 8b b0 da 8d 98 37 a3 82 6a 83 16 82 6c 9a 2a b6 05 f8 8e c2 65 90 c0 eb d4 8e 89 17 b5 04 22 54 83 81 48 30 c7 40 60 a8 64 dd ed 25 ee 2e e2 cc 98 3b b1 da 4f b1 4f 96 82 a0 05 8f 07 35 75 e1 47 44 1a d1 e8 bd 30 06 ee 42 7e 14 55 d7 97 82 e5 20 7d dc 83 c7 86 26 ec 13 96 7a 1e c7 e2 27 49 40 5d 87 1f c0 58 3a c9 92 9f 58 ff 8e f3 ab 32 cb e3 a2 46 5f cb Data Ascii: 2KJ2&Cu3;'](n506X['eEww5f<7K&`@uBG<g/EB~#!GB_TAZ@i<,&VsM7j]l*`TH0@`d%.;OO5uGD0B~U]&z'!@ JX:X2F_
2021-12-02 15:37:58 UTC	866	IN	Data Raw: f6 a6 93 91 77 ee 4b d2 89 5c e2 10 35 23 4e 36 e4 e0 22 2b 22 72 f9 ab fe 39 81 47 49 3b 21 11 1e 4f 06 d3 9b 60 14 9c 06 55 90 b5 6e a9 e4 7b 08 aa ad df 1d df 7a c3 f6 c8 97 95 37 a2 65 d2 bb ec f5 6f 89 ac ac 49 23 b2 37 41 c7 6f 47 7b 09 8b 68 d1 30 ba ee f7 c7 17 3d 7f 44 bc 2a fb 8a 86 28 f9 ec d3 62 25 b9 8a ad e4 46 e7 d3 2e 00 19 d1 3b ee a3 d6 8c 08 7c c9 6e 24 1a 49 78 0a 68 d3 f1 7b 01 45 2c d9 15 ca 6b b9 71 70 ed c3 60 92 78 92 83 a9 46 f0 ba aa 66 3d ff 6c 5c 5b 4d fc 23 f9 46 68 47 f8 19 21 45 5d fe ce fc c1 d8 3b bd 22 b9 23 3b c0 6b d7 73 de ef 13 4b 64 fc b2 5d c3 c0 1f 76 b1 2a b2 1c c9 37 46 6f 28 e9 f7 49 05 93 90 f1 76 05 93 5e 00 aa 70 75 15 9c 07 12 9f c8 ee 71 64 ba 3a c1 e8 cc 1b 76 f8 4e 75 83 e1 b5 27 4b 45 d9 f5 9e 4c 57 Data Ascii: wKl5#N6"+~rG!;!O`Un{z7eol#7AoG[h0=D*(b%f.; n\$ixh[E,kqp`x Ff=I\ M#fHG E];"#;ksKd]v*7Fo(lv^puqd:vNu' KELW
2021-12-02 15:37:58 UTC	867	IN	Data Raw: 87 f3 f3 75 ba 5c 26 ab cd d9 38 8b cd d9 7d 32 3f bf 3f 84 f5 5c 2c d6 db 68 75 ae 7b 59 11 7e 3f 51 36 62 35 8e 36 b0 1f de cd c4 62 fa fd a4 74 4c 0f 51 ee 67 62 bd c6 97 ab e8 9f 69 bc 8a 46 ef 8b 19 c1 70 31 7e bf 9e 24 5b 7c f9 97 4d b2 3c 5b a7 0f 0f f1 7d 8c c5 35 a3 68 74 27 ee c9 55 16 02 a4 b8 e5 58 ba 89 67 3a 86 ae 3a b6 c6 52 ac 2d 92 45 51 b4 62 24 3e fc e9 0d 94 c6 57 fb 77 1b a0 17 1b 20 99 a0 74 03 5e 8b fd 7f 18 1d cb d3 0c d5 b3 c4 d3 c6 7f 97 ad 04 12 8f 24 9c a5 21 f6 c0 5c 90 88 c9 12 a9 4d 34 5c 0c 46 b2 a1 b5 07 d6 bb ae 89 5d d7 d8 b2 2b 99 26 87 6a 50 37 01 75 e6 cd 56 91 89 10 c3 90 79 1e 42 88 14 62 de da a4 6d 69 de bb 03 e6 af f1 79 81 14 1a 27 fb 6d b6 94 1e a9 00 7c df cc 05 c0 31 19 db a8 2c 3a 81 01 52 ba 74 86 61 1b 2c f1 7f 53 Data Ascii: x.)3'JkM\$+x.<3BLRf&i]>^1't>)P[+~+~+~]4xZ*\$6De"q:F`Dl\$!M4fV+&jP7uVyBbmjy'm 1.;Rta,S
2021-12-02 15:37:58 UTC	868	IN	Data Raw: a7 c2 0b fc 78 2e a4 82 85 fa 07 29 33 27 97 05 e8 1e 4a 6b 4d 8d 24 fd 9e 13 f1 a4 14 b5 e5 9c a7 d4 87 2b 13 fc e5 ac 78 84 8d 2e ca 84 c0 01 3c eb f4 89 03 33 42 4c d4 90 52 1a 66 d5 9b 8e 26 69 7c 3e e8 b6 5e cd 15 02 05 d2 01 00 00 e9 00 c9 e4 31 c1 dc 27 eb d7 74 3e 29 50 5b f9 05 2b 27 f4 8f a6 d1 7e 2b 7e cd 5d da e8 b6 34 b4 78 08 83 ab 5a 2a d0 f5 8d 24 c0 d6 36 db b9 9d 03 bc 44 d4 88 65 b0 22 dd b3 d8 9a ae e2 71 3a 46 60 f6 d4 83 c4 d3 c6 7f 97 ad 04 12 8f 24 9c a5 21 f6 c0 5c 90 88 c9 12 a9 4d 34 5c 0c 46 b2 a1 b5 07 d6 bb ae 89 5d d7 d8 b2 2b 99 26 87 6a 50 37 01 75 e6 cd 56 91 89 10 c3 90 79 1e 42 88 14 62 de da a4 6d 69 de bb 03 e6 af f1 79 81 14 1a 27 fb 6d b6 94 1e a9 00 7c df cc 05 c0 31 19 db a8 2c 3a 81 01 52 ba 74 86 61 1b 2c f1 7f 53 Data Ascii: x.)3'JkM\$+x.<3BLRf&i]>^1't>)P[+~+~+~]4xZ*\$6De"q:F`Dl\$!M4fV+&jP7uVyBbmjy'm 1.;Rta,S
2021-12-02 15:37:58 UTC	869	IN	Data Raw: 91 d1 83 dc be d5 b9 60 f0 28 91 fd 12 e3 fe e0 7a 78 13 f4 82 cf 41 96 64 95 5b 2a b9 eb e7 de 3a cd fe 6d ad 5b 9d f9 32 f6 62 5e 06 e1 55 d8 b9 65 b6 b2 4e 8a d9 de 04 0d bf 1a ed 25 8a a0 c2 43 af dd e9 f4 2f 43 bf c7 a2 2a 7b 27 84 39 f9 ea 73 b2 92 5c 33 66 76 bd 8b 61 13 80 8c ec ed 77 c0 35 3d 06 5f b2 a3 fa d2 12 91 02 da 34 fc 30 e0 88 25 bb 59 78 6d d7 0f da 3e 26 cc 0a 4f 72 50 54 1a b6 33 36 0b fd 7a bf 98 35 8b 8f e4 85 97 17 c6 07 84 cc 79 b9 56 af fb d7 fd da e7 16 ab 1d d9 89 5a b5 9f 8b 4e 87 cd 44 a6 16 ab 3d 5c fb dd 26 56 c5 96 23 79 79 e6 0d 27 9d 0e 63 30 89 8a ae 76 30 08 03 48 85 56 2b b8 08 24 31 91 5d 7a c8 7c 35 82 5e bd d6 6d d0 4e 35 83 6e bb 26 2b 45 d9 35 97 cc 57 33 08 fd 0c 5e 86 a8 ec 50 42 3e b2 a3 1d 99 a3 cc 47 05 c9 Data Ascii: `(zxAd[*:m[2b^UeN%C/C^*9sl3fvaw=_.40%Yxm>&OrPT36z5yVZND=I&Vyyc0v0HV+zl]z5^mN5n&+E5W3 ^PB>G
2021-12-02 15:37:58 UTC	871	IN	Data Raw: 44 53 0e 61 b9 fa a5 13 d7 3d b9 e8 0e 7f f8 69 bd 84 f5 e3 01 70 ed e3 fb c5 d5 ea dd cd fb 37 ab db bb 35 bb aa 05 ae ff 73 75 f3 e1 7e f5 e1 7e cd bb 92 cb d5 60 f2 b5 5a 7f bd 61 30 f9 81 46 3f 60 29 98 83 2f 5f 12 1b 39 ff f8 6e 7b 2f ff 72 bc f8 eb eb 4f 2b 21 c4 5f 8e ef 3e 2e 3e 54 ff 59 74 de dd ae ae 7f 7e 7d f0 ee fe e3 dd d3 e3 e3 bb 4f 1f 3f de dc de 1f bd 5d 6f f8 d1 d5 cd 6f c7 57 5f 77 e5 78 f1 e1 ee 5f ab db 63 15 d6 6e fb f5 41 e7 7e 71 fb 76 75 0f e3 e7 cb f7 8b 0f ff 7c 7d 50 11 2e 5e d2 b9 7a bf b8 bb 83 2f 6f 5f ff f7 e9 d7 db d5 9b 27 71 46 30 f0 c3 db 27 77 ef 6e fe 05 5f fe cf fd cd c7 a3 bb 4f d7 d7 bf 5e fd 0a 8b 3b 59 ad de 2c 17 57 05 a9 35 0b c0 5a d9 cc 2a 03 ef cc b4 12 99 93 0d 2a 75 a5 88 ed 30 58 20 91 cd c7 ee 3a ea Data Ascii: DSA=ip75su~~`Za0F?`)/_9n{r/O+!_>.>TYt~}O?}ooW_wx_cnA~quv]P.^z/oWqF0'wn_O^;Y,W5Z*uoX :

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	895	IN	Data Raw: 97 ca 13 ad 9d 96 6b 54 f4 df f9 99 e1 a2 ec 01 0e a5 35 d5 d0 84 af 04 a6 47 8f ae fa 55 d4 33 74 6d 47 e6 8f 36 b7 3f e8 f0 8d 39 dc 19 f1 cf 50 86 e1 24 0c ce 46 bd 6b ed 44 c7 e3 03 6b 16 a9 ca 54 bf 0a 56 f8 59 ef ee c5 43 9f 55 e0 d7 0a 0a 3f b3 b2 24 91 6a ae 14 38 e3 e8 29 c8 36 8a 3a 59 45 af bf 5c 33 2b 47 7c bf a5 7a fe 7f 90 2e dd e5 af 04 ba 36 21 c0 d6 02 75 37 66 71 ac 06 c8 78 a0 27 f8 36 57 17 3d 8f 2e b3 71 ac e0 75 c8 e1 27 01 0f 50 b8 eb 86 e2 d5 73 9e 8a 6b cf 62 72 26 92 b7 15 8f 8b 91 2d 65 6f 27 44 d3 fd 8b 9d 5a da 11 c9 88 57 df 99 4a 0b c5 e2 c4 07 3e 11 3c f2 51 48 03 1e c5 14 26 b9 71 6f 0d da 2d 41 6e 19 c9 08 73 00 82 ef 34 93 82 e2 83 e7 9f 06 97 57 ff 2e 98 87 f8 e3 7b 23 54 1c c5 7e e0 03 bf 01 af 0a 24 7e d2 e4 76 88 fb Data Ascii: kT5GU3tmG6?9P\$FkDkTVYCU?\${j8}6:YEl3+G z.6!u7fqx6W=,qu!Pskbr&-eo'DZWJ><QH&qo-Ans4W,{#T-\$~v
2021-12-02 15:37:58 UTC	896	IN	Data Raw: d8 e9 fa 75 24 af 3a 0e cf eb f9 5c f4 d2 f4 1f b4 98 b9 7e d1 54 cf c4 95 9c 1d 97 b1 8f 30 e8 c1 56 74 23 f4 e4 be 9e c5 df d2 de 35 05 04 8e 29 5a 3d 8b 9a 0a e1 ba 59 73 84 89 a3 42 b8 8e 53 eb 39 68 68 42 cb 2e fd b5 d1 11 1e 19 f0 26 75 59 d7 59 71 3d 93 41 e7 53 23 6b 5e b9 9c cc 75 96 e5 62 f4 b9 3b 40 87 de e9 7f 72 84 8f e3 96 79 85 c5 55 a3 73 09 e8 32 6c 77 1a 08 9b 7b 22 81 6b 76 ee 24 bf 47 b4 51 e8 b4 d6 e6 a0 36 1d 00 6d 15 e9 29 b3 83 3a 6b 67 37 e9 90 04 86 e3 27 1a 15 62 dd 16 a2 65 31 80 a1 d9 b8 53 59 8c ec c0 71 6d a3 e0 02 88 4a d4 e5 38 a5 b0 ef df 35 06 7d 42 e0 ba 7f 5f 10 dc 34 68 fa 72 fc 6a c1 be df 4f 53 52 9e 5d c3 42 fb fe a0 e3 da 82 6b 38 6f 29 ee bb 37 83 5b 42 e1 fa a5 dc eb eb 7f 00 50 4b 07 08 99 e0 54 92 df 0f 00 Data Ascii: u\$:\~T0Vt#5)Z=YsBS9hbB.&uYYq=AS#k^ub;@ryUs2lw{"kv\$GQ6m):kg7be1SYqmJ85)B_4hrjOSRjBk8o)7[BPKT
2021-12-02 15:37:58 UTC	898	IN	Data Raw: 01 7c db a7 0b 01 74 f4 85 0b a8 58 05 d0 38 30 8b d1 15 42 c4 c2 46 51 46 21 ae bc b5 12 0b 2a 84 12 90 e4 64 d6 56 25 78 ef 8a 2c 42 ac 88 e6 a6 70 0b 1e bf 03 d3 6c ab 51 05 04 9a f3 40 6a 51 c0 3e 7a b0 6c a4 da 6f 2c 15 4f b7 36 3a c9 2b 94 6a 49 ea 5c c0 fd c0 ee e2 19 48 92 8c 46 3a c9 02 fb 47 f5 0d e4 4d 6c 4e 28 9a b0 b6 11 66 93 64 8c 96 42 e3 2d e0 09 42 29 ac 98 79 4f 4a a8 9d 85 e9 29 c4 95 c7 5f d2 c2 c0 21 a8 5c a6 e5 3b eb 50 45 19 2d 50 a2 03 48 84 83 a9 c1 23 2c e7 43 67 14 c5 c0 da 10 9b 12 55 4d 6f 6e 6c c7 9a 8c d3 22 92 09 1f 2d 0f ae 65 bc 5d c7 5f 42 02 cf ee 4d 64 b8 a2 10 41 12 4c 48 8e 18 04 6b 35 69 f7 b6 f3 42 f2 2b 76 5a 75 11 99 de 61 65 4d 6f 52 82 56 a6 e5 ba f3 97 95 b4 1a 60 11 ee ea a6 26 e2 24 52 6a 14 76 47 79 9a 2d Data Ascii: tX80BFQFI*dV%x,BplQ@jQ>zlo,O6:~j lHF:GMN(fdB-B)yOJ}_\!;PE-PH#,CgUMonl"-e _BmdALhk5iB+vZuaeMoRv'&\$RjvGy-
2021-12-02 15:37:58 UTC	899	IN	Data Raw: 9c a2 02 a4 7a 4d ae 72 d1 ef 14 dc d0 5e ed 98 de cb 2c 16 8f ae f7 96 e3 2d 4d 9b 51 c4 3c 4d 67 ad ca 52 fd cf 11 7c 4d ea de 92 90 a6 e9 bc d4 06 ec 0b a1 65 b8 39 50 8b ef b1 fa a6 74 42 22 91 c9 9a 40 e6 2f 22 67 1d 2c 68 7f f4 5c 2d df d1 1f 37 56 b3 c6 03 88 c1 79 0a 00 20 b0 01 38 c8 44 e0 86 68 7a 4a 49 df 6c 12 e0 5b 5b 68 60 4a 00 e9 92 60 d5 82 71 de 21 39 a4 72 4b 53 eb 24 1f 80 f1 4e a9 00 b8 47 5c 7a f4 90 9c 23 6d a4 7d ba 8a a5 02 2c 9c fa c3 9a ce 1f 00 90 22 02 96 39 20 4a db 46 46 76 b7 0b e2 c4 29 fa 07 31 7d 5c 69 2b 7c 44 87 a4 41 37 45 75 d0 c4 f7 90 2d 75 05 fd a9 ac 35 ba e9 c8 52 bf f7 1b 62 ba a9 77 4d 9d 67 db cb 1d f4 63 07 1d 5d 24 57 ba 8e 35 e7 40 7f 6b 4a d0 1d b4 00 d4 d7 00 eb d1 14 0c 8e 65 0e 06 2d ae 40 bc 21 d0 05 Data Ascii: zMr^,-MQ<MgR Me9PtB"@/g,h\~7Vy 8DhzJl [[h'J'q!9rKS\$NGz#m),"9 JFFv)1}~i+ DA7Eu-u5RbwMgcJ\$W5@kJe-@!
2021-12-02 15:37:58 UTC	900	IN	Data Raw: 55 ce cf b0 ab 6c 3b cc c7 9f 2f 28 99 cd b2 0a c6 b0 fb 61 05 d7 d3 09 a8 c2 c5 c5 e4 7c c2 d8 84 3b a7 e4 74 9d 4e 16 27 e3 f9 29 79 ea 6c 32 bf 1c 73 a9 c8 9d 97 73 ba ce 26 d3 32 c2 cb 0a 99 3d 65 8a 0f 37 8b e3 14 45 1d 03 45 9e e9 9f 39 15 d3 71 4e bf f2 af f4 38 c9 d9 db 1c e2 f3 4f 8b 38 c9 79 49 00 cb ec 9b 3b f4 e5 14 0c 88 73 1f 82 0d 89 c7 54 cb b0 94 e1 e8 83 0a b8 fa c0 9d ae 0c 2a 58 5c 23 53 73 34 e4 fa 2d 4e 47 e4 43 af af c7 57 b3 f9 aa 24 62 93 87 63 fe 81 c5 a0 22 8a ef d9 4d 99 13 61 e6 0b f6 41 25 67 e5 78 79 8d 5a 45 84 af 64 50 37 3f 63 1f 54 85 52 91 07 35 bf f2 5d fd a0 06 10 d7 bf 01 7d 90 a7 43 c5 8b fb f2 91 53 97 ea d7 0b b8 ca 9c d2 0e eb 39 9b 97 e5 3f f2 62 c6 fd 8f 67 61 25 1c 38 33 5f 80 be a0 60 0e 5f e5 1b c9 0f 8d 87 55 Data Ascii: UI;([a; tN')yl2ss&2=e7EE9qN8OBy;st*X\#Ss4-NGCW\$bc"MaA%gxYzEdP7?cTR5j)CS9?ba%83`_U
2021-12-02 15:37:58 UTC	901	IN	Data Raw: 76 3b fa 9b f0 7f e8 2b d4 b9 64 5e 33 e7 84 f2 82 f3 4c c5 d1 92 3c 63 36 c8 c3 28 e3 15 2a 2f 12 19 95 c0 3a e6 a5 1a ca cf 58 88 8d 50 48 29 53 ea 2d 79 d9 37 a1 06 b2 90 58 54 49 cb 90 76 ac 2a 43 7d aa bb 44 44 c5 b0 a3 7f c7 2f 0d 55 21 5f 6e 54 ff 97 ae de 69 b9 a5 f7 30 23 9f 06 f1 4d fc 61 44 16 28 33 3a ac 01 d6 34 0d e5 b6 da 04 55 b1 38 06 85 62 4b e5 7d ab c8 1c 2b 0e cd a4 a2 d9 15 56 2a ef 9d 43 0e 43 e8 f0 f9 e8 28 e1 e1 26 e6 81 0a da 08 01 47 25 d8 f6 f5 0a f1 31 3d 9d 22 40 56 cb 9f be 7c 7a b8 2d 3f fd 74 b3 dd de 35 f7 bf f0 d1 af ec eb cb f2 f3 fb 9b 87 fb bb 6f bf f2 af 78 01 e2 63 f4 75 be 38 1f cf a6 7f 2f 16 df 46 64 91 0c 70 a4 ea d1 fe 59 91 7f 56 2b 17 5c d6 90 f5 9e 9b 11 27 3f 35 e4 f9 9c 9a 9b fb 0f cd ed 0f 6a fa d3 a3 9a Data Ascii: v;+d^3L<c(*(:XPH)S-y7XTiv*c)DD/U!_nTi0#MaD(3:4U8bK)+V^C&(G%1=@"V z-?t5oxcu8/FdpYV+!^?j5]
2021-12-02 15:37:58 UTC	903	IN	Data Raw: 78 ae 48 f6 46 39 46 06 c0 02 84 b5 f2 56 6b 9a 22 81 87 70 22 62 59 0e ed 89 56 00 7c 24 1a 87 97 93 51 68 19 5d 37 7b dc 31 7e 2d 41 9d 61 8f 03 8b 06 7d 04 e3 4c 42 f4 ea b4 6d 70 0e c7 3d 7d 5c 8b a1 11 d1 2f 10 b5 37 1f 7f 3e fb 38 ea cf 1c e3 db 94 62 0c b6 83 fe 63 dd 16 dd 43 a6 e5 39 84 a0 3d 48 6a 45 d3 a7 58 82 bc d3 4d 0e 36 77 40 a4 15 de 05 42 86 ff 22 da c1 59 33 2f 6a 31 2d 30 97 fd fc 32 d7 04 f7 09 65 9c ce b5 53 cb 7e c2 1c b1 a4 d6 0c a3 99 54 b0 93 be a2 4f 83 98 db d7 d5 56 03 6e 08 99 aa ca 3f ef 3c 49 14 bd 1b 0e c4 c9 6f 6f c5 e8 17 c0 cf 51 3e c1 cf d1 ce f8 cc e4 b8 5f 3a 35 a3 08 e9 a0 b7 a3 a8 44 d9 f6 a5 ef 69 54 6d 3c 7c 28 bd 85 53 1d 43 53 23 32 15 3e 1f b0 08 be b3 cb a8 c4 02 ca b0 21 c4 3b e0 08 ac 36 e7 8a e8 7a 13 c0 Data Ascii: xHF9FVkp"b"bYV[Qh]7[1~-AaJLBmp=jV7>8bcC9=HjEXM6w@B"Y3j/1-02eS~TOVn?<looQ>_~5DiTm< {(SCS#2> ;6z
2021-12-02 15:37:58 UTC	904	IN	Data Raw: 36 7a c3 2a 16 c5 df ae a7 8b 22 71 4d ae c7 1c d6 b2 7a 7b 55 3c b2 dd e9 e0 28 51 75 39 5d 2c e6 8b e9 ec bc 8b dd f5 f2 fa 05 f9 08 5f 25 61 9c 01 e6 44 e1 ac 58 bd 99 2f 5e 21 8e ce ce 8a 05 85 e3 9b e9 d9 34 f1 77 86 a3 0d aa 1a 5a 60 ee de df a0 92 e5 f8 b2 c8 9a 92 9b e6 0d 6a 79 43 7b b6 be 3a 4d 5c 93 22 68 aa 63 7e 2c 95 3b e1 4e c4 ae 16 d3 d7 e3 d3 b7 eb c9 78 35 5e 5f 2f c7 e7 45 26 9d 92 53 e6 44 cd 92 68 4d be b8 e4 e0 26 2f 7f 31 3f 4f ca 63 a6 61 ca 08 af ae af d6 af a7 cb e9 8b 69 08 b2 c1 2d cd dc db 4b b5 cd cf 56 6f c6 8b e1 c8 cf e1 5f a2 e5 7a f6 6a 36 7f 93 c8 e6 9a d4 44 f6 f5 74 52 0c 57 fb 0c 2b 19 d0 b0 bc 9c cf 57 2f 67 c5 32 f1 6a ee 32 68 a2 e4 6d 91 82 55 e6 36 4a 90 5b 9e af cf 50 90 11 bd ab 39 b0 66 99 94 af dc 31 5d 27 Data Ascii: 6z*"qMz(U<(Qu9) _~%aDX/^!4wZ"}yC{:Ml^hc-;~Nx5^/_E&SDhM&1?Ocai-KVo_zj6DtRW+W/g2j2hmU6J[P9f1]
2021-12-02 15:37:58 UTC	905	IN	Data Raw: 3a 8b e9 25 ed 5f 91 bb 5e 67 96 5d 8f a3 24 73 f7 b6 3e df 5f 7d 9e 7f be ec 7d f7 64 4f d0 60 fd 96 b3 2c d2 ac 3f 2c b2 d4 ae 6d bd f5 9d 39 37 e3 6c 97 9f 7f be bc 78 dd 91 af 87 fd 3b 37 f3 fc 2c 48 db 61 42 bf d6 6a 13 4e b1 86 6e ea ad cb 3d ba 8e 14 f4 14 cb f1 38 0c a3 87 87 24 06 1c c9 1a db 07 01 7d fa 99 5e 3c 3c 9c f3 df bd 9d 9d 68 6b 58 cc 17 51 91 a0 df 5b 5d 72 3f 90 fb ea c8 45 75 86 c5 d6 05 03 13 c3 45 a4 d7 ba 04 97 18 80 b9 7f 18 c6 f4 0f 2d 32 35 ba 45 bd 57 1a 3f 9a cd a2 3b ea d4 5e 4c 3d e1 a8 33 5c 64 13 cf 9a 89 1b 89 58 a4 12 be 12 8c 3b f2 e8 cf 11 66 83 cd cf b9 07 cf b9 9e 4d 17 53 34 42 8b 17 e6 3b 3b 7a c0 ea a9 88 26 fa 4b d4 19 44 f3 8b 55 f1 66 36 bd ce 08 59 b8 39 0d 39 ee 10 b0 8d dd 54 44 57 79 4f e4 22 52 07 c4 ac Data Ascii: :%_^g]Ss>_}dO',?.m97lx;7,HaBjNn=8\$)^<hkXQj[r?EuE-25EW?;^L=3dX;fMS4B;;&KDUf6Y99TDWyo"R

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	942	IN	Data Raw: c0 4a f3 26 f8 c2 de 60 2e 6a 89 c1 d8 72 10 69 e1 50 2e 2a 94 18 e7 3b c6 af 63 e4 46 46 ec b9 54 c0 e2 55 52 04 78 89 8e 46 82 54 23 c6 70 1a bb f4 46 bb c7 b4 ac d5 6d aa ac 8e 94 cc e5 52 86 dd d5 1b b9 b8 05 13 f7 56 35 62 7c e7 76 00 e5 56 35 22 c8 21 e6 92 b8 c0 cc ea 45 fe 86 0d 64 45 10 ac 04 24 9b 4a 20 a8 16 1d 94 46 ca 78 97 59 a9 79 41 ce ca 69 d6 82 01 9d 4d 21 ff 74 80 49 a5 07 8c a9 90 04 e8 7a 93 fc 6f 52 fa 6a 2e c8 f5 2b 5a d4 4f af a9 99 8c c0 b2 12 04 6c b2 1a 62 09 a9 31 56 42 16 c6 a4 c8 4f 00 0e 1d 26 3d b1 de 41 46 21 4e 59 9c 3c b5 cf 17 03 93 c4 ac 8f ca 41 ca db c7 ca 61 cc 66 13 59 ea ad 92 cb e5 08 5d 3a e2 32 46 e8 c2 1b 65 72 bc da ed 49 07 51 74 2b 53 f4 57 a2 e8 37 a4 b1 cc 9a 23 be 8d 2e 66 87 d5 1f 75 12 97 dd 30 f3 79 Data Ascii: J&`.jriP.*;cFFTURxFT#pFmRV5b vV5"!EdE\$J FxYyAiMItIzoRj. +ZOlb1VBO&=AF!NY<AafY]:2FerlQt+SW 7#.fu0y
2021-12-02 15:37:58 UTC	944	IN	Data Raw: b0 cf 03 96 bb 77 fe d1 bb 0f 1b ae 03 8f f8 e4 75 dc 7f b8 cd fb bc e3 3e c1 62 24 b5 fe 7f b7 04 6b f4 7f ff fd 77 02 b5 f9 1f b4 b7 e2 3d 2f 41 65 34 80 e8 a8 cf 82 f9 ee d5 d5 51 ef f6 81 d8 1e 89 93 41 78 0b f4 7a bc 7c bb 98 60 2c e8 83 03 54 b7 fa c1 df 6f 0b 14 2d 91 d0 1a 5f 64 8e d7 b1 eb a8 ec 50 e1 7a 31 29 de 4a 19 c1 4b 7f 94 63 8d c5 44 92 eb 9f 07 ec ab 0b d6 2c 89 cb 95 43 5c 4f d2 02 18 2f da ad 88 95 8c 79 3d 2a f3 00 ca 54 95 94 51 0b 31 80 0f 79 56 97 c6 9a 11 32 56 1c a6 c7 71 6c 9d a5 3c 22 37 77 4a bd 42 b7 28 ec 36 a7 e2 23 a4 50 34 6c 99 0f 1e 31 05 40 f5 1f a5 94 12 a1 62 ae 7d 17 a4 94 06 3b a6 7f 33 5f eb df 71 1c ed c8 88 bc 11 51 cc ec 08 e8 07 19 e7 db de c8 d2 ac a3 64 58 cd c6 1d 2d df 1e 71 ae 82 e3 7b b6 7d f2 67 8a 2e Data Ascii: wu>b\$kw=/Ae4QAxz[`,To-_dPz1])KcD,CiO/y=*TQ1yV2Vq <"7wJb(6#P4l1@b);_3_qQdX-q g.
2021-12-02 15:37:58 UTC	945	IN	Data Raw: ca 4c 82 64 22 0a c7 df 73 76 3a b9 07 87 20 31 8b 8e b7 35 0f f4 ed ae d3 37 06 12 81 4f 5d e5 2e 09 4e 5d f6 c5 e5 e7 cb d0 e3 49 27 d4 b0 63 fb f1 54 6b 42 4e 1e d8 55 34 8f 9a fa 2f 2f b8 b8 b2 7c 60 0c 69 05 fe 8b d5 40 99 70 28 2d 99 9d e3 10 31 f1 61 6c 10 a9 69 68 a2 92 91 6e 8d 48 13 1e 94 a2 4d b1 25 96 2f ed 00 19 be 9d 17 3d 94 63 8d c5 44 92 eb 2b f5 c7 3b 47 63 70 27 9e 0b 92 7a 38 20 4d 70 cf 59 e3 ba 1c 60 38 c6 aa 0d 6f 00 53 6b 9b 04 d1 0f 1e 46 92 20 a7 1f 47 dd ab 34 6a f4 7b b7 df 6f 8f 46 0a fd 57 ad b7 f5 6c 84 07 c1 5e b6 4c a2 eb 6c af 7b 75 b5 76 ea 19 e2 13 9b 72 fb 5e a4 f5 90 87 8a 64 ca 8f 25 7a 75 75 d8 d2 4c b4 7f 44 f5 63 c8 f7 68 d0 1d 00 0d 39 e0 91 d1 f1 06 af ae a8 5f 1e b1 99 b4 dd 31 36 1f 51 f7 b7 d6 08 ef 5e ec 34 c9 49 Data Ascii: Ld"sv: 1570J.Nj 'cTBNU4// 'i@p(-1aliHnHM%/=Il+;Gcp'z8 MpY`8oSkf G4j{oFWi^Lk uvr^d%zuuLdCh9_16Q^4l
2021-12-02 15:37:58 UTC	946	IN	Data Raw: 31 0f 10 f5 9e 41 08 19 82 98 6a 02 4f 6f 2c f4 62 a0 33 57 c8 31 80 51 e1 0d c1 e2 8c 3c 2f a9 14 d9 04 5c ce 44 0a 34 87 94 a8 76 bb cd c5 09 3b 99 80 0a 8c 90 ef 7d f6 f5 03 67 6b 01 23 ee 1c da de 9d 43 ab d1 36 73 44 b8 aa 59 20 b6 73 76 b7 bb 46 bc b4 3f d4 3a d0 24 bb cd 24 0b 19 d6 64 49 6c 92 dc 22 bb 7a b1 fd 96 5e 6c 75 2f ec 2d a0 9d 3c 8f d1 25 83 33 9a 8d 56 8e 5c d9 45 dc e8 c6 18 10 ac 88 20 45 dc 54 db 14 7d 73 96 a8 7b a1 42 26 97 87 6d 17 b6 36 1b b2 f6 61 45 53 dc 3b 68 a7 53 66 2c ee 6a 5a 7d a2 a6 4c 48 e8 88 2d d4 d5 a5 ba 34 4c 16 3e 2c 4d b1 05 65 ab 62 40 6a 5f 1a 11 6b 7f 49 39 21 34 ee 18 3d f6 3c b5 1a e3 af 5d 7d 5b a7 b8 1f 8b 62 16 85 8a 47 19 af bf 1d 77 27 4a 81 10 79 d0 e5 a7 d9 0a fd 06 4a e2 0d b5 02 e5 e5 70 7e e5 91 Data Ascii: 1AjOo,b3W1Q</AD4a;}gk#C6sDY svF?.\$dIl "z^lu/-<%3\AE ET)s(B&m6aES;hSf,jZ LH-4L> ,Meb@_i_kl9!4=< j} [bGwJyJp~
2021-12-02 15:37:58 UTC	947	IN	Data Raw: b0 d0 8b 18 96 db 6c be 22 7f 97 f6 b6 91 23 87 be ed 6a 18 b5 dd 06 a4 f2 d6 ea 4b c0 e0 a5 56 0e 4c 5c 6a 51 df 76 89 0a 70 f2 eb 2f 82 a9 0c 52 2e 87 a9 82 83 3c 9c b1 db d2 8f 2b 4d a7 c1 60 f4 f9 f0 ee c0 b1 68 5e 24 ba 15 98 09 68 86 33 5b dc eb 60 3c 40 3a cd 60 91 77 26 3e 86 68 4e 2d 76 9e 03 f5 4a 57 59 7a 1e 4a cd 6f 36 3c 0f fd bb 1b b1 3c 6b ec ae 0b fa 62 66 84 43 1e d5 94 33 74 52 84 45 fa a4 5b 36 99 b8 d8 e6 ec 71 01 a1 2e 8d d6 6a 7d 13 03 7f 21 bb 70 6e 51 1e 03 7d d4 8b f8 4b 0d a0 b6 54 8c 60 59 78 be b2 94 31 08 55 b3 5f 94 c4 12 8a 1c 87 f6 b4 5b 73 ea 15 97 c8 17 56 2f cb ad c4 b8 84 45 d4 4c d0 c0 d2 b8 8e ad 79 8a f4 82 e8 b8 13 98 24 bd a8 cc da 95 bc 18 70 8d a0 45 60 50 a7 70 10 88 f2 1c f2 72 29 1c 87 88 ab d4 de d1 b3 56 91 Data Ascii: l"#jKVLj Qvp/R.<+M'h^\$h3 `<@:`w&+hN-vJWYzJo6<<kbfc3tRE[6q.} pnQJkY`XtY1U_[sv/ELY\$Pe`Ppr)V
2021-12-02 15:37:58 UTC	949	IN	Data Raw: 40 33 44 e5 59 3d a8 59 57 7f 5b be 29 97 04 b9 2d 07 8f 30 6a 85 bc 2d ca 09 c1 5c 18 ee 91 1b ee 90 96 90 29 f2 ee 9c f9 ed 52 da a0 db ea 55 4c 72 02 ed 1a 7e e0 d1 07 7c 98 ca 98 2e 86 5f 05 04 7f 89 ab 5b db 1d 08 2e c1 48 71 5c 30 a3 ec f2 6e 2a 33 15 eb aa af 32 3c e3 68 63 0e 9d ca 5a 94 07 d7 a6 3e 19 b7 10 41 f5 fd 82 12 de 9b 75 10 dd a9 89 69 e0 cf 77 c8 e7 79 de 77 48 e9 2d fa a3 eb 90 32 af 29 63 ee b9 66 d5 25 29 3b 4f 78 ad 82 ad 44 ef c1 55 f2 f4 42 83 f1 a8 dc e2 40 98 6d 96 e5 d6 ca b5 5f b1 7e 6a 56 ec 68 56 7c 6d 7b d5 e2 69 0b 68 69 0a d2 f1 9d 9e 5b 68 0c 4f e9 82 e6 80 21 9c 2e 7d c9 25 d3 9e 01 82 21 8e 56 cb d1 54 fb 62 59 26 2d b5 9d 22 cc b6 63 24 25 91 40 55 ef 0f 03 77 95 73 5a 40 b0 96 25 58 c2 e2 3f 4b 23 ab 32 a3 b4 d7 e0 Data Ascii: @3DY=YW)-0j-)RULr- _ .} .Hq 0n*32<hcZ>AuiwywH-2)c(f%);OxDUB@_m_-jVhV m{ih {h!0.} % VTbY&-" j\$c%@UwsZ@%X?K#2
2021-12-02 15:37:58 UTC	950	IN	Data Raw: 7b 0a 6b 44 71 14 4b df 1e e0 b7 16 7f 2b 7c 6a e7 c5 5e c2 7f fe 32 76 9d 97 b0 d5 86 0e 25 18 ef 32 0f 95 97 29 0f 50 d4 61 a5 b4 31 e5 05 fc 67 15 e4 fa d3 94 72 3e a1 e8 59 0f e0 dd 78 85 52 67 67 f4 7e 36 07 96 99 be 5b ef 18 12 72 68 65 10 8d 36 64 b2 d2 6a 6d 4e 9c 4e 19 a6 d1 0c 70 17 57 56 48 81 ea 96 4b 4a ba c8 60 f1 a6 9c a9 90 42 99 96 b2 e0 64 32 5a aa 0f df 79 e2 14 fe a3 3e 3e 89 3e 39 f4 aa df a8 b3 51 f5 71 d7 7e f0 90 c2 5f 12 c0 2e 46 3a 3d 79 f9 fa e5 05 de 15 a8 c7 76 6f 2b fe 28 1d fe 51 d8 68 df 57 01 48 dc d6 71 18 75 9c 3a 47 11 75 2f 62 f7 65 b4 1a 76 5b c7 90 d8 9f cc e7 0b f8 90 64 a3 09 46 0f 3a fa 11 a0 79 e0 d5 65 a6 66 14 2f dd e8 9f 9c e8 6d c5 87 0f fe 6f 29 ba 34 a6 5f e8 f1 33 ff 97 44 3c 93 7f d5 cf b3 ea de b4 1e 72 Data Ascii: {kDqK+ j^2v%2)Pa1gr>YxRgg-6[rhe6djmNNpWVHKJ`Bd2Zy>>>9Qq~_F.:=yvo+(QhWHqu:Gu/bev(df:yef/m o)4_3D<r
2021-12-02 15:37:58 UTC	951	IN	Data Raw: ee 1a 81 78 15 c5 5b d8 66 9a a8 4b 0c ed 3f 3a da 3a a9 7b bf 85 4d 9c de 3d 4f 6a 2b f9 a8 f1 25 9f 37 9b 33 15 7e 9c af 4c fb 30 7c 8e d0 94 16 b0 2b a7 27 8f 1d a2 a6 17 d9 fb f5 68 91 f9 5d 99 c9 f9 f3 cf 0e 3d f5 44 1e 8a 10 87 b7 44 76 93 02 41 1e 58 db 85 bd 68 4c 78 ac 62 c3 0d d8 40 c6 c1 bf 8e 5f c3 73 1b 48 29 9c 50 48 a3 5f c7 df 57 71 4c 80 40 b1 08 7b a0 f9 72 35 05 54 ed 22 ad 41 a0 dd 29 03 1c 11 7b 7d 4f 49 ed 4c 6a 01 56 2d ab 1c 18 6b 73 58 71 16 05 c3 d2 aa 42 31 4b 89 02 0f 52 e4 13 a0 77 a7 98 fe 02 f6 15 3a 10 70 1d 5e b1 8e 18 a3 56 1c d2 f6 07 29 0e f2 fc 93 65 29 69 85 7f a6 9a 18 a5 ed ac 6c cb b1 92 61 ab b9 03 8a bc 36 b4 76 82 d7 34 ce 4f b4 e6 65 c9 64 d6 49 dc 21 1f 22 9e 7f 46 ca 69 13 18 c3 21 1a 6e 68 aa 2a b3 a8 2a 99 Data Ascii: x fK?:: M=Oj+^%73~L0 +^h)=DDvAXhLxb@_sH)PH_WqL@{r5T"A)} OILj-vksXqB1KRw:p^V)e}ila64Oed!! "Filnh**
2021-12-02 15:37:58 UTC	952	IN	Data Raw: e7 76 26 d7 71 14 b9 d0 e0 14 e5 ce 04 12 1a 58 4e d1 75 33 d9 fc 02 8a 9d 3d 8c a8 3b 33 f6 71 8a 9d 12 c5 31 c2 58 77 d6 86 30 5a 1b 93 09 da d7 b6 b6 3a 8e 28 b4 3d be ad 3c 11 85 ab e3 59 67 e6 af be ad 4d 84 f2 f6 fa ae 36 91 79 cd e7 81 e2 45 12 00 9d 62 33 32 bd d4 d6 d7 61 f3 29 4e 37 06 f0 3d 27 ef f6 bf ea 6d 74 78 e8 d0 dc ea 5b 14 5c 5f 62 16 4e 3b 2d a5 34 b2 82 97 76 4b bf 5e e3 ab 7a 79 cf 85 6e a4 0c 29 88 42 75 60 04 b5 2c 54 18 3b 18 84 1a 65 12 38 eb 50 2f 2e 63 1d 4f d1 09 d8 fb 26 c1 f3 16 53 fa 93 f9 07 cf 48 7c 75 23 d3 3a c6 92 5f bb e5 bd a2 06 6b eb af 83 88 ec 48 8b 67 d6 d4 ac 82 f1 05 50 6d d5 17 75 25 5c 8d c7 61 fc 30 9c 6d 45 5f 1e 61 68 ec 9d 95 1b 82 13 e9 7f d5 d0 0a 1b 3a 0e 57 dc 10 9e 50 63 68 68 50 6a 88 ce 99 aa 96 Data Ascii: v&qXNu3=;3q1Xw0Z:(=YgM6yEb32a)N7='mtx _ bN;-4vK^zyn)Bu`,T;e8P .cO& SHu;_kHgPmu%la0mE_a h:WPchhpJ

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	954	IN	Data Raw: 08 1d 1c ac 26 31 a6 56 68 09 19 b6 62 62 2c 26 88 43 f2 a3 e2 79 df 1a 9d b4 33 de 6c fa ae 51 41 1f 25 50 fd 20 ed a6 f2 da b4 5e ef e1 01 7b c0 5a c0 8f e7 53 d6 02 06 3a 7b 0f ab 73 44 8d eb 45 03 b4 5b d8 24 33 b4 a9 83 fd 43 eb 8e 30 38 93 38 e8 e1 07 2d 4a dd 09 5e 65 c9 ed e5 22 8b 40 0a 40 62 8c 6a f9 4d 75 2b 45 ae 06 f9 03 2a 78 4f c2 93 18 ed 93 b1 7a b4 6d a7 95 ec 4e bc 66 0a 09 16 89 bd 8f 1a f5 11 15 91 8a 45 62 c8 4f 3c 79 3d f1 2b cd da 4a 1e 18 6f d0 88 7f c9 7a 3d b3 64 38 5f 5c 24 b8 5d 2d ad 9e 2f 1e 04 a7 8f 4d a2 e6 fb c2 cc 55 ce b3 81 17 fe 8a 9a b3 f9 fc fa ce b3 84 c6 78 46 95 6c 36 59 73 b9 48 e0 38 c9 60 b9 03 56 4a 11 31 43 2f b3 66 b4 5e cd 97 04 7f c5 41 9c 89 a9 98 89 95 e2 e0 60 ed 88 6b f1 5e 58 cc d2 35 0c dc 75 3e 37 Data Ascii: &1Vhbb,&Cy3lQA%P ^{ZS:{sDE[\$3C088-J^e"@@bjMu+E*xOzmNfEbO<y+=Joz=d8_\$]-/MUxFl6YsH8`VJ1C/ f^A`k^X5u>7
2021-12-02 15:37:58 UTC	955	IN	Data Raw: 29 e7 d3 20 5e 57 c4 88 94 5f 52 85 d3 55 f6 32 46 a6 03 cb b0 9e e3 13 ea 36 12 8e 94 f8 85 16 98 06 55 06 dd 9d 75 76 77 65 da c2 7b 6b f9 32 4a aa 29 2e 13 9b 3e b1 6c 2c e8 ca 10 32 18 98 b7 fc ea d6 2f b9 3d cf 1b 4b f6 45 e6 48 52 5c a3 5d 8d b6 64 89 4f 6b c5 64 43 c0 31 86 4a 51 b1 77 a8 19 41 76 52 2f bc 29 2f 6a d1 2b cd da 4a 1e 18 6f 59 30 d0 0a 56 cf b5 94 c4 42 72 49 28 60 e3 00 59 76 44 88 74 4b e6 42 88 11 d3 80 48 5b 78 25 19 14 68 3c dc da 0f dc ce c1 6f 9e 2b 8c 80 bb c6 73 71 49 a4 b5 1a d4 c6 e6 12 08 5b 92 50 8e 0b 87 19 69 28 8f c0 7f 10 df ea 59 74 05 11 7e 8b 14 a2 b4 04 a1 c0 27 5a 4e 19 0b 3a 39 69 b0 ba 18 e6 04 2c b0 c5 52 4e 81 18 19 05 8c 97 85 7c 59 c6 e5 ca 7a 7f ec 33 03 d6 64 9b 69 8c c4 92 af fd 17 c4 11 c0 a6 97 66 8c Data Ascii:) ^W_RU2F6Uuvwe{k2J}.>!,2/=KEHR]dOkdC1JQwAvR]/jGxoY0VBrl(`YvDtKBH[x%h<o+sqI[Pi(Yt~ZN: 9i,RN Yz3dif
2021-12-02 15:37:58 UTC	956	IN	Data Raw: f9 f1 4c 7a 9d 8a 60 54 bb 43 f8 6a d2 c9 8e 4a fa a7 2e 14 6e b7 e5 ee b4 c8 57 4b fa 3b ba e9 7c 1d a7 25 2c 84 e9 d7 a7 59 92 35 aa d0 23 5d 43 28 1c 06 ee c5 c3 f7 9f 2e f9 9f df 71 c8 ac f7 2e 0f c2 28 a5 67 bf a3 ec 3d 9d 0b 6a 23 b5 5b 17 dd 57 45 34 be ea 1a 1d 1c 61 93 99 a5 2d 37 02 e0 6d b2 cc 6e 4a 20 39 e3 b8 21 4f 44 89 88 18 c5 60 00 0b ae 71 65 51 5f 35 81 3a 12 05 f3 68 94 cc c3 b1 78 e0 c5 0c 63 f1 20 97 2e 0e 93 5a 66 39 55 9a dc ab ed 65 a4 92 d2 8c c0 3f 23 33 d7 c8 4c 2c 30 46 70 d0 c8 8b 9a 29 d3 a0 a4 73 1e 42 85 3c 36 83 42 49 65 ef b8 4e 25 b0 16 16 5c 91 d4 ee c7 22 7e e7 d6 44 0a ba c6 48 1c 96 7c 5e 22 73 d8 91 50 f9 89 ab 68 72 f1 07 ba b3 27 17 ff 85 94 0c 93 8b 3f d2 c1 0c 1f f5 a2 b2 27 53 6b 4d 60 32 b0 bd 3d 51 0e a1 Data Ascii: Lz`TCjJ.nWK: %,Y5# C(.q.(g=j#[WE4a-7mnJ 9!OD`qeQ_5:hxc .zf9Ue?#3L,0Fp)sB<62leN% "-DH `^s Phr?`SkM`2=Q
2021-12-02 15:37:58 UTC	958	IN	Data Raw: 54 6f d0 81 58 78 5b 6b 6a b7 3d e4 62 7b db 80 60 97 29 d2 42 6b 56 47 a0 02 04 02 17 77 df de c1 60 ff 10 d7 f5 de 9e 92 38 ca 0a 08 49 47 5c 84 e0 c5 bc e1 0f 23 b7 3e 6a b5 f3 a7 17 98 2f 88 86 0d 7f ad b1 06 44 6e 82 d2 be 5d df 7b 71 70 08 93 48 76 a5 30 54 7c 21 4b 88 25 82 42 32 9c da 97 a7 7f 24 cd a3 85 50 61 84 fd 14 94 84 b2 32 14 9f 0f 45 9e d7 40 3e fa 75 bb e1 48 e9 71 1b f7 32 11 1b 66 d3 63 a2 76 85 61 25 1b 9b 8c 9a d5 db 23 11 50 4c 17 06 a3 33 f3 e5 91 37 30 c0 01 bf cd 90 20 34 4b 6b f7 7c 57 9f fb bb bb 27 43 f6 d6 1e 11 21 2b c3 81 ea 1f 9b 3e e6 16 80 7b da 20 fe c1 64 66 44 cc f6 5b 8e 94 f3 7c da e6 f1 c5 d2 3c ba 5d 3f 9a fa 08 5c 05 c9 85 8b 98 43 a5 37 74 fb f0 c2 55 14 af 6d bb 2d 9d ae 35 75 78 25 92 d2 81 aa 73 23 e1 8c 27 Data Ascii: ToXx[kj=b(`)BkVGw`8lG/#>j/Dn][qpHvOT lK%B2\$Pa2E@>uHq2fcva%#PL370 4Kk W'C!>{ dfD[<]?^C7tUm-5ux%#s#
2021-12-02 15:37:58 UTC	959	IN	Data Raw: 22 c3 99 79 3c 18 d9 9e 9b 3c 8a b1 1a 74 18 d1 b6 1d 8b bd 3f de 34 04 6f f0 29 5c 29 a2 70 36 b3 dc c0 bf 64 3f d1 bc d6 3a 1c 22 8d 28 25 63 c4 21 9c e5 9f 2c 72 26 ba 18 0d 1d 83 dd 21 42 4a d9 43 38 97 6e cc 8e 0c 33 64 58 f2 6f e1 ca a8 fc 81 54 f1 9e 1a eb 5a 11 16 e9 7f 7a 0a 2f a8 db f6 14 f4 a0 03 6b 36 bf 69 0a bf b0 6e b2 c3 cb 52 0c 42 c4 73 bc 99 27 0d 4a 32 a6 43 2f f2 dc 2d 5d 2b 85 c9 03 9e c2 18 01 37 7c 8e 7b 31 60 0f 46 14 40 ed 03 43 68 cf bf 9a 7d 53 04 00 c3 5b f3 ec 53 4a c3 b2 fc c0 2f 74 46 89 a6 39 14 72 ff 96 44 98 af 2f bb 1d fe 55 70 04 4e 3f cd 99 cb 2f a0 65 b9 00 71 d0 a9 9c d2 85 63 e9 a2 3d 66 dc b7 9c a7 1c 1e ec 00 8a 65 2b 6e 80 18 2e 5c cf f3 cc 37 bf d6 5a 20 3f 19 5c 29 e4 e4 45 ca e4 f1 aa bf cc 97 30 a6 8d a5 04 Data Ascii: "y<<t?4o))p6d?`(%c!,r&lBJC8n3dXoTzZ/k6inRBs`J2C/-]+7[1`F@Ch]S[SJ/F9d/UpN?/eqc=fe+n.l7Z `?)E0
2021-12-02 15:37:58 UTC	960	IN	Data Raw: 00 e1 9b e8 cd 60 d2 8e a6 df 04 62 a4 18 11 51 71 0d 2b 0e 56 cc ce 3d 81 0e eb 13 e0 22 31 95 10 59 b6 10 da fc 52 cd 60 7f 3d 0f f9 72 19 5c c1 30 b7 5d 91 4b f5 69 17 ee e4 2a 7b 81 1c 25 2c 26 b7 b7 63 41 50 4a 11 da 74 f8 85 e9 58 e4 ce e0 fe c9 5d 75 4e 4e cf e0 aa 6b 8c c6 88 82 d9 50 8b 6a 66 0d 11 cd c4 8e 29 2c d3 c9 4f bf 86 12 6f 49 58 b4 06 12 7b ed be 63 91 a0 94 fb 36 5f 4e 84 d1 0c 0f cf 58 1d 65 89 e2 f8 4d 4b 20 37 31 95 65 58 1e 11 e3 aa 31 2a 58 ce a4 a6 e6 86 63 38 d0 07 ee 7d 34 a6 08 7a b8 99 ac 1c 7c d1 da c2 da 36 42 ca 13 95 35 c2 5e 15 2c 02 e4 2a f5 f0 08 57 c0 d0 0c 6b a8 d3 f0 41 3d 2e d4 e4 58 2d 96 7a 81 01 28 67 6d dc b3 29 ba b8 36 d2 34 c2 8c 1b 62 af 62 66 30 e4 9b cc 37 8d 18 66 88 7f 4c f4 34 72 f7 b2 e7 16 ef 82 4d 42 4f Data Ascii: `bQq+V="1YR`=r0 Ki* %,&cAPJtX uNNkPj),OoIX[c6_NXeMK 1eX1(c8)4zJ6B5^,*WkA=X-z(gm)64bbf 07fL4rMBO
2021-12-02 15:37:58 UTC	961	IN	Data Raw: 08 14 cc 46 66 a9 38 15 19 6a 96 3c e5 74 72 13 2c c6 04 86 ab 71 f8 3c 71 8f 69 e7 57 63 dc 26 8e 8f 88 18 af 84 69 f0 a5 0f 43 cd 22 bf 66 13 06 db b9 47 16 17 2e cd a3 8c b2 b4 4a 7f 45 af c1 ab c9 5a 88 cc e5 6b 43 e9 97 c5 44 9d 10 fa 1b 23 a0 99 7b 1b 05 4f 69 c9 b2 e5 aa 0a b2 c4 07 45 44 24 c4 8d 4f 08 c3 11 1c 4f fd 72 5c a4 cb 2a 58 ce a4 b3 60 50 ce 7c 41 c9 07 d5 cc 17 19 41 82 bf 4c fd 3a 37 48 f0 5a 3d a9 5c 2a c1 2b 94 b0 e5 45 f0 56 ff 44 10 88 e0 af fa f1 6d 4c d0 28 9e f2 e8 2a 38 e5 9f f5 79 3f c3 33 e2 53 04 27 f8 05 33 90 20 c5 00 5e 4e 82 1f 51 22 e3 82 07 7f 13 0f 69 15 fc 0f 7e bd c9 33 0c 85 b3 41 8d 50 bf b6 a6 9d e0 51 98 64 06 53 fc 86 79 4c 30 e3 5f 30 f0 08 7e e1 9f ac c9 0d ae ea df d0 5b 07 f3 fa 59 45 20 58 a0 48 79 89 26 Data Ascii: Ff8j<tr,q<q Wc&iC`fG.JEOZkCD#{Oied\$LOr^*X`P AAL:7HZ= ^+EVDmL`(*8y?3S'3`^NQ`i~3APQdSyL0_0~ YE XHy&
2021-12-02 15:37:58 UTC	963	IN	Data Raw: 24 9b 11 cc c3 38 61 9d 47 77 70 78 fb e2 fc f5 2b da 32 a2 de 1c ff e9 d9 59 e0 8c 4b 1a e5 8f a7 54 88 64 df fe e9 c9 d9 db 1f 4f 9f 9e 7c e0 22 e2 a7 f3 15 dd 77 3f e2 d5 f9 c9 eb 77 af 08 7d 89 57 0a f1 f3 ab 1f a8 a1 5f 10 11 e8 6c 1c 3e fa e0 5e 44 7b bf 5e 7a 8f a6 fe 6c ca dd 2b a2 d4 1b 7c 36 19 cc 27 89 61 96 e2 8f 62 61 87 e7 8a 1b 82 68 0b c9 ed 4a 26 c5 ad f3 b6 08 31 f3 8c 6e 06 84 75 93 c6 52 8d da ce 61 09 d2 ee 31 d5 60 f9 df ce 9f e1 6e 50 26 55 cf f9 f1 fc d9 de 9f 9c c1 fb ec 7d 76 91 4d df bf 0f 38 51 db a5 df bb 50 49 db f0 1b cd dd 9e 59 f0 d9 78 7a 9f f5 d5 83 df eb d7 6f e4 0b d8 1b 07 59 5e b9 fd 86 f1 b1 d7 bb 7d 9f f5 7a 71 4a 28 80 18 9a 5e 46 fb d6 db 4a 17 4b 3a 4d 51 56 d1 98 d6 18 16 8f 0a 84 79 a3 fa 88 c0 e9 4a 55 42 db Data Ascii: \$8aGwpX+2YKTdO `w?w _>^Dj(^z + 6^abahJ&1nuRa `nP&UjvM8QPIYxzoY^}zqJ(^FJK:MQVYJUB
2021-12-02 15:37:58 UTC	964	IN	Data Raw: 3a 8c 67 3b e6 57 9a 13 04 1a 96 0b a5 91 1a ad 4c 2b 3a 87 ba ee 68 bc 39 92 78 e8 55 81 ed 06 ef cc b1 da 17 c2 24 b4 35 85 b0 ed c8 6b fd 55 e5 ab 23 2a 9d 4d 53 91 88 c4 83 69 29 2f 99 27 9b 17 81 19 3c ff b7 cb 31 2f 4c b5 70 d1 39 25 11 fd 9d 16 cb a2 c9 d4 54 0b b8 50 34 a0 ae e2 30 34 fc aa 6b ed e5 44 e8 2d 61 45 c7 85 6b 71 52 bb 16 0f a9 64 97 66 e7 39 01 1d 69 57 e5 8f c8 c2 94 e6 a6 49 08 bb c3 0c 1d 66 6d ba 23 c4 36 0f aa 10 61 1f f0 33 cc 05 64 bd 26 6e 3a e2 a6 55 48 61 58 87 a9 e4 08 6e 49 c7 e5 a2 ea 83 e7 8e 2e 39 32 99 84 c7 b5 20 2f d6 c6 a5 c9 61 cf 8c d8 c7 a6 3a ee 22 a9 db 48 74 1b 06 9e 12 c0 aa d6 25 a3 09 82 f0 c1 2d 43 24 40 86 f8 ef 90 2f a2 53 e3 e8 cb e2 23 71 8e 2e 1c 70 3d c4 8c 7f 76 6a c8 1c 56 43 ac 41 00 82 21 b8 Data Ascii: :g;WL+:h9xU\$5kU#*MSi)/<1/Lp9%TP404kD-aEkqRdf9lWlfm#6a3d&n:UHaxnI.92 /a`Ht%-C\$@/S#q.p=v VCA!

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	988	IN	Data Raw: f4 6d 39 ee c9 6b 77 af 97 55 e5 aa 7b eb 72 33 f0 ef c4 9d 9e 8d e9 4c a8 9c a2 e9 82 ae d9 4d 1a f0 c2 da 54 ef 57 ee 95 7d 14 66 50 37 08 34 d0 72 f4 ec fd fb d1 f1 bb c3 d7 ef 5f bc 79 f7 2a 0e 0c ed 60 ca d4 cd e5 d3 2a 63 32 3f 59 84 c1 9e da 56 c4 29 c7 6c 43 4e 7f c7 51 e0 e4 fa 35 54 e9 00 0d 07 8a 7d c9 8a b7 1e 02 8b 18 09 d9 0b 15 f0 38 cc 71 4b a7 20 38 c3 34 11 dd 1d 51 58 1d 51 9e 53 8f 39 f9 6f 63 fd e5 e0 ec 34 14 bd 5f f2 f9 6f ea 76 37 57 67 97 59 ba c8 aa 01 04 68 4f 07 83 be f7 44 58 b2 95 ee 60 70 4f 1e 0d a9 a4 b4 b4 94 d3 33 bc 6d fb 04 83 f2 25 46 6b 29 43 d8 94 e6 39 b8 2c 51 0b 2d a5 64 08 67 dc 61 a9 3e 6d 2a c1 60 29 e9 75 85 d8 59 53 ff 04 76 14 04 5a 37 df 63 d5 da ee 11 53 99 e2 0b a2 2c 7c 91 01 a1 67 70 3a 89 42 18 4d 12 Data Ascii: m9kwU{r3LMTWJ}fP74r_y**c2?YV)ICNQ5Tj8qK 84QXQS9oc4_ov7WgYhODX`pO3m%Fk)C9,Q-dga >m*)uYsVz7cS,jgp:BM
2021-12-02 15:37:58 UTC	990	IN	Data Raw: fb 27 6f ec f1 59 2c 8f 93 0c e2 c8 9f 68 ec 7e f0 62 08 7d 68 ce 94 37 ac c9 5f 59 5f cb 3e b9 ef bd 17 75 dc b5 06 a8 fa 7f f2 f4 64 3d 2d 37 ed a5 e2 dc ac 9a 9a 65 7e 8e 04 a4 90 18 7e fe 56 68 72 65 36 57 a6 73 e9 3c 4d 87 e7 e8 f6 f2 ee 8e 3a c2 3a 4e 69 6c b3 57 19 ab 73 d7 a3 a2 94 4e 31 10 10 e8 dc 1e fd aa fa ae 16 69 f4 19 a5 33 12 92 69 cc 67 2e db 1e b9 46 63 e2 b5 23 5f 4c 7e 0e d7 9e b8 b1 af 49 9d 43 ff 36 f4 14 70 ec 85 dd 58 81 39 97 68 9c a2 0a 4e 93 bd 95 4c 69 f6 a3 9e b7 8e db c5 4d 91 ae f2 f9 50 84 9e 7e 91 e7 e6 f8 46 b8 fa 64 6e b9 be 81 39 c0 5b b1 ae 99 e3 a2 01 36 bc 3a 8b d8 d2 e2 3a dd 24 a6 54 5f 19 c9 c7 45 64 6f 25 ba 6c 47 89 b5 d9 35 de b7 64 48 12 5d 43 47 41 85 25 ca b9 31 1d 62 90 de d9 13 bc b6 0e 17 a2 96 ba 27 3b Data Ascii: 'oY,h~b)h7_Y_>ud=-7e~~Vhre6Ws<M::NilWsN1i3ig.Fc#_L-IC6pX9hNlMp~Fdn9[6:::ST_Edo%lG5dH)CGA %lb';
2021-12-02 15:37:58 UTC	991	IN	Data Raw: 24 27 74 5b 9b 5b a2 ee d8 04 9d 57 0d a4 90 0e 31 95 b1 61 43 e2 a5 58 0a ab ec ab c2 b9 21 fe 66 69 ee 95 8a 8e 57 45 db 35 8c 0e 5e 16 79 ed 12 cb 8e 41 f6 97 24 aa 46 64 3a f5 a4 a2 2e 35 ca 62 56 16 fb 32 a6 9c 96 4d 06 f1 83 28 7e 13 ba 84 5f fc 29 6e 6c 40 86 27 7d a3 97 da 8f bc 69 0e 63 49 83 e2 5c 71 80 f1 31 83 6c 52 a2 c3 13 04 f1 b3 f8 1d e4 90 94 ec 4f 71 10 bf e2 fc d7 08 23 a9 42 69 c4 af f9 d9 bb 3d 83 fb bd ca 64 39 86 80 53 36 9f f2 75 66 6c 73 25 cf 73 03 b2 2d 29 58 8d d2 19 9d c3 91 be 48 92 e5 1d 83 f8 86 53 c4 21 d7 ab 6a 2d 94 6d b2 a4 5f 62 fa 6d ab 3c 8a e4 54 86 44 bc 4b f6 22 6e 76 90 65 0b d1 ba b3 1f 77 d1 b2 92 dc 25 a0 e4 ea 55 3f df b2 35 06 63 ee 1b 9e 3c a0 1c 36 7c ca 5f 73 6a 5b 00 c7 24 84 2d e0 48 f5 69 b1 18 f0 Data Ascii: \$t{[W1aCX!fiWE5'yASFd:.5bV2M(~_~)nl@')jcl\q1lROq#Bi=d9Sdufls%&;-)XHS!j-m_bm<TDK"nvew%U?5 c<6]_s]{\$-H_i
2021-12-02 15:37:58 UTC	992	IN	Data Raw: e6 72 ef a9 30 0a a4 eb 1d f1 7a 0b b1 b5 db 1c 82 2b f6 23 f6 0e f8 a7 33 5c 52 89 a3 6a ff ea f1 03 c6 e5 1f 19 3b 73 71 ff 4b c3 67 4a ff 8f 46 50 53 17 ff a3 d1 73 06 cb ac 4c 6d 3e e1 8c de ed ed c0 fd b4 66 77 06 b3 c1 70 7f 30 19 8c 07 6a 1c 54 60 57 37 af c7 00 ab d8 86 fe 70 29 fb 0b 19 af fe 71 88 25 b7 88 82 b8 9d dd f9 ad 64 46 0d af a6 4e bc 66 a9 c4 50 ac 2d f5 10 b6 4d 41 da cd fd 83 0d 50 fb 5b 51 ac fe 3c 73 9a 69 42 33 50 ae 1f a6 71 32 f1 26 df 3b be 38 2c ae 63 b9 e1 cf 1c 3d 38 ec 2d cd d9 98 a6 8c e6 0d 73 e6 78 37 a4 67 03 7c 05 b9 85 6a 07 b7 83 d7 6a 6e c5 87 88 db 37 c8 0b af df 2c 93 72 23 4d 82 bd 32 47 bc ae 35 e7 88 91 0e 03 e6 bf 68 85 92 f4 db 6d b2 b8 7b d3 36 56 a7 0e ee ee 68 9a d8 56 f5 b7 87 66 77 b6 36 8f e2 48 50 de Data Ascii: r0z+~#3Rj;sqKqJFPSSLm>fwp0jT`W7p)q%&dFNfP-MAP[Q<siB3Pq2&;8;c=8-sx7glljn7,r#M2G5hm{6VhVfw6HP
2021-12-02 15:37:58 UTC	993	IN	Data Raw: fa ab 2d db f4 34 d1 34 cf 34 ca 81 2c d1 f3 c2 01 03 0d 29 51 c4 bc 78 26 ec e0 80 5d 8b 05 09 e2 cf a7 47 6a 59 b1 9d 94 c8 a9 6c c8 57 bc cf c2 40 c9 d4 dd bd 56 77 64 70 5e da a3 45 05 be d0 01 9a da 76 5c 2a ea 2e 10 2c b3 51 63 57 b2 22 b4 39 52 09 42 28 0d 4d 2a 70 80 fc 2c a7 1c ea 50 55 b0 93 d9 65 00 dc 35 01 30 e6 ed ba 19 7c ca eb cb 81 bc de 0c 84 24 1c 88 57 c8 80 96 9d 29 c7 d0 c6 e9 7c 9e 6d 36 f9 59 4e 1b e7 66 44 5b fd 79 56 a7 f9 72 33 19 20 88 f9 66 f2 e8 11 8e 63 da 4e cb 51 5a 5c 20 ae fa 3f 36 1c d1 1c bb 7d 53 3f 4a d7 19 23 90 47 f9 3c 7b a4 0f 8c ff b5 5a c8 c6 52 47 9e 6d 38 b7 d6 b4 1d 0b 95 4d 17 ed 63 f2 10 c7 e5 66 a0 66 6e c8 1a 75 53 76 ef 61 00 03 a6 87 ac 6b b5 9b 8b cd 2a 9d 67 16 5e 53 25 47 1b 3a 44 32 94 50 2f 81 d1 Data Ascii: -444,)Qx&GjYlW@Vwdp^Ev!*,QcW*9RB(M*p,Pue50)\$W)m6YnFdJyVr3 fcNQZ\ ?6)S?J#G<{ZRGm8Mcffn uSvak*g*%G:D2P/
2021-12-02 15:37:58 UTC	995	IN	Data Raw: e5 38 b9 cf c2 d2 41 29 97 b1 d5 88 a9 9c 34 dc a8 05 26 3a 3d 6f 9b 65 b6 2d 5c 81 73 6b a2 7a 2a 13 dd 1b 76 2e 35 4d 47 b6 72 00 0c cd 40 0d 19 0e a0 0b c9 97 46 5a 10 5f 64 3e 6e 35 fc 2e 53 91 16 8d 57 d3 34 19 f8 14 fa da 55 53 64 97 c3 9b cd 3d da 96 75 a8 e3 5c a9 28 57 d2 98 4f 89 f8 04 09 96 3b bb 4c 0e 38 80 29 93 2c 41 fc 21 e1 d0 a4 f2 5a c8 64 79 cf 57 73 10 7f 94 c8 28 b7 9f 27 c7 a3 cf 6f 35 81 f5 8c cd 20 e3 1b 4a bc 31 89 87 3f bc f9 db 41 56 b9 8f 35 0a bc 79 f1 e2 fd d1 f1 87 a3 d7 cf 1b 85 a4 a6 ad 8e b9 f2 35 df f9 e1 e8 c7 37 3f 6f 63 76 59 eb fe cc fb e3 c3 77 c7 dd 1f d2 d0 de 3d 50 92 8f f7 c7 5a a4 bb 5a fc b7 63 e7 f5 df ca f1 64 b5 90 eb 9d 13 95 28 71 b5 f8 5b 4e 0c 37 02 5e 22 55 3d 20 fd 90 ee 73 90 04 f2 42 3f 71 2d 6c ef Data Ascii: 8A)4&:=oemlskz*v.5MGr@FZ_d>n5.SW4USd=u(l(WO;L8),AlZdyWs(o5 J1?V5y57?ocvYw=PZZcd(q N7^U=sB?q-l
2021-12-02 15:37:58 UTC	996	IN	Data Raw: 5d 39 cf cf 86 93 f7 a5 3c d0 f7 00 6f 0b b8 e3 2f 81 f7 12 ef 8f e9 68 fa 16 93 ff f8 db 03 5a 83 d9 c1 3e 23 11 29 05 a8 27 15 18 98 f5 34 60 6a 0f 81 5d f3 82 7e e6 44 03 bd ac b5 66 f4 8c 32 0e 0a 86 8d 31 88 08 fb 0c 9e f0 f8 5b da e9 38 ee 88 84 fe 56 a3 75 03 44 30 63 44 56 5f 04 11 00 9d 75 b1 e6 ae 29 c5 31 0f 16 c2 6c 10 7d 5e 8b 81 4c 36 5a 95 8b 2b 62 a4 82 e2 e2 95 52 ac 06 f1 49 00 c3 0a fa e7 d0 58 bf d0 ef 8a cd 5c 8c fa 75 5e 56 59 f3 79 64 cd 65 fc f4 0b 5a 3f 57 74 28 b5 5e e4 16 25 ad f5 8e 48 da f2 aa 6e 25 af 88 a4 68 25 d6 62 0e 42 a4 ca 32 ab 3b 1a 50 6b 73 11 37 5d 85 01 dc b0 e4 1a 8f c0 75 e8 c9 a2 43 16 f7 bd 66 c6 f0 fd 65 96 d5 7d 39 c4 29 a7 fb e5 1c e8 71 3d af 54 c0 85 de d7 f9 7a d3 f7 0e f8 0a fd 2f b5 19 4f d7 5b 2c 98 Data Ascii:]9<o/hZ>#j'4`j]-Df21[8VuD0cDV_u)l]~L6Z+bRIXu^VYydeZ?Wt(%%Hn%h%&bB2;Pks7]uCfe)9)q=Tz/O[,
2021-12-02 15:37:58 UTC	997	IN	Data Raw: 3f 1c 3e fb 2f f9 e0 5f e2 e7 d4 b9 e3 a3 c9 b7 7f de c6 cf de bf 9f dc b2 99 c1 cb e3 97 6f 5e e3 8b 0e a8 2e 84 9e 7b 21 b1 dc 03 d9 de c7 e6 cd 11 bd c1 65 12 1f be 7e f9 ea d0 14 35 c2 fc 66 49 a3 69 30 05 8d 6d c3 a4 56 38 be 1c fb ce 79 f1 e1 0d f5 eb e5 6b ef fd 1b d6 b3 e9 5c dc 66 f3 5e 2c c2 dc 57 1f 9e ff f4 ee b0 9d e7 b9 42 27 76 9b ff e1 ed 8f 87 bf 42 1f 4d 03 43 99 4d 47 de 12 c5 f5 9e c3 ba ba 99 dd 7a 4d d6 ce 6a 5f 1f be f2 2b 84 00 cf cb 71 fc f2 d5 cb d7 ff e9 e5 39 ce 41 98 bd 50 ab d6 ff f2 cb 77 47 cf da 9f 36 02 31 5a fc af 8e 9e d3 b2 bc fd bc 99 78 d1 8a be 03 c8 3e ae 3b b1 9b c5 cb bc 68 84 32 8a 37 ab ae 74 16 c9 b8 75 7d ff 9d ad 6b b3 6a d4 f5 fd 9f a5 ae d5 a2 2b bd 55 d7 fe e3 ff b0 95 ad 16 8d ca f6 1f ff 45 6a 5b 5e 74 Data Ascii: ?>/_o^.{le-5fi0mVByklf^,WB^vBMCMSGzMj_+q9APwG61Zx>;h27u)kj+UE [^t
2021-12-02 15:37:58 UTC	998	IN	Data Raw: 8d a8 29 4d f3 7c 39 e3 d5 b1 a1 08 39 86 80 95 c8 68 74 32 c1 a4 10 4e 31 b4 83 16 1d a9 54 e7 c8 df 2c 88 15 fb c5 b5 9d 94 ea 74 5a 78 f1 32 2a 7c 83 cb 88 f1 fb 53 fd 5a 1e f7 f6 e1 7a 42 bb d8 38 3b 10 d9 b0 98 0a 9a a7 b1 45 54 e1 49 ac e7 15 96 2d 31 32 72 0c 05 fb e3 f1 9f 02 3e a3 86 a5 8a d6 32 f5 5a 81 d0 35 a1 ee 6b 79 4d b4 c2 12 98 53 ca 2b bf 0b e6 bc 31 30 49 11 37 06 30 a9 89 f7 30 8d 4e 4a 84 e7 f5 c4 a1 ee 36 71 d7 34 9d e9 f0 c4 f3 86 f3 55 ba f9 38 2b 92 72 42 2b f4 1e 2f 2a e5 89 b0 a2 dc 1d e8 09 ce 5b 0e 35 f9 54 fb dd e3 df 87 ec cf 20 1e 57 38 17 dd 0d 0d 4e a5 09 64 6c 1d aa 4a 1d 93 5a 9c 03 60 a0 22 0a 14 d7 4b 8f ed a0 ba 72 ed 74 f4 74 77 17 b2 5d e5 2b f3 9a e5 7a 8d 04 6d 06 cd 0e 5e 6c a9 41 c3 8b 4d 3c fd 03 9b c5 dd 1a Data Ascii:]M 99ht2N1T,tZx2*]SZzB8;ETl-12r>225kyMS+10l700Nj6q4U8+rB+*/[5T W8ndJJZ``Krttw]+zm^IAM<

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1011	IN	Data Raw: dc eb 2a 66 60 32 19 ed 75 15 77 3a 99 a4 c4 94 8b a9 4e 8e 69 f8 62 aa 93 43 3e 19 d5 3d cc dd 98 6a 76 b4 6f 4e 75 bc 6f 4d 35 1d 3d 38 d5 72 8e 21 94 f5 5c f7 58 d7 98 6b 77 b4 ab e7 3a 1e a3 9c 41 ce 75 74 b4 9f e9 b9 a6 47 bb 87 7a ae 27 c7 5d 85 75 27 a3 e3 b1 31 57 e0 90 f4 5c 19 e0 55 3d 57 06 cc 8c 35 d7 ac 67 09 36 80 55 35 e7 7a d2 b3 e6 7a 98 fd ae cd ff 18 64 a1 11 05 e7 16 39 cc 14 96 1d b1 13 f3 2c 8c c7 a3 b1 06 5a 3a 3a d1 e2 8b c9 71 7a 78 a0 81 76 d4 dd df d3 40 3b 38 da dd 55 40 db 3f e8 21 ee 3c 12 80 01 fe fa 44 02 2d 3b de df eb a9 b3 30 9a ec 1d 76 4d 69 d0 09 b3 80 76 c8 2c a0 ed 65 06 d0 b2 6c 77 fc af 90 06 49 a2 9d 73 84 8f a5 dc 15 69 6a 10 ef a3 79 f9 59 91 00 28 65 d3 b7 d7 11 5c 4a ea f6 1a 8d d3 34 55 f4 53 da 3b 3e 3e 52 Data Ascii: *f2uw:NibC>=jvoNuoM5=8r\Xkw:AutGz]u'1WU=W5g6U5zzd9,Z::qzxv@;8U@?<D-;0vMiv,elwIsijyY (eJ4US;>>R
2021-12-02 15:37:58 UTC	1013	IN	Data Raw: 98 35 ee b0 40 0d 70 66 89 5b 2c c1 5d cf 9f 01 13 b6 90 a6 53 15 f7 15 5a c4 1f 5f bf fa f3 b7 17 1f 5f 9c bf 3c fb f1 f5 c5 c7 6f 7f 3c 7f df ff 14 7f 7c 71 f6 ee 3b fb e5 66 fc f1 87 b3 d7 e7 17 17 f0 7b 16 7f bc f8 f6 fc 0d fc 4a 63 6e 18 ff ee 0e 81 f5 26 fe 88 57 55 ff e3 ca 89 b3 20 c3 f4 7d 69 8e 40 b7 51 a3 93 1f 45 f0 2b 84 9d 8b 27 0c 70 be 58 60 cc 35 7e b8 5b 7f ea 61 18 60 71 c0 5b 7f da dd 08 94 29 7d f0 a7 1e 7a d5 1a 39 d9 8d 4f bb 78 b8 b4 bd a8 19 bb 4d da 0c a6 da 37 b3 85 bf 85 7d 3f 46 24 41 82 47 26 63 e1 b1 96 15 6e 8a 86 8b 7f fa 68 c1 2c 83 8b aa 33 ba b5 75 ae 6e a1 42 a0 27 c7 fd bf 94 58 ab ba 12 c4 0c 23 54 15 03 ba 5b f4 cd cf 43 18 70 c1 e3 94 d3 71 76 22 eb 50 cc 5e 6e d0 64 22 77 1e 1f 9 a 25 14 57 c8 09 aa 4a fb 3f da c0 Data Ascii: 5@pf[,]SZ__<o<q;f{Jcn&WU }i@QE+P'X'5-[a'q]]z9OxM7)?F\$AG&cn{h,3unB'X#T[CpSqV"P^nd"w%WJ?
2021-12-02 15:37:58 UTC	1014	IN	Data Raw: bd 46 45 e4 46 80 ef 41 bb 77 ca 63 54 72 cf 07 16 93 4b c7 26 6c a5 3a e3 39 33 8e 3f a1 c3 4f 02 1d a6 8f 47 87 e8 09 a5 2e 97 84 0d 74 32 40 19 d8 7b 50 b5 bd 83 28 07 1e 80 e7 95 33 ae 96 fe 75 c3 cd c2 9a 6e 96 e5 72 d6 31 af 57 b8 9c b6 b6 36 4c f1 d8 ad c0 f1 2e 17 d8 52 1e de 30 5e 09 0e c4 39 23 1e 7b d4 5a 2f 6d 85 51 9f 79 22 3c db b5 57 a8 30 69 46 b3 e3 28 be a5 fd 40 48 ee 2e 81 1b eb 33 0f 67 6b 89 a4 70 bd 71 dc 08 4a eb e6 bd 0b 29 8a 9f 79 7e 4b 2b fc bd 7a fd 26 cc 28 c0 f3 fd 46 cd b5 6e 63 76 19 32 cd 90 f1 d0 0a 3c 13 63 8d c2 fe b9 bc 6b 2d ee 50 e2 05 0b 9d 02 a3 2a 28 6e 4e 51 4b 2e 1e 16 59 52 dc 3d a4 b8 77 e5 17 93 e0 16 af 90 dc de 73 c9 ed 1a 79 bd eb 90 d3 7b 36 eb 31 73 58 0f 9c 2c 52 3a 95 76 cb 27 8c f7 f1 fb b3 37 e7 Data Ascii: FEFAwcTrK&I:93?OG.t2@{P{3unr1W6L.R0^9#{Z/IQy"<W0iF(@.H.3gkpqj)Y~K+z&(Fncv2<ck-P*(nNQK.YR=wsy{61sX,R:v'7
2021-12-02 15:37:58 UTC	1015	IN	Data Raw: 5c c3 ea 79 f7 1b 2d 0c e8 f1 0c c7 c5 4e 02 14 d4 4e 02 44 d4 4e 92 47 f1 a5 1a 7c 11 f7 0e a3 58 3d 96 f6 63 8e 8f 57 c6 36 ff 68 01 86 0d c3 7d bd 26 34 d9 73 b8 31 66 b8 5c 71 35 64 3c ed 58 1f 27 42 bf e0 25 14 0a 0a ca d0 ab af 37 d4 11 ba 57 1e 26 8f 96 6b 3d e4 26 3e c0 f6 4a 5e 24 00 24 16 93 b0 2e 0a 78 4c 33 e7 23 c6 00 a3 f7 db 64 2e b4 1d 05 40 b6 be eb 00 e7 7f 37 4d e7 4d 1e f2 22 90 e8 a2 83 39 1f c6 c2 a1 bf 66 a0 66 1b a4 a9 3a f9 18 b3 9c 7b 3f 7d ca e7 d5 5d 3a 7d c7 66 70 30 30 cd 82 21 49 60 0f c4 e6 74 c2 6e 72 57 fd 5a c2 5f 1d b0 d3 48 15 ec 26 11 86 23 bc b0 8c 53 e2 7a 20 e7 a6 a0 03 7e d0 44 96 9c fc 4d 76 66 7c 7c 5e 61 b2 55 c1 0a 4e 59 b2 7f 1c 8f 59 72 1d df b2 e4 38 be 63 c9 6e 3c 63 a8 31 06 d4 9d ce 33 0c 74 92 04 02 50 Data Ascii: ly-NNDNG X=cW6h}&4s1fq5d<X'B%7W&k=&>J^\$\$,xL3#d.@7MM"9ff:{?}):fp00!l'tnrWZ_H_#Sz ~DMvf]^aUNYYr8cn<c13tP
2021-12-02 15:37:58 UTC	1016	IN	Data Raw: 40 ba 7d 06 82 12 e3 23 cf 5c 5b 90 6f c5 87 89 37 94 de 86 f1 5b 84 33 75 5e c4 15 c9 88 58 72 33 60 66 72 65 43 35 69 32 21 ed 45 81 49 96 e2 0d 27 d9 18 60 00 15 6a 33 e4 96 31 8e f4 e0 1e 6b f6 19 92 3f 48 80 f6 03 0a bc 48 ba 9f 4e 55 be 2e 3f b3 f9 f3 14 33 8e 0f b1 4c ff 06 f3 44 66 f5 fe 79 92 27 28 21 0d 2a 1e 2c 38 30 fb 27 78 e7 05 06 83 1b 84 9f 92 fb 5b a0 c0 fb 98 87 35 76 88 f2 be 2f ad 6b 87 d2 c7 d0 49 68 cf e9 28 e8 e8 af 71 0b bf 4a 16 ab 8d c8 cd 08 0d 1b 89 f6 1f df b0 2c ef 6b 57 7e 43 af 9c a9 82 d5 dd 94 26 1c e7 88 44 d5 5b 7a e2 1f 68 ee 8c 18 80 98 2f 47 07 ff 89 91 77 ed 5b a9 69 30 fb 6d 9e 7c ea dc 4d ed ec 2f 17 3c e0 6b 18 4c 73 e8 fb 53 67 d3 83 26 51 d1 21 24 69 a8 59 6d b1 a8 16 69 ba 40 61 4d 75 59 58 29 63 50 a1 67 9a Data Ascii: @}%#[o7{3u^Xr3'freC5i2IEI"}j31k?HHNU.~3LDfy(!*,80/x[5v/klh(q,j,kW~C&D[zh/Gw[i0m M/<LkLSg&Q!SiYmi@a MuYX)cPg
2021-12-02 15:37:58 UTC	1018	IN	Data Raw: a9 6e ed 27 ce f1 0b 09 8c d8 3a 5a 32 cf a2 86 83 ff 37 b5 66 26 ab cd 91 a9 16 1f 58 69 2d 36 7e 36 13 55 88 81 92 6c ee cf 98 d9 62 8e 78 cf ec e2 67 dd 45 68 ca 88 a0 34 9e 4b 94 15 c1 d3 c6 73 a3 ca 77 86 2f eb ac 03 54 7c 3a 93 f9 ef 96 4b 12 5c 39 6f ed d3 6e 88 b9 74 9b 7f d6 c3 d8 70 65 bb ba d4 df ad 52 a4 12 b1 ce 9f 2e f9 57 bd db 7f d5 e7 e9 52 9c ff 2b a3 e7 ff 56 25 2d 24 44 b6 98 62 00 4f 93 ff 31 41 f6 17 c2 82 de ab de ec 8b 58 d7 79 36 3e df 42 0f b0 8a 83 4c 25 dd 0d 81 4e 6a 05 3b 35 ad 49 1c 00 97 8a 72 37 0a 9f 5f 71 7e 01 a8 1c 12 63 92 ca be b3 39 07 e6 90 91 9b 0f d2 b5 98 93 d6 1c aa 83 b9 cc 71 c7 3f 85 24 77 e2 b9 0c b4 fe 96 85 1a 83 02 ca b4 75 07 26 d2 32 f2 c7 61 9d 9f 50 06 1d 3b 28 7e e0 cf b3 fb 89 cc 5a 9e df c1 3d 7b 2b Data Ascii: n':Z27f&Xi-6~6UlbxgEh4Ksw/T :Kl9ontpeR.WR+V%- \$Db01A]y6>BL%Nj;5lr7_q~c9q? \$wu&2aP;(-Z=+
2021-12-02 15:37:58 UTC	1019	IN	Data Raw: 0a 9d 71 53 82 8a 3d 68 47 8d ee f8 a8 9f a8 db 50 bb f1 3b 9f 19 25 6d d3 66 6d ff dc 6c da ac cd 9f 85 59 f3 e6 fc ec 25 fe 2b 4f 87 61 47 91 c6 59 5c c5 c2 70 38 be 53 18 56 47 f6 3c 0f b8 23 be aa 82 86 c7 d2 af cc dc af 8a 9a 53 f6 f2 1d 9e ae 11 0d 4e 76 54 f2 49 e3 33 aa a4 e0 1b fa 5e a0 a4 3d e0 c5 e1 9a e1 22 f9 55 c5 35 b0 f4 4f 58 c6 0b f4 62 36 08 1a 4a 41 9a ff c6 8 41 35 cc 93 69 3d d5 37 5a 73 92 be 3c 8a 94 b1 8e 1c 67 e6 b5 66 7e a0 99 98 b2 7d 1f 76 63 92 53 02 c9 35 98 db a2 f7 a9 6d 17 82 71 fc 5c 93 10 a3 37 a7 a2 29 b3 27 97 1a 8e 3b 4b 65 b8 31 30 14 df 2a cd 2b a5 4c 2e 00 cd 71 39 9a 00 a6 9c 2e 2c 3c 07 12 b9 d2 a5 55 3e c6 3a 9e 49 52 46 66 05 a5 ad ad b1 10 23 9e de 66 6d b9 75 9f 02 c7 fa 85 24 88 9f cb f9 2f ad 19 d9 0b 4c Data Ascii: qS=hGP;%mfmIY%+OaGYIp8SVG<#SNvTI3^="U5OXb6JAA5=7Zs<gf~jvcS5mq 7);Ke10*+L.q9,<U>:IRF# fmu\$&L
2021-12-02 15:37:58 UTC	1020	IN	Data Raw: d9 53 87 b3 c1 02 1c f2 c4 2b 1e e1 d9 dd 64 02 fb 4b a9 33 16 8c 0e ee 4a 9c df d2 6a 4a a2 10 3e bc 2d 00 d8 f6 0b de 9c 7a 87 26 e2 33 d8 33 99 6a 4f dc a5 af 32 bd 59 d0 34 fe 22 1d 71 b2 57 ef 28 1c cc 19 c9 c1 5f a0 9f 57 32 95 73 90 91 62 75 03 59 a6 bd 87 03 7a 12 bd 71 40 e8 6f e2 39 90 5b 23 27 8b ce df cb 3a 2e 64 18 84 b8 99 73 34 d5 10 03 17 26 92 08 59 b4 c5 4b 0c aa e3 52 a9 dc db da 47 f3 17 d7 ed 5b 6e 20 b4 5c 8a 63 57 dd cd de 93 b4 8a c6 27 eb 69 98 89 78 97 35 b5 d4 73 9c 18 1f 31 e1 5b 39 3b 7e ae 6d 5a 86 77 f3 4a 9e ab 90 13 88 f0 ea 27 3e 09 fe 72 15 ad ed 9c ab d1 b4 53 1c ef d3 58 6f db 3b ae aa 6d 07 1d a2 05 23 0e 93 3f aa b9 0a 9b 65 f1 82 4b 28 cd b5 90 8e 42 6c 20 b8 0e 73 70 68 0b 3e 88 44 a4 70 22 ca ec 26 ed 69 3f c0 ce Data Ascii: S+dK3j]>~z&33jO2Y4"qW(_ W2sbuYzq@o9{#::ds4&YKRG[n l'cxW5s1[9;~mZWj>rSXo;m?#eK(BI sph>Dp"&i?
2021-12-02 15:37:58 UTC	1022	IN	Data Raw: c4 4f e8 cf 22 f0 c4 b6 ad 4b 27 bb b5 b6 68 38 eb db 10 82 4c 5f 5d 2e d0 7c a8 ba 14 7b fa 5a e0 e7 ee ad 16 78 a9 5a 0b 16 6d d2 20 72 72 a5 f2 43 fb ad 21 e5 6f fe d2 d9 fc 24 9d 05 fb de 46 11 b3 7d d2 9f b5 a4 78 60 52 83 ca 6d 77 48 ce 77 75 24 e4 9f cc d7 4e 23 5c 33 0f cb ef 31 30 b6 a5 a7 ac 74 88 8c 1e 98 73 82 67 c4 9e 76 e2 4e af ce f3 78 2e 50 13 48 d4 e0 ad a8 a2 28 1f f9 22 b1 ad 3d e4 6b 11 ed 0c 0d 97 ad f7 9e fb f8 69 62 95 b0 47 4b 11 f7 01 37 10 30 6a 4b 51 b8 00 35 03 cf 40 83 6d 61 ee b5 d1 cc ed d5 14 50 b0 c3 44 9f 61 e4 63 9e c4 c2 d8 d1 ff 04 f2 b3 46 cb 0d 54 55 34 f8 7a 37 b0 fa dc 8f 1e 83 36 61 20 f9 85 2d 4a 06 c6 10 c7 a0 f8 3b 71 83 3b 1a b6 90 27 61 f4 10 1b 6b 69 0b 89 f1 75 a2 28 2f 2a f6 80 07 d3 1d e7 18 ad ca 87 a7 Data Ascii: O"K'h8L_].{ZxZM rClo\$F}x'RmwHwu\$N#310tsgvNx.PH("=kibGK70jKQ5@maPDacFTU4z76a ~J;q;akiu(/*

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1023	IN	Data Raw: 77 80 29 47 58 eb c0 b4 9a aa 35 62 b2 c9 fe 9a e8 5b 5d 40 75 bd fa 3b f5 c9 d3 06 40 a7 8d 60 c3 7f 7e b7 b6 ec 65 d3 ac aa 80 8b af eb 29 37 84 76 86 6c 59 3f 84 b4 83 23 58 96 0f db 1f b6 61 65 f8 8e de 81 c7 0e fc 7f b5 72 e7 6b 9d 1b 51 6b c7 1e 9b b6 df 86 f6 b0 40 6d ba 38 5f 9e 60 e5 b1 f3 35 b8 76 ff 84 e5 36 ad 94 2f 86 07 a7 49 13 96 0b 20 08 29 c2 c4 d3 d3 27 b0 d5 dd 9d 0f a3 cb 27 4e 75 6b e2 ee 74 9c a3 c2 45 7d 46 08 6e a7 b8 3e 34 ed 9e fb ed 51 f3 e0 a2 ca a6 59 9c 3e 11 8d e8 37 9e f3 ec 86 09 97 b3 7e a4 e2 18 38 a5 86 39 1e 35 07 a2 3b 9a a7 a0 9f d4 74 f8 f5 f8 74 1b a8 ad 6d 55 90 a6 e1 5f 0b 4e 52 fa 01 df b5 de af 39 2d b6 61 a1 b3 93 0d dd 7d ad a2 6d 72 10 ba 88 4b 5a b8 7b 20 c3 89 4b b7 b4 38 2f 56 69 93 1e 76 76 25 d4 a0 2c Data Ascii: w)GX5b[]@:;~e)7vY?#XaerkQk@m8_`5v6/I)"NuktE]Fn>4QY>7-895;ttmU_NR9-a)mrKZ{ K8/Vivv%,
2021-12-02 15:37:58 UTC	1024	IN	Data Raw: bc 09 1a ee 4d e7 de b2 c7 f4 ef 73 88 a6 a5 6b 72 b0 8c bf de 59 da 05 1c 91 c4 02 21 ac d5 d6 c0 f7 bf 62 d9 f0 7e 93 ea f0 64 c9 0e d2 68 f0 da d4 fe 21 06 22 dd da da f0 bc f5 b8 06 9e c2 8d ef cb 70 e5 c9 93 3d a8 85 45 56 8e 97 6b a9 9b 81 8a 2d 25 c2 f0 a2 31 b8 3d 37 99 ca de 17 4b f7 d2 84 12 25 da 71 6a ff 8b c2 00 34 c5 aa f1 e9 c8 7e a7 d2 cb b8 1a 30 a4 84 48 37 eb ea be 4c a9 10 af 21 30 62 93 cc cc b9 71 24 ac 9c 0a 3c 7b 8a bf 86 bc 29 c3 75 cd 69 32 21 37 39 a5 bf 59 f3 32 b7 2b 13 93 c9 d5 e4 6d 4a f1 2c e5 35 b5 ce ed 4b dd 92 1d a2 b4 47 6e 6f 94 d9 2d fc a3 b0 8e 80 5d bd 96 87 d8 14 e0 3a df 5b d6 7f 68 24 cd 8a bb 76 c3 5a b5 17 77 d7 d7 b0 29 61 3f 2d ea f2 79 c9 de 51 72 aa a6 41 1b 89 9c 3d 0d a0 5d 05 a5 b5 6a aa ae 52 46 d7 2a Data Ascii: MskrY!b~dh!"p=EVk-%1=7K%qj4~0H7L!0bq\$<{)u2!79Y2+mJ,5KGno-;}[h\$VzW)a?-yQrA=]jRF*
2021-12-02 15:37:58 UTC	1025	IN	Data Raw: ae 84 87 4f 71 6b 0c b4 f7 88 b5 c8 9e 8c 6a f4 b6 63 fe 63 77 9b 1c 23 e8 f7 de 36 c0 4e 35 c5 a1 97 f3 4d 93 e0 fc 61 c1 cb 58 4e 56 02 81 4f 9f cf f5 12 8b a2 2b f1 a3 47 fe db 36 8d 8d 06 06 03 44 db 5b ee fb 71 79 af 12 be d2 11 58 ac ae e2 d6 e8 ae 6a 7d 4e 17 46 b1 ed 7b fc 4d 25 56 38 7a a7 52 df c4 d9 85 b2 a8 c0 64 b0 aa 5e 1f c7 8f da 04 be 2d c4 a1 ee 57 70 d2 97 4b 0c 10 66 d8 23 8c e3 79 43 0e a8 b3 c0 b0 6d f9 c7 90 5f 5d 7b 79 48 c0 9c 6f b5 69 32 21 37 39 a5 bf 59 f3 32 b7 2b 13 93 c9 d5 e4 6d 4a f1 2c e5 35 b5 ce ed 4b dd 92 1d a2 b4 47 6e 6f 94 d9 2d fc a3 b0 8e 80 5d bd 96 87 d8 14 e0 3a df 5b d6 7f 68 24 cd 8a bb 76 c3 5a b5 17 77 d7 d7 b0 29 61 3f 2d ea f2 79 c9 de 51 72 aa a6 41 1b 89 9c 3d 0d a0 5d 05 a5 b5 6a aa ae 52 46 d7 2a Data Ascii: Oqkjccw#6N5MaXNVO+G6D[qyXj]NF[M%V8zRd^-WpKf#yCm_!xyHoi]M&BT4?rv^c(Yw^NtHW __6s!}[3S4mT-z9,]slBQj9ipSA
2021-12-02 15:37:58 UTC	1027	IN	Data Raw: 82 82 cd bd e0 2e 32 8f 8c 1e 14 74 44 b8 b3 fa 1d 16 0d c8 c7 80 54 61 e8 e6 21 4c ba c2 c6 e2 46 28 b7 6b 56 e1 38 5e 65 32 92 96 01 0a 94 cc 29 e4 ae f3 56 3e fb f2 0a a5 b6 83 12 65 6f 46 af 69 96 35 76 19 97 76 d0 1e 13 b8 8c a7 87 17 d4 d2 43 60 b8 54 34 e7 15 ca 90 d1 4a 5e c6 45 72 63 62 e3 96 7b 6f 9e a4 86 1d ef 21 3a 5c b3 d3 86 f5 50 32 c8 c2 03 7d 54 7e 79 d3 2e f0 11 61 96 67 ca 10 89 5c 2e 1f 4f 33 b8 1f 5e ab 86 f5 40 c8 af 1f 04 19 99 c0 3e ae d3 36 ac 16 a7 f3 8c c0 f7 72 5e de 4a d2 a1 09 a6 82 90 1c a8 88 e2 9f 6f f2 f1 8d 8c 27 ce 63 f8 f7 85 b3 11 ef 34 10 21 a3 ad 78 d4 d2 1d 09 bd 68 e7 94 6a 5c 96 32 e2 73 9b 85 a6 6c a2 cb bc 78 fb d3 f7 56 99 16 72 f2 55 0a 83 1f f2 e2 33 60 ea db 44 78 f4 45 27 e5 67 fe 2c db f8 f1 87 47 b4 70 Data Ascii: .2DTa!LF(kv8^e2)V>eoFi5vvc^T4J^Ercb{p!:^P2}T~y.agl.O3^@>6r^Jo^c!xhj!2slxVrU3^DxE'g,Gp
2021-12-02 15:37:58 UTC	1028	IN	Data Raw: ca 39 16 58 00 f7 a1 24 1d 5c cc 28 84 1d 40 ba 23 96 2f 93 ee a0 3c 3d 1a 94 3b 3b f2 76 6b 2c 7f 43 61 07 d0 41 41 68 b2 93 ea 32 2c 77 58 f4 a7 a3 2b 60 52 54 2c d2 69 86 97 a1 cf 49 93 a8 3a a0 2b 79 d1 b0 70 60 e1 c3 52 2e 06 d1 72 46 71 29 20 ad bd 4e ee 6b 33 1c 85 bd b6 75 d1 15 97 26 d5 50 44 48 e6 20 0f f6 2a 99 d4 07 f5 40 ce cc 9b a4 04 6e 3e 08 73 f0 94 78 ca 38 76 64 ac 26 24 3c 98 02 29 2a 6a 17 62 09 9c b9 16 00 92 5a 6c 6e 1f 08 29 46 aa b8 00 c9 94 07 f5 d1 9a 2f 2f 60 57 e0 8a e2 e6 0a cb db ca 42 66 08 86 bc 85 db 9e d2 86 5c c8 aa a2 a7 b2 a1 07 25 09 f2 d7 f0 75 a3 a4 4d de 81 1d f9 2b d4 ba 90 f3 b0 cb 73 11 11 95 44 6e 93 9f cd 8a bd 9d 70 46 b3 b4 0a a3 d8 48 16 c5 7c 06 76 c9 55 8e c6 b9 ae 7a 60 0a f4 06 6d c2 3c 2e a4 52 09 7f Data Ascii: 9X\$!(@#<=;;vk,CaAAh2,wX+^RT,il:~+yp^R.rFq) Nk3u&PDH_*@n>sx8vd&\$<~)jbJN]F!/"WBfB%uM+sDn pFH!vUz^m<.R
2021-12-02 15:37:58 UTC	1029	IN	Data Raw: d8 1b 75 57 28 79 71 a4 a6 0f b4 d7 ab 25 9d ff f7 28 aa ac 8d f2 9f d0 53 3d c6 8e d1 d1 50 90 52 c2 12 03 02 96 7e 40 4b a1 37 aa 5f 64 ed c5 50 e8 90 aa 74 19 73 ae cb 48 51 21 f2 08 45 c6 3c 49 6b 6b 92 ed bc 59 95 e1 2f be 5e cb e0 af 73 d8 ac 67 68 e8 e4 30 5a 01 c0 e6 1c c4 19 80 52 c8 55 86 a9 5f d7 20 bf 47 7d 82 c8 02 6b 08 e6 b1 b1 86 90 c7 50 8d 01 8e c3 57 4e 43 d6 d0 47 cc c9 25 ce 50 98 d1 cb fa 1a 4a 9b 74 19 96 9b fd 3f a7 f4 1b 16 d6 51 f3 08 49 fa 95 33 cf df a7 11 2c a0 4a 5d 17 68 e7 b6 ad 6d f7 26 09 90 75 bf 54 c4 e8 0f 4d 62 a0 c1 f3 c6 67 27 d3 af 6a 66 2f c2 7b 8a 71 8b c4 4f ff 97 b4 3f 88 f5 b8 f2 a7 ce 74 34 d2 9f e6 23 e7 58 7c 2d 5e 49 3f 59 4e a5 93 e7 2b 7e 7c 4b 8f c1 ca a4 5a 3f b9 64 2b 2f 8a ed fc 01 e2 35 c6 a8 02 3d 8c Data Ascii: uW(yq%(S=PR~@K7_!dPtS HQIE<IkY/^sgh0ZRZU_ G)kPWNCG%PJ?;QI3,J]hm&uTMbgjff{qO?4#X!-^!f?YN+~ KZ?d+!5=
2021-12-02 15:37:58 UTC	1030	IN	Data Raw: 56 f6 c9 2e 75 ef b2 05 fd 14 5b c6 43 22 21 53 17 d9 15 c6 70 de a4 d5 4d 67 32 2d e1 2e 0f 2b 6d 19 60 6c f6 76 2f 7a 72 84 7d 99 c6 e7 0d 31 ed bf 16 ad ef 54 66 c3 e2 b6 cd e2 ba 49 ba 2f 7a f3 e3 7a e3 71 25 63 65 ea e8 1f b9 31 a6 24 a9 f4 c3 d6 56 4a e5 68 bd 2c 07 1d 7f 3b bd dd 6f 38 18 f5 70 da ce f0 a2 1d 5e 42 0c b0 6d 8e 96 06 aa c4 08 fd 45 2c 8c 5b 70 cd 2f 4a 19 92 a7 3f 8d 7d 91 7a fa e3 b8 66 12 e9 08 fd 64 d0 91 31 25 6a 4e 30 8e cf 70 8c 32 65 e1 82 81 21 6a e1 45 21 65 f0 dc 62 64 23 5f 2e f3 d3 a4 24 4b 49 c0 48 40 98 cd cd 75 23 79 9b 1f 1e 68 91 0c 30 11 00 34 15 47 4d 29 9c d7 c2 6e 15 2b 99 7f c3 cc 14 95 82 f1 ce 4f 2b 0a 16 ad 83 f7 58 a2 a0 62 6b ab 38 65 76 89 c2 2a 51 f2 40 e3 ae fe d9 da 8c 18 9e 18 f5 b5 37 e9 a2 59 16 15 Data Ascii: V.u[C"!SpMg2~.~m^!v/zrj]1Tf!zzq%ce1\$VJh,;o8p^BmE.[p/J?]zfd1%qjN0p2e!jE!ebd#_.\$KIH@u#yh04G M)n+O+Xbk8ev^Q@7Y
2021-12-02 15:37:58 UTC	1032	IN	Data Raw: 7d 60 92 33 f8 45 fb ed 85 b4 31 fa 23 b6 49 26 16 64 52 b9 57 bb b0 68 8d 00 39 b9 5f 4a c2 3a 37 49 f0 d1 a1 1f a6 65 5a 01 88 e4 96 9a d4 4a c0 ed ef 10 8d 80 14 7c 85 14 65 c6 0b cd 92 27 f9 2c cd 96 f9 ec 06 e6 06 ff 94 d9 12 e8 a4 79 99 67 4f f2 86 18 55 3c de 7d 3c 8d c7 f1 ad 34 96 e7 ab 5b b3 81 5f 28 0b 74 b9 e4 d2 c2 5e 1a a5 cb 78 f6 14 dc 7e ea 0b 6e 9f 89 97 62 81 93 5b d1 87 d0 98 0a 55 69 e2 8b 86 ee 94 59 1b f6 9e f6 80 6c cc 87 f9 44 66 78 d9 c6 2b b3 bc d1 79 ad 31 33 f7 bb ba 0e 1b 71 eb 1a 0a d3 09 26 84 14 d4 63 9a b1 c8 33 b7 91 67 44 fa 3e a6 19 41 ba 9b b3 79 03 34 97 35 f5 c7 ce c9 24 d6 a4 09 90 f2 b7 50 1e 16 88 39 94 7f 05 f7 be 60 7a 7f 59 7a 55 41 b8 1a 6e 11 2f 84 25 4a 72 cd 64 ca 80 4a be c3 03 95 b6 2a c2 4a 46 28 d6 0a Data Ascii: }^3E1#&dRWH9_J:7!eZJ]e^,ygOU<~<4[!t,^x~nb[UIYIDfx+y13q&c3gD>Ay45\$P9^zYzUaN/%JrdJ^JF(
2021-12-02 15:37:58 UTC	1033	IN	Data Raw: 45 1f 1a 90 70 1b 91 76 0c 8f 1e 90 a8 f7 e0 80 d2 df f8 80 2a 34 6c 58 79 7c 53 b4 78 3e 52 b4 41 53 6b 5c f2 c7 32 c3 69 49 78 aa a0 df 24 89 3f 1f 68 41 48 e1 90 4c 44 77 63 33 12 9d b5 51 79 5e 78 11 0e 55 8a 7e 94 2d 2b 9a f0 6b af 79 a8 45 ed 87 18 47 c2 37 05 21 ca fd ba 91 c5 5e f1 92 a2 d0 6d 89 78 1a 6f 34 74 eb 62 40 63 bc 8e d3 99 b4 40 86 6b d3 3c 34 9e 03 21 a6 22 a0 62 9b e8 86 ca cf ca 0e d9 57 b9 ac 8a 7d 04 6b 4c 99 3d db 7a 96 a7 34 c2 44 b8 72 b7 eb 6d 66 6c 11 01 d1 2b 6f fa e4 f5 8b c1 30 53 31 e7 55 9c 71 d7 49 33 ff d0 e5 3e a2 80 2c 0d db 4b 84 29 da d9 f3 45 ff d5 34 57 83 c7 a5 67 bb 02 ba 1b fa 37 ac fa e7 b6 97 d5 6b d7 a6 b0 98 b5 b7 71 8b 48 f4 5c a3 82 b5 7c 4e 3e d4 d4 07 ee fa ff ab a2 0c 5a 81 05 1f 88 25 68 60 1a 63 83 Data Ascii: Epv^4!Xy[Sx>RASK2!lx\$?hAHLDwc3Qy^xU~~+kyEG7!^mxo4tb@cc@k<4!"bW]k=z4Drm!f+o0S1Uq!3>,)E4 Wg7kqH\N>Z%h^c

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1059	IN	Data Raw: de 26 8d 99 62 e9 95 23 5a e5 83 d2 4f 43 9d cc df 06 56 3f 2c d8 cc 0d 97 2d 50 cf 2c 13 33 cb 9c 0c 46 d4 1d f4 d2 02 c6 11 56 81 cd c2 b8 65 a6 28 e4 bb b0 51 d6 79 6c df 75 33 3b 56 96 6e 62 87 80 29 b9 31 02 78 78 b8 ba 90 36 8b df 3a c4 d0 dd 1c ca 4e 2b 77 d4 56 3e a6 df 5c fa e6 7c 3a bd fd 85 df 51 43 2d c0 78 8d 9a 8c 81 a6 4a bf b9 aa 23 ce 5a 3d a8 02 38 b8 d5 a1 a3 3c 2e 51 0c 1f 57 8f 0a 6d fa 60 23 a8 b8 c7 da 7a b2 c8 b1 b6 ac ce 9a 04 2d b5 ac 82 f9 fb 31 62 e4 54 2e 5b ca 26 f0 27 83 54 85 01 ed 23 ba 92 a3 4b db 37 1c 72 ad de f0 62 4a 68 f7 c4 68 b7 5a 24 b6 7d ae 65 bd ab 1b dc 5a 3d 7b 8f 11 ee 29 1f ab aa 4a 67 5f 41 fb 2c c3 63 bb 38 a3 ba 5c 1d a4 42 26 95 76 c4 71 b5 c7 c6 5a 2b 10 f8 d7 88 34 77 20 d4 18 77 e2 6a bf c1 c3 b7 40 Data Ascii: &b#ZOCV?,-P,3FVe(Qylu3;Vnb)1xx6:N+wV> :QC-xJ#Z=8<.QWm#z-1bT.[&T#K7rbJhhZ\$)eZ=()Jg_A,c8 B&vqZ+4w wj@
2021-12-02 15:37:58 UTC	1060	IN	Data Raw: 01 23 3c f5 2f 68 68 8b a2 56 d6 19 d3 2c b7 d2 b2 c5 31 e0 c3 56 75 99 b4 18 30 79 6b 06 5b 4f 32 6e 55 79 ab c6 41 99 1d 6f 0a 12 24 c3 10 16 ed 2d 5b 66 bb fc 80 e2 5b cb a6 f8 41 d7 e3 1c 70 ca a2 f1 e8 b8 7e 89 db 51 d5 a1 d8 14 a7 52 9d 06 34 c1 8f 93 c1 20 87 6d 0d cd 12 14 c2 8c 30 ba c5 75 8a be e2 79 65 e3 81 52 1a d6 1b 16 2c a6 ac 95 84 3a 7a b1 be e3 30 bb 33 f6 84 76 cc c9 04 06 6d 3e ba c4 03 2f fb c5 c6 01 6b f3 7e 49 80 97 4c b9 89 d3 1e ea 4d 4a 4b 25 f8 45 75 bd ba 25 49 9a 79 2f b8 e4 d5 90 0d 37 02 33 03 17 c4 4e 1d 4e 90 94 03 0a dc 4c a1 e7 25 7c 42 de 78 ea 6b 1b 99 cd c8 e4 70 53 78 27 e6 69 68 d4 36 cf ea f5 09 d6 58 2f a3 a1 fe 93 c8 21 2e 36 8a 90 56 03 e4 e6 6e e1 de ae d4 44 5a 09 46 c0 98 87 9a 13 3f 18 d6 5a ac 5d e1 f6 1b Data Ascii: #</hhV,1Vu0yk[Q2nUyAo\$-[f[Ap-QR4 m0uyR,:z03vm>/lk-ILMJk%Eu%ly/73NNL%[BxkpSx`ih6X !.6VnDZF?Z]
2021-12-02 15:37:58 UTC	1061	IN	Data Raw: 50 05 10 22 3f aa 6a 6b 0b 2f 5e 73 1e 0f 45 55 ff f4 69 b6 a6 0d b2 58 86 3d 31 cd 4b e6 d5 d8 d8 3e 94 3e 98 69 50 db c8 e5 89 c2 af ed f2 f2 48 91 06 8b 4c b4 48 1b 35 82 bf 5e d1 2e 0c 84 3e 3f 13 e4 cd 1b 87 61 8d 2b c4 74 35 0e bb da 62 f8 8a 0d 37 cc ed 8d c8 3c e3 fa 5c 93 21 99 73 a8 07 0d 05 76 bd c0 69 95 d8 81 52 1a d6 1b 16 2c a6 ac 95 ab 53 3b f4 e5 75 54 a3 78 de 38 6d 1f 95 36 52 e6 45 53 ed 5a 47 42 f5 91 3a 09 af b1 f0 5a a3 14 1e 24 45 54 6f c2 a0 58 b3 1b 00 04 45 7a 18 7d 7b 2f 4e 48 2d 15 db 52 4a 61 f0 26 fe 32 c6 c0 2b 63 66 b2 16 33 47 9a 01 d3 7f 38 8a ac 67 37 13 91 65 08 d7 90 4d a2 a2 b3 ea 68 f1 d7 b6 ad 94 6d a3 78 27 c6 ce a5 89 55 cc 5f e0 4d 02 D5 27 ac 55 e3 7c fa b6 88 2f 90 a4 de 16 f9 94 0b a8 be b8 7e d3 c9 0d 43 Data Ascii: P"?jk/^sEUiX=1K>>iPHLH5^>?a+5b7< !svi&wZS;uTx8m6RESZGB:Z\$EToXeZ){/NH-RJa&2+cf3G8g7eMhm x'U_M'U /~C
2021-12-02 15:37:58 UTC	1062	IN	Data Raw: 73 3a 82 21 33 a1 4f 7a d1 33 0d cd c6 64 66 c7 49 f2 73 1d f2 8b 60 95 76 6b 63 8a eb 8b 7c 35 2c c5 30 6c d8 f7 b5 a9 32 83 2b 99 9d 92 a7 22 8c ab 8d ac c9 68 d5 16 2e e0 69 1d 7f bd b7 d9 6c 35 c9 6d 27 47 fe b6 40 37 1b ca 42 a9 2a e3 8b f4 c5 ab c1 67 15 85 6e 6d 8b d4 84 a6 c1 9b 20 aa 16 92 1c 01 6b c3 ae 6b 81 36 c1 a1 8c 65 15 a2 47 75 7b 83 81 47 26 b6 6a 30 63 f0 fd fa 26 43 be 9d 15 03 81 b5 dc 58 6c 40 da 06 66 42 27 b9 5a a0 b2 5d d9 8c d0 66 93 b7 04 50 6d d3 50 de df f5 e8 69 3c 61 18 13 6b 5b 04 7c bb f6 c0 d4 16 1f ae db 8a 33 52 75 21 d4 9f 1d e9 fb d9 f9 91 b7 05 c6 19 b2 21 89 1b cc 92 2c e9 d5 c3 b1 96 79 2b 25 b7 99 6c 96 82 aa 3d 5b aa fa bd 2e 4d 8d 67 4c 63 4b cb 1b 34 18 a7 86 32 95 02 ad e7 75 34 7a 9f b3 a7 51 13 9c fe b5 1b Data Ascii: s: 3Oz3dflls`vkc 5,0l2+^h.il5m'G@7B*gnm kk6eGu{G&j0c&CXl@fB'Z]fPmPi<ak[3Ru!l,y+%l=[.MgLcK42u4zQ
2021-12-02 15:37:58 UTC	1064	IN	Data Raw: 3f 3c 0d b4 2e 12 13 3f 72 ba b6 ce 3e ef 60 44 a3 e9 c0 18 12 e9 55 05 df cf be d4 2e 66 28 cb 42 15 23 94 e1 1c ca 1c ba a3 fd 68 7a c3 b7 90 f1 6f 14 90 e6 ad 93 16 3a 0c f6 a9 b2 3e 17 29 08 6e 9c 22 7a 3b 05 4e 0f e2 fd 68 b0 3f 9f de fc 54 0e 94 28 0d e0 71 b3 06 8b 71 c3 06 5f 16 4d 1a 34 eb 40 33 ea 1b bc da ac 97 5fa 24 46 6f d7 61 48 22 ec 78 a4 65 f1 d0 0b ff b8 76 06 e1 51 45 23 bc 57 5d 05 56 01 a0 aa 44 ab a2 79 59 01 d5 d8 b8 2f bb a0 f8 a3 2c 1c e8 95 64 fb bf 5f 07 53 d3 a8 e1 d1 5a 48 0a b3 ce 4d 69 ad 1d 43 ac 47 67 65 28 b1 6e f7 f3 69 e3 c6 3d af 11 58 3c ca 65 88 6b 60 f9 69 5c 52 5a 7a d8 b0 bf 6b 74 b2 78 c5 a9 09 b3 19 14 7c 22 be d4 15 88 d5 31 b3 5b 53 0f 68 b2 2a 49 1d a0 e0 64 6e 8b 98 c1 a9 26 61 53 39 da 1f 87 8b 05 1d 84 Data Ascii: ?<.:?>`DU.f{B#hzo:>)n"z;Nh?T(qq_M4@3_FoaH"xevQE#Wj]VDyY ,d_SZHMicGge(ni=X<ek`iRZzxtk "1; Sh*d'n&aS9
2021-12-02 15:37:58 UTC	1065	IN	Data Raw: 0a 5c 4d d8 a1 a1 e7 0c d1 6f 15 b1 04 61 4c 4b ce a7 65 94 4c fb fd 3a 47 4b d5 83 d5 ec 0c c3 2a 98 4c 07 29 27 0c 99 48 dd 16 ec 26 47 46 d6 e2 45 7a ea 09 5e 55 1f f6 59 05 b4 ea 54 37 be 20 d7 14 4a ab 0c 0c 8e a3 d1 87 69 42 4b 6d 20 06 52 9a 9d 10 b8 01 07 0d 92 b6 29 37 b7 04 32 cb 94 2d 53 59 0e 73 1d 01 d8 0e c0 da 9c 5c 5b 46 b7 4b a3 09 64 79 f9 ef 3d 49 6e aa c7 b6 2d c0 9b a1 2e e3 d5 f6 68 ae 05 7a 1b 52 bd 11 dc a6 5c de 8a 8c 6f 8d e2 12 c8 35 0e ad dd 58 6e 0c 66 75 3b 52 53 0a 78 fd 21 d8 0e d8 5a e4 96 9d b7 bc 0e df 13 e7 7d 03 df c2 08 a3 11 37 37 83 90 25 a2 c1 d1 a6 eb b2 6c 9b 66 7a 8b f0 34 46 6c 93 be 2d fa 10 95 dd 6d 3e ee db 25 6e 9b ae 43 11 3c f3 0e 83 7b 13 cf 2d 58 df ed 83 2d e4 cf 96 a8 dd be a3 50 97 07 9b 4b f0 56 48 Data Ascii: \MoalKKeL:GK*L')H&GFEEz^UYT7 JiBKm R)72-SYs[FKdy=In-A.hzR\o5Xnfu;RSx Z)77%lFz4FI-m>%nC<{-X-PKVH
2021-12-02 15:37:58 UTC	1066	IN	Data Raw: 25 ce 85 52 00 a4 a5 11 b9 06 4c 6b c9 6a 81 32 2a fa 7a 55 89 df d7 22 b9 69 21 a6 29 dc 58 1b 41 f1 38 6e 15 4d 9d 63 26 60 f6 fe 7d 13 44 ca 98 d5 1b a9 a2 da cd b5 b1 9b 6b 73 cb cb c5 b6 82 ac 78 14 ef 0d 65 ad d3 5a b6 31 a4 ca 2e cd 46 a3 5b 58 a4 ba 36 25 ca 67 5b ca 76 54 6c 0d 4d f1 a8 de 03 b2 ea 43 cb b6 31 98 72 33 4d a3 91 34 97 df 16 d3 60 d2 d8 0d 3c cf ba 70 8b 38 66 30 00 31 f5 16 46 eb 27 9e ed df c5 6c 66 f2 cb 1b 1e e8 5c 88 88 cd 24 3a c0 05 9a 69 e9 39 d4 a9 4c 95 11 bd f9 c9 ca a5 94 c2 c3 d2 32 85 aa c6 fa fe 99 fa 6f d7 fa 48 41 15 38 ee e9 25 67 b2 d5 7e 5b 22 af db 4a cc a1 86 af 6f 38 f6 79 80 85 47 53 f2 f9 7a 58 13 a2 b2 f2 6d 5a 32 34 1c 09 59 00 30 75 b4 7f aa 9c 5d cd 44 b3 18 72 72 ed d3 c9 35 5d fc 94 4e b6 d1 74 92 Data Ascii: %RLkj2*zU"i!)XA8nMc&`)DksxeZ1.F[X6%g[vTIMCl1r3M4`<p8f01F!f!\$;i9L2oHa8%g-["Jo8yGSzXmZ24Y 0u Drr5]Nt
2021-12-02 15:37:58 UTC	1068	IN	Data Raw: 3d 81 c5 cf 61 f1 57 29 8e 0f 89 ac 5e d9 5e ca 63 90 3a da a1 41 70 12 d1 c5 c2 c6 e7 2b 85 b0 8f 25 8d e6 e1 78 7a 1d 9a db 7d c2 fe 08 22 d2 56 08 c7 4f 90 c1 58 4a 9a 92 7b 8e f2 bd 9d 80 22 71 7a be 8a 08 da 48 92 d4 db 8e 7e c9 5b 2a 7d 9f 32 fe c2 c2 59 2e 41 c2 19 9f 3b 0f 1e cc e6 21 16 89 06 52 f8 69 27 98 8e df 40 40 c0 a2 83 e5 72 e7 75 4f bf e5 26 5d c1 fe 3f 78 a0 3e 7b 8a 93 bd 6d c3 38 d9 4e cf 73 5f c3 44 52 50 c0 83 55 7e da 0f c5 b4 7f ca ff f6 9e f1 bf e9 0b e2 c1 1d 9f 75 6c 62 fa c8 6d 3e fb e4 64 e4 bd 4d 1a 3d 4b 1a c5 53 a5 49 3c c5 06 30 8f 33 af ff 5b 9f b0 5e 87 1f 16 b2 60 ac f2 41 a8 d4 6b 7c 67 e0 da 41 32 48 a0 d9 2c 87 69 14 db d7 6f 92 31 be a7 8c 8a f6 6a f6 3e 68 89 4f 40 77 87 c6 f1 dc b6 7c bc 0f 20 06 a0 00 40 00 38 Data Ascii: =aWj)^c:Ap+%xzj"VOXJ{"qzH-[*]2,Y.A; Ri@"@ruO&{">x>[m8Ns_DRPU-ulbm>dM=KSI<03[~^AkjA2H,io1 j>hO@w @8
2021-12-02 15:37:58 UTC	1069	IN	Data Raw: dc 15 fc 86 e8 f2 8c fa c3 de 07 f8 3d 5a 1c cf e7 f4 b6 77 ca 7e 7f 60 5a ba 37 a7 ec 8a ab ad de 5b 76 f1 69 02 b1 2e 68 c8 a0 77 cb 9f 9e 8a cb 27 fc f2 a9 20 a7 47 f9 f5 19 47 b8 72 3a a3 49 7f 6a df 89 1c cc bf 45 b6 c8 2a 4c e8 58 d0 24 80 a0 8a 2d a3 29 9d fe 70 43 67 d0 71 eb 01 95 4c b0 1e cc a7 d3 f8 03 f4 17 2e 74 83 29 74 f1 3c e4 7c ee 5a c7 16 97 00 3f ba 0a c2 ae 25 d8 61 91 1d 71 12 63 d4 6d 1f 90 d9 7c 34 9d 8f 40 4c 7f 38 38 20 60 0e 2e 55 5d 1a 60 54 42 2e 85 31 21 cf c0 ed 7e 70 43 63 7f 78 32 8d f0 fc 48 7c 6b d0 d1 c8 5d 2e 07 e7 16 70 52 46 eb 2b 84 c2 3c 13 42 af 51 47 f6 9e 81 91 7c 6d 79 10 20 a9 d3 5b db 21 cf 84 95 06 6d f4 15 2c 22 e8 a2 af ce 33 88 cf 1e 4c c2 1b 78 7c 69 3f d3 02 72 df f5 20 e4 84 ce 84 73 a0 12 9b 92 00 Data Ascii: =Zw~ Z7[vi.hw' GGr: jE*LX\$)pCgqL.t t<[Z?%aqcm 4@L88`.U]TB.1!~pCcX2H k .pRF+<BQG y !m,"3Lx j? r s

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1070	IN	Data Raw: c1 7f 79 d3 07 a5 41 3e bb 6f a0 d1 b1 fb 79 b9 0c 59 76 10 24 b8 d7 77 db c7 bb bb cf c5 65 b2 18 13 81 72 6b f7 b9 e5 e9 1d 2f 97 11 38 3f 98 9d 16 b7 96 4b fb d8 6d f7 91 ba 31 c8 3c a3 f9 58 92 f6 79 77 17 66 ef 0d d0 6d c1 cb f3 d8 72 08 52 ab dc e6 53 0b 3b f0 72 77 f7 19 92 f1 19 bc 8c c4 5c 75 5f 12 11 40 75 61 d6 a2 21 ef 0e 49 92 86 4f 47 58 4b c7 6b 43 41 18 86 ee 84 88 45 a6 ee 8c cc 99 a9 e8 de b0 75 ba 88 fb 8f 81 6d a1 3f 60 91 cf c0 62 76 e7 51 da 47 9d d3 ff 86 49 d1 27 9f 13 dd d7 ef 70 80 2b 0e 86 9b 62 01 28 03 47 be 0a 41 14 3a cb 3b 2c 0d 03 ef f4 55 0b dd ef 30 92 e1 39 7b 2c b0 48 ac 44 c2 e8 c9 c6 80 13 45 d5 8c 11 9b 7d 26 77 ab 0c 30 9c d8 2f 8f 86 6c ad 07 64 89 0c dd cf dc 4f 82 86 e2 cf 99 b9 39 8c 3c 6b 94 42 04 de 41 33 85 Data Ascii: yA>oyY\$werk/8?Km1<XywmfRS;rwlu_@ua!lOGXKkCAEum?`bvQGI'p+ b(GA;;,U09{,HDE}&w0/lD0/9<kBA3
2021-12-02 15:37:58 UTC	1071	IN	Data Raw: b2 1e cc 47 58 f7 8b f9 67 3d 7b 94 a6 74 b4 04 d2 68 f2 27 73 15 cc b9 a1 24 87 a4 27 e2 15 de 89 c5 17 f2 55 c9 40 f8 c6 94 33 8b f7 7d 08 f7 c3 20 ad a7 54 6e a2 5d 93 49 36 18 44 9c f2 60 95 03 35 16 de 19 30 96 06 04 38 2e 93 f7 93 5e bf c7 e0 4f dc 01 63 3d c6 23 93 14 2c d8 ab 89 eb d9 13 34 ce cc 6a f6 c1 67 57 0c 8e 3d 59 2e 7d a7 e3 0b 13 c8 a7 35 55 6a 82 b9 68 dc c9 17 30 79 8b bd e6 a1 38 23 23 70 0f 7a 41 5a 0c 1a c8 62 d0 b1 4b cf c8 8b 1e 27 7a 9c 74 0a 6f ba 77 e2 aa 9b de ef 4f e0 a2 3f 21 2a 26 f0 6f cc 08 80 ab 00 c6 c9 65 d1 12 69 c0 ac 33 4b 85 69 24 26 dd 54 40 f9 a2 cf c9 43 06 98 82 8d 13 2f b1 b0 d6 3d 80 3e 83 54 a5 d0 7c 43 87 7d ec f0 c1 4f a2 a8 25 22 d8 cc e3 f0 07 0e 03 e0 00 3f d8 35 f6 95 e5 62 25 49 62 f5 53 73 94 a3 bd Data Ascii: GXg={th's\$U@3} Tn]6D' 508.^Oc=#,4jgW=Y.}5Ujh0y8##pzAZbK'ztowO?!&oei3Ki&T@C/=>T]C]O%"? 5b%lbSs
2021-12-02 15:37:58 UTC	1073	IN	Data Raw: a0 0f 06 28 17 64 a0 6c 73 80 69 48 26 2e db 0b 10 00 44 32 49 3d 0f 59 6e ea 26 85 ee 86 87 e4 00 db e4 8b 59 d5 46 f9 a7 d8 6a a0 69 0d 46 08 ba 04 40 37 81 f8 54 7a 03 13 cc 64 28 db 25 51 64 8e 93 b8 f4 3a 53 55 a6 ea 0a af c3 6a dc 31 d7 9e fc 92 1e 04 75 bf da 38 c9 31 72 3b 56 23 b7 63 08 d9 10 f0 71 a2 15 d4 ac 7c 04 ee 72 40 d2 c4 df f3 24 8b 31 a6 0e 38 03 7d f2 1b e6 7d 46 93 fe 68 32 e2 6b 3b 81 e2 c8 69 55 c0 6c 37 56 c1 33 17 37 1d ec 78 82 19 01 db 73 d4 8b 5c c5 29 64 45 bf 10 8c 8f 9d 4c c1 30 f4 15 78 ce 7e ba d1 ee 6e 90 6e 52 40 40 dd 68 b9 0c c4 2b b9 71 f2 f3 83 fb 9d 5f 44 22 f1 0d a3 9a a8 04 7f c5 57 94 3f 61 9c fb 06 a2 de 63 54 a7 b9 b8 5c db dd 85 5e 50 ac ba 2d d7 ec 06 5a 6e 65 55 44 ec 42 b6 df 2c 97 1e 84 d5 c7 20 f2 6f 30 Data Ascii: (dlsiH&.D2l=Yn&YfjIF@7Tzd(%Qd:SUj1u81r;V#cqjr@",M\$18])Fh2k;iUI7V37xs)del0x-nnrR@+h+q_D"W? acTV^P-ZneUDB, o0
2021-12-02 15:37:58 UTC	1074	IN	Data Raw: 65 1a 96 57 3e 53 38 b6 c8 62 3c 45 65 c8 8b ca 3e d8 e2 27 56 3d b3 1f e9 9c ea 8a 3b e4 2d ee 54 f7 1f 9f 53 2c 75 56 32 ff 6f 21 aa 3a 4d b7 ae 77 e1 b9 fd d6 3d c5 b9 a8 6c 61 f7 f7 e0 b5 30 bf 7f bd 17 66 b6 af a7 cb 1b d8 66 87 4d 6c d1 b8 60 3f 3b 22 42 3b 25 3c dc 33 3a 8f 6e d5 65 12 61 c3 59 52 14 ac ca 5b e2 2b 45 06 c0 a3 d1 18 dc 90 17 ee 57 61 9d c9 bf 01 19 fc b1 c4 c9 90 30 df bf ba 4f 99 5e d1 cb ef f0 9e a3 2c 09 b7 21 02 05 2a 2f 85 0b c7 54 8f ba 37 64 b9 fc 0a 41 07 d5 06 9f 85 ad c8 4e 16 91 3a 77 4f 5d cd 64 ca fb 7c 2f a7 b6 55 92 6d 76 7c 9a dd fd 58 94 18 76 53 1e 18 76 6e 1e 70 39 e7 eb 73 89 3b f2 9b 7b 0b 3f a0 f3 63 4a 7e 07 8f b3 3c 8e 50 7c 22 02 22 42 45 de f8 e7 61 08 9f ba e7 ef 49 ee c1 05 19 a1 56 7a ea 48 c3 f8 d4 61 Data Ascii: eW>S8b<Ee>V=-;TS,uV2o!Mw=la0ffMl' ?;"B;{%<3:neaYR{+EWAo0O^,!"/T7dAN:wOjdl/Umv/vSvp9s;{?cJ-<P ""BEXalVzHa
2021-12-02 15:37:58 UTC	1075	IN	Data Raw: f5 e4 5e ae 40 79 8c 6e 6f 90 cf 2b e0 6d c3 a9 08 00 8a 2f 3e 65 ce a2 64 67 ed 15 9c 8a 9c 71 ff 2a 7f 99 cf be c4 da 34 8a 6b ad 55 f3 0e 65 7d ac e7 7f c6 a6 fc cf 6b 36 00 b7 ee d7 64 2b 14 9a a9 01 1f 97 33 50 65 be 92 b4 da dd 3d e4 e7 d5 a6 b7 92 0d 4b cb e5 6d b2 e1 c2 f6 9d 23 bf 7b 6b 2c 3b 4e cd 6d 5a 21 f6 4e 94 8b 10 76 54 31 4d 2a 11 93 9a 0f a7 fb 33 ab e0 2c 72 6b 5e 2e f8 b1 2f a5 f5 14 9a a3 52 51 d0 2e fd 0f ed d0 02 fd dc 1c b6 ad e8 03 ef aa 6f 2a 17 c4 4a 19 82 47 68 8a d3 62 Data Ascii: ^@yno+m>edgq*4kUe]k6d+3Pe=Km#[,NmZ!NvT1M*3,rk^/R.Q.oJGh b
2021-12-02 15:37:58 UTC	1075	IN	Data Raw: 92 58 ee 52 2d 84 be bc 20 57 2e 1e 39 3b 0f 07 a3 05 38 20 61 90 46 3d e7 63 50 00 78 3e 07 fc e0 47 a7 b2 3a 1d b6 c2 7e 05 36 05 ef b3 8d 3d 49 1d 1f 07 fb c9 0e 0c cc 27 78 08 d2 75 f6 a0 85 6c e5 da 18 5e bc 56 dc 9a af a2 61 1f eb 61 85 af 11 48 5f 43 56 40 75 41 33 c0 2c e5 a3 d8 c7 51 0c 2f 34 a7 43 d9 29 89 6f 3e 23 4f b2 6f 24 e7 78 ca 37 32 cf d5 03 3b f9 2b 0c c4 8e 7e 90 33 7b 10 5e ac 92 2a d4 1e cb 7a 53 3e 75 99 7f 88 79 f0 27 54 6a a1 c4 53 14 2a 89 68 07 76 fa 0e e5 26 21 4c f3 eb 4f d8 b6 8e 64 6f 82 9c 48 6a 19 8a c2 31 7e de 07 53 e4 fd 54 9c fa 72 5b 48 1f 8b 46 87 bb bb 83 cc 29 23 72 9f 4e fb 90 e8 c9 ff 90 65 9b 41 ed d8 97 cb e5 6b ac e4 24 03 ed dc 00 47 9e f6 8b 3a d5 cf 55 02 f6 cd 95 80 7d 59 09 c8 8f df f9 8a ab d0 bc 13 0a Data Ascii: XR- W.9;8 aF=cPx>G;-6=l'xul^VaaH_CV@uA3,Q/4C)o>=Oo\$X72;+~3(^*Z>uyT]S'hv&!LOdoHj1-STR[H F)#rNeAk\$G:U}Y
2021-12-02 15:37:58 UTC	1077	IN	Data Raw: d3 2f e8 0c db de 72 89 67 4f 5a f8 15 36 fc c2 a6 fa 90 1e a5 ef 76 ad 39 0d 46 53 bc bd 93 6b 94 3c 82 16 fc 37 be 3e 19 70 7f 1b 5e 94 87 fb 79 74 2e 4f 19 5e 44 cc fd 91 8d f0 65 fc 16 88 e9 48 68 31 32 dd 74 10 92 23 a0 1f 1d 1c 10 b4 dc a3 48 d9 05 1b a0 62 e6 81 75 64 8f d3 2c da 1d 6e aa 52 5f c3 95 9c 89 32 7a e3 d4 fd 98 74 1e 8c 11 17 9b 54 ca 37 81 78 6a 92 8f 82 3e 07 06 fc 74 7f d7 85 a6 d7 a3 f0 86 b5 d4 86 a5 a8 65 1b 5a 8c 16 67 c3 59 7c 6b 6b 8d 79 3a 16 8f c9 b5 a4 02 c6 d5 a2 e4 a7 cf 56 20 45 b6 26 94 d9 1a 31 02 fc 22 1d 40 3c e3 c3 77 b0 44 9a 91 29 0c d2 bd 2c 3d 96 62 49 04 92 dd dd 9d 40 da a9 31 49 65 21 3c 1a 76 23 16 ef 4a b0 29 75 07 8e 9e d9 e1 63 6c 26 43 8a 03 4f e4 c8 29 63 25 46 48 ee e6 fa ec b6 35 1e 32 96 8f f1 34 21 Data Ascii: /rgOZ6v9FSk<7>p*yt.O^DeHh12t#Hbud,nR_2ztT7xj>teZgY[kky:V E&1'@<wDJ),=bl@1le!<v#J)ucl&CO) c%FH524!
2021-12-02 15:37:58 UTC	1078	IN	Data Raw: c7 85 1d 6b 8c d5 02 c6 72 28 b0 65 bb 1f 53 25 f7 7b 81 6f 3f 18 3d 53 73 7c 23 da 87 57 d6 fd 0f fb 54 31 97 25 08 7f a8 f5 67 43 82 4a d2 8f 08 59 1b 2e 7b 7b 2e 94 60 65 d4 8c de f3 e4 28 86 79 ac 54 4d 7a a4 8f 5c a1 b1 c4 1b 82 c9 e1 2a 38 40 f6 6b 2e cf c2 cd 93 f4 34 80 e5 3f 81 38 24 47 c6 0f 61 43 1c e7 ff ed ab 21 ce 7c ce 52 d1 d0 40 d1 e5 df 91 8a ec 4c 6e cb 58 6f df 52 96 fd 4c 4f da c1 b0 44 1b 4f c2 16 c0 5d a8 fe 03 19 58 45 e2 c0 7f e2 5a ae c1 3a 8a 00 69 51 a0 bb 83 01 e5 4d 32 cf 6e af 88 8f ca 3a 7f b1 27 ee 2e e6 c7 e8 af 95 2b a1 cb 84 4b f9 97 72 d8 ed 60 03 68 38 0a 7d 85 cf 8c a5 2f 81 2d fd dd 86 2e c9 36 5b 7a 7f 7f 4a f3 07 6b 16 77 52 b7 5f 10 f8 71 83 d3 7e 44 8f 2a bd 68 53 91 5d 1f 04 65 a7 19 97 6c 27 33 89 2d c2 9d d1 Data Ascii: kr(eS%{o?=-Ss #WT1%gCJY.{. `e(yTMzl*8@k.4?8\$GaC!R@LnXoRLODO]XEZ:iQM2n:'.+AKr'h8j)/-.6[zJk wR_q-D*hS]e!3-
2021-12-02 15:37:58 UTC	1079	IN	Data Raw: 09 bd 5b 77 cf 6f 1d e0 d9 a3 3b f3 0b a9 dd 99 5f 23 39 76 c7 01 42 b2 4a 0c d2 77 b3 05 b2 b1 ba f4 ef 1e 1f 33 fd a8 a0 84 c0 ef 5b e3 d9 7d 9a db 4d 52 0d 56 73 2f 2c 6b 55 90 12 94 5f cd 55 9d 5c 1f dc 00 d7 da 40 8f f1 0c 10 51 a1 5d 75 bf bf b6 f0 92 e1 e3 a3 fc 56 d6 b0 06 ad 82 e5 f5 ba 90 00 4e 5d d0 6d a9 54 76 b0 45 1c 97 b2 ae d7 75 f1 e1 f1 f1 d6 f7 9c bd 03 13 e8 fe c8 be 76 6e 4a 25 fc 0f 62 8e f3 76 84 3c 48 3d b2 4d fc 58 63 3f 20 6f 6b f4 17 24 fc 9c a4 fa 27 de f6 6c 64 6f 5b 92 6d 92 60 93 e5 9a 89 c8 b2 f3 25 dd d6 f8 91 60 e6 48 ae 32 dc 01 4f 2c 40 6e d2 9f c7 c7 3b 18 58 ff ae 2a 5e 61 62 60 8f 40 ba 41 68 4a cf e9 6f d5 85 eb 00 e3 66 52 68 3e 3a f5 f8 5f 7c 33 55 e6 aa 3d 18 76 7a 5d f3 fa d0 78 79 53 bf 2f 6b 8a 8f 9a a1 48 d4 Data Ascii: [w;_#9vBJw3]MRVs[,kU_U@Q]urVn]mTvEuvnJ%bvc<H=MXc? ok\$ldo[m '% H2O,;X^*ab`@AhJofRh):-_] 3U=vz]xyS/kH

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1141	IN	Data Raw: c6 0e e5 d2 50 2e 1d ca c8 50 46 0e 65 68 28 43 87 32 30 94 81 43 e9 1b 4a df a1 f4 0c a5 e7 50 ba 86 d2 75 28 c6 06 5d c7 06 c6 04 8e 05 8c 01 9c fa 9b ea 3b b5 37 95 77 ea 6e aa ee d4 dc 54 dc a9 b7 a9 b6 53 6b 53 69 b7 ce a6 62 56 7a 07 f5 05 cd 6c f3 6a d1 b6 64 ad 88 ad 87 56 db d6 5a 57 d2 ae a3 36 89 6d 11 6d 40 db 7e da dc b6 b5 75 e3 d8 6d 63 1a d3 69 4b d3 fc 4e eb 1b 87 71 fc c5 b8 98 e3 61 c6 29 1d 9f 34 6e ec 78 b1 71 7c c7 ef 4d 57 71 7a 8a e9 5c 4e df 32 dd d1 e9 8d a6 03 57 fd 57 ec 95 b4 d8 20 aa 86 0e fd 76 44 98 5a 11 f4 5f 36 d2 3a dc d2 b1 25 01 42 b0 44 9a 0f 63 41 b5 f0 8f 9f 9d 5a 0f 83 b5 f6 a9 15 41 ff 65 95 37 fc 90 aa f6 30 b1 da 21 3e 8c 05 55 c3 af 36 53 cc 2a ae 1b 6e 6e 84 0c 28 e6 4f fb 20 a5 43 56 be 9b da e8 41 46 94 07 Data Ascii: P.PFeh(C20CJPu[;]7wnTSkSibVzljdvZW6mm@--umciKNqa)4nxqj MWqz N2WWV vDZ_6:%BDcAZAe7 0 >U6S*nn(O CVAF
2021-12-02 15:37:58 UTC	1142	IN	Data Raw: d1 69 36 0f 48 76 35 1f 45 6c 3e c2 6c 3e a2 2d 33 3a cd e6 01 c9 9e e6 11 9b 5f 62 36 bf a4 2d 73 79 9a cd 03 92 5d cd 2f 23 36 bf c4 6c 7e 49 5b e6 f2 34 9b 07 24 7b 9a 47 6c 3e c6 6c 3e a6 2d 33 3e cd e6 01 c9 ae e6 e3 88 cd c7 98 cd c7 b4 65 c6 a7 d9 3c 20 d9 d3 3c 62 f3 09 66 f3 09 6d 99 c9 69 36 0f 48 76 35 9f 44 6c 3e c1 6c 3e a1 2d 33 39 cd e6 e2 9c a2 52 ce 1c 4a 30 39 4d 2a 43 b0 aa e1 55 53 e7 e0 e8 4a ad 77 f0 f5 55 ce 32 28 36 3f ec 83 fd 22 71 50 f2 a1 a1 a8 bd 89 d1 08 29 2e 55 be 38 Data Ascii: i6Hv5E > -3:_b6-sy]#6 -l[4\${Gl}> ->3>e< <bfmt6Hv5D > ->39RJ09M*CUSJwU2(6?~qP).U8
2021-12-02 15:37:58 UTC	1142	IN	Data Raw: 8e 30 1f 00 7e f4 f0 21 b2 d0 66 5a 98 22 b4 12 fe 97 05 e8 e1 48 b2 e7 a0 b4 30 fb 7b 42 cb b3 34 f3 ed 83 70 61 5f c2 23 ed 86 09 8a db 30 be 55 a1 aa a2 a7 df 01 cb 80 ea 90 16 cb 70 7a 42 14 fc 5e d3 cd 09 51 ac 4c c5 1c f5 a0 f1 13 30 5b 9d 72 e4 c3 8f 2e 84 2b b4 b0 cb c1 df 9b d4 64 8d 16 54 ae c0 be ac 4a 54 75 2d 57 06 c7 52 20 f9 d8 4c 6e a6 d6 dd 9e e5 c0 53 fd 22 5a ab 39 92 84 a8 42 28 47 a8 8c ea a0 68 ab f9 01 bc 3d e2 19 82 65 5d 22 c5 f1 74 4c 31 94 b9 d2 62 e9 d9 a7 a2 f9 55 57 b4 e5 9d d1 50 42 7e 29 2e 75 0e 6a d9 61 a6 55 c2 25 7f 5b 0d 25 93 9c 1c 8e 89 60 a2 27 1d 6a 6a 52 7c 1d 70 a5 70 4d b1 d2 ab f6 51 95 18 fb 75 77 5b a7 4a 46 34 c2 58 d1 a6 71 49 5e 7d ab 86 51 aa 59 ed c2 c1 58 64 1f e3 7f 5d 09 6c 16 4d 93 50 2d 80 aa b0 5b Data Ascii: 0~lfZ"H0[B4pa_#0UpzB^QL0[r.+dTJTU-WR LnS"Z9B(Gh=e]"tL1bUWPB~).ujQU~%["jir]ppMQuw[JF4Xq l^}QYXd]JMP-[
2021-12-02 15:37:58 UTC	1143	IN	Data Raw: af 6b ac 02 bc b7 d5 5e 87 6b fb aa ae 16 8c dd e4 e7 c9 67 0a 6e 0e 8a 4e 8f 6f 26 9a a3 46 ad 91 36 a8 2d 30 fb b1 c4 63 b3 45 fa b9 c2 b3 63 c2 93 23 b4 09 db d7 aa 39 62 fd 1a c3 cb 1f 4b 3c c2 5c a4 9f 2b c8 3c 22 3c 3d ce 9c b2 7f 9d 9a 63 f6 af 2f 48 fe b1 c4 e3 ae 45 fa b9 42 e5 c3 c2 33 a2 e5 09 fb d7 aa 39 62 ff 1a 43 fd 1f 4b 3c da 5f a4 9f 2b e0 3f 2c 3c 23 e6 9f b2 7f 9d 9a 63 f6 af 0f b0 e0 b1 c4 31 0b 44 fa b9 60 d2 c2 33 90 0b 08 fb d7 aa 39 62 ff 1a 61 17 1e 4b 1c 79 41 a4 9f 0b 7c 21 2c 3c 03 0f 81 b2 7f 9d 9a 63 f6 af 0f 3c e2 b1 c4 f1 23 44 fa b9 20 24 c2 c2 3d 2c 86 6c ff af 55 73 c4 fe 35 42 60 3c 96 38 0a 86 48 3f 17 10 46 58 b8 57 85 6c ff af 55 73 cc fe f5 01 79 3c 96 38 96 87 48 3f 17 9c 47 58 b8 b7 82 c9 f6 ff 5a 35 c7 56 5f Data Ascii: k^kgnNo&F6-0cEc#9bK< +<"<=c/HEB39bCK<_+?,<#c1D'39baKyA !,<c<#D \$=,lUs5B^<8H?FXWlUsy<8H?G XZ5V_
2021-12-02 15:37:58 UTC	1144	IN	Data Raw: 91 2a 81 3d c0 19 d2 31 01 9a 4a e6 8b a0 53 91 4c 1e dd 49 b0 b4 09 c0 54 19 01 39 16 4b 01 ab c2 38 43 3a 26 40 56 a9 7c 29 3e 46 03 57 55 74 27 c1 b6 58 cc c7 92 11 ac 12 d8 03 9c 21 1d 13 a0 ac d4 7a 34 8c 66 45 32 79 74 27 c1 5e 89 e3 b0 56 ea 2b 1f 46 b6 22 99 3c ba 93 60 cf 6f 62 10 57 46 0c d6 c2 27 01 e8 0a e3 0c 69 9a 0e 77 25 b2 37 91 b4 f3 83 5e 81 62 02 0a a0 90 32 90 c1 87 33 b1 f5 0f 8b cf c6 c0 92 99 03 5a 85 10 77 2c 0e 4a f1 00 02 91 c3 90 01 89 25 73 52 45 92 30 40 15 39 94 95 56 f5 08 84 2c d5 3a 34 48 96 cf 10 74 92 30 3a 0e c2 14 70 99 13 01 b3 a0 14 1c 33 0b e1 88 57 8e 06 f6 c1 b8 62 d5 3b 05 3f 2b d1 81 c3 3e 93 d5 18 09 b5 aa 0d 4e 2b 55 7f 47 7a 53 9e e7 a6 78 41 ed e8 5a 48 4d 3d cc 2b b7 ae 04 43 0a cc 16 5d 5f 8a f5 64 b0 ad Data Ascii: *=1JSLIT9K8C:&@V >FWU!X!z4fE2yt^V+F"<^obWFL,^w^7^b23Zw,^%sRE0@9V,^4Ht0:p3Wb;?>+N+GzS xAZHM=+C_]d
2021-12-02 15:37:58 UTC	1146	IN	Data Raw: 32 41 9f 49 c6 44 8b f1 52 6c a4 5e 09 50 68 7c 7a 11 f5 19 1a 04 d4 11 e1 2f 4b 83 00 fc 99 cc 9a 6c 99 14 e0 33 8f 8d d4 2b 01 f2 8c 67 8a fa 0c 0d 76 a6 88 f0 97 6d 99 a0 cf 24 63 9c c5 78 29 36 52 af 04 68 33 3e f3 8c fa 0c 0d 6a a6 88 f0 97 a5 41 00 ce 4c 66 4d b6 4c 0a 90 99 c7 46 ea 95 00 61 c6 33 45 7d 86 06 2f 53 44 f8 cb b6 4c d0 67 92 31 cb 62 bc 14 1b a9 57 02 54 19 9f 02 45 7d 86 06 29 53 44 f8 cb 9e e3 05 7d 26 19 9b 2c c6 4b b1 91 7a 25 40 92 f1 4c f1 a9 6f 70 ee 6b 4f 7e 93 61 c8 64 d6 74 cb 24 4e 80 a9 19 70 36 f4 18 5f af 46 7d 86 06 1d 53 44 f8 cb d2 20 0b 37 26 b3 26 5b 26 05 68 cc 63 23 f5 4a 80 18 e3 99 a2 3e 43 83 8b 29 22 fc 65 5b 26 e8 33 c9 98 62 31 5e 8a 8d d4 2b 01 4a 8c 6f 65 44 7d 86 06 11 53 44 f8 cb d2 20 00 1f 26 b3 26 5b Data Ascii: 2AIDRl^Ph zm/Kl3+gvm\$cx)6Rh3> AlfMLFa3E)/SDLg1bWTE)]SD]&,Kz%@(LopkO~adt\$Np6_F]SD 7&[&hc# J>C)"e[&3b1^+JoeD]SD &[&
2021-12-02 15:37:58 UTC	1147	IN	Data Raw: 05 42 a4 e9 14 0e 91 a6 53 50 44 9a 4e a1 11 69 3a 05 48 a4 e8 04 26 91 a2 12 b0 44 8a 4a 20 13 29 2a 01 4e a4 a8 04 3e 91 a2 12 10 45 8a 4a a0 14 69 8f c1 81 8a b4 3d 70 ac 22 49 c5 e1 8a 24 0d 47 2c 92 34 1c b4 48 d2 70 dc 22 49 c3 a1 8b 24 0d 47 2f 92 34 1c c0 48 d2 70 0c 23 49 c3 61 8c 24 0d 47 32 52 75 27 c0 8c 14 95 c0 33 52 54 02 d2 48 51 09 54 23 45 25 80 8d 14 95 c0 36 52 54 02 de 48 51 09 84 23 45 25 40 8e 14 95 c0 39 52 be 40 41 1d 29 17 0b 06 a 150 3c 2e d9 fe 7d 80 c1 1e 24 ec 91 ce 9c fc 48 7c 84 9b 66 0c 68 17 85 40 52 ce 9f 60 25 32 78 ca 90 ed df 96 1e 74 fc 94 ce 9d 63 a6 84 18 2a 84 31 a0 5e 1c 1a 49 77 cc 04 43 d1 00 49 15 dd 49 b0 94 09 c0 24 19 01 39 d6 4a 01 4b c2 38 4 3 3a 26 40 26 e9 41 23 c5 62 11 df ea ba ce 95 0e 9f 64 04 64 59 Data Ascii: BSPDNi:H&DJ)"N>EJi=p"l\$G,4Hp"l\$G/4Hp#a\$G2Ru'3RTHQT#E%6RTHQ#E%@9R@A)P<.)\$H fh @R' %2xtc*1^lwCII\$9JK8C:&@&A#bddY
2021-12-02 15:37:58 UTC	1148	IN	Data Raw: 1c d9 53 6a ad 02 dd 28 f5 01 99 49 81 28 96 99 26 9d 0b ce 2c 2a df ad 4b 1c d1 0c 6f 94 5a ab 40 36 4a 8d e8 66 4a 20 dd 53 ce 87 71 16 95 ef d5 e5 c8 9e 52 6b 15 e8 46 a9 0f f2 4c 0a 44 51 cf 34 e9 5c c0 67 51 f9 6e 5d e2 d8 67 78 a3 d4 5a 05 b2 51 6a c4 41 53 02 e9 9e 72 3e 34 b4 a8 7c af 2e 47 f6 94 5a ab 40 37 4a 7d e0 68 52 20 8a 8f a6 49 e7 82 48 8b ca 77 eb 12 47 49 c3 1b a5 d6 2a 90 8d 52 23 62 9a 12 48 f7 94 f3 e1 a6 45 e5 7b 75 39 b2 a7 d4 5a 05 ba 51 6a a9 08 10 d8 05 d0 65 e8 a1 5a 45 0e 9c bc b9 4c fe 09 60 e8 80 f3 4c 00 69 6a b7 f0 8c 18 69 6a 46 7c 5e 98 b4 84 6a 78 db 9e d9 48 69 09 35 f1 66 f7 29 28 5c 43 3e 71 cd 90 69 c4 7a a8 66 e0 34 a7 14 f4 4e 0a bd 69 5d 33 82 1a bd 3e ab 19 47 cd 2f 08 87 52 13 7c e8 58 e1 8f 0d 39 98 6a 50 52 Data Ascii: Sj (l(&,*KoZ@6JfJ SqRkFLDQ4 gQn gxZQjASr>4 .GZ@7J JhR lHwG!R#bHE{u9ZQjeZEL`LijjF j^xHi5f) (>qizf4Nj3>G/R X9 PR
2021-12-02 15:37:58 UTC	1150	IN	Data Raw: 58 8e 4c 98 2d 91 23 1b 63 4b e4 ca 04 d8 5a cd 51 74 2d 9e 7c 06 68 2d 21 36 8a ab 15 2c dc bd 50 18 2d 9d 49 ab b7 5e 28 9c 16 ef 6d b5 d7 01 03 d2 5a cd 51 14 2d 9e 7c 26 08 ad a0 68 2f 52 35 b7 39 6a d4 1a 69 83 da 30 b3 56 73 1c 30 4b a4 9f 0b 2d 2b 26 dc 95 9e 6b fb 5a 35 47 ac 5f 23 3c d6 6a 8e 63 63 89 f4 73 01 63 45 84 bb 55 c8 f6 fd 5a 35 c7 ec 5f 1f 12 d6 6a 8e c3 60 89 f4 73 61 60 85 85 bb 55 88 03 60 b9 f6 af 55 73 c4 fe 35 82 5e ad e6 38 e2 95 48 3f 17 dc 55 58 b8 57 85 6c ff af 55 73 cc fe f5 e1 5b ad e6 38 b8 95 48 3f 17 b2 55 58 b8 17 c3 91 ed ff b5 6a 8e d8 bf 46 28 ab d5 1c c7 b1 12 e9 e7 02 b1 0a 0b f7 aa 90 ed ff b5 6a 8e d9 bf 3e d4 aa d5 1c 87 ac 12 e9 e7 c2 ab 0a 0b 77 ab 10 07 ab 72 ed 5f ab e6 88 fd 6b 04 a8 5a cd 71 74 2a 91 7e Data Ascii: XL-#cKZQt ~h~P,~l^("mZQ~ &h/R59ji0vS0K~+&kZ5G_#~cjcscEUZ5_j^sa`U`Us5^8H?UXWlUsy[8H?UXjF(j>wr_kZqt*~

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1430	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 d2 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'G>H&2u58DcM@Or'Po['ch,FNwg9NY Z!Pn;]FY_o&XCztg5bWK6=B/JyV!T(XVmL!R !0E),[YZBwDw!2
2021-12-02 15:37:58 UTC	1431	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 32 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)Qmirr oring_webr
2021-12-02 15:37:58 UTC	1432	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 b1 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 88 d6 a7 a3 3e 7e 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\$mqw8[*W>wN)]?-S
2021-12-02 15:37:58 UTC	1434	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 1d 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.oN9
2021-12-02 15:37:58 UTC	1435	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 6b 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 a6 5a f7 6b cd 07 d7 1d e1 4f b8 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({f4_@skOnPlz=e%QJXwklb4zaAgNZ33}OjQtjJhS*-3SNZg)GXwkPEck<itl] 3@YZlg,_iK
2021-12-02 15:37:58 UTC	1436	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 07 b2 8d ad 9c 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 00 09 00 00 00 00 00 00 00 00 00 10 00 ed 01 00 00 00 00 Data Ascii: 5"ia1k!h"Vx7!_etX?8lQk~V9W&0,m)gl36O1au>[b:k7=\$o.pnx!*6zFco,~0-@+~o9?PKV"PK*Q
2021-12-02 15:37:58 UTC	1437	IN	Data Raw: 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 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 08 00 2a 8c 04 51 00 00 00 00 02 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 15:37:58 UTC	1439	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 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 10 00 ed 01 4a 42 01 00 5f 6c 6f 63 61 6c 65 73 2f 68 75 2f 50 Data Ascii: M2_locales/hr/PK)QX=ze12_locales/hr/messages.jsonPK*QJB_locales/hu/P
2021-12-02 15:37:58 UTC	1439	IN	Data Raw: 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 08 00 2a 8c 04 51 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 ed 01 de 52 01 00 5f 6c 6f 63 61 6c 65 73 2f 69 64 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 db d0 86 a4 8f 0e 00 00 6b 2e 00 00 19 00 00 00 00 00 00 00 00 00 a4 01 1a 53 01 00 5f 6c 6f 63 61 6c 65 73 2f 69 64 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 00 00 00 00 00 00 10 00 ed 01 f0 61 01 00 5f 6c 6f 63 61 6c 65 73 2f 69 Data Ascii: K)Q]Q06B_locales/hu/messages.jsonPK*QR_locales/id/PK)Qk.S_locales/id/messages.jsonPK*Qa_locales/i
2021-12-02 15:37:58 UTC	1440	IN	Data Raw: 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 02 00 00 00 00 00 00 00 00 10 00 ed 01 40 fd 01 5f 6c 6f 63 61 6c 65 73 2f 6d 73 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 48 dc de c1 d2 0e 00 00 6f 2f 00 00 19 00 00 00 00 00 00 00 00 00 00 00 a4 01 7c fd 01 00 5f 6c 6f 63 61 6c 65 73 2f 6d 73 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 00 00 00 00 00 00 10 00 ed 01 95 0c 02 00 5f 6c 6f 63 61 6c 65 73 2f 6e 62 2f 50 4b 01 02 14 03 14 00 08 08 08 00 Data Ascii: QZD_locales/mr/messages.jsonPK*Q@_locales/ms/PK)QHo/_locales/ms/messages.jsonPK*Q_locales/nb/PK

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:58 UTC	1441	IN	Data Raw: 00 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 0c 00 00 00 00 00 00 00 00 10 00 ed 01 f5 a1 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 76 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 c9 be 49 61 f4 0e 00 00 09 30 00 00 19 00 00 00 00 00 00 00 00 00 00 00 a4 01 31 a2 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 76 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 0c 00 00 00 00 00 00 00 00 10 00 ed 01 6c b1 02 00 5f 6c 6f 63 61 6c 65 73 2f 73 77 2f 50 4b 01 02 14 03 14 00 08 08 08 00 29 8c 04 51 e4 9d 96 78 af 0e 00 00 c1 2e Data Ascii: :_locales/sr/messages.jsonPK*Q:_locales/sv/PK)Qla01:_locales/sv/messages.jsonPK*Ql:_locales/sw/PK)Qx.
2021-12-02 15:37:58 UTC	1443	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 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 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 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 Data Ascii: :_locales/zh_TW/messages.jsonPK)QO3DnKangular.jsPK)Q(background_script.jsPK)Q7cast_sender.jsPK)Q-I4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	209.182.194.220	443	192.168.2.6	49695	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:47 UTC	10	IN	HTTP/1.1 302 Found Date: Thu, 02 Dec 2021 15:37:42 GMT Server: Apache Location: 9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-0000000000&y=87SkZlcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true Vary: User-Agent Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
70	192.168.2.6	49772	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:59 UTC	1444	OUT	GET /images/microsoft_logo_7lyNn7YkjJOP0NwZNw6QvQ2.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: acctcdn.msauth.net

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
71	192.168.2.6	49771	152.199.21.175	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:59 UTC	1444	OUT	GET /images/favicon.ico?v=2 HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: acctcdn.msauth.net

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
72	152.199.21.175	443	192.168.2.6	49772	C:\Program Files\Google\Chrome\Application\chrome.exe

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

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:00 UTC	1466	OUT	GET /images/dropdown_caret_KXSzjGsyILZaoTf0sl9X-A2.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: acctcdn.msauth.net

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
75	152.199.21.175	443	192.168.2.6	49773	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:00 UTC	1466	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: 5366397 Cache-Control: public, max-age=31536000 Content-MD5: 5h8LmH5/oEhH5cNR2+nY3g== Content-Type: image/svg+xml Date: Thu, 02 Dec 2021 15:38:00 GMT Etag: 0x8D9846FFE07F84C Last-Modified: Fri, 01 Oct 2021 00:11:18 GMT Server: ECAcc (frc/8E8B) Vary: Accept-Encoding X-Cache: HIT x-ms-blob-type: BlockBlob x-ms-lease-status: unlocked x-ms-request-id: 882c997f-901e-0047-44c3-b63aeb000000 x-ms-version: 2009-09-19 Content-Length: 224 Connection: close
2021-12-02 15:38:00 UTC	1467	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 33 36 22 20 68 65 69 67 68 74 3d 22 33 36 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 33 36 20 33 36 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 32 32 2e 34 38 34 6c 2d 38 2d 38 2c 2e 39 36 39 2d 2e 39 36 38 4c 31 38 2c 32 30 2e 35 34 37 6c 37 2e 30 33 31 2d 37 2e 30 33 31 2e 39 36 39 2e 39 36 38 2d 38 2c 38 5a 22 2f 3e 3c 72 65 63 74 20 77 69 64 74 68 3d 22 33 36 22 20 68 65 69 67 68 74 3d 22 33 36 22 20 66 69 6c 6c 3d 22 6e 6f 6e 65 22 2f 3e 3c 2f 73 76 67 3e Data Ascii: <svg xmlns="http://www.w3.org/2000/svg" width="36" height="36" viewBox="0 0 36 36"><title>assets</title><path d="M18,22.484l-8-8,.969-.968L18,20.547l7.031-7.031.969.968-8,8Z"/><rect width="36" height="36" fill="none"/></svg>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
76	192.168.2.6	49775	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:01 UTC	1467	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/favicon_a_eupayfgghqiai7k9sol6lg2.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
77	192.168.2.6	49776	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:01 UTC	1467	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/45_sgsjshsdggdjdghvcvcj.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
78	209.182.194.220	443	192.168.2.6	49775	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1468	IN	HTTP/1.1 304 Not Modified Date: Thu, 02 Dec 2021 15:38:01 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Vary: User-Agent Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
79	209.182.194.220	443	192.168.2.6	49776	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1468	IN	HTTP/1.1 304 Not Modified Date: Thu, 02 Dec 2021 15:38:01 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49699	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:37:47 UTC	11	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/?client_id=0000009918-0000-0slr-iw00-000000000&y=87SkZIcm5hbmRlekB3aWNrZXJzbWl0aC5jb20%3D&redirect_uri=https%3a%2f%2foutlook.office.com%2fowa%2f&resource=client_id&response_mode=form_post&response_type=code+id_token&scope=openid&msafed=0&client-request-id=45f4d5f9-4657-4816-9528-af3f59994174&protectedtoken=true HTTP/1.1 Host: pickap.acepickapart.com Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: document Referer: https://pickap.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
80	192.168.2.6	49781	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1468	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/microsoft_logo_ee5c8d9fb6248c938fd0dc19370e90bd.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
81	192.168.2.6	49782	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1468	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
82	209.182.194.220	443	192.168.2.6	49781	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1469	IN	HTTP/1.1 304 Not Modified Date: Thu, 02 Dec 2021 15:38:02 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Vary: User-Agent Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
83	209.182.194.220	443	192.168.2.6	49782	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:02 UTC	1469	IN	HTTP/1.1 304 Not Modified Date: Thu, 02 Dec 2021 15:38:02 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Vary: User-Agent Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
84	192.168.2.6	49783	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:03 UTC	1469	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_white_5ac590ee72bfe06a7cecfdf75b588ad73.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
85	192.168.2.6	49784	209.182.194.220	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:03 UTC	1469	OUT	GET /hergsl/9cef6f38045264f7cbaec8b47ad485f3/include/src/ellipsis_grey_2b5d393db04a5e6e1f739cb266e65b4c.svg HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: pickap.acepickapart.com If-Modified-Since: Thu, 02 Dec 2021 15:37:47 GMT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
86	209.182.194.220	443	192.168.2.6	49784	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-02 15:38:03 UTC	1470	IN	HTTP/1.1 304 Not Modified Date: Thu, 02 Dec 2021 15:38:03 GMT Server: Apache Last-Modified: Thu, 02 Dec 2021 15:37:47 GMT Accept-Ranges: bytes Vary: User-Agent Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
87	209.182.194.220	443	192.168.2.6	49783	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

General	
Start time:	16:37:36
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 "https://pickup.acepickapart.com/hergsl/kut.gxs?op=JFernandez@wickersmith.com
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: chrome.exe PID: 4580 Parent PID: 2948

General	
Start time:	16:37:37
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=1560,8371606130546468176,1673999905795240130,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1920 /prefetch:8
Imagebase:	0x7ff7c15e0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis