ID: 491715
Cookbook: browseurl.jbs
Time: 20:32:56
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

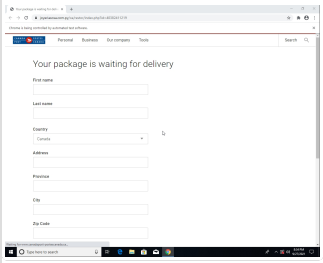
Windows Analysis Report https://www.joyeriasosa.com.…

Overview

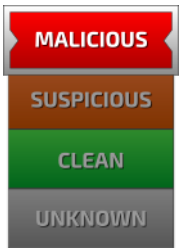
General Information

Sample URL:	http://https://www.joyeriasosa.com.py/ca/
Analysis ID:	491715
Infos:	

Most interesting Screenshot:



Detection

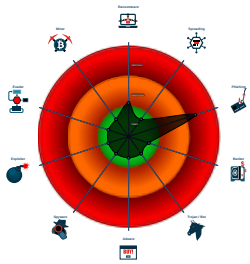


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Phishing site detected (based on fav…
- Antivirus detection for URL or domain
- Phishing site detected (based on log…
- Found iframes
- No HTML title found
- HTML body contains low number of …
- Suspicious form URL found

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 6316 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'https://www.joyeriasosa.com.py/ca/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 2964 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1616,3579062385751043411,707075701747647181,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1676 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 7096 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=audio.mojom.AudioService --field-trial-handle=1616,3579062385751043411,707075701747647181,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6564 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 8184 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=video_capture.mojom.VideoCaptureService --field-trial-handle=1616,3579062385751043411,707075701747647181,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6112 /prefetch:8 MD5: C139654B5C1438A95B321BB01AD63EF6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Phishing:

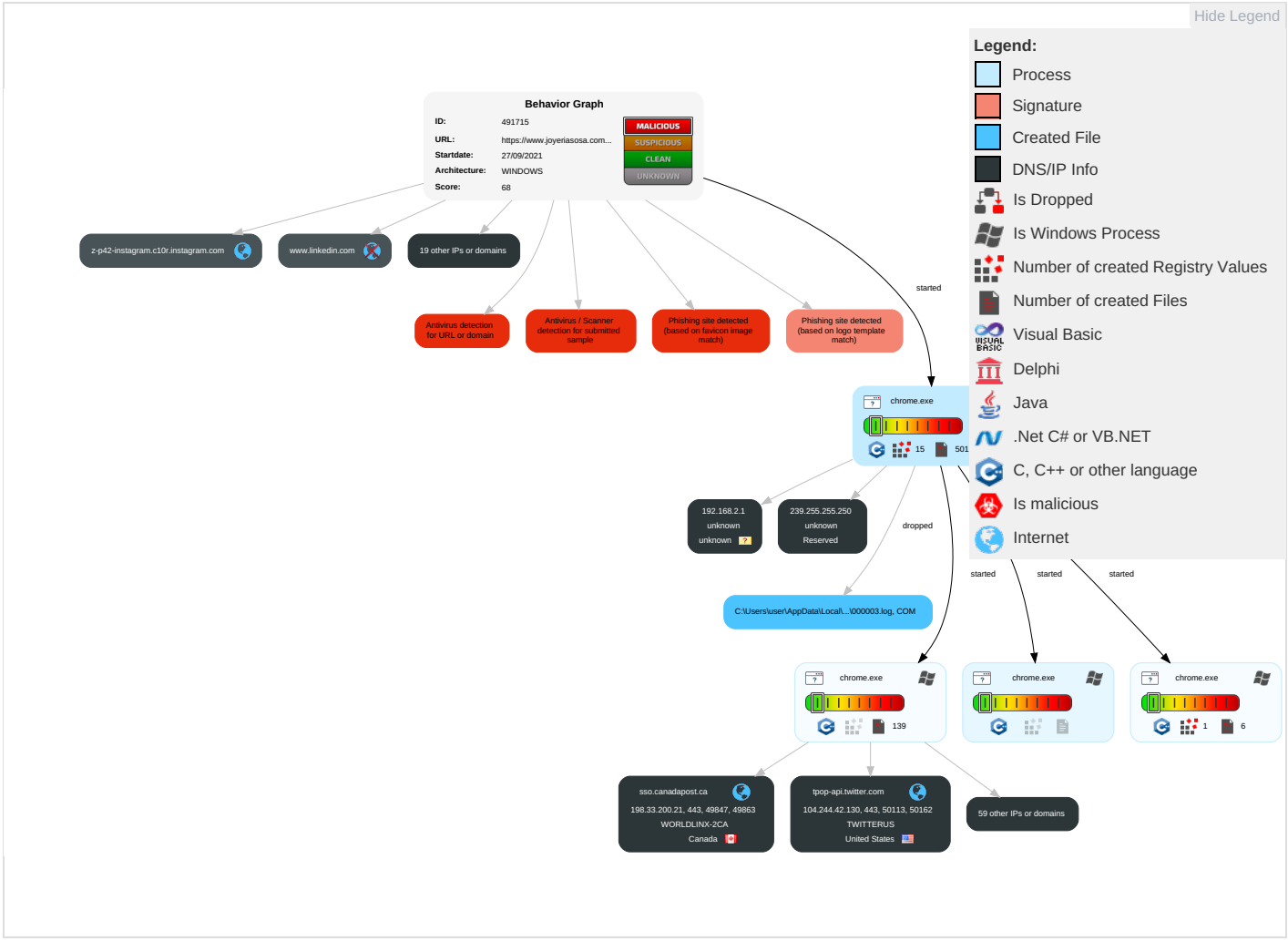
Phishing site detected (based on favicon image match)

Phishing site detected (based on logo template match)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Drive-by Compromise 1	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 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
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 4	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 5	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap	

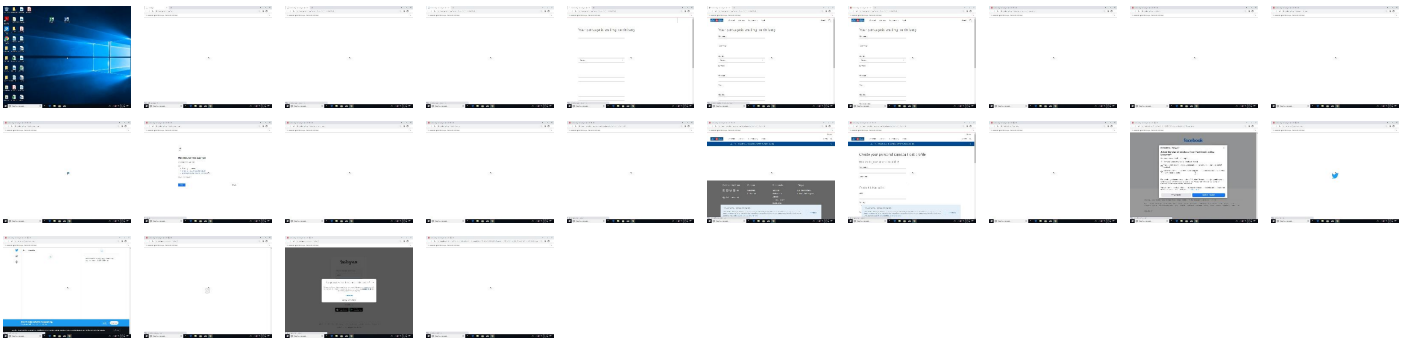
Behavior Graph

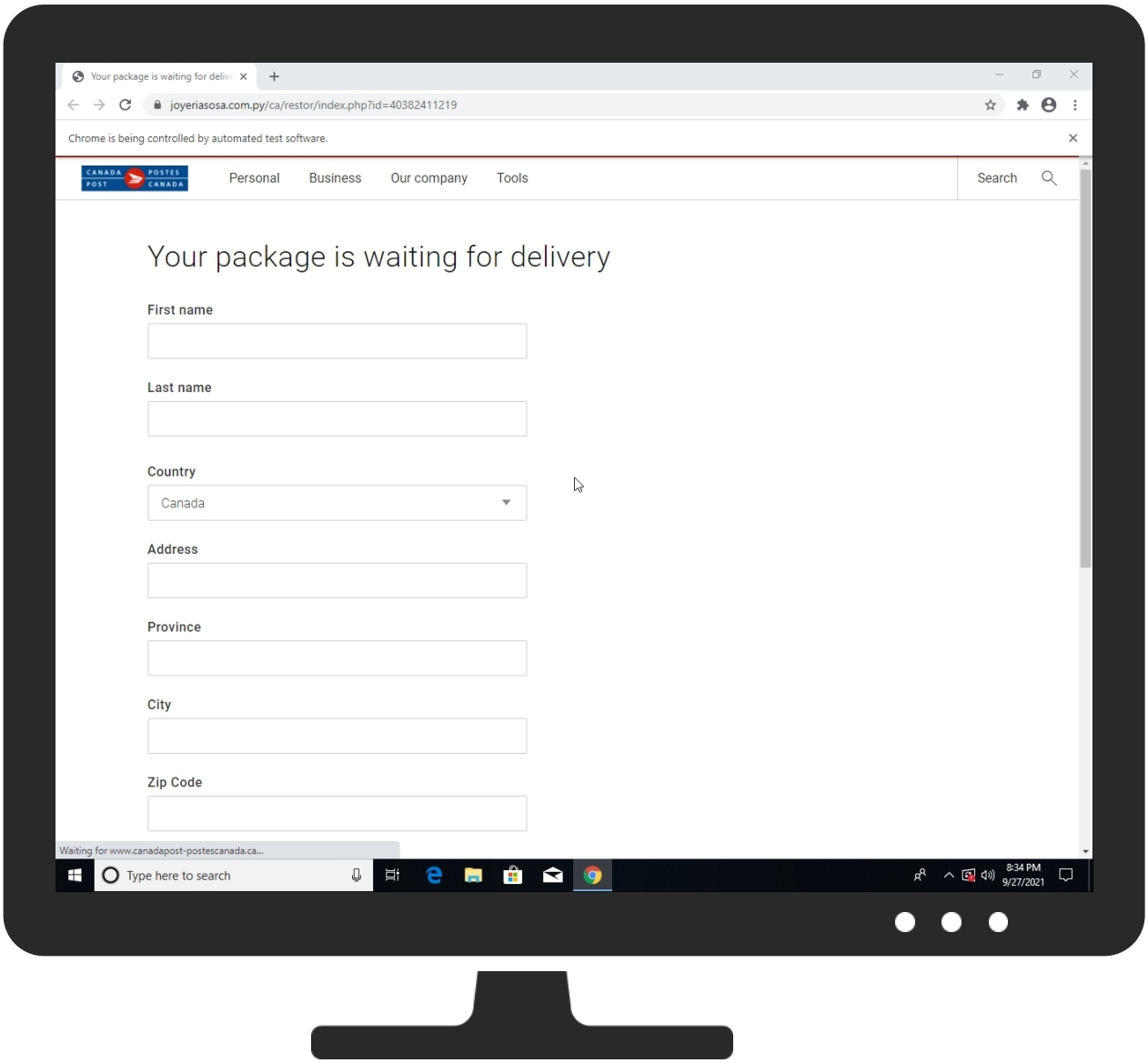


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://https://www.joyeriasosa.com.py/ca/	100%	Avira URL Cloud	phishing	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.joyeriasosa.com.py/ca/restor/assets/api.js.download	100%	Avira URL Cloud	phishing	
http://https://www.joyeriasosa.com.py/ca/restor/assets/614267586032718	100%	Avira URL Cloud	phishing	
http://https://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/assets/favicon.ico?version=	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/assets/favicon.ico?version=	0%	Avira URL Cloud	safe	
http://https://www.joyeriasosa.com.py/ca/restor/assets/search.png	100%	Avira URL Cloud	phishing	
http://https://sso-osu.canadapost-postescanada.ca/pfe-pap/en/registration/personal#Canada	0%	Avira URL Cloud	safe	
http://https://www.joyeriasosa.com.py/ca/restor/assets/saved_resource.html	100%	Avira URL Cloud	phishing	
http://https://www.joyeriasosa.com.py/ca/restor/index.php?id=4038241121922Your	100%	Avira URL Cloud	phishing	
http://https://canadapost-postescanada.ca/-lg	0%	Avira URL Cloud	safe	
http://https://6048943.fls.doubleclick.net2	0%	Avira URL Cloud	safe	
http://https://sso-osu.canadapost-postescanada.ca/lfe-cap/en/login	0%	Avira URL Cloud	safe	
http://https://twitter.github.io/birdwatch/join	0%	URL Reputation	safe	
http://https://sso-osu.canadapost-postescanada.ca/pfe-pap/en/registration/personal#P	0%	Avira URL Cloud	safe	
http://https://joyeriasosa.com.py/WL	0%	Avira URL Cloud	safe	
http://https://www.joyeriasosa.com.py/ca/restor/assets/foundation.min.js.download	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gstaticadssl.l.google.com	172.217.168.67	true	false		high
dart.l.doubleclick.net	142.250.203.102	true	false		high
undefined.ca	168.235.64.196	true	false		unknown
cs45.wac.edgecastcdn.net	93.184.220.70	true	false		high
dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	54.154.124.189	true	false		high
adservice.google.com	172.217.168.34	true	false		high
z-p42-instagram.c10r.instagram.com	157.240.17.174	true	false		high
platform.twitter.map.fastly.net	199.232.136.157	true	false		unknown
tpop-api.twitter.com	104.244.42.130	true	false		high
scontent.xx.fbcdn.net	157.240.17.15	true	false		high
canadapost.ca.ssl.d1.sc.omtrdc.net	13.36.218.177	true	false		unknown
t.co	104.244.42.133	true	false		high
twimg.twitter.map.fastly.net	151.101.12.159	true	false		unknown
facebook.com	157.240.17.35	true	false		high
www.google.com	172.217.168.36	true	false		high
sso.canadapost.ca	198.33.200.21	true	false		high
star-mini.c10r.facebook.com	157.240.17.35	true	false		high
cs531.wpc.edgecastcdn.net	192.229.220.133	true	false		high
pagead46.l.doubleclick.net	172.217.168.34	true	false		high
twitter.com	104.244.42.65	true	false		high
accounts.google.com	172.217.168.13	true	false		high
s.twitter.com	104.244.42.131	true	false		high
www-google-analytics.l.google.com	142.250.203.110	true	false		high
www-googletagmanager.l.google.com	172.217.168.40	true	false		high
www.joyeriasosa.com.py	167.172.159.206	true	false		unknown
googleads.g.doubleclick.net	142.250.203.98	true	false		high
play.google.com	172.217.168.14	true	false		high
clients.l.google.com	172.217.168.46	true	false		high
www.google.ch	216.58.215.227	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.1	true	false		high
static.ads-twitter.com	unknown	unknown	false		unknown
canadapost.demdex.net	unknown	unknown	false		high
abs.twimg.com	unknown	unknown	false		high
siteintercept.qualtrics.com	unknown	unknown	false		high
cm.everesttech.net	unknown	unknown	false		high
api.twitter.com	unknown	unknown	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
zn0xleir6swszany9-canadapostdigital.siteintercept.qualtrics.com	unknown	unknown	false		high
www.canadapost-postescanada.ca	unknown	unknown	false		unknown
sso-osu.canadapost-postescanada.ca	unknown	unknown	false		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
video.twimg.com	unknown	unknown	false		high
platform.linkedin.com	unknown	unknown	false		high
dpm.demdex.net	unknown	unknown	false		high
sslstats.canadapost.ca	unknown	unknown	false		high
www.facebook.com	unknown	unknown	false		high
assets.adobedtm.com	unknown	unknown	false		high
pbs.twimg.com	unknown	unknown	false		high
www.linkedin.com	unknown	unknown	false		high
adservice.google.ch	unknown	unknown	false		high
6048943.fls.doubleclick.net	unknown	unknown	false		high
www.canadapost.ca	unknown	unknown	false		high
connect.facebook.net	unknown	unknown	false		high
static-exp1.licdn.com	unknown	unknown	false		high
static.xx.fbcdn.net	unknown	unknown	false		high
analytics.twitter.com	unknown	unknown	false		high
www.instagram.com	unknown	unknown	false		high
9852050.fls.doubleclick.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.joyeriasosa.com.py/ca/restor/assets/api.js.download	true	• Avira URL Cloud: phishing	unknown
http://https://www.joyeriasosa.com.py/ca/restor/assets/614267586032718	true	• Avira URL Cloud: phishing	unknown
http://https://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/assets/favicon.ico?version=	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://www.joyeriasosa.com.py/ca/restor/assets/search.png	true	• Avira URL Cloud: phishing	unknown
http://https://9852050.fls.doubleclick.net/activityi;dc_pre=CMG27M_ln_MCFVYY0wod1sYDVA;src=9852050;type=optim0;cat=perso0;ord=4161029190815;gtm=2od9m0;auiddc=1301920779.1632800086;u1=%5BProduct%5D;u2=%5BPage%20Name%5D;u3=%5BURL%5D;u4=%5BReferral%5D;u5=%5BLanguage%5D;u6=%5BJourney%20Step%5D;~oref=https%3A%2F%2Fsso-osu.canadapost-postescanada.ca%2Fpfe-pap%2Fen%2Fregistration%2Fpersonal?	false		high
http://https://www.joyeriasosa.com.py/ca/restor/assets/saved_resource.html	true	• Avira URL Cloud: phishing	unknown
http://https://twitter.com/canadapostcorp	false		high
http://https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard	false		high
http://https://www.facebook.com/login/?next=https%3A%2F%2Fwww.facebook.com%2Fcanadapost	false		high
http://https://www.joyeriasosa.com.py/ca/restor/assets/foundation.min.js.download	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
168.235.64.196	undefined.ca	United States		3842	RAMNODEUS	false
172.217.168.40	www-googletagmanager.l.google.com	United States		15169	GOOGLEUS	false
157.240.17.35	facebook.com	United States		32934	FACEBOOKUS	false
172.217.168.46	clients.l.google.com	United States		15169	GOOGLEUS	false
157.240.17.15	scontent.xx.fbcdn.net	United States		32934	FACEBOOKUS	false
18.203.8.109	unknown	United States		16509	AMAZON-02US	false
142.250.203.98	googleads.g.doubleclick.net	United States		15169	GOOGLEUS	false
104.244.42.65	twitter.com	United States		13414	TWITTERUS	false
142.250.203.102	dart.l.doubleclick.net	United States		15169	GOOGLEUS	false
192.229.220.133	cs531.wpc.edgecastcdn.net	United States		15133	EDGECASTUS	false
104.244.42.133	t.co	United States		13414	TWITTERUS	false
172.217.168.1	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
13.36.218.177	canadapost.ca.ssl.d1.sc.omtrdc.net	United States		7018	ATT-INTERNET4US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.154.124.189	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com	United States		16509	AMAZON-02US	false
104.244.42.131	s.twitter.com	United States		13414	TWITTERUS	false
104.244.42.130	tpop-api.twitter.com	United States		13414	TWITTERUS	false
198.33.200.21	sso.canadapost.ca	Canada		3848	WORLDLINX-2CA	false
172.217.168.13	accounts.google.com	United States		15169	GOOGLEUS	false
172.217.168.34	adservice.google.com	United States		15169	GOOGLEUS	false
172.217.168.36	www.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
167.172.159.206	www.joyeriasosa.com.py	United States		14061	DIGITALOCEAN-ASNUS	false
93.184.220.70	cs45.wac.edgecastcdn.net	European Union		15133	EDGECASTUS	false
151.101.12.159	twimg.twitter.map.fastly.net	United States		54113	FASTLYUS	false
199.232.136.157	platform.twitter.map.fastly.net	United States		54113	FASTLYUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491715
Start date:	27.09.2021
Start time:	20:32:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://www.joyeriasosa.com.py/ca/
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:	15
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:	mal68.phis.win@58/444@49/27
Cookbook Comments:	• Adjust boot time • Enable AMSI • Browse: https://.undefined.ca/web/en/pages/support/default.page • Browse: https://.undefined.ca/cpc/en/our-company/about-us.page • Browse: https://.undefined.ca/shop/shop.jsf • Browse: https://.undefined.ca/cpc/en/personal.page • Browse: https://.undefined.ca/cpc/en/business.page • Browse: https://.undefined.ca/cpc/en/our-company.page • Browse: https://.undefined.ca/cpc/en/tools.page • Browse: https://sso-osu.canadapost-postescanada.ca/pfe-pap/en/registration/personal# • Browse: https://www.facebook.com/canadapost • Browse: https://twitter.com/canadapostcorp • Browse: https://www.instagram.com/canadapostagram/?hl=en • Browse: http://www.linkedin.com/company/canada-post?trk=company_name
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\Dictionaries\en-US-9-0.bdic	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	451603
Entropy (8bit):	5.009711072558331
Encrypted:	false
SSDEEP:	12288:ZHfRTyGZ6lup8Cfrvq4JBPKh+FBlESBw4p6: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 GMDS.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 GVMDS.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\165ee120-c63f-4ffb-ad2c-90e89fa0e12e.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\165ee120-c63f-4ffb-ad2c-90e89fa0e12e.tmp

Size (bytes):	174261
Entropy (8bit):	6.047727256747523
Encrypted:	false
SSDEEP:	3072:12d5xv5TawDZG6TsIVmlyzM3k6LXQCTpSaS9FcbXafIB0u1GOJmA3iuRQ:EdnvNawDcIRmUAU6LQCtSZaqfIlUOoSS
MD5:	DECAAA76360090DA8480DE724E258868
SHA1:	9D5A45A6F27696D4BA49EA579895EF8B4A57CB49
SHA-256:	37ADB28F33E8BB2742036DB6537B20DFBA6FBC6363A5E88F6E41ECC64572A609
SHA-512:	BEE00ADD568FFFA3214B6F55073D969CEAF1E51914C5FBCF6DB66F96119350D2F5EE3EEA028ECFB780B87117987A71B0547D3555CC90664EA01F885B17C3AEA4
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":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632800037367171e+12,"network":1.632767639e+12,"ticks":6493213208.0,"uncertainty":4413043.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799617040"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\22e671a2-db13-4d91-bbfb-43d62992b615.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):	182744
Entropy (8bit):	6.077390460562561
Encrypted:	false
SSDEEP:	3072:yUv2d5xv5TawDZG6TsIVmlyzM3k6LXQCTpSaS9FcbXafIB0u1GOJmA3iuRQ:F+dnvNawDcIRmUAU6LQCtSZaqfIlUOoD
MD5:	9CB74150782B143FA3CB1B88A7E8BA61
SHA1:	2CE3A9878DAE64CD29C9CE7E0BB7B8D35CBC6AC5
SHA-256:	AC6D878DF2CDC4B9A914160261D5913F0F13B7D368E371F0F37B0D13FEE652BA
SHA-512:	D80CD55C419D7AF19BC85F40492B4A4B19536D356A553C382E43DEFE4E881F87E3598D17AC672531809D0970B833A349982197873D84C730658DF3A8455D6482
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":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632800037367171e+12,"network":1.632767639e+12,"ticks":6493213208.0,"uncertainty":4413043.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\32867817-c983-4cb2-99ef-bf03b46e0fd0.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):	182745
Entropy (8bit):	6.077390389157594
Encrypted:	false
SSDEEP:	3072:vdB2d5xv5TawDZG6TsIVmlyzM3k6LXQCTpSaS9FcbXafIB0u1GOJmA3iuRQ:VAdnvNawDcIRmUAU6LQCtSZaqfIlUOoD
MD5:	7E49EFB2F67116383C4F27D969560420
SHA1:	A0E4E4E7020A19734EFB5F9260AC09412B046AB4
SHA-256:	2E4A8B22A1BB4D60FC5C3CB92C678E651CC99AE1F361881AF5BFA3B71834BDA1
SHA-512:	1E73173E532E22AE43186738F26196F5CF33A62FA83498CD0B8904FDD799F7EF15B2AA14EA7ECF4E023EF42183EC50657EE21767D3879B35EA3AF22D79A74DF4
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":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632800037367171e+12,"network":1.632767639e+12,"ticks":6493213208.0,"uncertainty":4413043.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799617040"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\336d6a0a-1c02-4f51-b589-383f2a78e53f.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\336d6a0a-1c02-4f51-b589-383f2a78e53f.tmp

Size (bytes):	182744
Entropy (8bit):	6.077390436399961
Encrypted:	false
SSDEEP:	3072:ypY2d5xv5TawDZG6TsIVmlyzM3k6LXQCTpSaS9FcbXafIB0u1GOJmA3iuRQ:gzdnvNawDcIRmUAU6LQCtSZaqfIlUOoD
MD5:	C2A057296208970BBD84C44549402E72
SHA1:	C3E1A861828A9B0C52436618CFA8384469C388C8
SHA-256:	759644E478219AEA9839D86856F44C7CB2208888675EF5C33D3AB4A94F87ACF6
SHA-512:	1F4A37CA8C1B6A3DF92FBA4918960FF4F7EA736A15B25739561963AA78DD6B4FFF91F5DAC106E938FB91EB6C6302484AEE1E21463B451EAE2C00B06F1B228BFC
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":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632800037367171e+12,"network":1.632767639e+12,"ticks":6493213208.0,"uncertainty":4413043.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\3e420b0c-a4f1-4ff5-ba49-284a9991c9f4.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SysEx File -
Category:	dropped
Size (bytes):	94708
Entropy (8bit):	3.7475640528108713
Encrypted:	false
SSDEEP:	384:RDDY0WN/WZGAVFHsDNwr5vsY3Twm7HGbG3qr1KsGxziyG1rhYmViZaQIMzO2CANC:J+KV52mDbYeLCMeY3TCgK6wcdC
MD5:	9FB809171C64CD4A8618372C02359B99
SHA1:	8C0A2E4A81C13BA43A417D14071C2D26681DAC16
SHA-256:	752931B2F8BF6D7757616E5F05501C16794E5A01C92A3C0908D94B09731003E7
SHA-512:	7B3A7F983CFF95B5A227F463C960F8C708CA496A259C6DD029529B95CB0142A69FF51ECE66C311E814884DEDF7D7E99E379383BBEEF609932BE447B3A097336E
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....F8.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\73337b27-b375-40b6-af7e-13fd51c1b790.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	92724
Entropy (8bit):	3.747078707792424
Encrypted:	false
SSDEEP:	384:fDDY0WN/iGhsDNwr5vsY3Twm7HGbG3qr1KsGxziyG1rhYmViZaQIMzO2CANh1wZS:lKV52mDbYeLCMeY3TCgK6wcd3
MD5:	1809C28F820C4B1953A694B686A6653C
SHA1:	27CA78E0F03596B7360812941C34E944517B1AF8
SHA-256:	DB9C610F425FB38DD7627DBFCC5ED002EA0E6085B3645C6E156D6AD1B5A68F1F
SHA-512:	DD6C735C8FCA76B5036C5FFC21D5EAC294A39338A19300D71FF13B0D42A215B23565709DAF74BD72E9423D2AE1D331CE228DF244DD19BA9932E5F8D3C3A0662
Malicious:	false
Reputation:	low
Preview:	0j.....*...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....F8.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\94b92712-0cd0-4411-b27e-74cfd4b8c137.tmp

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\94b92712-0cd0-4411-b27e-74cfd4b8c137.tmp	
Size (bytes):	182745
Entropy (8bit):	6.077390287254501
Encrypted:	false
SSDEEP:	3072:vcj2d5xv5TawDZG6TsIVmlyzM3k6LXQCTpSaS9FcbXafIB0u1GOJmA3iuRQ:EydnvNawDcIRmUAU6LQCtSZaqfllUOoD
MD5:	177D46B442AC69AB43581538D21C08D4
SHA1:	1436ECD6E23CED02F81E0AD7CE0044C34325C02D
SHA-256:	780545CB61A70E4ED64FB94E042D487D780D7A15CA0C2551B9DFEB92B3B17BA6
SHA-512:	9275F604A8E3B3DAF500ABAF5FFFD364FDD58FE1221FF3D0CFCE5D236DDD36E8E0570BB4C7104C805A4FCADF99FAE913919AE060C7E9EAD2F765FAE1CF38FC11
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":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.632800037367171e+12,"network":1.632767639e+12,"ticks":6493213208.0,"uncertainty":4413043.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13276832799617040"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\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):	120
Entropy (8bit):	3.254162526001658
Encrypted:	false
SSDEEP:	3:FkXft0xE1G1mstft0xE1G1mstft0xE1n:+ftlE1G1mkftlE1G1mkftlE1n
MD5:	E9224A19341F2979669144B01332DF59
SHA1:	F7F760C7104457DF463306A7F7BAE0142EFCEB5B
SHA-256:	47DD519C226D23F203ACAE0EC44DF9BB6208828E24F726E1602EA52F63C3E2BE
SHA-512:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D021294256372C916B8155AC
Malicious:	false
Reputation:	low
Preview:	sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%sdPC.....s}.....M..2.!..%

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\3e7a0772-8995-478b-ad35-85542e9a5af6.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):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556
SHA-256:	DD2C9F43F622F801FCC213CDE8E3E90EF1D0D26665AE675449A94CEC7EB1D453
SHA-512:	84D3930579FD73C7D86144D5CDC636436955BA79759273C740D2D72BC4847F2F7F165BBCA3EB2E4DFB01777D6A5F141623278C1BF74615C5A491092CE3FD1602
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[],"expiration":"13248543677350473","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543677350474","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31344},"server":"https://dns.google","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501474403","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":31656},"server":"https://clients2.googleusercontent.com","supports_spdy":true},{"alternative_service":[{"advertised_versions":[],"expiration":"13248543501454993","port":443,"protocol_str":"quic"},{"advertised_versions":[],"expiration":"13248543501454994","port":443,"protocol_str":"quic"}],"isolation":[],"network_stats":{"srtt":39369},"server":"https://www.googleapis.com","supports_spdy":true},

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4bbb8959-ebd2-48b0-a085-b92d83e0b0e1.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):	5758
Entropy (8bit):	5.193705354851142
Encrypted:	false
SSDEEP:	96:n1CWtlh9of0OqcKIPbok0JCKL82k11HbOTQVuwn:n1CW19oLqcQ4K9k1p
MD5:	B76184BB55AF3D840942B78C1DC00715
SHA1:	C64E7219A67BA8D1B3EC735E762E0C03175EEFAE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\4bbb8959-ebd2-48b0-a085-b92d83e0b0e1.tmp	
SHA-256:	97C38C5DD57EEF0D6E8A4BBE74D881200994BE68C99AAEE8E9B5CB9C78DF1864
SHA-512:	F34216FE7C5CC0AC91061B17FAD3E0988BBD91712287037846A5925A7B810873E55E3388E09C1348620E0AFB0602E05578B7464F19F4531B64E6DB779F8FCAA8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13277273634977157","alternate_error_pages":{"backup":true},"announcement_notification_service_first_run_time":"13245951485614034","autocomplete":{"retention_policy_last_version":85},"autofill":{"orphan_rows_removed":true},"browser":{"default_browser_infobar_last_declined":"13245951692116406","has_seen_welcome_page":true,"navi_onboard_group":"","should_reset_check_default_browser":false,"window_placement":{"bottom":974,"left":10,"maximized":true,"right":1060,"top":10,"work_area_bottom":984,"work_area_left":0,"work_area_right":1280,"work_area_top":0}},"countryid_at_install":21843,"data_reduction":{"daily_original_length":["0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","7355378"],"daily_received_length":["0","0","0","0","0","0","0",

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\58486973-d1fa-4729-8c59-21c1e2b05d40.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):	22595
Entropy (8bit):	5.53586794460519
Encrypted:	false
SSDEEP:	384:uMQtSLlulX81kXqKf/pUZNCgVLH2HfDWrUjHGGnTdFX4C:lLly81kXqKf/pUZNCgVLH2HfCrUDGGnB
MD5:	3E33AFF56E3BD6E3B47AF5110FECBDCB
SHA1:	772A78C801E8871D10FC1C91B5744CCE21973E91
SHA-256:	F369C27522DE8BC31E079ECA1F1A8CB30D91CA827FD1C52E52CF1ACCD2744017
SHA-512:	9B081A96BC9CA5CE8E06BF0CD14657A966234BFFCF66B8B3D539F0314F7C08C2040E28F0C2180D8488E84B45CAD60DBE72001A9122F70213A641AF0EA97766
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":"13277273634547132","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":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtl3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtIpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","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):	334
Entropy (8bit):	5.2380459509336434
Encrypted:	false
SSDEEP:	6:mYTfIq2PWXp+N23iKKdK9RXXTZIFUtpXTyJZmwPXTWzkwOWXp+N23iKKdK9RXX5d:nEva5Kk7XT2FUtpXeJ/PX65f5Kk7XVJ
MD5:	78EA624B9641F8EFC8D80A09F744020D
SHA1:	132F53F5DFD33E2CBC155ADEA8BB399AACB2A49B
SHA-256:	0C7B6F70B7609587E86D2581EC92A8C793427E03342598D1CB0D40052A423E40
SHA-512:	A0E1D283535F6476C2E95546816AE1AA75770FA7D908BBE01D07131CE921DF8D29FC05BB4639D4ABBD95C9348C5E8101472CC342D88B37251754484CA9A6638
Malicious:	false
Reputation:	low
Preview:	2021/09/27-20:34:12.586 13a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/09/27-20:34:12.600 13a4 Recovering log #3.2021/09/27-20:34:12.604 13a4 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):	334
Entropy (8bit):	5.2380459509336434
Encrypted:	false
SSDEEP:	6:mYTfIq2PWXp+N23iKKdK9RXXTZIFUtpXTyJZmwPXTWzkwOWXp+N23iKKdK9RXX5d:nEva5Kk7XT2FUtpXeJ/PX65f5Kk7XVJ
MD5:	78EA624B9641F8EFC8D80A09F744020D
SHA1:	132F53F5DFD33E2CBC155ADEA8BB399AACB2A49B
SHA-256:	0C7B6F70B7609587E86D2581EC92A8C793427E03342598D1CB0D40052A423E40
SHA-512:	A0E1D283535F6476C2E95546816AE1AA75770FA7D908BBE01D07131CE921DF8D29FC05BB4639D4ABBD95C9348C5E8101472CC342D88B37251754484CA9A6638
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Preview:	2021/09/27-20:34:12.586 13a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/09/27-20:34:12.600 13a4 Recovering log #3.2021/09/27-20:34:12.604 13a4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.223192125673924
Encrypted:	false
SSDEEP:	6:mYTiROq2PWXp+N23iKKdKyDZIFUtpXTDZZmwPXTRPIzkwOWXp+N23iKKdKyJLJ:nDva5Kk02FUtpXJ/PXls5f5KkWJ
MD5:	B5CB5D0D4DE0D278CC24EFFE2C9CBA89
SHA1:	BBE02246FFF0883D8AB64EFD5328EDDA5870EBA8
SHA-256:	E1FC0D80E7F249497052137B98B1BCA2294CEC0739A7E8E1E08150325CE1DE4E
SHA-512:	A3EDAFF3F3A986665F6F2263AC12EFBB3388BF29DD425F66A45D48C2EEBFB0BE9848342B75C28F77F658F8375FF7F77272412E7DEA5DE8EF3B6951892BD0AEB7
Malicious:	false
Reputation:	low
Preview:	2021/09/27-20:34:12.473 13a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/09/27-20:34:12.476 13a4 Recovering log #3.2021/09/27-20:34:12.554 13a4 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.oldDB (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.223192125673924
Encrypted:	false
SSDEEP:	6:mYTiROq2PWXp+N23iKKdKyDZIFUtpXTDZZmwPXTRPIzkwOWXp+N23iKKdKyJLJ:nDva5Kk02FUtpXJ/PXls5f5KkWJ
MD5:	B5CB5D0D4DE0D278CC24EFFE2C9CBA89
SHA1:	BBE02246FFF0883D8AB64EFD5328EDDA5870EBA8
SHA-256:	E1FC0D80E7F249497052137B98B1BCA2294CEC0739A7E8E1E08150325CE1DE4E
SHA-512:	A3EDAFF3F3A986665F6F2263AC12EFBB3388BF29DD425F66A45D48C2EEBFB0BE9848342B75C28F77F658F8375FF7F77272412E7DEA5DE8EF3B6951892BD0AEB7
Malicious:	false
Reputation:	low
Preview:	2021/09/27-20:34:12.473 13a4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/09/27-20:34:12.476 13a4 Recovering log #3.2021/09/27-20:34:12.554 13a4 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\Code Cache\js\0056eaeb62b6a5cf_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.646290279259781
Encrypted:	false
SSDEEP:	6:msGllPYk+f2pombMOmhmJ2j/gBx4u2KK6t:E++amJmkJqAH
MD5:	5AC685DE5F7456CF7EDA182D41E2FD26
SHA1:	E6C6A22347D5410D3F2D394E532E31278954D350
SHA-256:	4D3DD3A9803184F44F6AC9B742F7FA080BFA95EE36D2410CD19B38FBB0B2E6E2
SHA-512:	9093F220D9D16934F62ADB3FB80D48396CACA474D53AFF21CBE9B054B6DCCDB38943D5C370A8B4376506869BF98DF18D89E8817723FD3058A4A7CCFA4AA320A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....g....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yp/r/CDBUf3L5Iup.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.3.-.+/.....q.....`.....lrd.O3.9._!I.(.p..Z/..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00a2bedfea6eb590_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\00a2bedfea6eb590_0	
Size (bytes):	230
Entropy (8bit):	5.503703205735758
Encrypted:	false
SSDEEP:	6:m6DXYj018IrAsLMTu/gJZtl63BLlutUndUDK6t:fj1tj/MZtl63JlG
MD5:	8BC5E96A620CE9950E2287788157F780
SHA1:	5CA757FFD41E7DF24842F41FE1AED1E47E169A9B
SHA-256:	DECF30BF2DAC130E60D05D9530F6332CB0AE006B3853BD05C453C6E9E68A2F13
SHA-512:	6BDE66A51AC623E126F30F8A9686DA70B187C6F29217CD8A30F9DDFA096B1C694C066B7ADE1FD3ADE53D763E2F9A212BDE07F1572AAAEE0B191DDF588EE50 D0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....c....._keyhttps://abs.twimg.com/responsive-web/client-web/vendors~main.f1d741a5.js .https://twitter.com/h.7..+/.....,.....:.ht"3..Q..ML...W...b.N...AI. I..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\04c7817aee41a924_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.696200072462959
Encrypted:	false
SSDEEP:	6:mKXXYk+f2pomNsmhmJ2CH+/gbakDLkMpuy4dYtbK6t:nD++amNsmkJve/2a1lyCk
MD5:	5CBD19DCCB6DBF0CE753445D21F009B4
SHA1:	7A0ABE6CDE44AFF17A1CC84EE59783B8B6A414E1
SHA-256:	522CDAB4A5ADCD4C9B1E104EE80A6DDD81C8FC8AEC4536EB9936905864C76649
SHA-512:	8F2174B0539707C7F9D6F4E1AC5880731091FAA4EAAD2A7FF0BF40F6C6A457D73C52BDBA2FC806E79C81A9813B4244B5CE35AB01DFDE23E6B6771546B22C655 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....{R...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yf/r/preQ7R4Ukbb.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.*...+/.....>B..dI..K._...1..o. .....H..A..Eo.....#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0626491c06962654_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	210
Entropy (8bit):	5.353378598739112
Encrypted:	false
SSDEEP:	3:m+lew4tlA8RzYkwLLIK7CVRCLEfD/LoeQzl//lHC+5NGe+T3Mg4msFvpK5kt:m2EYk+OzbshJ/g0l3MAuK6t
MD5:	B53ADD3A218F0C70AD1D542B8299063C
SHA1:	2299A11C6D87B164D402FB0F99A21C58332A79ED
SHA-256:	8CECC633CA7411D9DDA8DE47FE93D257AA48A71817DC3B9FB8430B705F568F5E
SHA-512:	8EC063DFB0A578C3EED1281CCABBD1B295B24A75FE3A56DD95D45C8D878487753AE2BBE925DEFFC45FAE5D39D4F47546DAE3B06D67F637DCBD81EECFDD4E 1784
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N.....r....._keyhttps://static.ads-twitter.com/uwt.js .https://canadapost-postescanada.ca/...-.+/.....&.6.,.h.U..*.....}..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\074e0538ee659be8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	5.686991484919832
Encrypted:	false
SSDEEP:	6:msTXYAWGUJ3WIJzOolRFvNjbs3kl/g8Kufl7/5sZK6t:+dLvSUtPKufwxw
MD5:	8130C533901AA1E7903E417D81CD3E69
SHA1:	078618EECDE93FAB574FF44990807361BA410B5A
SHA-256:	A9DD6EE64A3313CD0009B20E3C81E41116935733571083CA71C7514FD1E63998
SHA-512:	63C5CD9505F4F6D1F978AAF72B1D775C8EFF3B9A95BC254929E02F9114E306FD579603ED8328B130E0C5DF672BF5D92D41ABF20E48A3743DFED615BBC0FE8FE 5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\074e0538ee659be8_0	
Preview:	0\r..m.....v....g....._keyhttps://connect.facebook.net/signals/config/614267586032718?v=2.9.46&r=stable .https://canadapost-postescanada.ca/8..-.+/....._. ...$z.0.Z.8...X..~....\.|..LZ..A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\086505a62f36d523_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.514258401609371
Encrypted:	false
SSDEEP:	6:muYQkbsHAf5KA+IuzXDGCOobs9+/ghAhBBvI0z4anK6t:ngxKA3uzXD4o7BJ5N
MD5:	4DD2EBFC7917F95B6C4D7D8910EB1625
SHA1:	4C0FF60CD0738BABE1501955451467B2260ED5F6
SHA-256:	8DE252AC3D30E1891E60A82077B0A2E1CC8EC483F7F6FBF329E8C7BEFE36D54C
SHA-512:	73FDDDFF2CEA8147C2D6A83C97E2888E805797E8CF8F4B20EE08A642165E8CF63DFF1D9C9BE7FED0A98979614208943011A5019BE80098432A4F2F59CBB54D3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}/....._keyhttps://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/en/main-es2015.js?v=2109.01-SNF-National.2650 .https://canadapost- postescanada.ca/..-.+/.....S../.}..#...7.G."`%o.....Q.cbG.A..Eo.....+R.#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\0bf980cdeb7ad5c3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.601159999143935
Encrypted:	false
SSDEEP:	6:m4nYk+f2pombEyhmJ2EWO+/gf54yjfJ21fn/PbK6t:N++amlkJO/Sf4hN
MD5:	E77893EFDF29EC26D24E83E90A1F8F96
SHA1:	0F5872668E458E70C434592C60EB440F77A75684
SHA-256:	BFD1BFA3ED0942D8CC49A868F6D76D86AE8C2D1212791748D456EF2579BEE5DE
SHA-512:	E079843F40A569410FA057B272FC1E25A1EA17565407CD6837CB26EF9A4120218F98AC68D844040E97478DFFD615C2286CABC50633EABAF8437093FC99726804
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...Hl.\...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/y0/r/fvmSzDrhmwU.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.>...+/.....}.....L+.x.:~..$W~.Phvc...._/ .S.7..u.A..Eo.....o.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\10b5101f0e5bedce_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.5170580458243155
Encrypted:	false
SSDEEP:	6:mQQ3Yj018IrAWQqMqhv/gEuapRnVlhK6t:ny1tBQahv/nuapt
MD5:	C3DB1264D010F53597F75F6D19C2524C
SHA1:	C6EB78FA2459FF0EE02FDE3E0E39F8529812C345
SHA-256:	01F80214910434AB3A7361881214B24C1C7A62B71DD7197BEAF42EC03E4C629F
SHA-512:	55C461A2D0E74D61A26DF2901DB36C959A8259A18FC9CF0D38198D975B1D1C4DB7B84CECC9087C0BA3FF5B78CAEB18FF7CF678FFC3294E09E1D74B2EC7100 DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d.....r...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SideNav.68c3eaa5.js .https://twitter.com/.'J..+/.....1].-W.s$.J.S.0.Ytbo...,...'. .7.A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1394793b1f589eeb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.533442793494761
Encrypted:	false
SSDEEP:	6:m+YGLDlynflGB7W80wlyxKLQ+/g8fLFrdayP44ZK6t:sflGtW80wgxQl/HLFrday3T

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1394793b1f589eeb_0	
MD5:	23F371A767004ACE5B94D824879F14D4
SHA1:	2C6702CCE6E871B021329760CB97ED0B82142B12
SHA-256:	504DC8A6383E2383F4B582B0E28F4FB01D07FE2AE037D0E0E9583B0B51AB488E
SHA-512:	AB01F44A044A72325647018D2B7ECCDA7A0F62DCFD29DDD7832CCA89C8C7D38D5D882BB1A179EE0089429C72C4C99080285ED3C1BC5F62A03F669A162F484E6
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b...P.5...._keyhttps://www.instagram.com/static/bundles/es6/Vendor.js/48e0f28aa478.js .https://instagram.com/SBo..+/.....2U....F....[*P....qs...9.*.Wy.. .A..Eo.....V.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\13bd2d851129203f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.535064651644968
Encrypted:	false
SSDEEP:	6:mFO9YkvwytVQMEnNN/o/gqllr5SkilK6t:qOlvwytmNNQ/N/r5O
MD5:	6AF9D7B8341C1C1FC940D6622934649A
SHA1:	822E37DB64CC322861DCBD8F40F0243296DBF56E
SHA-256:	34D64830D51B66EDB5E65B316E0152A09ECFA462800C928EF993C634766B81AA
SHA-512:	54F8C2F323FEFA999832C061F61FAB141F686407B1326EFCDB3AAC9F37295A8FFC7B759AC103D363C47884241AE66A641C38BF727DA4C5E09AD589CB661C905
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W.....9....._keyhttps://static-exp1.licdn.com/sc/h/ckvx8rxuibokruuyiz5ft17o7 .https://linkedin.com/.....+/.....&.....k...N..BS....._@.6H8C.(...A..Eo.....D.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\15f2ef6a39fe047e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	397
Entropy (8bit):	6.0769228274446
Encrypted:	false
SSDEEP:	6:mRnYWVBCYpeQ6vrUxgYrv5JCbRz9pqhlbK6tR0hqzzbHkUiv5JCbRz9r:ozVBCYMQeUxNJ8LqhlNXgIzbEU6J8N
MD5:	F0535A2A9CC0A9E8FE6019B09EE463F6
SHA1:	DDA0F09F2BFBB5EDBD7DDE75D64C836F5E3D3233
SHA-256:	0D72EBF28CB522E124F4293AC0415B52264D1DEF0CE432176270575A8E890132
SHA-512:	6580E0E82EDA22EF18FC41470BBD3AE2DCE20FB339F9A11A5C461DBA301436D554E8F75559A9BE0C855CA57A6C720B6CB5422C86355AF4549B26D033B2885DE
Malicious:	false
Reputation:	low
Preview:	0\r..m.....8....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/CoreModule.js?Q_CLIENTVERSION=1.50.0&Q_CLIENTTYPE=web .https://joyeriasosa.com.py/r.H+.+/.....+D.....^}.....R`....".Dq.....V....M.A..Eo.....B.O.....A..Eo.....r.H+.+/..2..A1B05E1055623783FEBC922E4E3491695B41DF0E8E2A9A28C0C35F4AF712B9CA^}.....R`....".Dq.....V....M.A..Eo.....t'L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\170bbeec2ba01fa4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	311
Entropy (8bit):	5.9765132852844545
Encrypted:	false
SSDEEP:	6:mM7AnYWVBiO8Q3oOS/6mpeQl6lnwrUY5fgHwVEkoneRK6t:h7OVBCjOS/6mMQYlneUUfDV/
MD5:	CC437C5CB7669B01092A52A409BD6B62
SHA1:	C4929D790EC1ED0B88C6DD75F956E2CAC5143B2D
SHA-256:	24514ACCA4558CEB94D95E7DC5D3B10CD297882176690DE18A3E5BA3D98CBAD1
SHA-512:	6896885190E6222B23F607DDEA72FA0CE947008C765DD08AA7EB7D577FFC8F1382A211503DB6AAB927D4DF0DE158D46CA755E7773535A7230CCF299CDE26C07
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/1.a4037f4820369ddf14c3.chunk.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_BRANDID=canadapostdigital .https://joyeriasosa.com.py/.1k+.+/.....L.....{+g(.EY"..^..J...9?&h<..?d...A..Eo....._.3|.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\176e7d1d913270bc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.413478621901344
Encrypted:	false
SSDEEP:	6:mwh0lXYGL+MIwJJwMTiH/gqSJilxhm4JA7/bK6t:dGIwv2/lUD7zN
MD5:	DAF0413D30BD5F401D316B66227C1038
SHA1:	957C5901202D766243AF5B294FB4BAF94EA412E8
SHA-256:	27E4C9871A0A046F1E52474E625E46F21F09E0DF6DDC077D9E3366DC41165A5C
SHA-512:	DE9BBD7EFE5DDAC36A355737500054DEF29EC631F48E80C07C4234B61337AC9F067DB1978D47A0B424A8E2AD460E9270C5911B37DF27A60B106F8451D0AF4DA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....G.....I....._keyhttps://www.google-analytics.com/analytics.js .https://twitter.com/M.a..+/.....:.&..L...jC...1UR@u<$mz.B...u..A..Eo.....L.0.....A..Eo..... .....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1892d03ad82cfaf5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.805081023288703
Encrypted:	false
SSDEEP:	6:mBEYk+f2pomWBsz5oKq8hmJ22/gXrSLJdK6t:KU++amlzeKpkJP/LN
MD5:	F0AE900CC13F071154202E19DE6199D3
SHA1:	477BF8DB32BB26A07D687A443113DC27516B7A6E
SHA-256:	5A3DA753E4B0DDD7B243224F843A52DD337264AE5EF0A65889DBA5B0F89D072F
SHA-512:	474C5884B079ED96E5931569A7E0F6BB84D478F06991568EC28177F04849D75D07FC13DC807E1CC82B4B10FE69F13FF77F1B89901F273F8B0FAFF614AE7B3C19
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....x...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3ij9m4/yg/l/en_GB/L1d008k8MHH.js?_nc_x=lj3Wp8lg5Kz .https://facebook.com/.*.-.+/.....n..8#O.\6.^.Z ...,..Z 1.....R..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1a0faf414bb6566c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	274
Entropy (8bit):	5.664037897692514
Encrypted:	false
SSDEEP:	6:moG+EYj018IrAMUoALzJTJcpuH7iiiMP+/gFGbXoC4iK6t:O+w1thUFNS8H1+/TbXh
MD5:	B3F8AF5864980101DABE9020256BFA78
SHA1:	298B435EBEA660324413FB394E0C74352A56ADE3
SHA-256:	044FBFB0CBAF83461E82335BE0910E75AA27AD1F0451BB8001B82DFE5CA14DAA
SHA-512:	87F5D301840BC4CA9B4518EEEE262BD28A183BFB7E4659338B2E177EEC312C9264867FBA3D0525C3C65DE4A8915FF45B243019F18031D42E8D9DF70A74F9C67
Malicious:	false
Reputation:	low
Preview:	0\r..m.....).....keyhttps://abs.twimg.com/responsive-web/client-web/shared~ondemand.InlinePlayer~loader.AudioOnlyVideoPlayer.3304a215.js .https://twitter.com/..V. .+/.....O.....8N...G~.....'C.6.]2{}.`.A..Eo.....A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c9ecaf5609273a8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.698992595006271
Encrypted:	false
SSDEEP:	6:m2nYk+f2pomW8aKSW6g6whmJ2xK9/gpjFZSJZEm4TllZK6t:LD++amAKS1g6wkJw+/iFZHmY
MD5:	9A576962212A281BF9BBBED09A08C86A
SHA1:	597A4D862003BFF1A73DDE87592A696681C9B748
SHA-256:	81E81D4A1F507FD87C1EFE987F9CD2AC80777D449CB8FDB8CF50C5BA83011BB4
SHA-512:	DE67A88C6C9722CB2530BC8D7AE79CD235ABE6F788E882D7273A3348FF2B9C7B36604C7FB3BCD0342C63BC9A1DDF7F26EA2ADE6445C7708964605B459ACF61 D

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1c9ecaf5609273a8_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.....x...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3igbH4/y6/l/en_GB/wey-VXyEpgl.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.w...+/.....C....J.mr.+.]...X.=....ddr..A..Eo.....*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\1f79a6fcefd964c9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.685500012431434
Encrypted:	false
SSDEEP:	6:mA/6EYk+f2pomUxw674zhmJ22a+/gfjUMhhK6t:N/6U++amopmkJbpaP7
MD5:	BF3C6768E5A934459E1E497951951D43
SHA1:	97746024B3E70DE3B7951A35DA4170329317ED36
SHA-256:	D206168BB848C7859C3519B22AB85D358D7E64FD31CC003C5D1FFF647A9053D8
SHA-512:	EC159025F5A1A039477288EFE928F4A42E413D3C8C774C57D41D6814499B4231FF7DF8938ECDA9646EDD29DBDDE40FCEB9D345F68EC8A80404455E1A13E7E3AF
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h...b....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yF/r/dATna7NWzvc.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/c..-.+/.....9.b.r.....91 ...0!%).3FW.|..A..Eo.....(.Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\210a28b6f66b04c6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	311
Entropy (8bit):	5.959530540488121
Encrypted:	false
SSDEEP:	6:mM7dYWVBPj++R/6mpeQl6lnwrUkn8gHMUFF4eUJhK6t:h7NVBPJR/6mMQYlneUc8+a7
MD5:	810ADD4A90330A3C982F599AFD6D39D1
SHA1:	4433C6470FC8E9DADD149A2340477466A4CB10C2
SHA-256:	236BE8C833AD9309EC627F48BA36A1AFF0BFFC4D3C23A6AC04AC7D0F2B7105FB
SHA-512:	1FADC3E39A2BEF1DE7FAB64B8AE5412484E8343B832BB78B12676788EA0EC0AEECC8EDFB364F594CEDAC22285FA34669F9E183DAE847A8097B08001BBC254E50
Malicious:	false
Reputation:	low
Preview:	0\r..m.....7...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/2.4c79ed6728cc3054bba2.chunk.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_BRANDID=canadapostdigital .https://joyeriasosa.com.py/.!k+.+/.....L....._...YH.W.a.1.9.....I..&..-.....A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2222223c94efd7ab_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.500238625909515
Encrypted:	false
SSDEEP:	6:misVYj018lrAE7uP2uVpMzv/g+y0oS7var8K6t:u1tnuPO/taC
MD5:	726FEA5531F705393D15B1183D2B15B9
SHA1:	401983926B43321A6CABAB6A7645EDEADDC62A1C
SHA-256:	97AE27433C687D0F9EB98F951A0B20592452007A4582E33A23C2DC7EB83B4601
SHA-512:	3E21ADEC8A83CE867FA41751565EC95217A1B16DED30A69D37AF9661C239AE0DB73F027E8EB628331BF1101EEC99EE7A534AD0F1FBB901072B18C3DBB0A154B7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j...b..!...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.AbsolutePower.330a4a05.js .https://twitter.com/..t..+/.....*4.1...:.j..[..N..yq$....*....A..Eo.....*T^.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22bab256d48f9c47_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	241

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\22bab256d48f9c47_0	
Entropy (8bit):	5.546452768144993
Encrypted:	false
SSDEEP:	6:mJergYj018IrAqmYG/QaM39l/g4D/NpK4sbK6t:+erk1ticH/DrA
MD5:	D33542302F23274AF329350E34FCDB6B
SHA1:	688B01C2E3380A587660583B8061482635D29637
SHA-256:	CB823C314CED846CDBCA726F773B2728DF25DEA928D026640D83634B8F9B0527
SHA-512:	88301A073D12FFECBFF16E3E2EFF813C771D0F8B4EDCCD82E034886124F97D4CE1A49C69128FE84538655C6111F51751424714CCF894E04B31B90BBC49426A94
Malicious:	false
Reputation:	low
Preview:	0\r..m.....m...S{....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.TimelineRenderer.3bfe2a35.js .https://twitter.com/.d]..+/.....A.....Y.>..q+.m...,.. NBk.$.V..I.\..A..Eo.....P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2338dd1b5334c723_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.534233505255744
Encrypted:	false
SSDEEP:	6:ms/yEYkvwyPZkTfNpJQKl/gwFhKgAkK6t:JyUvwyhQNptl/hFhTV
MD5:	36F179BD8F10FB79A6C8926B1B65A3B5
SHA1:	3B8EA63DC3593FE5351870F54D316C6D44D136BB
SHA-256:	2EA3A397441AD01C8BE533660F2BA9BFE0DB91BAA45C101F788D4D4ECCB9B2C9
SHA-512:	0723AF663B9AEC43D0BA6C1EAE7D84BECE16928814EA51724B9FB9B3628ED313F33F1F6463FCC762D371DB3F38571D19B79032C6AFA549FE98B950203EAF81A A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....V....,.<...._keyhttps://static-exp1.licdn.com/sc/h/jehaalv6vyu4p2w9378icw2c .https://linkedin.com/.....+/.....&.....)&...1....,Q.t..._LC./.Lb.e.A..Eo.....hk..... .A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\26e75e566fc7581b_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.305467028388883
Encrypted:	false
SSDEEP:	6:mY9EYGLyhUGEBcw/t2RTrUUgTJDhX24+GozK4w/bK6t:F9FhUGK4fUUSLXP+Gow/N
MD5:	D4374A8F1BA296243A7C91FFF1E9F2E4
SHA1:	45BFA5CC8778418444D9561FD779864B43A6FC03
SHA-256:	5DE243D1AD2F531CAEF0437C19F47E534A5FD97373B7A114146EC21D6E82D8FF
SHA-512:	2CF214BE8633E6F4696976BA529951DB002C49F368161DDB93050CEBDEEE5E56761A16C04C290ECC8973EDD251CDC26451C6ED4011B1160436C35CBC897A28
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....y....._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/saved_resource .https://joyeriasosa.com.py/Ak*+.+/.....B.....C.c.....|...`....A..v}.C.....A..E o.....bc.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27c6de2b1e7c2ac6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1487
Entropy (8bit):	5.619398413716885
Encrypted:	false
SSDEEP:	24:sDSvrp0B2uydyyeSKZHzNqtAjlZcSbVNGyb+gNqtAjlZcSbVNGybEOBam:scrpBu8fKZHzNoAZcSbVNGybXNoAZcSp
MD5:	E4833C402AFF73E1D68D997E1A280874
SHA1:	5DD64B9B4E1562825743036B7C4935B5A0CE3F6F
SHA-256:	70FF75BF5752820551A9DB7C7B48F9A64D6463C6116B5122B7997B9CEA6FC571
SHA-512:	44D375920818BFD66547CDFA3C3364BF332B8ACF193B50DE2879DFFFD87959D6927CC2480DCF534CA5205BA7D668F33E76EB56FAFAE20667BA8F401800D6921
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\27c6de2b1e7c2ac6_0	
Preview:	0\r..m.....K....._keyhttps://www.googleadservices.com/pagead/conversion/674834224/?random=1632800088166&cv=9&fst=1632800088166&num=1&npa=1&label=S1hGCOWN-eEBELDO5MEC&guid=ON&resp=GooglemKTybQhCsO&eid=375603260&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&sendb=1&ig=1&frm=2&url=https%3A%2F%2F9852050.fls.doubleclick.net%2Fddm%2Ffls%2Fr%2Fdc_pre%3DCMG27M_ln_MCFVYY0wod1sYDVA%3Bsrc%3D9852050%3Btype%3Doptim0%3Bcat%3Dperso0%3Bord%3D4161029190815%3Bgtm%3D2od9m0%3Bauiddc%3D1301920779.1632800086%3Bu1%3D%255BProduct%255D%3Bu2%3D%255BPage%2520Name%255D%3Bu3%3D%255BURL%255D%3Bu4%3D%255BReferral%255D%3Bu5%3D%255BLanguage%255D%3Bu6%3D%255BJourney%2520Step%255D%3B~oref%3Dhttps%253A%252F%252Fsso-osu.canadapost-postescanada.ca%252Fpfe-pap%252Fen%252Fregistration%252Fpersonal&ref=https%3A%2F%2Fadservice.google.com%2Fddm%2Ffls%2Fi%2Fdc_pre%3DCMG27M_ln_MCFVYY0wod1sYDVA%3Bsrc%3D9852050%3Btype%3Doptim0%3Bcat%3Dperso0%3Bord%3D4161029190815%3Bgtm%3D2od9

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d30113ef3dbc95e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.421357475089889
Encrypted:	false
SSDEEP:	6:mEJnYGLAAmrDXdLTArRCVzbsS/gZE/A1E55N4YK6t:utnArRCKicry5vp
MD5:	4B566AB41561FD4EC409954D434A9453
SHA1:	CBFC5EA8F7D434E2F48A4702288FB79490B57AB1
SHA-256:	38931E30F39282A6BD031963664AE864470EE20817DB3BAA5A8208F5D1F65C1F
SHA-512:	42E92C84F845E392017ACE1D0E7111E9D22C998272049359AE2C3549649CDEAA99D72E5E15A0AD648C7DEA223782FF458D33BA0C79C39EE3D0A66724BD6ECB7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....L,...._keyhttps://www.googleadservices.com/pagead/conversion_async.js .https://canadapost-postescanada.ca/...-.+/.....<.....(.j..+.Ay.r..Ah.@.P.~B.....VI.A..Eo.....'.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2d43af485268a710_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	265
Entropy (8bit):	5.589090931642739
Encrypted:	false
SSDEEP:	6:mBKllPYj018IrAMUscKjzBDwL0pMtn/1l/gi0YSbbCOTonDaK6t:2K/n1thUsNq1n/1l/OYSbbdv
MD5:	A4A2EFD019B2A756A1BE9F214E624DF3
SHA1:	3BE7E073BA928F2D58B5255921507234B28E6672
SHA-256:	129B3040965EEC6433508B97A28267B09D78533D7E8E35D2D2BA7324B16B41F5
SHA-512:	A3BB56838942B5C51F611D9E2DF8886DA6C643E74D474C2F261200ECA44897AA50645343BE283284FC252E3F65183547CB64825CB82E9912337D17DC0A9DB2D9
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s.R....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.LoggedOutHome~loader.SignupModule.ab4d2225.js .https://twitter.com/.rX..+/.....^w.y.....n.8....<nk.d.l....A..Eo.....mMK.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\2ed40e783d52bcb3_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.553547027944636
Encrypted:	false
SSDEEP:	6:mLTYj018IrAzHDLMG+/gvfXWnOGy81/59K6t:8T1tye/ITGy8/
MD5:	82E443FDFEDCEB9D67584041C9041B0F
SHA1:	5BAA536BB7095A05FF7CB19503C516EB7BAB4851
SHA-256:	6769E8AD9F12E5B72DAD0DCEC7ABE582F6733C1F1DD03EF7DBE3F0EC167613C0
SHA-512:	D4949161597A33684935374C113ED3A0558F9788D10CE9F95402076CE2C8E930E38ED8C83D0FDD1948C3AD2F1FC957C353A709906ADDAC817940783E17497D70
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g....}.&...._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.Dropdown.8c936585.js .https://twitter.com/.yA..+/.....lp<....S... ..[...G..'~.s.Q.A..Eo.....j>.T.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3129c282316f97ad_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3129c282316f97ad_0	
Size (bytes):	236
Entropy (8bit):	5.687645785761304
Encrypted:	false
SSDEEP:	6:meIYk+f2pomGcUzhmJ2Wc/gLW/5w4IK6t:rg++amGcUzkJ3c/9O
MD5:	A67112886BDA093D5E3CBABD53C56A2F
SHA1:	73F19E0F2C3E7304C8B35B686FB04325460D9547
SHA-256:	CD317E93154ECB76DF53698A1FDBAD77352EC59E8DC21C94F7D6B7FCAA33BDD8
SHA-512:	DC4AED9FACCE66A59A9AABFE40B5685153C8323CFB85E7C6A821ADB07730D5EADDD26E432B36DF9DDEE84E87304804155253FAC645EDA0402A1EBED01EEF5C2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....V....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yI/r/LvpJogDKEV-.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/~....+/.....g.....j....,.Tp...w8....b-.l.....R.A..Eo.....m.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\31d3a1eada029de9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.619902891959245
Encrypted:	false
SSDEEP:	6:mcYj018IrASXVnpMX09/gYG6eyrq/lhK6t:R1tFXVnD/H+l7
MD5:	162B7ADF3FA3E52D64665213AFC256AF
SHA1:	896FB065A8CC39A1DE47B133DD793B54FAEC2E91
SHA-256:	76E100F52ED7BFB4385E3E39F8554CB4B1D85FF6AAC810499772C1FDD48A2DF3
SHA-512:	F76394B674C7426DD529EF84FA29D8895B9C3F2296A6EAC27EC245999370B2A8896FE758D38283D31F27C5D9BAD2306019A21AC1896EB824FFE9BFC0BA0B3DD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g... #&....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.WideLayout.d9501b75.js .https://twitter.com/..U..+/.....$9O.*J....Zb....._.....s?..D...A..Eo.....S.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\35990ef7e5e910a1_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	298
Entropy (8bit):	5.621896790512354
Encrypted:	false
SSDEEP:	6:mcSnYcv0KgQnUPC2RoMTH/EkGzzbss+/gNHNwr/K44RK6t:e+SAC2rTfjGgxoNwrA
MD5:	CF85272952969DD9016CF5A7003A0D3B
SHA1:	45075675147B7F03776B84E7326AC4D332E6D75E
SHA-256:	5DEFE2D31EEE848E3F7A4AE9B616FB9047B2FAC9FAB6432A5D8BEB3386E75062
SHA-512:	53B444C2D63809AC2DBF0E907264EB946395DE037CE22AA3C0E59100D7260CB2B400B68CC45161628DA9A19375EEAEF6DEC2262BDF7D00CEB8B04E921F35928
Malicious:	false
Reputation:	low
Preview:	0\r..m.....].fR...._keyhttps://assets.adobedtm.com/8555ef77443acd85ab4eb6b187cf7ed7fe0f79eb/satelliteLib-f2fc6f00da802a0747b6ffed3c12e3931bfca496.js .https://canadapost-postescanada.ca/l=~-.+/.....K.*yA=>5...;_S.4S...%#....A..Eo.....L.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36dc6572deff4c1a_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	261
Entropy (8bit):	5.382208213585679
Encrypted:	false
SSDEEP:	6:mhYQkbsHAf5KA+bXDObs/UH/gWAfcYrUnQb7/bK6t:0gxKAmXDVW77s+yN
MD5:	0667922BEF8130A93BAD42AA4730F002
SHA1:	68C0D2B7EE2382CD826C372F4E9E9E97FA2D8AD1
SHA-256:	34193826AA94B201CDDC2A057C23637C12E1BDD5F670C3F0A661F1CCA6554A38
SHA-512:	7AC2A36EAC4FD04A1CEC64FD7B599B728FF4ABE37E6561AC3191048A1DB1ADA6DD378A936C6201F783650A209D795411F1D0BF9FD6D213645473A962D653FF4E
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\36dc6572deff4c1a_0	
Preview:	0\r..m.....1n....._keyhttps://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/en/3-es2015.js .https://canadapost-postescanada.ca/.i.-.+/.....3..... ..T..*bZ..q<GJ../..#.RZ.}k....T..A..Eo.....hJ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\373ec851e2daab46_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	5.64816961414887
Encrypted:	false
SSDEEP:	6:m8/Yj018IrAMUF/1nQZSQMq/g1Ilpwk40K6t:r31thUpNQZ/wl/vd
MD5:	8BE81757CC7C59BDC2A4717F8938D084
SHA1:	7FCA0F0453D16841ABB87D6AE2038E06E71CE2CE
SHA-256:	36CBABADF338197755AAA05A492EEF3177427BBF2BF31DA953BDAD6D72CCD468
SHA-512:	3F764EF990781F70153DC2E5C3BB57FE166A849E62F5D25DC06754124C448B4FC106A6AB5DDF709BB5EBEDC075F5B9ADAE6E8D952DA53FE33C61039D4CDB7 47
Malicious:	false
Reputation:	low
Preview:	0\r..m.....|....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.Typeahead~bundle.Explore.86745795.js .https://twitter.com/D.W..+/..... .....A.....,...IM.v1.'.....p.&.\..A..Eo.....`#w.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3bad6b7489b7059c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	230
Entropy (8bit):	5.423675501576773
Encrypted:	false
SSDEEP:	6:moygEYGLyhUGEBcw/tYrUuEgIrXojE1nj7K6t:k4hUGKkUuE5r46
MD5:	5FCB0BF79790780EC03BE503D0EF697A
SHA1:	7E793A97CF4DE35E12A420C8FCFDEA7879C5E374
SHA-256:	1F7390F872488E6998BBAE7C169C03340D0B399DFB32932AD731ADD76DCE93B6
SHA-512:	5E88BBF871F30B870AF6E0DA4A335E1012A25B77BB5F8FC5818046DD2F950EEE6936DE983CD023557AEDB29BBF8B6BE1227DA1F68E9C977834227ECEA342BB D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....b....N.0...._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/saved_resource(1) .https://joyeriasosa.com.py/...+.+/.....B.....6.....Q.'0.Z?.Sx..e.. .K.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cd3b24e2c91df60_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	244
Entropy (8bit):	5.5047371294462195
Encrypted:	false
SSDEEP:	6:mq4YGLSmXZC5HpCGNFV3jbshml/gb/mUaQ9koygrB//hK6t:cmHpDUhkAmJQLV/T
MD5:	197984874A6F3CAEFF4C352869A4A58F
SHA1:	D2450BEAAB942A356504F0422FF2024C9AF76F83
SHA-256:	60B938DD788506AF72913C8D77B75528527944A9720A33338ECAF092EC3E6396
SHA-512:	455E6BF5E0B6E2077460578CF64572EB0C88B03B220CA35B4498D1E4E60133A12A4F3AF8937D76BB48877B958038C5E168F36346AC3C2337FE21F14ECFC908B8
Malicious:	false
Reputation:	low
Preview:	0\r..m.....p....._keyhttps://www.googletagmanager.com/gtag/js?id=DC-6048943&l=dataLayer&cx=c .https://canadapost-postescanada.ca/.e.-.+/.....d...q a.B}.m"\)w.\r7.w.h.!9..a\.A..Eo.....RZ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3d4d0a8128dcc664_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	982
Entropy (8bit):	5.629559789049888
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3d4d0a8128dcc664_0	
SSDEEP:	24:4fl8hhgXXaOpJNRQROhfl8hZ395ulrNjTD:4ugHaOpJNRjunzmNjTD
MD5:	DB499E7189C3156F181B64EB2840A3C8
SHA1:	8B8B43FD046859B74118477C38046D1CBC7E18AD
SHA-256:	CC94E6C36C7301B88F18B1EA35E0BE691107A187065B47682AA3A3169B2B78D4
SHA-512:	D1ECC47BEC542A5D79DA397005D28FC6FC2809B558C16335642DA865DB24F25565A0AE04C130B51EE2C7EDF749FEE41CBEAB0FC1A3A574AA69B6ABF0C3F3610
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n.....=....._keyhttps://www.instagram.com/static/bundles/es6/LoginAndSignupPage.js/f2ebf06961bd.js .https://instagram.com/..q..+/.....o.....;...*A.....Y..L...]...A..Eo.....f.....A..Eo.....q..+/.....'.y.....O....`....w.9.....(S.`..`z.....L`.....Qb^.....__d..(S.....Ia.....,..i .....3....@.....@.....@...!..@.....IE.@.-....`P.q.....R...https://www.instagram.com/static/bundles/es6/LoginAndSignupPage.js/f2ebf06961bd.js..a.....D`....D`,...D`.....4...`....&...&.....D&.(S.....Iaf...k...IE..a.d.....`....DI]d.....@.....`....`Mv,.....x.....^.....z...,...N.....2.....:.....D...L...f...N...l.....K`....Dr(.....&.....&.....&.z..%&.[.....&.....&.....&.|.&.[....&....$Rc....`.....Ib.....".....c.....L.&.....d.....o.....;...*A.....Y..L...]...A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\40ccb7befe7a80ec_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.588278906595639
Encrypted:	false
SSDEEP:	6:mY7VYGLSmXZClWQvvD5bstnK9/ghtAQfdTvK6t:F71CX3DOtKFG//
MD5:	8A0DE934463DB8265D28E56167E38008
SHA1:	3FA19F30C9586678ADA07DA59DAB4EE9B3034E33
SHA-256:	B17E1C045952F134542F9B359070C3F8784C4F7D45D921CFC9B95F16B372CB0B
SHA-512:	9D233C67DDF179EAB7DE44E3082242800D3B01A8438803428EFFDD5D26F74257EBD2516C628C19BF4F5BFC51C7FBF58048AF7C4BEC8FA305E88D6C59ED321B5
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....#$`...._keyhttps://www.googletagmanager.com/gtag/js?id=DC-9852050 .https://canadapost-postescanada.ca/...-.+/.....O.....Q..;....w.}..=.....R.u.l..A..Eo.....)=v*.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\425a519eff40b1b4_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.3024318982631335
Encrypted:	false
SSDEEP:	6:mU0PYGLyhUGEBcwQWcr7xrUFfFg5dGjjRA7lDK6t:p0qhUG1WcpUbYsvRcl1
MD5:	467393D77E3E5D3D728D68EE02A18FBB
SHA1:	46403C5A039F83E7A2BEFE496D338779FCD24A3A
SHA-256:	97520EAA1FCA8187798BF7212DA6D97EB008F98049AD0EC8A56B68C6B4721B9E
SHA-512:	362485AF1CC276EA7D19EEB4A6E4BD8E88486426AEC7A6B33A4B633C4983182A12CA4B93696C27E067BF6BF05E9BE96776A2EEDD4A2D68FB16BEC572C00C62AB
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...2./....._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/foundation.min.js.download .https://joyeriasosa.com.py/WL.+.+/.....>.....:..r+.4..q.x...ae3.x/l.r>.P.A..Eo.....q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\46f0a54eecc456cd_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.788139073984499
Encrypted:	false
SSDEEP:	6:msl/VYk+f2pomYPqikxzhmJ2GBsNOKl/gkWrbifb4LaDK6t:7N++amYPqik5kJ5BCH/qrbiTL1
MD5:	B528E94B97C731998906ECEAD267C310
SHA1:	92EAB0687340C8C35A9494C7BF48B972430A675C
SHA-256:	8204CB1A38D0CD6AA1693752101BEC0697A0F54FB8AEF8687FA3AFCC905DAC6E
SHA-512:	C346C80BB1BD589C961FD0CC8314166407C084B7BAAF888092119C7E3FB0D47EF910729F817B531237006F0985314585C243602CA8BAFD4A0D62475A5EE739D2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\46f0a54eecc456cd_0	
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/ye/r/3mc4XDZ6Guq.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/E....+/.....P..C.1.Y.....>..W.%.:<.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\475c9c602d32efb6_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.961061811676898
Encrypted:	false
SSDEEP:	6:mcsYj5TfsaCwVk6xSzSuVWqSlNR1z9eYDRh+QHJXXrUM5fgNmUOAOMryK6t:xTkaCwVkASmNR1JL+QprU4fImXr
MD5:	90379F57B5BB877D321A0544CE264030
SHA1:	6A39A876F5353FC3B54D26B908974976998435D4
SHA-256:	96625D7D05736F2DB83891DC144A02DA5F8D2FBEBA3CE0CBABB9AA5289887426
SHA-512:	13814AD4CC6495A710BB7256FCC9A76814BB0206A08699266C214FEE57D2D7258FCF336DDB06EFB7B5F6C1982CF67065DFECFF1DE00E848F8F11219EF4D4D17
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}P....._keyhttps://zn0xleir6swszany9-canadapostdigital.siteintercept.qualtrics.com/WRSiteInterceptEngine/?Q_ZID=ZN_0xleIR6sWSZaNY9&Q_LOC=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219&t=1632800047710 .https://joyeriasosa.com.py/.O\+.+/.....(I.....(.Z.....M....@.U... ....P..A..Eo.....IJ.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\47693341c3792ab8_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12887
Entropy (8bit):	5.776412898725324
Encrypted:	false
SSDEEP:	192:Oh/e/7xdjZCn+SjlpAvf+d0+KLqLwneXjFKTA34Qvb6LVvzja0y/5j3Qe+aJWm:Oh/ejBKBpAeJ0qea0yhrseWm
MD5:	BE9335B14C4A17A7AB4722E730FC28D8
SHA1:	55AE32022B1ACC5268DE7C7759A4C279DADD08CE
SHA-256:	10F57E46EC78F186776E77F04404115FEDABD16F970EFCF1C5FD6EAC4CFC80C6
SHA-512:	F06150515648C9DCDFECD69CB16793D034121EB1F781333043A2D053F53C26F07A0B7A4E8AE3358BA299433FBCDAA77E8B0D32FB3A1DAF6E2014F312FF1C597
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/1.9bf84a1119dc09839d2c.chunk.js?Q_CLIENTVERSION=1.50.0&Q_CLIENTTYPE=web .https://joyeriasosa.com.py/..K+.+/.....D.....X.A^5;....d=uW....YkW...*D.....A..Eo...../`.....A..Eo.....'.5g....O....0..8.O.....4.....(S....`.....<L`.....Q.@j.<.....window...4Q....k%...WAFQualtricsWebpackJsonP-cloud-1.50.0.....Qb. .8....push.....`.....L`.....`.....Ma.....`.....0..b.....8...C`B...C`X...C`\...C`.....(S.\.`r....$L`.....HRc .....S...Qb:.....n.....Qb.....r.....Qb.^/.....o...c$.....Qbp.....28..`.....Pc.....push.28.a.....(S.....Ia.....d.....@.(.....d.....@.....@.-.....P.....v...https://siteintercept.qualtrics.com/dxjsmodule/1.9bf84a1119dc09839d2c.chunk.js?Q_CLIENTVERSION=1.50.0&Q_CLIENTTYPE=web..a.....D`....D`>...D`.....`....&...&..a.&.(S.....Ia.....I.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4a5ca371fad2af12_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	225
Entropy (8bit):	5.496496971277251
Encrypted:	false
SSDEEP:	6:mGYj018IrAkRPoIpM7U5O+/gW1ySqh/hK6t:f1t3Ry+/lyS4/7
MD5:	24D9E49CBC19C7885594FBE25753CD1E
SHA1:	6507CABE6678C480867005A64EDAA030FE84C2DF
SHA-256:	BF45ADD6DACBABF8A5BB79A144275106FF823DCEB96217ADC76E022CBD108A74
SHA-512:	B7D1DDD0C7265F80739E986F5959CCFD967DFF50C8BE9A4FCC58441677F90AF414F1F8A535085586BB9C7799432D491EEA955E81AFEC1825DAA9E2C1B3F51F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....]....Y....._keyhttps://abs.twimg.com/responsive-web/client-web/i18n/en.8cd700b5.js .https://twitter.com/.67..+/.....c.....a}.H....e.o..R... |..+K"..)....A..Eo..... fU.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c442c53b7ada357_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4c442c53b7ada357_0	
Entropy (8bit):	5.618934309276576
Encrypted:	false
SSDEEP:	6:mYYk+f2pomzi5whmJ2R/gTuHeThO/ZK6t:t++am1kJl/ITcr
MD5:	7B8E47BA1119D18733D6D2A40504A4FD
SHA1:	F68F62BA84AD409FB2C511A21C72DCF8B7041455
SHA-256:	B21DA381DF232E2F788CAC451202D7EEF249AAB647F29F23B0877D276A60269A
SHA-512:	91F8309F225C56D28B88AE0192981313236C42C8F9A2096688690A76916845A7C7A576A7C40E7F6097702AB814D27FDAA13B8F11A97C78AB74635D57AF428760
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....:SM...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yP/r/izEaetvGXuA.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/a....+/.....|.~...h.....jN#Ck..nq. .AE..vn.A..Eo.....E.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4dd6d7d251fe4a11_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.485418313495528
Encrypted:	false
SSDEEP:	6:mk5/gEYj018IrAnPAMJl/gsW4jHkGGUQbV4FRK6t:3hN1tkJ/zW44GUV+
MD5:	D3D014DEAF5746BE79411DAF061A9E8E
SHA1:	F76BDC427C72F564DAD58CCF8A9BE7264EC5458F
SHA-256:	C89689BCDC37C63FE662A289A0FFF87CB9765AE9AF924DBABE689B5B595D3626
SHA-512:	BB382823F9C69835810E5E69CA3BC770EF8788867C823DE9CE307F31AED29C2E9BAE8CC45FCE63537E0716AE14DAB50FF8D0514960F6413AB37FA1FD1E6DE1D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h....."....._keyhttps://abs.twimg.com/responsive-web/client-web/ondemand.LottieWeb.9845d985.js .https://twitter.com/./...+/..... .....N.S...,n.....XHi.:..u ....33..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\4ef333cf938a5662_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.221859530029586
Encrypted:	false
SSDEEP:	6:m+nYGLkbsTMWj7ySVNzbst/g/Whop7Nom4BnbK6t:OATMw1U1nO7HcN
MD5:	1FE3FAD0F488F1C832CA39FD365428E1
SHA1:	696A1572BACA33CDBB15FF801642C7341DF67E2F
SHA-256:	E30BA350DEDB5497AAC2C7EBD89AF3793391AF0441C7E21ADB3A57788A09EF38
SHA-512:	61C461A1408E41C0E68FC4401E6093A7B54C740B55DC91BB94FC35678097F064974F0031011A412278E3CAAF9E366909B58FA6A2006CEF8911DEFB801573BA10
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t....._keyhttps://www.canadapost-postescanada.ca/cwc/components/assets/scripts/cwc.js .https://canadapost-postescanada.ca/dr.-.+/.....q1l....d.F<. a.QD.a..q..D.9Gb.v_.A..Eo.....#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5203498dabed958d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.741336609757309
Encrypted:	false
SSDEEP:	6:m0VYk+f2pomWG5hmJ2D9/gJX4e9h3rK6t:PN++amR5kJ8/ixxd
MD5:	0DB3920D41644BC595BC69B3AF65C847
SHA1:	4E32C4E1C913BC0B422DA5D4776F8D4AA5B15B24
SHA-256:	504E528092056FAE73E55A05FFB5B576506A9B7C9451C8DA4CD96BC1B081C12B
SHA-512:	FA97FBA968AE77FEF7DA5E8CF7852D822F8BA13B80511A56DDF94D1BCC05BCA1AB00A74333E137E9BB744A3073E91059153A3226A1CB49BB62A0E75F28B45A96
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5203498dabed958d_0	
Preview:	0\r..m.....h....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yZ/r/ISOOMzX-W9g.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.=...+/.....s.....4....n...o.# ..$}.)..A..Eo.....0 .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\522e0eb6e9983828_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.901046713083394
Encrypted:	false
SSDEEP:	6:mTwYWVBPj++R/6mpeQl6lnqbsr3g0/BkPjrk9K6t:EKVBPJR/6mMQYln5r38Pjo
MD5:	EA5D9D7D1B9920B4C44C7F385162A0FF
SHA1:	0FD51CC9EA24D714441E6958C889CA297A1B79D3
SHA-256:	E0C02EFFF91CD162AF3D5E4C88C21C36B24C7ED3E7FFFD479830C4E9AB5FDCCB
SHA-512:	2A88896727BB0715BC782388953FF14294A09E6B9711FAE9B979A6693C43AC8332C664440F763207D708D54131BFF12B8F0C6977B777E3C7C36A61F8B5AD079F
Malicious:	false
Reputation:	low
Preview:	0\r..m..... [...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/2.4c79ed6728cc3054bba2.chunk.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_B RANDID=canadapostdigital .https://canadapost-postescanada.ca/.!k+.+/.....O.....0:B..W!.c.FY=:.(1.Y...be.....*.A..Eo.....d.n8.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5613e15ed26fb32c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	255
Entropy (8bit):	5.327313000490747
Encrypted:	false
SSDEEP:	6:mFyEYGLkbsQWyWQ1Obsp/gnWCp4LKZK6t:UynA0VR6W16
MD5:	7EEFB0520EB60E0D75152BE009112F24
SHA1:	597E36CA71F72DB750DD5E8334E18667B168E94C
SHA-256:	15FD28CB2EBE3412541A95FF46821E80C910105CFDB986E9CC763AE7459640B9
SHA-512:	71D53C93F77848ACB2D23C89BFC39A27FCED09B59228F5332A80845C80D472ED27431B58CCE7903CB79A3678056CD09F3E738A7C42457FB09291ADE24D97955
Malicious:	false
Reputation:	low
Preview:	0\r..m.....{....z.$...._keyhttps://www.canadapost-postescanada.ca/web/assets/js/foundation5/foundation.min.js .https://canadapost-postescanada.ca/.;}-.+/.....^..#0. .b3H.;.HY.^...t'E..Y[o..."..A..Eo.....Z.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5803cb66c92ff389_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	319
Entropy (8bit):	5.895393561140578
Encrypted:	false
SSDEEP:	6:mFmnYWVBiO8Q3oOS/6mpeQl6lnqbsPmfgEnlDFu+lsp/1K6t:NzVBCjOS/6mMQYln5+frlps3
MD5:	A1667EE4C1C1DF37163852F8B0367440
SHA1:	951E12C7DD8018C1FCE74F2A4B0FF6E75238BA8B
SHA-256:	9C7E929E02028C912BEDF4565C74E4706368A32C2F361C8933C4FD25AC3E3EE4
SHA-512:	A61920C134A7656FDED4E8A4915F5B553BD8CB521E3A8F443F900D81560DC8CD328D3010ABDE4F235B5D4F9D1DFF97E2575EF8E5C8C50125A7BAEDEF237993 E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....iqa....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/1.a4037f4820369ddf14c3.chunk.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_B RANDID=canadapostdigital .https://canadapost-postescanada.ca/.1k+.+/.....].....9..&...IAW.>.-u...Xh...V..I~..A..Eo.....:.N4.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5adb79c5065ef5a0_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.791866979193569
Encrypted:	false
SSDEEP:	6:moVYk+f2pomW9WTnKfahmJ2HKl/gQ55IslIwSykP4PfK6t:HN++am6SKfakJj/R5mwSfPK

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5adb79c5065ef5a0_0	
MD5:	5A0BAD79BA4829EFFB14EA09DFE41FC8
SHA1:	01909ACE1E90DA4954DCAA9D9619EC49C7F71B12
SHA-256:	DBCB738005E37826F6E23CD1041690B3F2E7995B65AC70AD2D9DD9680390A567
SHA-512:	2DD1B2D3335FEE27FFB070EB7AA87A68DB64677423475936404109 7B8BDA2338679A33F5AE46423702CA4CBE2CC4EF3D2B6E0029B0B98EE287D9DE0E4C6C4D 0
Malicious:	false
Reputation:	low
Preview:	0\r..m.....s....=....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iX3c4/yn/l/en_GB/f0h0OfDnw6R.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.....+/.....v.N.....}3.F ....e.xr.....A..Eo.....Y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5b8e0eeb84700194_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.34967524449438
Encrypted:	false
SSDEEP:	6:mVnYGLyhUGEBcwnr7xrU7+Hgv/k1zvzvFhD5ru3nK6t:sChUG8pUKHskNvzvbD1op
MD5:	CFB6A42D0390C280DD6532A4B6EF0AD1
SHA1:	C9C3CD7E1EF95D46E2D2CF6B3E3E31DDBC215C07
SHA-256:	36EFCE061D4F905CECC1A78942706A93A00C99C9B0600076722134D07347A0F0
SHA-512:	27C5CEF52C85D262BC0AB199D22AB11CFB9178D3871A27A464137F297D7FEC41A09F21E2A5CC7197D38C1E31770BEF5C7FF713540D89D5AC4245322B08830A3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...S.NL...._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/uwt.js.download .https://joyeriasosa.com.py/V.L+.+/.....=E.....TV.M[5L< .3s....N.e..T./..x..P. A..Eo.....y.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5e6fd0ff3c7fc4da_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.685567861715347
Encrypted:	false
SSDEEP:	6:mFXYk+f2pomUu5hmJ2h/g8LjBYgxdkH4mDK6t:Ez++amRkJU/xLjBNIX1
MD5:	258D7CB1B5F4D7C7936A5B099448C645
SHA1:	DCE4570F7A6733C0D495433465579FC3B5EA74C7
SHA-256:	490DC5F8D643FB2FEA06465F9BCFA3734B231005B9FD4DFAA1FFD3BE8AD33315
SHA-512:	FEA98C6211BDD30CB468B15DF87A067D21E974AAA062CFCD01425F3BEA54BA8CAB19C6163583085B8AB2D46F8591A7A0A93718DBA469CD9672811CAEC2AD9I 0A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....!...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yT/r/6LZHL05r2vJ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/^....+/.....t.....s.*..FR#.?.!..5...xf.. .I~..A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\5f13f5ee85425009_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.676052244063962
Encrypted:	false
SSDEEP:	6:mdYk+f2pomDvaahmJ2tN1l/g6k6qtp9oUaf/zZK6t:0++amDpkJml/VSpH8rT
MD5:	0BF26CDCBF9FE15FAEC183BCBAE47C73
SHA1:	B921CC1CCDFE4496132A7F88B42EEBA018128E8E
SHA-256:	755C8A623564375E47252024BB1AAE02C1594B94B329730034456D689C462DCF
SHA-512:	FE584309E5CB6725F81179E8168FB0E194FD481573245D255F9DE478A78D7CD02E8390125CEE3ED4EA569163C104C02967AB0AC77AE293B392061243E18F5543
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....L...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yG/r/6W2jbhhe5sX.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/L0...+/.....-.'....4.....5..R.O .....A..Eo.....n.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67be1b345951ee5e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.541152010779268
Encrypted:	false
SSDEEP:	6:monYkvwypOWVzNfU5O+/gqWgKUzfm9kP4JZK6t:tvwy1Nj+/oUzfKkWT
MD5:	959D5C5A2A85D6FF123A3258CAAEC697
SHA1:	338483B1F79143F326108F8E11A2720852111142
SHA-256:	CAF2BD391AC441A34C257815E81315E2BB25764815188DA63C44EBBEE6188820
SHA-512:	8F31FCE05372390B6E83633853DDA7433976E892FB2380D21F4AA386103E803BA6D56358335C09BCE5CDB72772469CCAB0E48024154F7CEFFA967F636C084E62
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W...[.Hh...._keyhttps://static-exp1.licdn.com/sc/h/a2svc0x4jgqcgv9votrvr9qmj .https://linkedin.com/.6...+/.....&.....+w.v@..-.>1^...h.Z...>V....Q...A..Eo..... .`A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\67fde904751a8066_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	784
Entropy (8bit):	5.667843658494917
Encrypted:	false
SSDEEP:	24:7ElKGFXAuyAyyeSKKBjN/ZI4LVYofcCZ+:7ElKgwurflJVYof+
MD5:	9B28A89973A7743D208862D448CAFF64
SHA1:	4E2C89A9DE9C3D8EE58EC2ED785FF0AF31686D08
SHA-256:	E4D9114C2F14F3319037B911BD4910182DE4DB8C3834967DCD33F94564930EDD
SHA-512:	60CD788AC5075805B1824C9DB7068C3EA3CEC059206A2008E3CF37AF29ABDBB2230CA643DA58B5F5A82491C182652493D1875BCEDB3F9BD261D4AADABA418E 1E
Malicious:	false
Reputation:	low
Preview:	0\r..m.....mk....._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1011747518/?random=1632800086782&cv=9&fst=1632800086782&num=1&value=replace%20with%20value&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa9m0&sendb=1&ig=1&data=event%3Dpage_view%3Bgoogle_business_vertical%3Dcustom%3Bid%3Dreplace%20with%20value%3Blocation_id%3Dreplace%20with%20value&frm=0&url=https%3A%2F%2Fsso-osu.canadapost-postescanada.ca%2Fpfe-pap%2Fen%2Fregistration%2Fpersonal&tiba=Canada%20Post&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://canadapost-postescanada.ca/s6.-.+/.....,?...p.../^.=.s;.Z-AR...-.?..|1.A..Eo.....w.s.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\68317e7eff14ab6e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	78680
Entropy (8bit):	5.465255418738345
Encrypted:	false
SSDEEP:	1536:54EQ6dYktIG805XuApQ9DyzpBMVA3U3AMs8ijcDOsGQkJJx5MgLvyQ6B:5pdYwfMApQ9DyzzFMkFadQM
MD5:	D489D7FEDAF7928BB40126527738EE24
SHA1:	B1CDD137415CB71192C8D138DBD5451AA0C765AE
SHA-256:	99D37DB3ABC07BB3C733C072B1F14D020C673D9D84F865F83A131DF8435E0E73
SHA-512:	FFF46D76EA5D3B077A641FDBA263373310DB985315EBC30113F070B773F18DFDABFDD89E954195EFEC1741860623B60EF615D80BC357B78E46BFA137516134E7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...(.h.....A1B05E1055623783FEBC922E4E3491695B41DF0E8E2A9A28C0C35F4AF712B9CA.....'..t....O.....2..6\7..... .....(S....`.....L`N....(S...`.....LL`"....@Rc.....Qb..Q.....e.....Qb.7.....t.....Qb:.....n...b$.....I`....Da....$....(S...`.....L`.....Qcz.. ....exports..$..a.....S.C..Qb..ZO....l...H.....a.....Qb.c.....call.....K`....D}8.....&.%.*.....&.%.*..&.(.....&.}...&.%./...%.0...'....&.%.*..&.(...&.(...&...&.'..W.....-...(.. .....,Rc.....`....DaH...@.....e..... P.....@....@.-....pP.....d...https://siteintercept.qualtrics.com/dxjsmodule/CoreModule.js?Q_CLIENTVERSION=1.50.0 &Q_CLIENTTYPE=weba.....D`....D`4...D`.....e....`....&...&....&....&.(S.X..`I....L`.....Qb.^/.....o.....e.....a.....G...C...K`....Dp(... .....&.(...&.Z.....$...&.(...&.}..)&.%.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\69bd9a040cbe528f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	300
Entropy (8bit):	5.67589614743792
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\69bd9a040cbe528f_0	
SSDEEP:	6:mBXYcv0KgOn075Ps7Ta5gaObsT3H/g5s3ykxa/bK6t:IOAgi7mJTf6N
MD5:	2DD6EFF534C646ED19D59E387FAAFDA1
SHA1:	D14D4565F8AD08FB4372A9FF3A6C4DEAD5FECFA3
SHA-256:	3571B007F1B2D66A1F408C73A2D327B0A9FD425F15C9B533260D0E781C3D0372
SHA-512:	CE5FC56F581F302C4FB3EF9EA87EC0ACEE079FC58DCD79DFF1DCC5FAAA7E8AEB09AFB7A1620F5F2584F91BB4B355FC8A5901C00CF3D1D0A96C7196EDE61A07A9
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://assets.adobedtm.com/0ccf8b9a711f/6e634e5f652e/a18280e20836/EXb471ab3b98694cd895b87487d7a7c6ec-libraryCode_source.min.js .https://canadapost-postescanada.ca/.%.-.+/.....9.....t..ID>....9.Ywn...j67!.*5...A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\6b61639f73cb2a66_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	228
Entropy (8bit):	5.523679816065577
Encrypted:	false
SSDEEP:	6:moYGLyhUGEBcwWIJerUng9YG744lhK6t:YhUGVUnY9N
MD5:	8AE722A714F76B72DE07B95E1BF859CF
SHA1:	FEC1A57AFBF03D14B61C56FE375D24AB43E8326C
SHA-256:	11A84D3447C63F8D8CC1A3AEB9AF1FF43DB25994A5567C3B3EB2487542E82DDD
SHA-512:	91038C3D3268B0A10F91D305BB8554BD47E2EEC253CE2CC7D4BAA862E83951750745DF4B8A367F0F855176AA447939113516FABBDB8B1CB914F5E48CCE3ED441
Malicious:	false
Reputation:	low
Preview:	0\r..m.....`...IH....._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/614267586032718 .https://joyeriasosa.com.py/..C+.+/.....~H.....L.....(.Zs...a{^.._.(....{.....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\729180b220b6c118_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	652
Entropy (8bit):	5.777350727388484
Encrypted:	false
SSDEEP:	12:iE31K4xfmoux2pHgyye3CMxPDPoIsHIwLVYoffECYmzEv/ckHtN:iElK4xf/uyAyyeSKDQI4LVYofcCDUUkr
MD5:	DC5E014C62F84F3388F891666C2E46E0
SHA1:	CFE825FA998DE55ED7AFCAA0E42622593520FC89
SHA-256:	FE7E4F6C04E7D12176A9FEE14ED609C4EBCBDD4AE95F590A8585A1D6CC24191D
SHA-512:	FF6277C3F54A559F0609D6CE52B9F54E18EE7D099544E4FE43B027EAA1221DABCE373E187C836A296D46B5D06C06EA576942C521B633DC6972AE336A5643440D
Malicious:	false
Reputation:	low
Preview:	0\r..m.....UZ...._keyhttps://googleads.g.doubleclick.net/pagead/viewthroughconversion/1011747518/?random=1632800086775&cv=9&fst=1632800086775&num=1&bg=ffffff&guid=ON&resp=GooglemKTybQhCsO&u_h=1024&u_w=1280&u_ah=984&u_aw=1280&u_cd=24&u_his=1&u_tz=-420&u_java=false&u_nplug=1&u_nmime=2&gtm=2oa9m0&sendb=1&ig=1&data=event%3Dgtag.config&frm=0&url=https%3A%2F%2Fsso-osu.canadapost-postescanada.ca%2Fpfe-pap%2Fen%2Fregistration%2Fpersonal&tiba=Canada%20Post&hn=www.googleadservices.com&async=1&rfmt=3&fmt=4 .https://canadapost-postescanada.ca/...-.+/.....@...W.....~.Of..S.....A._.A..Eo....."G.q.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\731f7cf08bdfe6a2_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	247
Entropy (8bit):	5.820936537620957
Encrypted:	false
SSDEEP:	6:mFD/lXYk+f2pomWsJ90oKrVJhmJ2gj7vl/gWCMY+47JhK6t:KN++amX90oKrVJkJFvl/8Sap
MD5:	1A5B7405FB910D8CDEA0F6C940F276F9
SHA1:	DF37D6C88EA4739C38C44696CCA6E72FFF8D2FA1
SHA-256:	D34E3EEB305867E03B6CD2D7096980E1CD585AF8E675B5B8E5FD75DF37907093
SHA-512:	155820FDB2788E62ECED1AF36F896BB5DDA0E4076BF990DD2BADA5D930E75E0006EA02BDD6C85D93649CF3BA2B564A850D066DD360B8E6066E6A9FCEC9CA3F15
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\731f7cf08bdfe6a2_0	
Preview:	0\r..m.....s...a.?....._keyhttps://static.xx.fbcdn.net/rsrc.php/v3iYXl4/yM/l/en_GB/Ou0wKR1sTZQ.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/.[...+/.....p.'...;...k. .S...C.<.M.....A..Eo.....N#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\7ccf34dbce7b4ca9_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	5.437959642918256
Encrypted:	false
SSDEEP:	6:muPPYj018IrAr+/F2RpMA/gbYwF1vUuhm49mbK6t:7P1tUMFYf/LwFquhYN
MD5:	2615462AC96D5420A0D6FD83970CA14A
SHA1:	22BB050A946A5A84ADE263A51B44734F9D7AA02C
SHA-256:	CC48D0DB85FAEE3B0435000E24882FB4DEA7F7D21C89020E1E98CE7929305FE7
SHA-512:	6A7A541B99015C880991D5E16B920B307DB59F3F354A2D39772D771B200ED8C9FFB567141A2B8842F4C9B5A900DC2151A4045024C8F553910B84550A446868F5
Malicious:	false
Reputation:	low
Preview:	0\r..m.....j....._...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.NewTweetsPill.e12e5de5.js .https://twitter.com/(.U..+/.....>.....E\i(.t....$vn.o(K.!a. _....n...v.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\837fc5f33ef27dd5_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	222
Entropy (8bit):	5.43406542227139
Encrypted:	false
SSDEEP:	6:mTYj018IrAoIlWVpMhQKvl/gNl/llE+aoTOuDkom4sK6t:m1tzllt9/l/E+NOuDh+
MD5:	CB99CBEF0B3E8521F49EE4496FA6CED4
SHA1:	7CD05CD5AF28A382B4181B587F5A04FCF12655A4
SHA-256:	137447C0B0BFF6F53B5F8B23BCB4C8111AE2C0DFF00EB4C69BC07054FEDC82FF
SHA-512:	C5ECF15A6C99EBE542D78702F07D47593C3C57CBE6256F48E33015E80E002EA1046A19D8E98FEF4E62D574667ABA5D55742319E267BE48C0F8E03A5A9C293BDA
Malicious:	false
Reputation:	low
Preview:	0\r..m.....Z.....+...._keyhttps://abs.twimg.com/responsive-web/client-web/main.d4f5c725.js .https://twitter.com/7./..+/.....J.....|K..|..]..q/.....wL...<.A..Eo.....o.:.... .....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\86d73214ad73585e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	262
Entropy (8bit):	5.401421449088847
Encrypted:	false
SSDEEP:	6:mOrUPYQkbsHAf5KA+qObsDWIl/gvIrVtK6t:54HgxKA1VTtuY
MD5:	523CD646A5CC52A29BA0829B85AE2C12
SHA1:	6003BB45BC3A624D5C943C4591070B9796CED2A8
SHA-256:	9CDC534C58E31B989CADF248DFA8148B965F47D3DD319782E993B7A308C610EF
SHA-512:	A6715E0525CBFD407DE9EA0DDC622F69789E70A21C3CFD17663DD4466401C794AE6BEF8ADC6BB729710489036D2704ED03F1F9A670535CA93F696A5257174D1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....N....._keyhttps://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/en/11-es2015.js .https://canadapost-postescanada.ca/.r.-.+/..... ...x`)"...9...8..g...g..,9:.&.....A..Eo.....Uh.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\870dbc9d451fe4db_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	5.458852955465902
Encrypted:	false
SSDEEP:	6:mIX6EYGLDlynflG9LY7Wdxaywly3Fl/g4l9xmbV5uhdDK6t:lXsflGpYSVwgVl/Vl9S5un1

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\870dbc9d451fe4db_0	
MD5:	1E80D0C8CC73A78522F79A45D5F0E9C3
SHA1:	A4F0A3FABEDDEAC3FCE0F29D18CEA50E9F062594
SHA-256:	080BEFD2DFB509242EE1298E71227E1FABEAD8746237A8C18A7AAD0EE672280D
SHA-512:	3EECCE040B2279EE16985049F272866B0B5AD16C208A3F19C1B23848116BBF30700A67A598FE3485C92B6ADDC4DBFCD468E9BC26AD98AA98AAD72090CB36AC F3
Malicious:	false
Reputation:	low
Preview:	0\r..m.....n....@....._keyhttps://www.instagram.com/static/bundles/es6/ConsumerLibCommons.js/cdbadb30deb2.js .https://instagram.com/..p..+/.....K.....$.#k...+ h.....9.....O..`.c s.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\88d41e5b293bf9bb_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	257
Entropy (8bit):	5.570849062995936
Encrypted:	false
SSDEEP:	6:mOhnYGLKdXNQKTKogAbsf+/gDQTtvodrsRnK6t:shNQKGogbfupFp
MD5:	928DF73D0BB34FFDAEE1358565E8BC41
SHA1:	6F35D54A6864B893EDB426D56A6E3AECF1E6B17B
SHA-256:	2AFEADC3A452EC8A2AA3A2F3DF43080A10A5EA2ADC6E74A036D2D206394D5986
SHA-512:	748AEFAF826F4E0CA7BEE64478EF96A479F8F9242029DBCAAF744E141A98856AC930CE873F4392DD0C32658625150BB0A64F0648277BED7F2B4805E480B4108F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....}...9)....._keyhttps://www.gstatic.com/recaptcha/releases/tftmXwdbgCvrXiHxr5HGbIaL/recaptcha__en.js .https://canadapost-postescanada.ca/...-.+/.....& .....g.0$.H...+M.....o.PF..i.{.nN.A..Eo.....;7`.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\8d3a9efd81c6830f_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2584
Entropy (8bit):	5.708494314317776
Encrypted:	false
SSDEEP:	48:C2EEQolg5k2l+a22rGq5jFPiwD7xcFdzAtsF+bDTkeEr:dtLSp+F2rGqNF7DOEuDr
MD5:	3BB612385AA0830D54368708B5BC36B6
SHA1:	9B87A48A5D5C6610E2DA751DBC837E9536AB2042
SHA-256:	718124B7804094EDDDF2E590016DF04A7888060813CBDD937C7B9469C16E012C
SHA-512:	3478B6635E77AE53D15EDF6E653A3FEF0DAD3C33431FC6A2E76D3871728DA4D62B07DA1D78217FD624A2956455C116AC107D355C7530035CBFD756790ABABE(A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....;..U...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/15.e8db891fc03030df5677.chunk.js?Q_CLIENTVERSION=1.50.0&Q_CLIENTTYPE=web .https://joy eriasosa.com.py/A.K+.+/.....D.....0....d..7;_/~Y"`...AO.....Z.A..Eo.....<.g.....A..Eo.....A.K+.+/.....'.....O....x.....(S....`R....0L `.....Q.@j.<.....window...4Q....k%...WAFQualtricsWebpackJsonP-cloud-1.50.0.....Qb. .8....push.....`.....L`.....`.....Ma.....`.....b.....j...C`.....(S..`....8L`.....PRc$..... ..S...Qb.^/.....o.....Qb.}.....d.....Qb.....r.....M.d.....Qb.....53..`.....Pc.....push.53.a.....(S.(.`.....L`.....(S.....Ia.....I.....@.-.....P.....w...https://siteint ercept.qualtrics.com/dxjsmodule/15.e8db891fc03030df5677.chunk.js?Q_CLIENTVERSION=1.50.0&Q_CLIENTTYPE=web.a.....D`....D`<...D`.....0...`....&...&..!.&..q.&....&. (S.(..`....]..K`....Dd.....,Rc.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\901026f2d2f76861_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	373
Entropy (8bit):	5.978292365685877
Encrypted:	false
SSDEEP:	6:m3LXYGLKdXNQKTKogRuz+/g1/r8PP4m/n9l/ZK6tN+3GP6aaOVqyL/kP4m/n:CqhNQKGog86Er8PAg9IrVV1RkAg
MD5:	FFCEC4584E35F47C74EFB766705FAEC3
SHA1:	74C301DD395B8E906AF30655CF96CB564382771F
SHA-256:	3C4ED5A5A08411437FA8E99EDE5357F788B854B1B5B1666A30BE756BF78805B9
SHA-512:	A4F0CE85945ACC5730193F1AC3ADA85C8746BCBFB45F9AA437858FC72AF47D1E65A6CD939DEF67F58395F84CD57C5F1926E3F21D26F9EFBF8218A4F2B57342(3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\901026f2d2f76861_0	
Preview:	0\r..m.....m....X....._keyhttps://www.gstatic.com/recaptcha/releases/tftmXwdbgCvrXiHxr5HGblaL/recaptcha__en.js .https://google.com/...-.+/.....%..... .j3A.. ..>p...4.A..Eo....._.....A..Eo.....-.+/.h...E232FC343637C7349613E5FBEE17AF0A240649CCC4D79374150D96D0424F1BB3.....%..... .j3A....>p...4.A..Eo.... ...F1.L.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\921d57f716686e04_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.624453720482158
Encrypted:	false
SSDEEP:	6:mUCAnYAWQf2IiPk9+86VclyhJ/1l/gpE3z9p7f4QnK6t:ppetcf6Wgf9l/vDfBp
MD5:	B060406BE823C0BA3C760BE058502683
SHA1:	7FD121767DB581552600F5AE6F2F36469B63EAF9
SHA-256:	54CA3476594D594E8B993AD7F9DE5CE6EA4D6C959EEC57276652273235832CA8
SHA-512:	7AE6A184AFB1E6C5FD7DC5950214AF69F17BCB10B05A155F27BA611CAFC7D5B7312BC407890F2C4DCAE544FDB91C4C8F72C9A9E155C81B52F7B80C216983182
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k...(....._keyhttps://connect.facebook.net/en_US/sdk.js?hash=f690181a28236a9150e5366f5c0cf10f .https://instagram.com/.j~..+/.....j.s-../..[*}....~v..2. .0..U.]{...A..Eo.....&.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\92f72e5c55078d19_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	233
Entropy (8bit):	5.382738757658672
Encrypted:	false
SSDEEP:	6:mmLYGLyhUGEBcw57Azr7xrUrO5fgZNJDJ03wQ7QhK6t:uhUGGMzpUa5fcN9m3B8
MD5:	184827F6EC9DE660FED3E8456D5AE69C
SHA1:	AC77ADC5BEB27B66304ACFA2D11D113A41D37DB3
SHA-256:	70AF0D3EE3F89A046110995D6C7FC9D3BF437E8754D377644CBCCA19FA80BA55
SHA-512:	7F9948568C11A91EB561A4092CDC3B46D356195BE4ECFCCF77C35F5C83E456906FB6A6F55A6A1CA705ECFE7E90A7A4735A99B5FA693E8C206E0E646C5AD4AF7
Malicious:	false
Reputation:	low
Preview:	0\r..m.....e...w....._keyhttps://www.joyeriasosa.com.py/ca/restor/assets/fbevents.js.download .https://joyeriasosa.com.py/N.C+.+/.....<E.....<.....t.#(...^x.C<..@..... wEf.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\93b288346b6bae6d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	276
Entropy (8bit):	5.656671031938239
Encrypted:	false
SSDEEP:	6:mvYj018IrAMUscZnWAKjzBD1QQePspMNO/ghlldphCzplGDK6t:W1thUsWWx5FQsOO/kITzGG1
MD5:	19D55308640AE984DAE0EA399C167A3E
SHA1:	EAC5B28CAA7D9B32BD4C647B0D19A275A56AB042
SHA-256:	C3435D17E37CA54AB9126C98AA337364516F777E5A45F5063C2E2C4ABCFE74A3
SHA-512:	39807575BCABC742EDEEC93418D86F1D9D2A419EC25D25DD43739545D9580F3138847BB82A164E667CA30C21D1DE6A157E9793CCC187E66382DF57DC33D3FB2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....).y...._keyhttps://abs.twimg.com/responsive-web/client-web/shared~bundle.Ocf~bundle.LoggedOutHome~loader.SignupModule.dd0c6555.js .https://twitter.com/.W..+/.....e.2W...]._[*._.Z...xy..#A.....A..Eo.....c.H.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98dc7f6a90777c4e_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	297
Entropy (8bit):	5.5570455836620205

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\98dc7f6a90777c4e_0	
Encrypted:	false
SSDEEP:	6:mIYQkbsHAf5KA+Myv0zGCOobswv/gnO1HinnL5RK6t:NgxKAmY4A6qA
MD5:	849B42A6D5060371745EB405DC23248B
SHA1:	BD527006C4D4E58982C9A076FEB86F9ACD80A986
SHA-256:	E28D26A7F5184A121E35D26F631F7FC8C8A69432AEFC1F3973B343B7B0EB3E95
SHA-512:	C29A2B49E2CF769CDAF5429BFFA2272927F8D0DB4067890D98E884589A637DB33C81DCAC9C4B8709DFCBEA4EAB116E85CC4B8984C2EF1D6BAEDE3F3C630D4 51F
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1...._keyhttps://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/en/polyfills-es2015.js?v=2109.01-SNF-National.2650 .https://canadapo st-postescanada.ca/T..-.+/.....;.n..mt7.6..#...*..J"....l....A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9a8286598e1e3746_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	295
Entropy (8bit):	5.556181343526319
Encrypted:	false
SSDEEP:	6:mhUYQkbsHAf5KA+usIfGCOobsA/g8tKjxdNrbTnK6t:PgxKA/f4AGFx
MD5:	3F3560819EA7DE888DB428AA3CC4AABE
SHA1:	CF599C5BF813FE6391BCADD87B45EB54D7A49C97
SHA-256:	212BADF45CF9F9C32FFC8348897C23051662A78C098929C69F6525AA2887EB48
SHA-512:	2A9704D5B70EE4DD28DD16AC18C10F4C05DF828ED4C73468CD6A2EF851B08D78C86B2B2D0BBF8EDB67DE1AE2F62EBF34BD46EDBD516EB48F1C6A442267E4 925
Malicious:	false
Reputation:	low
Preview:	0\r..m.....r...._keyhttps://sso-osu.canadapost-postescanada.ca/pfe-pap/resources/registration/en/runtime-es2015.js?v=2109.01-SNF-National.2650 .https://canadapost -postescanada.ca/..-.+/.....8...o+...~.....}d.).&._..A..Eo.....%.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9c1ee8b1cf4209fc_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	219
Entropy (8bit):	5.439917580507004
Encrypted:	false
SSDEEP:	6:mwllVYAWQf257Obs7n+/gqXwdNKY/OlhK6t:be5hDuX0Ol7
MD5:	5F74E17D472CEC23199CC86AF1436FD1
SHA1:	0AA00CD5F8F63EFD6D87A0D19EE52173366B36E5
SHA-256:	08236EE7DDBB24C094620B3018703286AB2BA0DAC8DC062353C7F7CD060E63A6
SHA-512:	F2CBD9196281AC2432B3320BED13BD457F7128898A52F1CFCCBB51C3A652CC4350AD8F3C7C905FA015E25E476996A5C3FBCACF274B88160C36DD512FEDAF51 1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....W....._keyhttps://connect.facebook.net/en_US/fbevents.js .https://canadapost-postescanada.ca/...-.+/.....:.9.l..".9...r<w...[.....A..Eo..... ..A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9feaaabdb20e3dda_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	323
Entropy (8bit):	5.662679810825384
Encrypted:	false
SSDEEP:	6:m487/VYj018IrAMUBDGO6JA7WYibVbwgoPMLm/gLulR3VJMr68llbK6t:l8zN1thU11ip0/hRFJMW0T
MD5:	F0A9B57679231507B11A2679EF83FD27
SHA1:	C3487EB7BE88E91E36E6DC4DD2CD55E28A50ECB1
SHA-256:	5575CD0EB2102F3F63A01BF132297FDA68CA40B8A7541D5339DEAFF99F14E9A3
SHA-512:	742D08B08BB94A34A6441051A2356DCC40EDFD7468CEDD70D672C3D39E601E1FF508DEAE978C779A7E0AC7B3EAB7CA5313130574D9CB054CEAD03BC547DE AF
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\9feaaabdb20e3dda_0	
Preview:	0\r..m.....<.^....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.AudioDock~bundle.AudioSpacePeek~loader.AudioContextSpaceMedia~loader.AudioContextVoiceMedia.30711d95.js .https://twitter.com/U.J..+/.....E.....C..xZ93....A..Eo.....W.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a0d5c09ce72482ba_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	237
Entropy (8bit):	5.5815815219016764
Encrypted:	false
SSDEEP:	6:m049Yj018IrAWD/3Msjl/gUcS7vFLrOK6t:211tBfl/z/6
MD5:	15976DC2DF5A5CF855EDF8A288E851BB
SHA1:	A9995320DEDE43CBD37AAB2CE1CC7BAFE09CE3CE
SHA-256:	5C06E8490BE0C172D58DED0085BF47E9C3B9B310C1F6DB92E2E49502E3EE71E9
SHA-512:	09FBE178AAE3174A2D968DD93148AA4C2923B3CB59C25A8E13D5801A8112A5F2649DC101C82D070709722E30042194524FC08DBFB894DC638058C121EC72DA1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i.....|....._keyhttps://abs.twimg.com/responsive-web/client-web/loader.SignupModule.03a2e115.js .https://twitter.com/..X..+/.....%.....b..eX...5..P]..>].H\....T.-.$..A..Eo.....;.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4876f3d612cba7c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	5.574839525697631
Encrypted:	false
SSDEEP:	6:megEYj018IrA0CxNuRcMMNO+/ggVJXXtWK6t:v1tFJqNO+//VJnW
MD5:	DDCE27864912BD604C1B240FB9CEA2F3
SHA1:	9EC5A76FA01C91FAF566778EED6D6C0BF7996A1C
SHA-256:	18551852E2E3F4D04BDDC42721A2F078E11674FB84551FFF705F87EF30A32D13
SHA-512:	4A8D813B614DEB05D5475BE10C8698123B98373994BF7AF7A9944088025B201901F10FCC70C7C1460EA9A8307CDC4739184FED07B70E400072295937D7E8068C
Malicious:	false
Reputation:	low
Preview:	0\r..m.....t..... >...._keyhttps://abs.twimg.com/responsive-web/client-web/loader.TweetCurationActionMenu.180a4145.js .https://twitter.com/1....+/..... .....<..M.7.(.l)#....oT0...V..J....A..Eo.....2.J.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4e911a49a59ae84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.721652847073973
Encrypted:	false
SSDEEP:	6:mQYk+f2pomZTTNPWxzhmJ2Y/ggtAMRa5PD8t0b1hnhhK6t:h++amZTTUxzkJpDfRqPD7
MD5:	3128AF845CC6D7B2B8F0CA731443C9C9
SHA1:	99CBA42991B9A6FD7ACE6C7097EA11D03CCF1115
SHA-256:	BE15A3AA1C525365646A07C6CF67BE1C1E6666CA4A0D7F231AF8DCB04E20447C
SHA-512:	30B074A068887E64E874BD376D5CA3F11B83CFFA91F1AF6A16FD70971DCDDED7D7E97F11E7480DA7BA25591C229A84708223659DD2E60C111B69478B5328493
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....)...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yr/r/BNzLtjA89q3.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/F).-.+/.....Q..t.f...S.-_.H.t.o.....Z.A..Eo.....~[.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4fb79e46d9afa55_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	312
Entropy (8bit):	5.840477704015251
Encrypted:	false
SSDEEP:	6:mUylPYWVBBcmpeQl6lnqbsj+/g0dvCVSrL/ZK6t:klLVBBcmMQYln5Spda8
MD5:	3B6349247BBBE3369328D4F5F13EF519

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a4fb79e46d9afa55_0	
SHA1:	FF4477ADDB3CA3A0F0D266AE3E672926423CEB36
SHA-256:	22A7B80E7E15AC549F82ED6046296E2625A49BFA7BD6F491605D6A5EAC8D64E0
SHA-512:	F40637C2D394BBEC93CF00ACA7DFDFB304C6C7E7DA9A17BAC7AF8B5E07A5F3C4877E5EB84131A411DC29CDD33D04002ACD7245EE27E40BF1A2B479D26A03E27A
Malicious:	false
Reputation:	low
Preview:	0\r..m.....1....._keyhttps://siteintercept.qualtrics.com/dxjsmodule/UserDefinedHTMLModule.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_BRANDID=canadapostdigital .https://canadapost-postescanada.ca/n..-.+/.....J/....f...[C.f.....8l..e`a.E.A..Eo.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a69cc10f7b1c4ede_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	229
Entropy (8bit):	5.595662874501263
Encrypted:	false
SSDEEP:	6:m3BVYGLDlynflGgKqSlly3D9/gwtQEuOglhK6t:7flGPqSlg3D9/sEuTN
MD5:	5D39C9BE38944E558C21D768AB4E4227
SHA1:	7FAA9C9F1E8A13AA2E373CD99378E677D8A852AA
SHA-256:	21501A227B06A7659FCB19BF0FF0AADE16620AD16312EC2EB966F3A9FB5DC27F
SHA-512:	71A3B7B4CC77EDD165E434DDEBFFFE8395F49097351071454ABAD503A2F7890E4E8578896120FB9F516D06976F6846C9AB8304CE051C93D0118E9DB257C395B2
Malicious:	false
Reputation:	low
Preview:	0\r..m.....a....=.F...._keyhttps://www.instagram.com/static/bundles/es6/en_US.js/475a81066879.js .https://instagram.com/.Eo..+/.....>S...W]..[.+}....:.X;.NM...s..A..Eo.....,.#.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aa2e8677d2817733_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	461072
Entropy (8bit):	6.127284250061953
Encrypted:	false
SSDEEP:	6144:QEAeO7Ps/1Kc8E39FjyQuJJ1mN+6lsT8eVCum5E6iyLZCj50waRAJUY:WPkbv3u/1m07IqmuyL5oqY
MD5:	8D731805103761187 92C974049CF1B67
SHA1:	CF75E6F0CDC48F6E100503C8EEBE37B8A1D1A4CF
SHA-256:	7FB97FD9A9B7AEF7CE88018AA58F7283E26571533C6F5AC73AD8C08E7F9C8446
SHA-512:	56EC55D8FF5C9B86DF97EE3E99C0F84AED37B69637A55E527A2A22DBFF73ED3E1897A4CA8F2F71ADB23D6C5A97061DBD4F84CCCF52F494ECE94FDB282B553E1
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@...+.. ....E232FC343637C7349613E5FBEE17AF0A240649CCC4D79374150D96D0424F1BB3.....'..L....O~...H...`.Cq.....D.....X...p..... .....L.....4.....l.....x.....4.....<.....`..`.....4.....x.....H.....|..... .....X...4.....0...t..... .4.....`..... .....4.....(S.<..`2.....L`.....(S...E..`BN.....L`..... .Rc.....z.....Qb.....M.....Qb..g.....r.....QbR.gm....V.....Qb.b.....D.....Qb.`=.....R.....Qb".O.....W.....Qb..8.....IX....Qb.Cfi....sO....Qb...3....sA....Qb.H.S....Eb....Qb&.*.....wm....QbN7_.....ms....QbnA.9....MD....Qb.K{.....va....QbJ.S!....N6....Qb.;.....hb....Qbb.+.....MN....Qb6.z.....c1....Qb

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\ae276f63f5a595de_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	215
Entropy (8bit):	5.536214189318176
Encrypted:	false
SSDEEP:	6:msBonYGLAAmrDXdLTAiKSYG+/gPvlc8qBC4K4FXhK6t:BBbtnAi+1W9cbBxX7
MD5:	4EB870EA36604FC6F8E97637E1EFA463
SHA1:	C93B9213E6862AD33D65C73BC38414412B9A0C29
SHA-256:	6CF24512ED757E7F45624292D4F782E86167E17B2643E478BB49EB4F974779BA
SHA-512:	D89B28301DBED72D73F76BDB8167189260812601A2C9A28ADE65E835FB9159783C3353D587A270F678FA8AA592F6BF0EE42285A9D71D629327494CD875D5E698
Malicious:	false
Reputation:	low
Preview:	0\r..m.....S....x....._keyhttps://www.googleadservices.com/pagead/conversion.js .https://doubleclick.net/.,.-.+/.....We...>4..9)%R..e.q.0....$.A..Eo.....8.A.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\aef1077583bb3dff_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	293
Entropy (8bit):	5.806696806579181
Encrypted:	false
SSDEEP:	6:mSsytXYWVBCYpeQl6lnwrUtKFg0llRBN+lJPtRK6t:4ytDVBCYMQYlneU4bl781r
MD5:	99EEE01D2D153307DC6777F436550487
SHA1:	9B3659A5B427C88E1B3577E3B0260968E7A90D58
SHA-256:	3280939E92F0E5336D6175A5C3BB79CA18B2C08B2B4DF847851B8E6E9E793A71
SHA-512:	57C9A555C300FBE2F6CD9529E9840703F218FD801804394B5EE2112EE7D2AF9D5436EDFFEFBEF119C8527B465084A9D524DAE42290742442B4F1939CDE7D9A0(
Malicious:	false
Reputation:	low
Preview:	0\r..m.....i#...._keyhttps://siteintercept.qualtrics.com/dxjsmodule/CoreModule.js?Q_CLIENTVERSION=1.61.0&Q_CLIENTTYPE=web&Q_BRANDID=canadapostdigital .https://joyeriasosa.com.py/-lg+.+/.....L.....?.@C....UU1...L..=J..E.cG.,.A..Eo.....j.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b44c478e468a0875_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	196
Entropy (8bit):	5.3257107327156294
Encrypted:	false
SSDEEP:	3:m+l611A8RzYcKVJ3ukWYR7MRbVjl//lHC1SXh9nixcAnNOueIm5m4blXpK5kt:mTYcw+k3M9Vjl/gEX3nTo4u9m4UDK6t
MD5:	C1672B49336DE6A936E8A068E69DBF15
SHA1:	B143EDBD9B8F262F827060852863D5BF0A789215
SHA-256:	5B681C1D623DE2E4DD0E0C93850FBD6CC4BA5ACDF8D1DBF540087BB7DB3A5BAD
SHA-512:	70D7E7702BDDCB59C2B69B484A8C7B6884155A86F386921C8CB34F63D1C50780B512516C431789F482135AA5807948562D39087C35EF051F1CD34A677EA25763
Malicious:	false
Reputation:	low
Preview:	0\r..m.....@....~o....._keyhttps://accounts.google.com/gsi/client .https://twitter.com/..p..+/.....v.....!}....9.....s...Q^.;.A..Eo.....7.P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b592e1fba12a1c84_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	292
Entropy (8bit):	5.665061797008413
Encrypted:	false
SSDEEP:	6:mSTEYj018IrAMUF/15enQ6OS9uFvpMZO/g3YUBaeh9tcyH4fV5/ZK6t:q1thUpCQOMSO/Sdbh9uy4p
MD5:	EBDA68A251310E9352567693A4366654
SHA1:	F0BF9974521FB0A4F12232276446F363D2F315AB
SHA-256:	307F544F1BE6B2814366EDBFD9857C5ADBB18F601B4CA9C02705B9F07D615C88
SHA-512:	A2D7F8ADDC4F10F0D31758DF1ABDC2E4AB725729951F16D2FBEE3032189EAB5FAF6A7B4D994C0105E0A125A8DB4FFF79D825D54A05CE1A4D5E3759286AE9CE FF
Malicious:	false
Reputation:	low
Preview:	0\r..m....._keyhttps://abs.twimg.com/responsive-web/client-web/shared~loader.Typeahead~bundle.Communities~bundle.Explore~bundle.UserLists.e887e325.js .https://twitter.com/.W..+/.....C.o.sF....\..|;..O^"x.6.{.....A..Eo.....P.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b882df6ca19dc297_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	5.5112183935592896
Encrypted:	false
SSDEEP:	6:mAdYGLDlynflG9LYAj2wlyhl/gwWtsEiqnxK4BlhK6t:IflGpYA/ghl//WtsRqn3N
MD5:	17D49B91F37A2FC89A225666C74481CA
SHA1:	7334A99246FAF482AD088A46BA2A39A7E31F247E
SHA-256:	39DF2D1E9F9ECA200039C960D0852675E4AA0E51A8656BA155A1AE0520255B83
SHA-512:	0FE629B13B6F07247EEDBC2EF567A137D4B554ED4C178FD0F73EDD1D5F0EB42160A6C1CE98D9A81B8700453785A4D896CD58DE3490F12047728086DC48F5A5D B

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b882df6ca19dc297_0	
Malicious:	false
Reputation:	low
Preview:	0\r..m.....d....Y....._keyhttps://www.instagram.com/static/bundles/es6/Consumer.js/972fab3a992c.js .https://instagram.com/..q..+/.....i.....'....(^.JAb.8..z..\..U....Q.|..A..Eo....._.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\b94da95239050458_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	236
Entropy (8bit):	5.612312254254818
Encrypted:	false
SSDEEP:	6:m7gEYk+f2pombM7hmJ2Aj/glXqyfRzhOj0rlK6t:gN++amckJDXayfl0r
MD5:	A543961EFFBBC4B3C6C74A0E14F7D020
SHA1:	0FD211A8C7C8D5E0067519E56F4263EE19DDFAA7
SHA-256:	33BAAC9DCA9468B468A892B6BCAFCA692695B48EBDE6DE6685C8EA82592F00CC
SHA-512:	EAB1443B68FD25F42EE2C92145BB135B5C433B692C7DA049E928F8003FE1A83EFF464FBAA753E733B221264F7CC22AC8121D8BCC4245931D4AF468F1B426068
Malicious:	false
Reputation:	low
Preview:	0\r..m.....h.....46...._keyhttps://static.xx.fbcdn.net/rsrc.php/v3/yp/r/XpFprvKSai6.js?_nc_x=Ij3Wp8lg5Kz .https://facebook.com/C..-.+/.....X..s...FQ...p4..K..-.i..r...D..b.A..Eo.....A..Eo.....

Static File Info

No static file info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:33:57.658428907 CEST	192.168.2.3	8.8.8.8	0x1a69	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:33:57.662437916 CEST	192.168.2.3	8.8.8.8	0xedaa	Standard query (0)	www.joyeriasosa.com.py	A (IP address)	IN (0x0001)
Sep 27, 2021 20:33:57.680425882 CEST	192.168.2.3	8.8.8.8	0x8576	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:05.080571890 CEST	192.168.2.3	8.8.8.8	0x2b7e	Standard query (0)	www.canadapost.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:05.393745899 CEST	192.168.2.3	8.8.8.8	0x9b8b	Standard query (0)	www.canadapost-postescanada.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:06.388298035 CEST	192.168.2.3	8.8.8.8	0x87b	Standard query (0)	siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:07.889863968 CEST	192.168.2.3	8.8.8.8	0x7d56	Standard query (0)	zn0xleir6swszany9-canadapostdigital.siteintercept.qualtrics.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:07.904360056 CEST	192.168.2.3	8.8.8.8	0xd052	Standard query (0)	sso-osu.canadapost-postescanada.ca	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:34:12.301143885 CEST	192.168.2.3	8.8.8.8	0x1fa1	Standard query (0)	sso-osu.canadapost-postescanada.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:12.303056002 CEST	192.168.2.3	8.8.8.8	0xbc8e	Standard query (0)	www.joyeriasosa.com.py	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:12.509995937 CEST	192.168.2.3	8.8.8.8	0x40d1	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:26.698777914 CEST	192.168.2.3	8.8.8.8	0xd7e8	Standard query (0)	undefined.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:43.560533047 CEST	192.168.2.3	8.8.8.8	0x7988	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:43.560561895 CEST	192.168.2.3	8.8.8.8	0x8e92	Standard query (0)	assets.adobedtm.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.600243092 CEST	192.168.2.3	8.8.8.8	0x1c9f	Standard query (0)	dpm.demdex.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.932517052 CEST	192.168.2.3	8.8.8.8	0x2fbb	Standard query (0)	connect.facebook.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.934195995 CEST	192.168.2.3	8.8.8.8	0xbdf5	Standard query (0)	static.ads-twitter.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:45.999835014 CEST	192.168.2.3	8.8.8.8	0x4ae1	Standard query (0)	canadapost.demdex.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.008858919 CEST	192.168.2.3	8.8.8.8	0xd521	Standard query (0)	sslstats.canadapost.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.118586063 CEST	192.168.2.3	8.8.8.8	0xc0e1	Standard query (0)	cm.everesttech.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.636924028 CEST	192.168.2.3	8.8.8.8	0x7a52	Standard query (0)	analytics.twitter.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.639736891 CEST	192.168.2.3	8.8.8.8	0xb3d6	Standard query (0)	t.co	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.800609112 CEST	192.168.2.3	8.8.8.8	0x6d34	Standard query (0)	9852050.fls.doubleclick.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.916457891 CEST	192.168.2.3	8.8.8.8	0x19dc	Standard query (0)	6048943.fls.doubleclick.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.958575964 CEST	192.168.2.3	8.8.8.8	0xea91	Standard query (0)	googleads.g.doubleclick.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.212965965 CEST	192.168.2.3	8.8.8.8	0xcd8c	Standard query (0)	adservice.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.310928106 CEST	192.168.2.3	8.8.8.8	0x7d1a	Standard query (0)	www.facebook.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.435825109 CEST	192.168.2.3	8.8.8.8	0x41c5	Standard query (0)	adservice.google.ch	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:48.628680944 CEST	192.168.2.3	8.8.8.8	0xfc83	Standard query (0)	www.google.ch	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:49.585244894 CEST	192.168.2.3	8.8.8.8	0xd80e	Standard query (0)	www.canadapost-postescanada.ca	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:51.901335955 CEST	192.168.2.3	8.8.8.8	0x97fd	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:52.166702986 CEST	192.168.2.3	8.8.8.8	0x806f	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:53.969491005 CEST	192.168.2.3	8.8.8.8	0xfa83	Standard query (0)	static.xx.fbcdn.net	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:53.982089996 CEST	192.168.2.3	8.8.8.8	0x8d0f	Standard query (0)	facebook.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:54.930268049 CEST	192.168.2.3	8.8.8.8	0x6345	Standard query (0)	twitter.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.221396923 CEST	192.168.2.3	8.8.8.8	0xf18a	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.243489981 CEST	192.168.2.3	8.8.8.8	0x4e76	Standard query (0)	api.twitter.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.243792057 CEST	192.168.2.3	8.8.8.8	0x2ea5	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.246485949 CEST	192.168.2.3	8.8.8.8	0x671d	Standard query (0)	video.twimg.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:57.637739897 CEST	192.168.2.3	8.8.8.8	0xb75c	Standard query (0)	abs.twimg.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:58.968427896 CEST	192.168.2.3	8.8.8.8	0x844d	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:59.352082014 CEST	192.168.2.3	8.8.8.8	0x2eff	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:01.574044943 CEST	192.168.2.3	8.8.8.8	0xeb75	Standard query (0)	www.instagram.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:02.837346077 CEST	192.168.2.3	8.8.8.8	0x3ba4	Standard query (0)	pbs.twimg.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 20:35:02.999962091 CEST	192.168.2.3	8.8.8.8	0x2f12	Standard query (0)	www.linkedin.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:04.212171078 CEST	192.168.2.3	8.8.8.8	0x1c52	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:04.947318077 CEST	192.168.2.3	8.8.8.8	0x475a	Standard query (0)	platform.linkedin.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:05.599908113 CEST	192.168.2.3	8.8.8.8	0x27b3	Standard query (0)	static-exp1.licdn.com	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:07.408952951 CEST	192.168.2.3	8.8.8.8	0xbfa1	Standard query (0)	play.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:33:57.693983078 CEST	8.8.8.8	192.168.2.3	0x8576	No error (0)	accounts.google.com		172.217.168.13	A (IP address)	IN (0x0001)
Sep 27, 2021 20:33:57.697438002 CEST	8.8.8.8	192.168.2.3	0x1a69	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:33:57.697438002 CEST	8.8.8.8	192.168.2.3	0x1a69	No error (0)	clients.l.google.com		172.217.168.46	A (IP address)	IN (0x0001)
Sep 27, 2021 20:33:57.800726891 CEST	8.8.8.8	192.168.2.3	0xedaa	No error (0)	www.joyerias osa.com.py		167.172.159.206	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:01.237009048 CEST	8.8.8.8	192.168.2.3	0xab1c	No error (0)	gstaticadssl.l.google.com		172.217.168.67	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:05.141032934 CEST	8.8.8.8	192.168.2.3	0x2b7e	No error (0)	www.canadapost.ca	www.canadapost.ca.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:05.412592888 CEST	8.8.8.8	192.168.2.3	0x9b8b	No error (0)	www.canadapost-postescanada.ca	www.canadapost-postescanada.ca.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:06.406918049 CEST	8.8.8.8	192.168.2.3	0x87b	No error (0)	siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:06.406918049 CEST	8.8.8.8	192.168.2.3	0x87b	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:07.909447908 CEST	8.8.8.8	192.168.2.3	0x7d56	No error (0)	zn0xleir6swszany9-canadapostdigital.siteintercept.qualtrics.com	siteintercept.qprod2.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:07.909447908 CEST	8.8.8.8	192.168.2.3	0x7d56	No error (0)	siteintercept.qprod2.net	prodlb.siteintercept.qualtrics.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:07.961576939 CEST	8.8.8.8	192.168.2.3	0xd052	No error (0)	sso-osu.canadapost-postescanada.ca	sso.canadapost.ca		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:07.961576939 CEST	8.8.8.8	192.168.2.3	0xd052	No error (0)	sso.canadapost.ca		198.33.200.21	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:12.329129934 CEST	8.8.8.8	192.168.2.3	0x1fa1	No error (0)	sso-osu.canadapost-postescanada.ca	sso.canadapost.ca		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:12.329129934 CEST	8.8.8.8	192.168.2.3	0x1fa1	No error (0)	sso.canadapost.ca		198.33.200.21	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:12.498440981 CEST	8.8.8.8	192.168.2.3	0xbc8e	No error (0)	www.joyerias osa.com.py		167.172.159.206	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:12.552300930 CEST	8.8.8.8	192.168.2.3	0x40d1	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:12.552300930 CEST	8.8.8.8	192.168.2.3	0x40d1	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.1	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:26.726380110 CEST	8.8.8.8	192.168.2.3	0xd7e8	No error (0)	undefined.ca		168.235.64.196	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:43.583292007 CEST	8.8.8.8	192.168.2.3	0x8e92	No error (0)	assets.adobedtm.com	cn-assets.adobedtm.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:34:43.590035915 CEST	8.8.8.8	192.168.2.3	0x7988	No error (0)	www.google.com		172.217.168.36	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dpm.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.154.124.189	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.214.44.171	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.48.145.41	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.248.38.136	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.208.156.200	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.194.53.150	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.171.163.246	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.620424032 CEST	8.8.8.8	192.168.2.3	0x1c9f	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.247.192.108	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.631499052 CEST	8.8.8.8	192.168.2.3	0x1d00	No error (0)	www-google-tagmanager.l.google.com		172.217.168.40	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.946681023 CEST	8.8.8.8	192.168.2.3	0x2fbb	No error (0)	connect.facebook.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:44.946681023 CEST	8.8.8.8	192.168.2.3	0x2fbb	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:44.948395014 CEST	8.8.8.8	192.168.2.3	0xbdf5	No error (0)	static.ads-twitter.com	platform.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:44.948395014 CEST	8.8.8.8	192.168.2.3	0xbdf5	No error (0)	platform.twitter.map.fastly.net		199.232.136.157	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	canadapost.demdex.net	gslb-2.demdex.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	gslb-2.demdex.net	edge-irl1.demdex.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	edge-irl1.demdex.net	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.203.8.109	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.248.156.174	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.49.107.116	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		34.247.192.108	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		18.200.208.216	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		54.247.138.82	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		3.248.38.136	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.022358894 CEST	8.8.8.8	192.168.2.3	0x4ae1	No error (0)	dcs-edge-irl1-876252164.eu-west-1.elb.amazonaws.com		52.30.146.101	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.050857067 CEST	8.8.8.8	192.168.2.3	0xd521	No error (0)	sslstats.canadapost.ca	canadapost.ca.ssl.d1.sc.omtrdc.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.050857067 CEST	8.8.8.8	192.168.2.3	0xd521	No error (0)	canadapost.ca.ssl.d1.sc.omtrdc.net		13.36.218.177	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.050857067 CEST	8.8.8.8	192.168.2.3	0xd521	No error (0)	canadapost.ca.ssl.d1.sc.omtrdc.net		15.236.176.210	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.050857067 CEST	8.8.8.8	192.168.2.3	0xd521	No error (0)	canadapost.ca.ssl.d1.sc.omtrdc.net		15.188.95.229	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.156872034 CEST	8.8.8.8	192.168.2.3	0xc0e1	No error (0)	cm.everesttech.net	cm.everesttech.net.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	analytics.twitter.com	ads.twitter.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	ads.twitter.com	s.twitter.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	s.twitter.com		104.244.42.131	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	s.twitter.com		104.244.42.195	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	s.twitter.com		104.244.42.67	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.649506092 CEST	8.8.8.8	192.168.2.3	0x7a52	No error (0)	s.twitter.com		104.244.42.3	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.651664972 CEST	8.8.8.8	192.168.2.3	0xb3d6	No error (0)	t.co		104.244.42.133	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.651664972 CEST	8.8.8.8	192.168.2.3	0xb3d6	No error (0)	t.co		104.244.42.197	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.651664972 CEST	8.8.8.8	192.168.2.3	0xb3d6	No error (0)	t.co		104.244.42.69	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.651664972 CEST	8.8.8.8	192.168.2.3	0xb3d6	No error (0)	t.co		104.244.42.5	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.828010082 CEST	8.8.8.8	192.168.2.3	0x6d34	No error (0)	9852050.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.828010082 CEST	8.8.8.8	192.168.2.3	0x6d34	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:46.943985939 CEST	8.8.8.8	192.168.2.3	0x19dc	No error (0)	6048943.fls.doubleclick.net	dart.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:46.943985939 CEST	8.8.8.8	192.168.2.3	0x19dc	No error (0)	dart.l.doubleclick.net		142.250.203.102	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:34:46.986428022 CEST	8.8.8.8	192.168.2.3	0xea91	No error (0)	googleads.g.doubleclick.net		142.250.203.98	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.247909069 CEST	8.8.8.8	192.168.2.3	0xcd8c	No error (0)	adservice.google.com		172.217.168.34	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.349282026 CEST	8.8.8.8	192.168.2.3	0x7d1a	No error (0)	www.facebook.com	star-mini.c10r.facebook.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:47.349282026 CEST	8.8.8.8	192.168.2.3	0x7d1a	No error (0)	star-mini.c10r.facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:47.476978064 CEST	8.8.8.8	192.168.2.3	0x41c5	No error (0)	adservice.google.ch	pagead46.l.doubleclick.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:47.476978064 CEST	8.8.8.8	192.168.2.3	0x41c5	No error (0)	pagead46.l.doubleclick.net		172.217.168.34	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:48.656085014 CEST	8.8.8.8	192.168.2.3	0xfc83	No error (0)	www.google.ch		216.58.215.227	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:49.632443905 CEST	8.8.8.8	192.168.2.3	0xd80e	No error (0)	www.canadapost-postescanada.ca	www.canadapost-postescanada.ca.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:51.923091888 CEST	8.8.8.8	192.168.2.3	0x97fd	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:51.923091888 CEST	8.8.8.8	192.168.2.3	0x97fd	No error (0)	scontent.xx.fbcdn.net		157.240.17.15	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:52.193635941 CEST	8.8.8.8	192.168.2.3	0x806f	No error (0)	facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:53.983057022 CEST	8.8.8.8	192.168.2.3	0xfa83	No error (0)	static.xx.fbcdn.net	scontent.xx.fbcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:53.983057022 CEST	8.8.8.8	192.168.2.3	0xfa83	No error (0)	scontent.xx.fbcdn.net		157.240.27.27	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:54.003370047 CEST	8.8.8.8	192.168.2.3	0x8d0f	No error (0)	facebook.com		157.240.17.35	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:54.943507910 CEST	8.8.8.8	192.168.2.3	0x6345	No error (0)	twitter.com		104.244.42.65	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:54.943507910 CEST	8.8.8.8	192.168.2.3	0x6345	No error (0)	twitter.com		104.244.42.129	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.233971119 CEST	8.8.8.8	192.168.2.3	0xf18a	No error (0)	abs.twimg.com	twimg.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.233971119 CEST	8.8.8.8	192.168.2.3	0xf18a	No error (0)	twimg.twitter.map.fastly.net		151.101.12.159	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.255327940 CEST	8.8.8.8	192.168.2.3	0x4e76	No error (0)	api.twitter.com	tpop-api.twitter.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.255327940 CEST	8.8.8.8	192.168.2.3	0x4e76	No error (0)	tpop-api.twitter.com		104.244.42.130	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.255327940 CEST	8.8.8.8	192.168.2.3	0x4e76	No error (0)	tpop-api.twitter.com		104.244.42.66	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.255327940 CEST	8.8.8.8	192.168.2.3	0x4e76	No error (0)	tpop-api.twitter.com		104.244.42.194	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.255327940 CEST	8.8.8.8	192.168.2.3	0x4e76	No error (0)	tpop-api.twitter.com		104.244.42.2	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.257324934 CEST	8.8.8.8	192.168.2.3	0x2ea5	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.257324934 CEST	8.8.8.8	192.168.2.3	0x2ea5	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.257324934 CEST	8.8.8.8	192.168.2.3	0x2ea5	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 20:34:55.257324934 CEST	8.8.8.8	192.168.2.3	0x2ea5	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:55.264003992 CEST	8.8.8.8	192.168.2.3	0x671d	No error (0)	video.twimg.com	cs296.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.264003992 CEST	8.8.8.8	192.168.2.3	0x671d	No error (0)	cs296.wpc.edgecastcdn.net	cs2-wpc.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.264003992 CEST	8.8.8.8	192.168.2.3	0x671d	No error (0)	cs2-wpc-eu.8315.ecdns.net	cs531.wpc.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:55.264003992 CEST	8.8.8.8	192.168.2.3	0x671d	No error (0)	cs531.wpc.edgecastcdn.net		192.229.220.133	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:57.652201891 CEST	8.8.8.8	192.168.2.3	0xb75c	No error (0)	abs.twimg.com	twimg.twitter.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:57.652201891 CEST	8.8.8.8	192.168.2.3	0xb75c	No error (0)	twimg.twitter.map.fastly.net		151.101.12.159	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:58.551106930 CEST	8.8.8.8	192.168.2.3	0x190f	No error (0)	www-google-analytics.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:58.989042997 CEST	8.8.8.8	192.168.2.3	0x844d	No error (0)	www.instagram.com	z-p42-instagram.c10r.instagram.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:34:58.989042997 CEST	8.8.8.8	192.168.2.3	0x844d	No error (0)	z-p42-instagram.c10r.instagram.com		157.240.17.174	A (IP address)	IN (0x0001)
Sep 27, 2021 20:34:59.378173113 CEST	8.8.8.8	192.168.2.3	0x2eff	No error (0)	accounts.google.com		172.217.168.13	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:01.595065117 CEST	8.8.8.8	192.168.2.3	0xeb75	No error (0)	www.instagram.com	z-p42-instagram.c10r.instagram.com		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:01.595065117 CEST	8.8.8.8	192.168.2.3	0xeb75	No error (0)	z-p42-instagram.c10r.instagram.com		157.240.17.174	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:02.855592966 CEST	8.8.8.8	192.168.2.3	0x3ba4	No error (0)	pbs.twimg.com	cs196.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:02.855592966 CEST	8.8.8.8	192.168.2.3	0x3ba4	No error (0)	cs196.wac.edgecastcdn.net	cs2-wac.apr-8315.edgecastdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:02.855592966 CEST	8.8.8.8	192.168.2.3	0x3ba4	No error (0)	cs2-wac-eu.8315.ecdns.net	cs45.wac.edgecastcdn.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:02.855592966 CEST	8.8.8.8	192.168.2.3	0x3ba4	No error (0)	cs45.wac.edgecastcdn.net		93.184.220.70	A (IP address)	IN (0x0001)
Sep 27, 2021 20:35:03.012443066 CEST	8.8.8.8	192.168.2.3	0x2f12	No error (0)	www.linkedin.com	www-linkedin-com.l-0005.l-msedge.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:04.242552996 CEST	8.8.8.8	192.168.2.3	0x1c52	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:04.970531940 CEST	8.8.8.8	192.168.2.3	0x475a	No error (0)	platform.linkedin.com	2-01-2c3e-0055.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:05.640223026 CEST	8.8.8.8	192.168.2.3	0x27b3	No error (0)	static-exp1.licdn.com	2-01-2c3e-003d.cdx.cedexis.net		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 20:35:07.436649084 CEST	8.8.8.8	192.168.2.3	0xbfa1	No error (0)	play.google.com		172.217.168.14	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- clients2.google.com
- www.joyeriasosa.com.py
- accounts.google.com
- https:
  - sso-osu.canadapost-postescanada.ca
- clients2.googleusercontent.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49751	172.217.168.46	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:58 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%3Dnmmhkkegccagdldgiimedpiccmgmieda%26v% 3D0.0.0.0%26installedby%3Dother%26uc%26ping%3Dr%253D-1%2526e%253D1&x=id%3Dpkedcjkdefgpdelp bcmbmeomcjbeemfm%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: nmmhkkegccagdldgiimedpiccmgmieda,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
2021-09-27 18:33:58 UTC	1	IN	HTTP/1.1 200 OK Content-Security-Policy: script-src 'report-sample' 'nonce-ccqUXA9ytWnKnDsHEo2sfg' '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: Mon, 27 Sep 2021 18:33:58 GMT Content-Type: text/xml; charset=UTF-8 X-Daynum: 5383 X-Daystart: 41638 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-T051=":443"; ma=2592000,h3-Q050=":443"; m a=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-09-27 18:33:58 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 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 33 38 33 22 20 65 6c 61 70 73 65 64 5f 73 65 63 6f 6e 64 73 3d 22 34 31 36 33 38 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="5383" elapsed_seconds="41638"/><app appid="nmmhkkegccagdld giimedpiccmgmieda" cohort="1::" cohortname=""
2021-09-27 18:33:58 UTC	3	IN	Data Raw: 77 79 4d 45 52 45 53 45 5a 47 56 6d 4a 6e 51 51 2f 31 2e 30 2e 30 2e 36 5f 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 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 3 4 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 Data Ascii: wyMERESEZGVmJnQQ/1.0.0.6_nmmhkkegccagdldgiimedpiccmgmieda.crx" fp="1.81e3a4d43a73699e1b7 781723f56b8717175c536685c5450122b30789464ad82" hash_sha256="81e3a4d43a73699e1b7781723f56b8717175c536 685c5450122b30789464ad82" protected="0" size="248531" status="ok" v
2021-09-27 18:33:58 UTC	4	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49754	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:58 UTC	0	OUT	GET /ca/ HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-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
2021-09-27 18:33:58 UTC	5	IN	HTTP/1.1 302 Found Date: Mon, 27 Sep 2021 18:33:58 GMT Server: Apache/2.4.29 (Ubuntu) Location: restor/index.php?id=40382411219 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49769	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	368	OUT	GET /ca/restor/assets/satelliteLib-f2fc6f00da802a0747b6ffed3c12e3931bfca496.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:00 UTC	448	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:00 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:00 UTC	448	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49770	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	497	OUT	GET /ca/restor/assets/9-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	590	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:00 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:00 UTC	590	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49771	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	606	OUT	GET /ca/restor/assets/3-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:00 UTC	689	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:00 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:00 UTC	690	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49772	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	638	OUT	GET /ca/restor/assets/11-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:00 UTC	706	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:00 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	707	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49773	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	690	OUT	GET /ca/restor/assets/15.e8db891fc03030df5677.chunk.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	768	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	768	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49774	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	707	OUT	GET /ca/restor/assets/1.9bf84a1119dc09839d2c.chunk.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	769	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	769	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49775	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	769	OUT	GET /ca/restor/assets/f(1).txt HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	771	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	771	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49776	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	769	OUT	GET /ca/restor/assets/f(2).txt HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	771	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	771	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49777	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	770	OUT	GET /ca/restor/assets/api.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	772	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	772	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49778	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	770	OUT	GET /ca/restor/assets/f.txt HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	773	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	773	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49753	172.217.168.13	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:58 UTC	1	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
2021-09-27 18:33:58 UTC	1	OUT	Data Raw: 20 Data Ascii:
2021-09-27 18:33:58 UTC	4	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: Mon, 27 Sep 2021 18:33:58 GMT Strict-Transport-Security: max-age=31536000 Cross-Origin-Resource-Policy: cross-origin Cross-Origin-Opener-Policy: same-origin Content-Security-Policy: script-src 'report-sample' 'nonce-0/AnLDjcB6W/NmMAYZho5A' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/IdentityListAccountsHttp/cspreport;worker-src 'self' Content-Security-Policy: script-src 'nonce-0/AnLDjcB6W/NmMAYZho5A' '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 Server: ESF X-XSS-Protection: 0 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-09-27 18:33:58 UTC	5	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",[]]
2021-09-27 18:33:58 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49781	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	772	OUT	GET /ca/restor/assets/js HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	773	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	773	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49782	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	774	OUT	GET /ca/restor/assets/satelliteLib-f2fc6f00da802a0747b6ffed3c12e3931bfca496.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:01 UTC	775	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:01 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:01 UTC	775	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49783	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	774	OUT	GET /ca/restor/assets/runtime-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:02 UTC	775	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:02 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:02 UTC	775	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49784	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:02 UTC	775	OUT	GET /ca/restor/assets/9-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:02 UTC	776	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:02 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:02 UTC	777	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49785	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:02 UTC	776	OUT	GET /ca/restor/assets/polyfills-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:02 UTC	777	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:02 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:02 UTC	777	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49788	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:02 UTC	777	OUT	GET /ca/restor/assets/3-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:02 UTC	778	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:02 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:02 UTC	778	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49787	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:02 UTC	778	OUT	GET /ca/restor/assets/main-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:02 UTC	779	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:02 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:02 UTC	779	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49791	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	779	OUT	GET /ca/restor/assets/11-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:03 UTC	780	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:03 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:03 UTC	780	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49792	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	780	OUT	GET /ca/restor/assets/foundation.min.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:03 UTC	781	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:03 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "3211e-5c26848200a80" Accept-Ranges: bytes Content-Length: 205086 Vary: Accept-Encoding Connection: close Content-Type: application/javascript
2021-09-27 18:34:03 UTC	781	IN	Data Raw: 2f 2a 0d 0a 20 2a 20 46 6f 75 6e 64 61 74 69 6f 6e 20 52 65 73 70 6f 6e 73 69 76 65 20 4c 69 62 72 61 72 79 0d 0a 20 2a 20 68 74 74 70 3a 2f 2f 66 6f 75 6e 64 61 74 69 6f 6e 2e 7a 75 72 62 2e 63 6f 6d 0d 0a 20 2a 20 43 6f 70 79 72 69 67 68 74 20 32 30 31 34 2c 20 5a 55 52 42 0d 0a 20 2a 20 46 72 65 65 20 74 6f 20 75 73 65 20 75 6e 64 65 72 20 74 68 65 20 4d 49 54 20 6c 69 63 65 6e 73 65 2e 0d 0a 20 2a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 6f 70 65 6e 73 6f 75 72 63 65 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 73 2f 6d 69 74 2d 6c 69 63 65 6e 73 65 2e 70 68 70 0d 0a 2a 2f 0d 0a 0d 0a 2f 2a 0d 0a 20 2a 20 44 4f 20 4e 4f 54 20 52 45 4d 4f 56 45 20 2d 20 4e 45 45 44 45 44 20 46 4f 52 20 46 4f 55 4e 44 41 54 49 4f 4e 20 35 20 4c 41 54 45 53 54 20 55 50 47 52 41 44 45 Data Ascii: /* * Foundation Responsive Library * http://foundation.zurb.com * Copyright 2014, ZURB * Free to use under the MIT license. * http://www.opensource.org/licenses/mit-license.php*//* * DO NOT REMOVE - NEEDED FOR FOUNDATION 5 LATEST UPGRADE
2021-09-27 18:34:03 UTC	797	IN	Data Raw: 70 6c 69 74 28 27 3a 27 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 70 20 3d 20 5b 70 5b 30 5d 2c 20 70 2e 73 6c 69 63 65 28 31 29 2e 6a 6f 69 6e 28 27 3a 27 29 5d 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 69 66 20 28 2f 74 72 75 65 2f 69 2e 74 65 73 74 28 70 5b 31 5d 29 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 5b 31 5d 20 3d 20 74 72 75 65 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 69 66 20 28 2f 66 61 6c 73 65 2f 69 2e 74 65 73 74 28 70 5b 31 5d 29 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 5b 31 5d 20 3d 20 66 61 6c 73 65 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 69 66 20 28 69 73 4e 75 6d 62 65 72 28 70 5b 31 5d 29 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 Data Ascii: plit(':'); p = [p[0], p.slice(1).join(':')]; if (/true/i.test(p[1])) { p[1] = true; } if (/false/i.test(p[1])) { p[1] = false; } if (isNumber(p[1])) {

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	814	IN	Data Raw: 20 61 72 72 61 79 20 6f 66 20 65 78 70 6f 73 65 20 65 6c 65 6d 65 6e 74 73 0d 0a 20 20 20 20 20 20 74 69 70 5f 61 6e 69 6d 61 74 69 6f 6e 5f 66 61 64 65 5f 73 70 65 65 64 20 3a 20 33 30 30 2c 20 20 20 20 20 20 20 2f 2f 20 77 68 65 6e 20 74 69 70 41 6e 69 6d 61 74 69 6f 6e 20 3d 20 27 66 61 64 65 27 20 74 68 69 73 20 69 73 20 73 70 65 65 64 20 69 6e 20 6d 69 6c 6c 69 73 65 63 6f 6e 64 73 20 66 6f 72 20 74 68 65 20 74 72 61 6e 73 69 74 69 6f 6e 0d 0a 20 20 20 20 20 20 63 6f 6f 6b 69 65 5f 6d 6f 6e 73 74 65 72 20 20 20 20 20 20 20 20 20 20 20 3a 20 66 61 6c 73 65 2c 20 20 20 20 20 20 2f 2f 20 74 72 75 65 20 6f 72 20 66 61 6c 73 65 20 74 6f 20 63 6f 6e 74 72 6f 6c 20 77 68 65 74 68 65 72 20 63 6f 6f 6b 69 65 73 20 61 72 65 20 75 73 65 64 0d 0a 20 20 20 20 20 20 Data Ascii: array of expose elements tip_animation_fade_speed : 300, // when tipAnimation = 'fade' this is speed in milliseconds for the transition cookie_monster : false, // true or false to control whether cookies are used
2021-09-27 18:34:03 UTC	831	IN	Data Raw: 20 69 66 20 28 74 6f 67 67 6c 65 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 74 68 69 73 2e 73 65 74 74 69 6e 67 73 2e 24 6e 65 78 74 5f 74 69 70 2e 63 73 73 28 27 76 69 73 69 62 69 6c 69 74 79 27 2c 20 27 68 69 64 64 65 6e 27 29 3b 0d 0a 20 20 20 20 20 20 20 20 74 68 69 73 2e 73 65 74 74 69 6e 67 73 2e 24 6e 65 78 74 5f 74 69 70 2e 73 68 6f 77 28 29 3b 0d 0a 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 69 66 20 28 21 2f 62 6f 64 79 2f 69 2e 74 65 73 74 28 74 68 69 73 2e 73 65 74 74 69 6e 67 73 2e 24 74 61 72 67 65 74 2e 73 65 6c 65 63 74 6f 72 29 29 20 7b 0d 0a 20 20 20 20 20 20 76 61 72 20 74 6f 70 41 64 6a 75 73 74 6d 65 6e 74 20 3d 20 74 68 69 73 2e 73 65 74 74 69 6e 67 73 2e 74 69 70 5f 73 65 74 74 69 6e 67 73 2e 74 69 70 41 64 6a 75 73 Data Ascii: if (toggle) { this.settings.$next_tip.css('visibility', 'hidden'); this.settings.$next_tip.show(); } if (!/body/i.test(this.settings.$target.selector)) { var topAdjustment = this.settings.tip_settings.tipAdjus
2021-09-27 18:34:03 UTC	847	IN	Data Raw: 64 2c 20 6f 70 74 69 6f 6e 73 29 3b 0d 0a 20 20 20 20 7d 2c 0d 0a 0d 0a 20 20 20 20 65 76 65 6e 74 73 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 73 63 6f 70 65 29 20 7b 0d 0a 20 20 20 20 20 20 76 61 72 20 73 65 6c 66 20 3d 20 74 68 69 73 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 53 20 3d 20 73 65 6c 66 2e 53 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 53 28 74 68 69 73 2e 73 63 6f 70 65 29 0d 0a 20 20 20 20 20 20 20 20 20 20 2e 6f 66 66 28 27 2e 64 72 6f 70 64 6f 77 6e 27 29 0d 0a 20 20 20 20 20 20 20 20 20 20 2e 6f 6e 28 27 63 6c 69 63 6b 2e 66 6e 64 74 6e 2e 64 72 6f 70 64 6f 77 6e 27 2c 20 27 5b 27 20 2b 20 74 68 69 73 2e 61 74 74 72 5f 6e 61 6d 65 28 29 20 2b 20 27 5d 27 2c 20 66 75 6e 63 74 69 6f 6e 20 28 65 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 76 61 72 20 73 65 74 74 69 Data Ascii: d, options); }, events : function (scope) { var self = this, S = self.S; S(this.scope) .off('.dr opdown') .on('click.fndtn.dropdown', '[' + this.attr_name() + ']', function (e) { var setti
2021-09-27 18:34:03 UTC	863	IN	Data Raw: 20 20 20 20 20 6e 65 78 74 20 3d 20 63 75 72 72 65 6e 74 2e 6e 65 78 74 28 27 6c 69 27 29 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 74 74 69 6e 67 73 20 3d 20 63 75 72 72 65 6e 74 2e 63 6c 6f 73 65 73 74 28 27 5b 27 20 2b 20 73 65 6c 66 2e 61 74 74 72 5f 6e 61 6d 65 28 29 20 2b 20 27 5d 27 29 2e 64 61 74 61 28 73 65 6c 66 2e 61 74 74 72 5f 6e 61 6d 65 28 74 72 75 65 29 20 2b 20 27 2d 69 6e 69 74 27 29 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 6d 61 67 65 20 3d 20 53 28 65 2e 74 61 72 67 65 74 29 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 65 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 66 20 28 21 73 65 74 74 69 6e 67 73 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 Data Ascii: next = current.next('li'), settings = current.closest('[' + self.attr_name() + ']').data(self.attr _name(true) + '-init'), image = S(e.target); e.preventDefault(); if (!settings) {
2021-09-27 18:34:03 UTC	879	IN	Data Raw: 73 65 74 74 69 6e 67 73 2e 62 75 6c 6c 65 74 73 5f 61 63 74 69 76 65 5f 63 6c 61 73 73 29 3b 0d 0a 20 20 20 20 20 20 6c 69 6e 6b 2e 61 64 64 43 6c 61 73 73 28 73 65 74 74 69 6e 67 73 2e 62 75 6c 6c 65 74 73 5f 61 63 74 69 76 65 5f 63 6c 61 73 73 29 3b 0d 0a 20 20 20 20 7d 3b 0d 0a 0d 0a 20 20 20 20 73 65 6c 66 2e 62 75 69 6c 64 5f 6d 61 72 6b 75 70 20 3d 20 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 73 6c 69 64 65 73 5f 63 6f 6e 74 61 69 6e 65 72 2e 77 72 61 70 28 27 3c 64 69 76 20 63 6c 61 73 73 3d 22 27 20 2b 20 73 65 74 74 69 6e 67 73 2e 63 6f 6e 74 61 69 6e 65 72 5f 63 6c 61 73 73 20 2b 20 27 22 3e 3c 2f 64 69 76 3e 27 29 3b 0d 0a 20 20 20 20 20 20 63 6f 6e 74 61 69 6e 65 72 20 3d 20 73 6c 69 64 65 73 5f 63 6f 6e 74 61 69 6e 65 72 Data Ascii: settings.bullets_active_class); link.addClass(settings.bullets_active_class); }; self.build_markup = functi on () { slides_container.wrap(' '); container = slides_container
2021-09-27 18:34:04 UTC	896	IN	Data Raw: 5f 63 6c 61 73 73 20 2b 20 72 69 67 68 74 5f 70 6f 73 74 66 69 78 2c 20 73 65 6c 66 2e 67 65 74 5f 77 72 61 70 70 65 72 28 65 29 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 72 65 6e 74 2e 70 61 72 65 6e 74 28 29 2e 72 65 6d 6f 76 65 43 6c 61 73 73 28 6d 6f 76 65 5f 63 6c 61 73 73 20 2b 20 72 69 67 68 74 5f 70 6f 73 74 66 69 78 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 20 65 6c 73 65 20 69 66 20 28 53 28 74 68 69 73 29 2e 70 61 72 65 6e 74 28 29 2e 68 61 73 43 6c 61 73 73 28 27 68 61 73 2d 73 75 62 6d 65 6e 75 27 29 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 65 2e 70 72 65 76 65 6e 74 44 65 66 61 75 6c 74 28 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 28 74 68 69 73 29 2e 73 69 62 6c 69 6e 67 73 28 27 2e 6c 65 66 74 2d 73 75 62 Data Ascii: _class + right_postfix, self.get_wrapper(e)); parent.parent().removeClass(move_class + right_postfix); } else if (S(this).parent().hasClass('has-submenu')) { e.preventDefault(); S(this).siblings('.left-sub
2021-09-27 18:34:04 UTC	912	IN	Data Raw: 29 2c 20 73 65 74 74 69 6e 67 73 2e 61 6e 69 6d 61 74 69 6f 6e 5f 73 70 65 65 64 20 2f 20 32 29 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 69 66 20 28 61 6e 69 6d 44 61 74 61 2e 66 61 64 65 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 73 73 2e 74 6f 70 20 3d 20 24 28 77 69 6e 64 6f 77 29 2e 73 63 72 6f 6c 6c 54 6f 70 28 29 20 2b 20 65 6c 2e 64 61 74 61 28 27 63 73 73 2d 74 6f 70 27 29 20 2b 20 27 70 78 27 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 65 6e 64 5f 63 73 73 20 3d 20 7b 6f 70 61 63 69 74 79 3a 20 31 7d 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 72 65 74 75 72 6e 20 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 72 65 74 75 72 6e 20 65 6c Data Ascii:), settings.animation_speed / 2); } if (animData.fade) { css.top = $(window).scrollTop() + el.d ata('css-top') + 'px'; var end_css = {opacity: 1}; return setTimeout(function () { return el
2021-09-27 18:34:04 UTC	928	IN	Data Raw: 23 27 29 2e 6a 6f 69 6e 28 27 27 29 2c 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 61 72 67 65 74 20 3d 20 24 28 27 61 5b 6e 61 6d 65 3d 22 27 20 2b 20 68 61 73 68 20 2b 20 27 22 5d 27 29 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 69 66 20 28 74 61 72 67 65 74 2e 6c 65 6e 67 74 68 20 3d 3d 3d 20 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 61 72 67 65 74 20 3d 20 24 28 27 23 27 20 2b 20 68 61 73 68 29 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2f 2f 20 41 63 63 6f 75 6e 74 20 66 6f 72 20 65 78 70 65 64 69 74 69 6f 6e 20 68 65 69 67 68 74 20 69 66 20 66 69 78 65 64 20 70 6f 73 69 74 69 6f 6e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 73 63 72 6f 6c 6c 5f 74 6f 70 20 3d 20 74 61 72 67 Data Ascii: #').join(''), target = $('a[name="' + hash + '"]'); if (target.length === 0) { target = $('#' + hash); } // Account for expedition height if fixed position var scroll_top = targ
2021-09-27 18:34:04 UTC	944	IN	Data Raw: 6e 2e 66 69 6e 64 28 27 3e 2e 6e 61 6d 65 27 29 2e 63 73 73 28 7b 6c 65 66 74 20 3a 20 31 30 30 20 2a 20 74 6f 70 62 61 72 2e 64 61 74 61 28 27 69 6e 64 65 78 27 29 20 2b 20 27 25 27 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2e 63 73 73 28 7b 72 69 67 68 74 20 3a 20 2d 28 31 30 30 20 2a 20 74 6f 70 62 61 72 2e 64 61 74 61 28 27 69 6e 64 65 78 27 29 20 2b 20 27 25 27 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2e 66 69 6e 64 28 27 3e 2e 6e 61 6d 65 27 29 2e 63 73 73 28 7b 72 69 67 68 74 20 3a 20 31 30 30 20 2a 20 74 6f 70 62 61 72 2e 64 61 74 61 28 27 69 6e 64 65 78 27 29 20 2b 20 27 25 27 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 Data Ascii: n.find('>.name').css({left : 100 * topbar.data('index') + '%'}); } else { section.css({right : -(100 * t opbar.data('index')) + '%'}); section.find('>.name').css({right : 100 * topbar.data('index') + '%'});

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	960	IN	Data Raw: 20 7b 0d 0a 20 20 20 20 20 20 69 66 20 28 74 68 69 73 2e 6e 61 6d 65 73 70 61 63 65 2e 6c 65 6e 67 74 68 20 3e 20 30 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 72 65 74 75 72 6e 20 74 68 69 73 2e 6e 61 6d 65 73 70 61 63 65 20 2b 20 27 2d 27 20 2b 20 73 74 72 3b 0d 0a 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 72 65 74 75 72 6e 20 73 74 72 3b 0d 0a 20 20 20 20 7d 2c 0d 0a 0d 0a 20 20 20 20 6f 66 66 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 7d 2c 0d 0a 0d 0a 20 20 20 20 72 65 66 6c 6f 77 20 3a 20 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 7d 0d 0a 20 20 7d 3b 0d 0a 7d 28 6a 51 75 65 72 79 2c 20 77 69 6e 64 6f 77 2c 20 77 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 29 29 3b 0d 0a 3b 28 66 75 6e 63 74 69 6f 6e 20 28 24 2c 20 77 69 6e 64 6f 77 2c 20 64 6f Data Ascii: { if (this.namespace.length > 0) { return this.namespace + '-' + str; } return str; }, off : functi on () {}, reflow : function () {} };}(jQuery, window, window.document));;(function ($, window, do
2021-09-27 18:34:04 UTC	977	IN	Data Raw: 7d 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 69 66 20 28 73 65 74 74 69 6e 67 73 2e 64 69 73 61 62 6c 65 5f 66 6f 72 5f 74 6f 75 63 68 20 26 26 20 4d 6f 64 65 72 6e 69 7a 72 2e 74 6f 75 63 68 20 26 26 20 2f 74 6f 75 63 68 73 74 61 72 74 7c 4d 53 50 6f 69 6e 74 65 72 44 6f 77 6e 2f 69 2e 74 65 73 74 28 65 2e 74 79 70 65 29 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 72 65 74 75 72 6e 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 20 65 6c 73 65 20 69 66 20 28 21 73 65 74 74 69 6e 67 73 2e 64 69 73 61 62 6c 65 5f 66 6f 72 5f 74 6f 75 63 68 20 26 26 20 4d 6f 64 65 72 6e 69 7a 72 2e 74 6f 75 63 68 20 26 26 20 2f 74 6f 75 63 68 73 74 61 72 74 7c 4d 53 50 6f 69 6e 74 65 72 44 6f 77 6e 2f 69 2e 74 65 73 74 28 65 2e 74 79 70 65 Data Ascii: } else { if (settings.disable_for_touch && Modernizr.touch && /touchstart|MSPointerDown/i.test(e.type)) { return; } else if (!settings.disable_for_touch && Modernizr.touch && /touchstart|MSPointerDown/i.test(e.type

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49794	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	813	OUT	GET /ca/restor/assets/15.e8db891fc03030df5677.chunk.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:03 UTC	830	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:03 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:03 UTC	830	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49760	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:58 UTC	5	OUT	GET /ca/restor/index.php?id=40382411219 HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-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
2021-09-27 18:33:59 UTC	6	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	6	IN	Data Raw: 33 34 61 30 33 0d 0a Data Ascii: 34a03
2021-09-27 18:33:59 UTC	6	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 73 61 76 65 64 20 66 72 6f 6d 20 75 72 6c 3d 28 30 30 35 34 29 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 20 2d 2d 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 61 73 79 6e 63 3d 22 22 20 73 72 63 3d 22 2e 2f 61 73 73 65 74 73 2f 66 2e 74 78 74 22 3e 3c 2f 73 63 Data Ascii: <!DOCTYPE html>... saved from url=(0054)file:///C:/Users/Administrator/Desktop/ca/billing.html --><html lang ="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"><script type="text/javascript" async="" src="./assets/f.txt"></sc
2021-09-27 18:33:59 UTC	22	IN	Data Raw: 2d 6f 6e 6c 79 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 78 6c 61 72 67 65 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 6c 61 72 67 65 2d 6f 6e 6c 79 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 6c 61 72 67 65 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 6d 65 64 69 75 6d 2d 6f 6e 6c 79 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 73 6d 61 6c 6c 2d 6f 6e 6c 79 22 3e 3c 6d 65 74 61 20 63 6c 61 73 73 3d 22 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 Data Ascii: -only"><meta class="foundation-mq-xlarge"><meta class="foundation-mq-large-only"><meta class="foun dation-mq-large"><meta class="foundation-mq-medium-only"><meta class="foundation-mq-medium"><meta class="found ation-mq-small-only"><meta class="foundation-mq
2021-09-27 18:33:59 UTC	38	IN	Data Raw: 0a 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 75 6c 20 63 6c 61 73 73 3d 22 72 69 67 68 74 20 75 74 69 6c 69 74 79 2d 62 75 73 69 6e 65 73 73 2d 6e 61 76 2d 73 65 61 72 63 68 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 6c 69 20 72 6f 6c 65 3d 22 73 65 61 72 63 68 22 20 61 72 69 61 2d 6c 61 62 65 6c 3d 22 53 65 61 72 63 68 22 3e 3c 61 20 69 64 3d 22 73 65 61 72 63 68 42 74 6e 22 20 68 72 65 66 3d 22 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 20 63 6c 61 73 73 3d 22 62 74 6e 20 62 74 6e 2d 73 65 61 72 63 68 22 20 72 6f 6c 65 3d 22 62 75 74 74 6f 6e 22 3e 53 65 61 72 63 68 3c 2f Data Ascii: <ul class="right utility-business-nav-search"> <li role="search" aria-label="S earch">Search</
2021-09-27 18:33:59 UTC	56	IN	Data Raw: 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 6e 74 2d 74 69 74 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 2e 75 6e 64 65 66 69 6e 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 62 75 73 69 6e 65 73 73 2f 70 6f 73 74 61 6c 2d 73 65 72 76 69 63 65 73 2f 6d 61 69 6c 69 6e 67 2f 6c 65 74 74 65 72 2d 64 69 73 63 6f 75 6e 74 73 2e 70 61 67 65 3f 22 20 74 61 72 67 65 74 3d 22 22 3e 47 65 74 20 62 75 73 69 6e 65 73 73 20 6c 65 74 74 65 72 20 64 69 73 63 6f 75 6e 74 73 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 75 6c 3e 0a 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 0a 20 20 20 20 20 20 20 3c 2f 64 69 Data Ascii: sers/Administrator/Desktop/ca/billing.html#">Back View restrictions <a href="http
2021-09-27 18:33:59 UTC	79	IN	Data Raw: 61 73 73 3d 22 70 61 72 65 6e 74 2d 6c 69 6e 6b 22 20 74 61 72 67 65 74 3d 22 75 6e 64 65 66 69 6e 65 64 22 3e 4d 61 72 6b 65 74 69 6e 67 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 6c 65 76 65 6c 20 6c 65 76 65 6c 31 22 20 64 61 74 61 2d 6c 65 76 65 6c 3d 22 32 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 62 61 63 6b 22 20 68 72 65 66 3d 22 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 Data Ascii: ass="parent-link" target="undefined">Marketing Back <a class="pare
2021-09-27 18:33:59 UTC	159	IN	Data Raw: 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 6e 74 2d 74 69 74 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 2e 75 6e 64 65 66 69 6e 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 62 75 73 69 6e 65 73 73 2f 70 6f 73 74 61 6c 2d 73 65 72 76 69 63 65 73 2f 6d 61 69 6c 69 6e 67 2f 6c 65 74 74 65 72 2d 64 69 73 63 6f 75 6e 74 73 2e 70 61 67 65 3f 22 20 74 61 72 67 65 74 3d 22 22 3e 47 65 74 20 62 75 73 69 6e 65 73 73 20 6c 65 74 74 65 72 20 64 69 73 63 6f 75 6e 74 73 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 75 6c 3e 0a 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 0a 20 20 20 20 20 20 20 3c 2f 64 69 Data Ascii: tor/Desktop/ca/billing.html#">Back Get business letter discounts </u l> </di
2021-09-27 18:34:00 UTC	239	IN	Data Raw: 6e 75 2d 69 74 65 6d 2d 62 61 63 6b 22 20 68 72 65 66 3d 22 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 6e 74 2d 74 69 74 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 2e 75 6e 64 65 66 69 6e 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 70 65 72 73 6f 6e 61 6c 2f 72 65 63 65 69 76 69 6e 67 2f 6d 61 6e 61 67 65 2d 6d 61 69 6c 2f 65 70 6f 73 74 2e 70 61 67 65 3f 22 20 74 61 72 67 65 74 3d 22 22 3e 47 65 74 20 62 69 6c 6c 73 20 61 6e 64 20 73 74 61 74 65 6d 65 6e 74 73 20 6f 6e 6c 69 6e 65 20 28 65 70 6f 73 74 29 3c 2f 61 3e 0a 20 20 20 20 Data Ascii: nu-item-back" href="file:///C:/Users/Administrator/Desktop/ca/billing.html#">Back Get bills and statements online (epost)
2021-09-27 18:34:00 UTC	319	IN	Data Raw: 93 20 41 69 72 20 6f 72 20 53 75 72 66 61 63 65 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 68 69 64 65 20 6c 65 76 65 6c 35 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 62 61 63 6b 22 20 68 72 65 66 3d 22 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 6e 74 2d 74 69 74 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 2e 75 6e 64 65 66 69 6e 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 70 65 72 73 6f 6e Data Ascii: Air or Surface Back <a class="parent-title" href="https://.undefined.ca/ cpc/en/person

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	384	IN	Data Raw: 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 68 69 64 65 20 6c 65 76 65 6c 35 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 6d 65 6e 75 2d 69 74 65 6d 2d 62 61 63 6b 22 20 68 72 65 66 3d 22 66 69 6c 65 3a 2f 2f 2f 43 3a 2f 55 73 65 72 73 2f 41 64 6d 69 6e 69 73 74 72 61 74 6f 72 2f 44 65 73 6b 74 6f 70 2f 63 61 2f 62 69 6c 6c 69 6e 67 2e 68 74 6d 6c 23 22 3e 42 61 63 6b 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 20 63 6c 61 73 73 3d 22 70 61 72 65 6e 74 2d 74 69 74 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 2e 75 6e 64 65 66 69 6e 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 6f 75 72 2d 63 6f 6d 70 61 6e 79 2f 61 62 6f 75 74 2d 75 73 2f 6f 75 72 2d 6c 65 61 64 6e 2f 61 62 6f 75 74 2d 75 73 2f 6f 75 72 2d 6c 65 61 64 Data Ascii: Back <a class="parent-title" href="https://.undefined.ca/cpc/en/our-company/about-us/our-lead
2021-09-27 18:34:00 UTC	465	IN	Data Raw: 65 64 2e 63 61 2f 63 70 63 2f 65 6e 2f 6f 75 72 2d 63 6f 6d 70 61 6e 79 2f 61 62 6f 75 74 2d 75 73 2f 66 69 6e 61 6e 63 69 61 6c 2d 72 65 70 6f 72 74 73 2f 32 30 31 38 2d 61 6e 6e 75 61 6c 2d 72 65 70 6f 72 74 2f 63 6f 72 70 6f 72 61 74 65 2f 70 75 62 6c 69 63 2d 70 6f 6c 69 63 79 2e 70 61 67 65 3f 22 20 74 61 72 67 65 74 3d 22 22 3e 50 75 62 6c 69 63 20 70 6f 6c 69 63 79 3c 2f 61 3e 0a 20 20 20 20 20 20 20 20 3c 75 6c 3e 0a 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 3c 2f 64 69 76 3e 0a 20 20 20 20 3c 2f 6c 69 3e 20 20 20 20 20 0a 20 20 20 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 2f 75 6c 3e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 20 20 20 20 20 20 Data Ascii: ed.ca/cpc/en/our-company/about-us/financial-reports/2018-annual-report/corporate/public-policy.page?" target="">Public policy
2021-09-27 18:34:00 UTC	542	IN	Data Raw: 70 63 2d 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 65 72 72 6f 72 3e 3c 21 2d 2d 2d 2d 3e 3c 2f 63 70 63 2d 66 6f 72 6d 2d 63 6f 6e 74 72 6f 6c 2d 65 72 72 6f 72 3e 3c 2f 64 69 76 3e 3c 2f 66 69 65 6c 64 73 65 74 20 63 6c 61 73 73 3d 22 66 2d 66 69 65 6c 64 73 65 74 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 6e 67 2d 75 6e 74 6f 75 63 68 65 64 20 6e 67 2d 70 72 69 73 74 69 6e 65 20 6e 67 2d 69 6e 76 61 6c 69 64 22 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 66 2d 67 72 6f 75 70 22 3e 3c 6c 61 62 65 6c 20 66 6f 72 3d 22 66 2d 63 6f 75 6e 74 72 79 22 20 63 6c 61 73 73 3d 22 66 2d 6c 61 62 65 6c 22 3e 43 6f 75 6e 74 72 79 3c 2f 6c 61 62 65 6c 3e 3c 73 65 6c 65 63 74 20 6e 61 6d 65 3d 22 63 6f 75 6e 22 20 66 6f 72 6d 63 6f 6e 74 72 6f 6c Data Ascii: pc-form-control-error>...--></cpc-form-control-error> </fieldset><fieldset class="f-fieldset"> <label for="f-country" class="f-label">Country</label><select name="coun" formcontrol
2021-09-27 18:34:00 UTC	590	IN	Data Raw: 74 22 20 63 6c 61 73 73 3d 22 62 75 74 74 6f 6e 20 62 75 74 74 6f 6e 2d 2d 70 72 69 6d 61 72 79 20 78 73 2d 6f 6e 6c 79 2d 66 75 6c 6c 22 3e 43 6f 6e 74 69 6e 75 65 3c 63 70 63 2d 73 70 69 6e 6e 65 72 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 70 69 6e 6e 65 72 5f 5f 66 72 61 67 6d 65 6e 74 22 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 73 70 69 6e 6e 65 72 5f 5f 63 65 6e 74 65 72 22 3e 3c 2f 64 69 76 3e 3c 2f 63 70 63 2d 73 70 69 6e 6e 65 72 3e 3c 2f 62 75 74 74 6f 6e 3e 3c 21 2d 2d 2d 2d 3e 3c 63 70 63 2d 66 6f 72 6d 2d 65 72 72 6f 72 2d 6c 69 73 74 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 31 31 79 2d 72 65 61 64 65 72 2d 6f 6e 6c 79 22 20 61 72 69 61 2d 68 69 64 64 65 6e 3d 22 74 72 75 65 22 3e 3c 70 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 Data Ascii: t" class="button button--primary xs-only-full">Continue<cpc-spinner> </cpc-spinner></button>...--><cpc-form-error-list> <p><a href="htt
2021-09-27 18:34:00 UTC	639	IN	Data Raw: 2e 30 36 33 61 35 2e 35 33 31 20 35 2e 35 33 31 20 30 20 30 20 30 20 31 2e 38 35 31 2d 2e 33 34 37 20 33 2e 33 31 32 20 33 2e 33 31 32 20 30 20 30 20 30 20 31 2e 38 39 33 2d 31 2e 38 39 32 63 2e 32 32 2d 2e 35 39 33 2e 33 33 38 2d 31 2e 39 2e 33 34 37 2d 31 2e 38 35 31 20 30 2d 31 2e 30 32 2e 30 36 33 2d 31 2e 33 36 37 2e 30 36 33 2d 34 2e 30 33 38 20 30 2d 32 2e 36 37 20 30 2d 32 2e 39 38 36 2d 2e 30 36 33 2d 34 2e 30 33 38 61 35 2e 35 33 31 20 35 2e 35 33 31 20 30 20 30 20 30 20 30 2d 2e 33 34 37 2d 31 2e 38 35 20 33 2e 33 31 32 20 33 2e 33 31 32 20 30 20 30 20 30 20 30 2d 31 2e 38 39 33 2d 31 2e 38 39 33 20 35 2e 35 33 31 20 35 2e 35 33 31 20 30 20 30 20 30 20 30 2d 31 2e 38 35 2d 2e 33 34 37 63 2d 31 2e 30 36 33 2d 2e 31 35 2d 31 2e 30 35 2d 31 2e 30 35 2d 31 2e 30 35 2d 31 Data Ascii: .063a5.531 5.531 0 0 0 1.851-.347 3.312 3.312 0 0 0 1.893-1.892c.22-.593.338-1.219.347-1.851 0-1.052.063-1.367.063-4.038 0-2.67 0-2.986-.063-4.038a5.531 5.531 0 0 0-.347-1.85 3.312 3.312 0 0 0-1.893-1.893 5.531 5.531 0 0 0-1.85-.347c-1.063-.105-1.378-.105
2021-09-27 18:34:00 UTC	655	IN	Data Raw: 65 66 69 6e 65 64 2e 63 61 2f 77 65 62 2f 65 6e 2f 70 61 67 65 73 2f 73 75 70 70 6f 72 74 2f 64 65 66 61 75 6c 74 2e 70 61 67 65 22 20 63 6c 61 73 73 3d 22 73 65 61 72 63 68 2d 6d 6f 64 61 6c 2d 6c 69 6e 6b 22 20 74 61 62 69 6e 64 65 78 3d 22 30 22 3e 0a 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 73 65 61 72 63 68 2d 69 63 6f 6e 20 73 75 70 70 6f 72 74 22 3e 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 20 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 73 65 61 72 63 68 2d 6d 6f 64 61 6c 2d 6c 61 62 65 6c 22 3e 53 75 70 70 6f 72 74 3c 2f 73 70 61 6e 3e 0a 20 20 20 20 3c 2f 61 3e 0a 20 20 3c 2f 6c 69 3e 0a 3c 2f 75 6c 3e 0a 20 20 20 20 3c 64 69 76 3e 0a 20 20 3c 2f 64 69 76 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 73 65 63 74 69 6f Data Ascii: efined.ca/web/en/pages/support/default.page" class="search-modal-link" tabindex="0"> Support </sectio
2021-09-27 18:34:00 UTC	657	IN	Data Raw: 0d 0a Data Ascii:
2021-09-27 18:34:00 UTC	657	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49795	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	813	OUT	GET /ca/restor/assets/cwc.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	830	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:03 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:03 UTC	830	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49796	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:03 UTC	879	OUT	GET /ca/restor/assets/1.9bf84a1119dc09839d2c.chunk.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:04 UTC	895	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:04 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:04 UTC	895	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49797	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	944	OUT	GET /ca/restor/assets/f(1).txt HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:04 UTC	985	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:04 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	985	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49798	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	976	OUT	GET /ca/restor/assets/saved_resource HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:04 UTC	985	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:04 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "f13c-5c26848200a80" Accept-Ranges: bytes Content-Length: 61756 Connection: close
2021-09-27 18:34:04 UTC	986	IN	Data Raw: 28 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 2e 51 53 49 3d 3d 3d 27 75 6e 64 65 66 69 6e 65 64 27 29 7b 77 69 6e 64 6f 77 2e 51 53 49 3d 7b 7d 3b 7d 0a 76 61 72 20 74 65 6d 70 51 53 49 43 6f 6e 66 69 67 3d 7b 22 68 6f 73 74 65 64 4a 53 4c 6f 63 61 74 69 6f 6e 22 3a 22 68 74 74 70 73 3a 2f 2f 73 69 74 65 69 6e 74 65 72 63 65 70 74 2e 71 75 61 6c 74 72 69 63 73 2e 63 6f 6d 2f 64 78 6a 73 6d 6f 64 75 6c 65 2f 22 2c 22 62 61 73 65 55 52 4c 22 3a 22 68 74 74 70 73 3a 2f 2f 73 69 74 65 69 6e 74 65 72 63 65 70 74 2e 71 75 61 6c 74 72 69 63 73 2e 63 6f 6d 22 2c 22 7a 6f 6e 65 49 64 22 3a 22 5a 4e 5f 30 78 6c 65 49 52 36 73 57 53 5a 61 4e 59 39 22 7d 3b 69 66 28 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 2e 51 53 49 2e 63 6f 6e Data Ascii: (function(){if(typeof window.QSI==='undefined'){window.QSI={};}var tempQSIConfig={"hostedJSLocation":"https://siteintercept.qualtrics.com/dxjsmodule/","baseURL":"https://siteintercept.qualtrics.com","zoneId":"ZN_0xleIR6sWSZaNY9"};if(typeof window.QSI.con
2021-09-27 18:34:04 UTC	1003	IN	Data Raw: 65 71 75 65 6e 63 79 2d 72 75 6c 65 73 22 3b 72 65 74 75 72 6e 20 51 53 49 2e 4c 61 74 65 6e 63 79 4c 6f 67 2e 73 74 61 72 74 43 6f 6d 70 6f 6e 65 6e 74 54 69 6d 65 72 28 51 53 49 2e 4c 61 74 65 6e 63 79 4c 6f 67 2e 63 6f 6d 70 6f 6e 65 6e 74 73 2e 43 4f 4e 54 41 43 54 5f 46 52 45 51 55 45 4e 43 59 29 2c 76 6f 69 64 20 51 53 49 2e 75 74 69 6c 2e 73 65 6e 64 48 74 74 70 52 65 71 75 65 73 74 28 7b 74 79 70 65 3a 22 50 4f 53 54 22 2c 75 72 6c 3a 6e 2c 68 65 61 64 65 72 3a 7b 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 3a 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 22 7d 2c 64 61 74 61 3a 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 28 65 29 2c 73 75 63 63 65 73 73 43 61 6c 6c 62 61 63 6b 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 72 79 7b 76 61 72 20 6e 3b Data Ascii: equency-rules";return QSI.LatencyLog.startComponentTimer(QSI.LatencyLog.components.CONTACT_FREQUENCY),void QSI.util.sendHttpRequest({type:"POST",url:n,header:{"Content-type":"application/json"},data:JSON.stringify(e),successCallback:function(e){try{var n;
2021-09-27 18:34:05 UTC	1035	IN	Data Raw: 49 44 3d 3d 3d 74 3f 6e 3a 65 7d 2c 6e 75 6c 6c 29 29 2c 5b 72 2c 6f 5d 7d 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 7d 72 65 74 75 72 6e 20 65 2e 70 72 6f 74 6f 74 79 70 65 2e 64 6f 53 50 41 52 65 6c 6f 61 64 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 77 69 6e 64 6f 77 2e 51 53 49 26 26 77 69 6e 64 6f 77 2e 51 53 49 2e 41 50 49 29 7b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 51 53 49 2e 41 50 49 3b 65 2e 75 6e 6c 6f 61 64 28 29 2c 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 65 2e 6c 6f 61 64 28 29 7d 2c 31 30 30 29 7d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 6e 64 6c 65 53 50 41 45 76 61 6c 75 61 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 74 68 69 73 3b 69 66 28 65 26 26 21 77 69 6e 64 6f 77 2e 51 53 49 2e Data Ascii: ID===t?n:e},null)),[r,o]}return null}}return e.prototype.doSPAReload=function(){if(window.QSI&&window.QSI.API){var e=window.QSI.API;e.unload(),setTimeout(function(){e.load()},100)}},e.prototype.handleSPAEvaluation=function(e){var t=this;if(e&&!window.QSI.
2021-09-27 18:34:05 UTC	1067	IN	Data Raw: 3c 69 3b 75 2b 2b 29 6f 5b 75 5d 26 26 6f 5b 75 5d 2e 70 72 6f 6d 69 73 65 3f 6f 5b 75 5d 2e 70 72 6f 6d 69 73 65 28 29 2e 64 6f 6e 65 28 63 28 75 2c 6f 29 29 2e 66 61 69 6c 28 73 2e 72 65 6a 65 63 74 29 3a 61 2d 2d 3b 72 65 74 75 72 6e 20 61 3c 31 26 26 73 2e 72 65 73 6f 6c 76 65 28 6f 29 2c 73 2e 70 72 6f 6d 69 73 65 28 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 63 72 65 61 74 65 41 72 72 61 79 46 72 6f 6d 41 72 67 75 6d 65 6e 74 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 3f 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 73 6c 69 63 65 2e 63 61 6c 6c 28 65 29 3a 5b 5d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 69 73 46 75 6e 63 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 22 66 75 6e 63 74 69 6f 6e 22 3d Data Ascii: <i;u++)o[u]&&o[u].promise?o[u].promise().done(c(u,o)).fail(s.reject):a--;return a<1&&s.resolve(o),s.promise()},e.prototype.createArrayFromArguments=function(e){return e?Array.prototype.slice.call(e):[]},e.prototype.isFunction=function(e){return"function"=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49799	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	985	OUT	GET /ca/restor/assets/f(2).txt HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:04 UTC	1002	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:04 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:04 UTC	1003	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49800	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:04 UTC	986	OUT	GET /ca/restor/assets/saved_resource(1) HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:04 UTC	1003	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:04 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:30:50 GMT ETag: "f13c-5c2686d518680" Accept-Ranges: bytes Content-Length: 61756 Connection: close
2021-09-27 18:34:05 UTC	1019	IN	Data Raw: 28 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 2e 51 53 49 3d 3d 3d 27 75 6e 64 65 66 69 6e 65 64 27 29 7b 77 69 6e 64 6f 77 2e 51 53 49 3d 7b 7d 3b 7d 0a 76 61 72 20 74 65 6d 70 51 53 49 43 6f 6e 66 69 67 3d 7b 22 68 6f 73 74 65 64 4a 53 4c 6f 63 61 74 69 6f 6e 22 3a 22 68 74 74 70 73 3a 2f 2f 73 69 74 65 69 6e 74 65 72 63 65 70 74 2e 71 75 61 6c 74 72 69 63 73 2e 63 6f 6d 2f 64 78 6a 73 6d 6f 64 75 6c 65 2f 22 2c 22 62 61 73 65 55 52 4c 22 3a 22 68 74 74 70 73 3a 2f 2f 73 69 74 65 69 6e 74 65 72 63 65 70 74 2e 71 75 61 6c 74 72 69 63 73 2e 63 6f 6d 22 2c 22 7a 6f 6e 65 49 64 22 3a 22 5a 4e 5f 30 78 6c 65 49 52 36 73 57 53 5a 61 4e 59 39 22 7d 3b 69 66 28 74 79 70 65 6f 66 20 77 69 6e 64 6f 77 2e 51 53 49 2e 63 6f 6e Data Ascii: (function(){if(typeof window.QSI==='undefined'){window.QSI={};}var tempQSIConfig={"hostedJSLocation":"https://siteintercept.qualtrics.com/dxjsmodule/","baseURL":"https://siteintercept.qualtrics.com","zoneId":"ZN_0xleIR6sWSZaNY9"};if(typeof window.QSI.con
2021-09-27 18:34:05 UTC	1051	IN	Data Raw: 65 71 75 65 6e 63 79 2d 72 75 6c 65 73 22 3b 72 65 74 75 72 6e 20 51 53 49 2e 4c 61 74 65 6e 63 79 4c 6f 67 2e 73 74 61 72 74 43 6f 6d 70 6f 6e 65 6e 74 54 69 6d 65 72 28 51 53 49 2e 4c 61 74 65 6e 63 79 4c 6f 67 2e 63 6f 6d 70 6f 6e 65 6e 74 73 2e 43 4f 4e 54 41 43 54 5f 46 52 45 51 55 45 4e 43 59 29 2c 76 6f 69 64 20 51 53 49 2e 75 74 69 6c 2e 73 65 6e 64 48 74 74 70 52 65 71 75 65 73 74 28 7b 74 79 70 65 3a 22 50 4f 53 54 22 2c 75 72 6c 3a 6e 2c 68 65 61 64 65 72 3a 7b 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 3a 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6a 73 6f 6e 22 7d 2c 64 61 74 61 3a 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 28 65 29 2c 73 75 63 63 65 73 73 43 61 6c 6c 62 61 63 6b 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 74 72 79 7b 76 61 72 20 6e 3b Data Ascii: equency-rules";return QSI.LatencyLog.startComponentTimer(QSI.LatencyLog.components.CONTACT_FREQUENCY),void QSI.util.sendHttpRequest({type:"POST",url:n,header:{"Content-type":"application/json"},data:JSON.stringify(e),successCallback:function(e){try{var n;

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1082	IN	Data Raw: 49 44 3d 3d 3d 74 3f 6e 3a 65 7d 2c 6e 75 6c 6c 29 29 2c 5b 72 2c 6f 5d 7d 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 7d 72 65 74 75 72 6e 20 65 2e 70 72 6f 74 6f 74 79 70 65 2e 64 6f 53 50 41 52 65 6c 6f 61 64 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 69 66 28 77 69 6e 64 6f 77 2e 51 53 49 26 26 77 69 6e 64 6f 77 2e 51 53 49 2e 41 50 49 29 7b 76 61 72 20 65 3d 77 69 6e 64 6f 77 2e 51 53 49 2e 41 50 49 3b 65 2e 75 6e 6c 6f 61 64 28 29 2c 73 65 74 54 69 6d 65 6f 75 74 28 66 75 6e 63 74 69 6f 6e 28 29 7b 65 2e 6c 6f 61 64 28 29 7d 2c 31 30 30 29 7d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 6e 64 6c 65 53 50 41 45 76 61 6c 75 61 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 74 68 69 73 3b 69 66 28 65 26 26 21 77 69 6e 64 6f 77 2e 51 53 49 2e Data Ascii: ID===t?n:e},null)),[r,o]}return null}}return e.prototype.doSPAReload=function(){if(window.QSI&&window.QSI.API){var e=window.QSI.API;e.unload(),setTimeout(function(){e.load()},100)}},e.prototype.handleSPAEvaluation=function(e){var t=this;if(e&&!window.QSI.
2021-09-27 18:34:05 UTC	1098	IN	Data Raw: 3c 69 3b 75 2b 2b 29 6f 5b 75 5d 26 26 6f 5b 75 5d 2e 70 72 6f 6d 69 73 65 3f 6f 5b 75 5d 2e 70 72 6f 6d 69 73 65 28 29 2e 64 6f 6e 65 28 63 28 75 2c 6f 29 29 2e 66 61 69 6c 28 73 2e 72 65 6a 65 63 74 29 3a 61 2d 2d 3b 72 65 74 75 72 6e 20 61 3c 31 26 26 73 2e 72 65 73 6f 6c 76 65 28 6f 29 2c 73 2e 70 72 6f 6d 69 73 65 28 29 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 63 72 65 61 74 65 41 72 72 61 79 46 72 6f 6d 41 72 67 75 6d 65 6e 74 73 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 65 3f 41 72 72 61 79 2e 70 72 6f 74 6f 74 79 70 65 2e 73 6c 69 63 65 2e 63 61 6c 6c 28 65 29 3a 5b 5d 7d 2c 65 2e 70 72 6f 74 6f 74 79 70 65 2e 69 73 46 75 6e 63 74 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 22 66 75 6e 63 74 69 6f 6e 22 3d Data Ascii: <i;u++)o[u]&&o[u].promise?o[u].promise().done(c(u,o)).fail(s.reject):a--;return a<1&&s.resolve(o),s.promise()},e.prototype.createArrayFromArguments=function(e){return e?Array.prototype.slice.call(e):[]},e.prototype.isFunction=function(e){return"function"=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49803	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1079	OUT	GET /ca/restor/assets/anchor.html HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1111	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "9ed1-5c26848200a80" Accept-Ranges: bytes Content-Length: 40657 Vary: Accept-Encoding Connection: close Content-Type: text/html
2021-09-27 18:34:05 UTC	1112	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 73 61 76 65 64 20 66 72 6f 6d 20 75 72 6c 3d 28 30 32 33 37 29 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 72 65 63 61 70 74 63 68 61 2f 61 70 69 32 2f 61 6e 63 68 6f 72 3f 61 72 3d 31 26 6b 3d 36 4c 63 35 47 61 45 55 41 41 41 41 41 50 4f 72 39 36 43 50 35 54 63 4c 67 4a 34 37 71 36 47 4d 6b 6c 34 71 49 62 42 46 26 63 6f 3d 61 48 52 30 63 48 4d 36 4c 79 39 7a 63 32 38 74 62 33 4e 31 4c 6d 4e 68 62 6d 46 6b 59 58 42 76 63 33 51 74 63 47 39 7a 64 47 56 7a 59 32 46 75 59 57 52 68 4c 6d 4e 68 4f 6a 51 30 4d 77 2e 2e 26 68 6c 3d 65 6e 26 76 3d 66 2d 62 6e 6e 4f 75 61 68 69 59 4b 75 65 69 37 64 6d 41 64 33 6b 67 76 26 73 69 7a 65 3d 69 6e 76 69 73 69 62 6c 65 26 62 61 64 67 Data Ascii: <!DOCTYPE html>... saved from url=(0237)https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lc5GaEUAAAAAPOr96CP5TcLgJ47q6GMkl4qIbBF&co=aHR0cHM6Ly9zc28tb3N1LmNhbmFkYXBvc3QtcG9zdGVzY2FuYWRhLmNhOjQ0Mw..&hl=en&v=f-bnnOuahiYKuei7dmAd3kgv&size=invisible&badg
2021-09-27 18:34:05 UTC	1131	IN	Data Raw: 57 35 6c 63 69 68 57 4c 45 55 73 55 43 6b 73 57 53 68 58 4c 44 45 35 4d 53 78 62 52 79 78 57 4c 45 56 64 4b 53 6c 39 4b 53 78 6d 64 57 35 6a 64 47 6c 76 62 69 68 58 4b 58 74 58 4c 6b 6f 6f 4e 43 6c 39 4b 53 6b 73 4d 43 6b 73 57 31 30 70 4c 47 73 70 4b 53 78 4b 4b 56 30 73 61 79 6b 73 5a 43 6b 6f 64 48 4a 31 5a 53 78 30 63 6e 56 6c 4c 47 73 70 66 53 78 61 54 54 31 6d 64 57 35 6a 64 47 6c 76 62 69 68 72 4c 47 67 73 53 69 6c 37 61 57 59 6f 61 44 31 30 65 58 42 6c 62 32 59 67 61 79 77 69 62 32 4a 71 5a 57 4e 30 49 6a 30 39 61 43 6c 70 5a 69 68 72 4b 58 74 70 5a 69 68 72 49 47 6c 75 63 33 52 68 62 6d 4e 6c 62 32 59 67 51 58 4a 79 59 58 6b 70 63 6d 56 30 64 58 4a 75 49 6d 46 79 63 6d 46 35 49 6a 74 70 5a 69 68 72 49 47 6c 75 63 33 52 68 62 6d 4e 6c 62 32 59 67 Data Ascii: W5lcihWLEUsUCksWShXLDE5MSxbRyxWLEVdKSl9KSxmdW5jdGlvbihXKXtXLkooNCl9KSksMCksW10pLGspKSxKKV0sayksZCkodHJ1ZSx0cnVlLGspfSxaTT1mdW5jdGlvbihrLGgsSil7aWYoaD10eXBlb2Ygaywib2JqZWN0Ij09aClpZihrKXtpZihrIGluc3RhbmNlb2YgQXJyYXkpcmV0dXJuImFycmF5ljtpZihrIGluc3RhbmNlb2Yg
2021-09-27 18:34:05 UTC	1147	IN	Data Raw: 42 72 65 57 4e 76 57 57 56 54 4d 32 78 54 5a 7a 6c 61 54 6d 59 76 52 55 74 7a 51 6b 31 70 51 6e 64 70 59 6e 52 34 56 6e 5a 6c 4e 30 39 6f 51 30 31 30 55 44 42 48 51 57 55 31 63 48 68 31 54 55 39 4e 62 6b 6c 72 54 33 56 6a 52 56 6f 72 5a 30 74 4e 4d 30 73 30 54 30 68 49 55 6c 4a 77 63 57 52 59 55 44 4a 54 4f 58 68 31 62 58 5a 72 59 32 56 43 4d 55 74 47 65 47 35 45 59 31 70 4a 59 33 42 4b 51 55 31 6c 4d 55 64 4a 55 48 6b 7a 52 6d 31 57 62 30 63 30 56 47 56 79 56 57 5a 76 52 45 59 72 59 6b 78 35 57 6d 74 4b 56 57 5a 43 53 6c 52 51 57 45 64 4b 51 30 4e 52 52 45 70 44 52 31 68 4b 5a 6b 31 70 52 6b 31 35 63 31 70 33 61 33 46 78 53 6e 5a 48 62 58 67 7a 56 7a 6c 30 63 6b 4a 57 64 58 4e 73 62 32 56 7a 56 45 31 58 4e 48 46 69 54 55 6c 30 4d 6c 42 35 57 48 63 76 52 Data Ascii: BreWNvWWVTM2xTZzlaTmYvRUtzQk1pQndpYnR4VnZlN09oQ010UDBHQWU1cHh1TU9NbklrT3VjRVorZ0tNM0s0T0hIUlJwcWRYUDJTOXh1bXZrY2VCMUtGeG5EY1pJY3BKQU1lMUdJUHkzRm1Wb0c0VGVyVWZvREYrYkx5WmtKVWZCSlRQWEdKQ0NRREpDR1hKZk1pRk15c1p3a3FxSnZHbXgzVzl0ckJWdXNsb2VzVE1XNHFiTUl0MlB5WHcvR

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49801	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1080	OUT	GET /ca/restor/assets/saved_resource.html HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1110	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "95-5c26848200a80" Accept-Ranges: bytes Content-Length: 149 Vary: Accept-Encoding Connection: close Content-Type: text/html
2021-09-27 18:34:05 UTC	1111	IN	Data Raw: 0a 3c 21 2d 2d 20 73 61 76 65 64 20 66 72 6f 6d 20 75 72 6c 3d 28 30 30 31 31 29 61 62 6f 75 74 3a 62 6c 61 6e 6b 20 2d 2d 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: ... saved from url=(0011)about:blank --><html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></head><body></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49804	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1081	OUT	GET /ca/restor/assets/saved_resource(2) HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1111	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:05 UTC	1112	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49802	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1081	OUT	GET /ca/restor/assets/insight.min.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1111	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:05 UTC	1111	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49763	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	54	OUT	GET /ca/restor/assets/css HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:33:59 UTC	72	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "177e-5c26847e30180" Accept-Ranges: bytes Content-Length: 6014 Connection: close
2021-09-27 18:33:59 UTC	72	IN	Data Raw: 2f 2a 20 63 79 72 69 6c 6c 69 63 2d 65 78 74 20 2a 2f 0a 40 66 6f 6e 74 2d 66 61 63 65 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 27 52 6f 62 6f 74 6f 27 3b 0a 20 20 66 6f 6e 74 2d 73 74 79 6c 65 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 73 72 63 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 73 2f 72 6f 62 6f 74 6f 2f 76 32 37 2f 4b 46 4f 6c 43 6e 71 45 75 39 32 46 72 31 4d 6d 53 55 35 66 43 52 63 34 45 73 41 2e 77 6f 66 66 32 29 20 66 6f 72 6d 61 74 28 27 77 6f 66 66 32 27 29 3b 0a 20 20 75 6e 69 63 6f 64 65 2d 72 61 6e 67 65 3a 20 55 2b 30 34 36 30 2d 30 35 32 46 2c 20 55 2b 31 43 38 30 2d 31 43 38 38 2c 20 55 2b 32 30 42 34 2c 20 55 2b 32 Data Ascii: /* cyrillic-ext */@font-face { font-family: 'Roboto'; font-style: normal; font-weight: 300; src: url(https://fonts.gstatic.com/s/roboto/v27/KFOlCnqEu92Fr1MmSU5fCRc4EsA.woff2) format('woff2'); unicode-range: U+0460-052F, U+1C80-1C88, U+20B4, U+2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49806	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1110	OUT	GET /ca/restor/assets/cpc-main-logo.png HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1128	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 02:11:20 GMT ETag: "9bd-5c268fe286200" Accept-Ranges: bytes Content-Length: 2493 Connection: close Content-Type: image/png
2021-09-27 18:34:05 UTC	1128	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 7c 00 00 00 1e 08 06 00 00 00 ee 22 7a ef 00 00 00 06 62 4b 47 44 00 ff 00 ff 00 ff a0 bd a7 93 00 00 09 72 49 44 41 54 68 de ed 5a 09 54 55 c7 19 a6 6d da 26 6d 5c b0 4b 6a 72 52 81 a0 18 45 54 44 8c 46 0d 06 15 91 60 22 6a d4 04 5b 25 d1 2a 1a c5 05 77 51 e3 52 17 16 35 02 82 6c ca 22 6a 45 45 d1 a0 01 45 05 41 05 64 91 a5 02 61 07 95 4d 21 80 f0 e0 ef fd 46 ee e5 be 0d 10 a9 47 e4 bd 73 be 77 de 9b b9 73 e7 ce 7c ff fc ff dc ff 1b 35 b5 c9 8e 89 1c 24 2a 74 09 b8 aa 71 5f 29 1c 48 85 2e 00 33 47 f7 2e 45 f8 9b 93 76 51 9f f1 1b 48 df 68 19 0d 36 5a 4e ef 4c dc 4c 6f 4c de ab 22 fc 75 c2 5b 93 76 d3 ac 8f 66 91 c7 40 3d ba ab d1 9d 92 34 de 96 c2 4d ad 3f d1 9e c1 23 69 dc 98 05 f4 ab c9 0e 2a c2 Data Ascii: PNGIHDR|"zbKGDrIDAThZTUm&m\KjrRETDF`"j[%*wQR5l"jEEEAdaM!FGsws|5$*tq_)H.3G.EvQHh6ZNLLoL"u[vf@=4M?#i*

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49809	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1131	OUT	GET /ca/restor/assets/runtime-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:05 UTC	1155	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:05 UTC	1155	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49813	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1155	OUT	GET /ca/restor/assets/styles__ltr.css HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/assets/anchor.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1157	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "cdfc-5c26848200a80" Accept-Ranges: bytes Content-Length: 52732 Vary: Accept-Encoding Connection: close Content-Type: text/css
2021-09-27 18:34:06 UTC	1158	IN	Data Raw: 2e 67 6f 6f 67 2d 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 7b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 69 6e 6c 69 6e 65 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 7d 2a 20 68 74 6d 6c 20 2e 67 6f 6f 67 2d 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2a 3a 66 69 72 73 74 2d 63 68 69 6c 64 2b 68 74 6d 6c 20 2e 67 6f 6f 67 2d 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 7b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 7d 2e 72 65 63 61 70 74 63 68 61 2d 63 68 65 63 6b 62 6f 78 7b 62 6f 72 64 65 72 3a 6e 6f 6e 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 70 78 3b 68 65 69 67 68 74 3a 32 38 70 78 3b 6d 61 72 67 69 6e 3a 34 70 78 3b 77 69 64 74 68 3a 32 38 70 78 Data Ascii: .goog-inline-block{position:relative;display:-moz-inline-box;display:inline-block}* html .goog-inline-block{ display:inline}*:first-child+html .goog-inline-block{display:inline}.recaptcha-checkbox{border:none;font-size:1px;height :28px;margin:4px;width:28px
2021-09-27 18:34:06 UTC	1175	IN	Data Raw: 6c 64 57 56 74 4c 62 46 66 30 49 61 5a 4e 47 64 2f 6a 71 6d 51 46 6d 7a 31 62 66 39 38 52 49 66 64 35 35 53 6c 31 30 6b 54 38 68 62 65 76 52 48 62 35 36 5a 71 71 5a 42 48 50 4d 31 49 31 71 2f 69 66 68 35 71 50 49 67 37 7a 77 59 55 48 74 6e 4b 5a 6d 45 73 7a 46 69 78 65 72 62 64 75 32 68 5a 71 50 49 67 2f 79 77 6f 63 46 74 58 4f 61 6d 6d 6c 67 6e 6e 43 43 55 69 2b 39 70 46 52 54 69 48 65 6d 49 67 2f 79 77 6b 63 43 61 75 64 55 51 4f 2f 32 59 47 37 5a 6e 66 76 4c 57 65 48 44 67 6e 70 33 43 71 42 33 65 7a 41 50 48 4d 6a 39 48 79 6a 77 59 55 47 39 4f 77 58 51 75 2b 4d 77 31 36 37 4e 66 57 49 50 48 77 6d 6f 64 36 63 61 67 4b 6a 50 52 4f 31 79 5a 66 42 6c 39 61 6d 46 53 51 4d 51 39 5a 6d 6f 58 61 34 4d 76 71 77 2b 74 54 42 70 41 44 4a 39 4a 6d 71 58 4b 34 4f 76 Data Ascii: ldWVtLbFf0IaZNGd/jqmQFmz1bf98RIfd55Sl10kT8hbevRHb56ZqqZBHPM1I1q/ifh5qPIg7zwYUHtnKZmEszFi xerbdu2hZqPIg/ywocFtXOammlgnnCCUi+9pFRTiHemIg/ywkcCaudUQO/2YG7ZnfvLWeHDgnp3CqB3ezAPHMj9Hyj wYUG9OwXQu+Mw167NfWlPHwmod6cagKjPRO1yZfBl9amFSQMQ9ZmoXa4Mvqw+tTBpADJ9JmqXK4Ov
2021-09-27 18:34:06 UTC	1193	IN	Data Raw: 72 6f 75 6e 64 3a 23 65 32 34 61 34 61 7d 2e 72 63 2d 62 75 74 74 6f 6e 2d 64 65 66 61 75 6c 74 2d 64 69 73 61 62 6c 65 64 2e 72 63 2d 62 75 74 74 6f 6e 2d 72 65 64 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 72 67 62 61 28 32 32 36 2c 37 34 2c 37 34 2c 30 2e 34 39 29 7d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 7d 2e 72 63 2d 69 6d 61 67 65 73 65 6c 65 63 74 2d 69 6e 73 74 72 75 63 74 69 6f 6e 73 20 73 74 72 6f 6e 67 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 39 30 30 3b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 66 6f 6e 74 2d 73 69 7a 65 3a 32 38 70 78 7d 2e 72 63 2d 66 6f 6f 74 65 72 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 52 6f 62 6f 74 6f 2c 68 65 6c 76 65 74 69 63 61 2c 61 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 Data Ascii: round:#e24a4a}.rc-button-default-disabled.rc-button-red{background:rgba(226,74,74,0.49)}body{margin:0}.rc-im ageselect-instructions strong{font-weight:900;display:block;font-size:28px}.rc-footer{font-family:Roboto,helvetica,arial,sans- serif;position:relati
2021-09-27 18:34:06 UTC	1209	IN	Data Raw: 72 65 70 65 61 74 3a 6e 6f 2d 72 65 70 65 61 74 7d 2e 72 63 2d 63 61 6e 6f 6e 69 63 61 6c 2d 73 70 65 65 64 2d 6c 69 6d 69 74 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 72 65 63 61 70 74 63 68 61 2f 61 70 69 32 2f 63 61 6e 6f 6e 69 63 61 6c 5f 73 70 65 65 64 5f 6e 61 6d 65 2d 6c 69 6d 69 74 2e 70 6e 67 27 29 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 6e 6f 2d 72 65 70 65 61 74 7d 2e 72 63 2d 63 61 6e 6f 6e 69 63 61 6c 2d 73 74 72 65 65 74 2d 6e 61 6d 65 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 73 74 61 74 69 63 2e 63 6f 6d 2f 72 65 63 61 70 74 63 68 61 2f 61 70 69 32 2f 63 61 6e 6f 6e 69 63 61 6c 5f 73 74 72 65 65 74 5f 6e 61 6d Data Ascii: repeat:no-repeat}.rc-canonical-speed-limit{background:url('https://www.gstatic.com/recaptcha/api2/canonical_ speed_limit.png');background-repeat:no-repeat}.rc-canonical-street-name{background:url('https://www.gstatic.co m/recaptcha/api2/canonical_street_nam

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49812	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1156	OUT	GET /ca/restor/assets/polyfills-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1157	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:06 UTC	1157	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49814	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:05 UTC	1156	OUT	GET /ca/restor/assets/main-es2015.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1157	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:05 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:06 UTC	1158	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49815	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1174	OUT	GET /ca/restor/assets/cwc.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1192	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1192	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49816	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1174	OUT	GET /ca/restor/assets/614267586032718 HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1192	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:30:50 GMT ETag: "3fa5e-5c2686d518680" Accept-Ranges: bytes Content-Length: 260702 Connection: close
2021-09-27 18:34:06 UTC	1213	IN	Data Raw: 2f 2a 2a 0a 2a 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 31 37 2d 70 72 65 73 65 6e 74 2c 20 46 61 63 65 62 6f 6f 6b 2c 20 49 6e 63 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0a 2a 0a 2a 20 59 6f 75 20 61 72 65 20 68 65 72 65 62 79 20 67 72 61 6e 74 65 64 20 61 20 6e 6f 6e 2d 65 78 63 6c 75 73 69 76 65 2c 20 77 6f 72 6c 64 77 69 64 65 2c 20 72 6f 79 61 6c 74 79 2d 66 72 65 65 20 6c 69 63 65 6e 73 65 20 74 6f 20 75 73 65 2c 0a 2a 20 63 6f 70 79 2c 20 6d 6f 64 69 66 79 2c 20 61 6e 64 20 64 69 73 74 72 69 62 75 74 65 20 74 68 69 73 20 73 6f 66 74 77 61 72 65 20 69 6e 20 73 6f 75 72 63 65 20 63 6f 64 65 20 6f 72 20 62 69 6e 61 72 79 20 66 6f 72 6d 20 66 6f 72 20 75 73 65 0a 2a 20 69 6e 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 77 69 Data Ascii: /*** Copyright (c) 2017-present, Facebook, Inc. All rights reserved.** You are hereby granted a non-exclusive, worldwide, royalty-free license to use,* copy, modify, and distribute this software in source code or binary form for use* in c onnection wi
2021-09-27 18:34:06 UTC	1246	IN	Data Raw: 7a 5d 2b 22 7d 7d 2c 73 74 3a 7b 74 79 70 65 3a 22 73 74 72 69 6e 67 22 2c 74 79 70 65 50 61 72 61 6d 73 3a 7b 6c 6f 77 65 72 63 61 73 65 3a 21 30 2c 74 72 75 6e 63 61 74 65 3a 32 2c 73 74 72 69 70 3a 22 61 6c 6c 5f 6e 6f 6e 5f 6c 61 74 69 6e 5f 61 6c 70 68 61 5f 6e 75 6d 65 72 69 63 22 2c 74 65 73 74 3a 22 5e 5b 61 2d 7a 5d 2b 22 7d 7d 2c 64 6f 62 3a 7b 74 79 70 65 3a 22 64 61 74 65 22 7d 2c 64 6f 62 79 3a 7b 74 79 70 65 3a 22 73 74 72 69 6e 67 22 2c 74 79 70 65 50 61 72 61 6d 73 3a 7b 74 65 73 74 3a 22 5e 5b 30 2d 39 5d 7b 34 2c 34 7d 24 22 7d 7d 2c 67 65 6e 3a 7b 74 79 70 65 3a 22 65 6e 75 6d 22 2c 74 79 70 65 50 61 72 61 6d 73 3a 7b 6c 6f 77 65 72 63 61 73 65 3a 21 30 2c 6f 70 74 69 6f 6e 73 3a 5b 22 66 22 2c 22 6d 22 5d 7d 7d 2c 64 6f 62 6d 3a 7b 74 Data Ascii: z]+"}},st:{type:"string",typeParams:{lowercase:!0,truncate:2,strip:"all_non_latin_alpha_numeric",test:"^[a-z]+"}},dob:{type:"date"},doby:{type:"string",typeParams:{test:"^[0-9]{4,4}$"}},gen:{type:"enum",typeParams:{lowercase:!0, options:["f","m"]}},dobm:{t
2021-09-27 18:34:06 UTC	1278	IN	Data Raw: 79 70 65 2c 6f 3d 62 2e 42 55 47 47 59 5f 53 41 46 41 52 49 5f 49 54 45 52 41 54 4f 52 53 2c 70 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 74 68 69 73 7d 3b 61 2e 65 78 70 6f 72 74 73 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 71 2c 72 2c 73 2c 74 29 7b 65 28 63 2c 62 2c 71 29 3b 76 61 72 20 75 3b 71 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 61 3d 3d 3d 72 26 26 7a 29 72 65 74 75 72 6e 20 7a 3b 69 66 28 21 6f 26 26 61 20 69 6e 20 78 29 72 65 74 75 72 6e 20 78 5b 61 5d 3b 73 77 69 74 63 68 28 61 29 7b 63 61 73 65 22 6b 65 79 73 22 3a 63 61 73 65 22 76 61 6c 75 65 73 22 3a 63 61 73 65 22 65 6e 74 72 69 65 73 22 3a 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6e 65 77 20 63 28 74 68 69 73 2c 61 29 7d 7d Data Ascii: ype,o=b.BUGGY_SAFARI_ITERATORS,p=function(){return this};a.exports=function(a,b,c,q,r,s,t){e(c,b,q);var u;q=function(a){if(a===r&&z)return z;if(!o&&a in x)return x[a];switch(a){case"keys":case"values":case"entries":return functi on(){return new c(this,a)}}
2021-09-27 18:34:06 UTC	1311	IN	Data Raw: 6e 65 78 74 28 29 29 2e 64 6f 6e 65 29 3b 64 3d 21 30 29 7b 67 3d 4f 28 67 2e 76 61 6c 75 65 2c 30 2c 62 2c 30 29 3b 67 26 26 63 2e 70 75 73 68 2e 61 70 70 6c 79 28 63 2c 4a 28 67 29 29 7d 7d 63 61 74 63 68 28 61 29 7b 65 3d 21 30 2c 66 3d 61 7d 66 69 6e 61 6c 6c 79 7b 74 72 79 7b 64 7c 7c 6e 75 6c 6c 3d 3d 61 5b 22 72 65 74 75 72 6e 22 5d 7c 7c 61 5b 22 72 65 74 75 72 6e 22 5d 28 29 7d 66 69 6e 61 6c 6c 79 7b 69 66 28 65 29 74 68 72 6f 77 20 66 7d 7d 72 65 74 75 72 6e 20 63 7d 28 62 2c 61 2e 6e 6f 64 65 31 54 72 65 65 29 3a 6e 75 6c 6c 7d 66 75 6e 63 74 69 6f 6e 20 50 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 61 29 7b 69 66 28 41 72 72 61 79 2e 69 73 41 72 72 61 79 28 61 29 29 72 65 74 75 72 6e 20 61 7d 28 61 29 7c 7c 66 75 6e 63 Data Ascii: next()).done);d=!0){g=O(g.value,0,b,0);g&&c.push.apply(c,J(g))}}catch(a){e=!0,f=a}finally{try{d||null==a["re turn"]||a["return"]()}finally{if(e)throw f}}return c}(b,a.node1Tree):null}function P(a,b){return function(a){if(Array.isArray(a))r eturn a}(a)||func

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1355	IN	Data Raw: 76 65 72 74 4e 6f 64 65 54 6f 48 54 4d 4c 45 6c 65 6d 65 6e 74 22 29 2c 6e 3d 66 2e 67 65 74 46 62 65 76 65 6e 74 73 4d 6f 64 75 6c 65 73 28 22 73 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 45 78 74 72 61 63 74 42 75 74 74 6f 6e 43 6c 69 63 6b 45 76 65 6e 74 50 61 79 6c 6f 61 64 22 29 2c 6f 3d 66 2e 67 65 74 46 62 65 76 65 6e 74 73 4d 6f 64 75 6c 65 73 28 22 73 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 45 78 74 72 61 63 74 46 6f 72 6d 22 29 2c 70 3d 66 2e 67 65 74 46 62 65 76 65 6e 74 73 4d 6f 64 75 6c 65 73 28 22 73 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 49 73 49 57 4c 45 6c 65 6d 65 6e 74 22 29 2c 71 3d 66 2e 67 65 74 46 62 65 76 65 6e 74 73 4d 6f 64 75 6c 65 73 28 22 73 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 4d 61 6b 65 53 61 66 65 22 29 2c 72 3d Data Ascii: vertNodeToHTMLElement"),n=f.getFbeventsModules("signalsFBEventsExtractButtonClickEventPayload"),o=f.getFbeventsModules("signalsFBEventsExtractForm"),p=f.getFbeventsModules("signalsFBEventsIsIWLElement"),q=f.getFbeventsModules("signalsFBEventsMakeSafe"),r=
2021-09-27 18:34:06 UTC	1372	IN	Data Raw: 3d 3d 22 75 6e 64 65 66 69 6e 65 64 22 3f 22 75 6e 64 65 66 69 6e 65 64 22 3a 67 28 73 65 6c 66 29 29 26 26 73 65 6c 66 26 26 73 65 6c 66 2e 4d 61 74 68 3d 3d 4d 61 74 68 3f 73 65 6c 66 3a 46 75 6e 63 74 69 6f 6e 28 22 72 65 74 75 72 6e 20 74 68 69 73 22 29 28 29 7d 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 64 3d 63 28 36 29 2c 65 3d 63 28 36 35 29 2e 66 2c 66 3d 63 28 36 37 29 2c 68 3d 63 28 33 38 29 2c 69 3d 63 28 33 31 29 2c 6a 3d 63 28 31 33 29 2c 6b 3d 63 28 31 34 29 2c 6c 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 66 75 6e 63 74 69 6f 6e 28 64 2c 62 2c 63 29 7b 69 66 28 74 68 69 73 20 69 6e 73 74 61 6e 63 65 6f 66 20 61 29 7b 73 77 69 74 63 68 28 61 72 67 75 6d 65 6e 74 73 2e Data Ascii: =="undefined"?"undefined":g(self))&&self&&self.Math==Math?self:Function("return this")()},function(a,b,c){"use strict";var d=c(6),e=c(65).f,f=c(67),h=c(38),i=c(31),j=c(13),k=c(14),l=function(a){var b=function(d,b,c){if(this instanceof a){switch(arguments.
2021-09-27 18:34:07 UTC	1421	IN	Data Raw: 29 7b 76 61 72 20 64 3d 63 28 33 33 29 2c 65 3d 4d 61 74 68 2e 6d 61 78 2c 66 3d 4d 61 74 68 2e 6d 69 6e 3b 61 2e 65 78 70 6f 72 74 73 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 61 3d 64 28 61 29 3b 72 65 74 75 72 6e 20 61 3c 30 3f 65 28 61 2b 62 2c 30 29 3a 66 28 61 2c 62 29 7d 7d 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 62 3d 63 28 36 29 2e 64 6f 63 75 6d 65 6e 74 3b 61 2e 65 78 70 6f 72 74 73 3d 62 26 26 62 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 7d 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 76 61 72 20 64 3d 63 28 35 33 29 3b 62 3d 7b 7d 3b 62 5b 63 28 34 29 28 22 74 6f 53 74 72 69 6e 67 54 61 67 22 29 5d 3d 22 7a 22 2c 61 2e 65 78 70 6f 72 74 73 3d 22 5b 6f 62 6a 65 63 74 20 7a 5d 22 Data Ascii:){var d=c(33),e=Math.max,f=Math.min;a.exports=function(a,b){a=d(a);return a<0?e(a+b,0):f(a,b)}},function(a,b,c){b=c(6).document;a.exports=b&&b.documentElement},function(a,b,c){"use strict";var d=c(53);b={};b[c(4)("toStringTag")]="z",a.exports="[object z]"
2021-09-27 18:34:07 UTC	1439	IN	Data Raw: 78 74 72 61 63 74 6f 72 49 44 3a 62 2e 69 64 2c 6a 73 6f 6e 4c 44 3a 66 61 28 29 7d 3b 63 61 73 65 22 43 53 53 22 3a 76 61 72 20 63 3d 70 28 29 28 62 2e 65 78 74 72 61 63 74 6f 72 43 6f 6e 66 69 67 2e 70 61 72 61 6d 65 74 65 72 53 65 6c 65 63 74 6f 72 73 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 72 65 74 75 72 6e 20 6e 75 6c 6c 21 3d 28 62 3d 61 28 62 2e 73 65 6c 65 63 74 6f 72 29 29 3f 62 5b 30 5d 3a 62 7d 29 3b 69 66 28 6e 75 6c 6c 3d 3d 63 29 72 65 74 75 72 6e 20 6e 75 6c 6c 3b 69 66 28 63 2e 6c 65 6e 67 74 68 3d 3d 3d 69 61 29 7b 76 61 72 20 64 3d 63 5b 30 5d 2c 65 3d 63 5b 31 5d 3b 69 66 28 6e 75 6c 6c 21 3d 64 26 26 6e 75 6c 6c 21 3d 65 29 7b 64 3d 67 61 28 64 2c 65 29 3b 64 26 26 63 2e 70 75 73 68 2e 61 70 70 6c 79 28 63 2c 64 29 7d 7d 76 61 Data Ascii: xtractorID:b.id,jsonLD:fa()};case"CSS":var c=p()(b.extractorConfig.parameterSelectors,function(b){return null!=(b=aa(a,b.selector))?b[0]:b});if(null==c)return null;if(c.length===ia){var d=c[0],e=c[1];if(null!=d&&null!=e){d=ga(d,e);d&&c.push.apply(c,d)}}va
2021-09-27 18:34:07 UTC	1456	IN	Data Raw: 61 6c 75 65 3a 61 7d 29 2c 32 26 62 26 26 22 73 74 72 69 6e 67 22 21 3d 74 79 70 65 6f 66 20 61 29 66 6f 72 28 76 61 72 20 65 20 69 6e 20 61 29 63 2e 64 28 64 2c 65 2c 66 75 6e 63 74 69 6f 6e 28 62 29 7b 72 65 74 75 72 6e 20 61 5b 62 5d 7d 2e 62 69 6e 64 28 6e 75 6c 6c 2c 65 29 29 3b 72 65 74 75 72 6e 20 64 7d 2c 63 2e 6e 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 61 26 26 61 2e 5f 5f 65 73 4d 6f 64 75 6c 65 3f 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 5b 22 64 65 66 61 75 6c 74 22 5d 7d 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 61 7d 3b 72 65 74 75 72 6e 20 63 2e 64 28 62 2c 22 61 22 2c 62 29 2c 62 7d 2c 63 2e 6f 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 2e 70 72 6f 74 Data Ascii: alue:a}),2&b&&"string"!=typeof a)for(var e in a)c.d(d,e,function(b){return a[b]}.bind(null,e));return d},c.n=function(a){var b=a&&a.__esModule?function(){return a["default"]}:function(){return a};return c.d(b,"a",b),b},c.o=function(a,b){return Object.prot
2021-09-27 18:34:07 UTC	1472	IN	Data Raw: 70 65 6e 64 43 68 69 6c 64 28 61 29 2c 61 2e 73 72 63 3d 53 74 72 69 6e 67 28 22 6a 61 76 61 73 63 72 69 70 74 3a 22 29 2c 28 61 3d 61 2e 63 6f 6e 74 65 6e 74 57 69 6e 64 6f 77 2e 64 6f 63 75 6d 65 6e 74 29 2e 6f 70 65 6e 28 29 2c 61 2e 77 72 69 74 65 28 22 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 46 3d 4f 62 6a 65 63 74 3c 2f 73 63 72 69 70 74 3e 22 29 2c 61 2e 63 6c 6f 73 65 28 29 2c 6b 3d 61 2e 46 3b 62 2d 2d 3b 29 64 65 6c 65 74 65 20 6b 2e 70 72 6f 74 6f 74 79 70 65 5b 66 5b 62 5d 5d 3b 72 65 74 75 72 6e 20 6b 28 29 7d 3b 61 2e 65 78 70 6f 72 74 73 3d 4f 62 6a 65 63 74 2e 63 72 65 61 74 65 7c 7c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 29 7b 76 61 72 20 63 3b 72 65 74 75 72 6e 20 6e 75 6c 6c 21 3d 61 3f 28 6a 2e 70 72 6f 74 6f 74 79 70 65 3d Data Ascii: pendChild(a),a.src=String("javascript:"),(a=a.contentWindow.document).open(),a.write("<script>document.F=Object</script>"),a.close(),k=a.F;b--;)delete k.prototype[f[b]];return k()};a.exports=Object.create||function(a,b){var c;return null!==a?(j.prototype=
2021-09-27 18:34:07 UTC	1491	IN	Data Raw: 6f 69 64 20 30 2c 6f 66 66 65 72 73 3a 7b 70 72 69 63 65 3a 76 6f 69 64 20 30 2c 70 72 69 63 65 43 75 72 72 65 6e 63 79 3a 76 6f 69 64 20 30 7d 2c 70 72 6f 64 75 63 74 49 44 3a 76 6f 69 64 20 30 7d 2c 54 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 69 66 28 6e 75 6c 6c 3d 3d 63 29 72 65 74 75 72 6e 20 61 3b 76 61 72 20 64 3d 6c 28 29 28 61 2e 6f 66 66 65 72 73 29 3b 72 65 74 75 72 6e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 74 79 70 65 22 3a 22 50 72 6f 64 75 63 74 22 2c 61 64 64 69 74 69 6f 6e 61 6c 54 79 70 65 3a 6e 75 6c 6c 21 3d 61 2e 61 64 64 69 74 69 6f 6e 61 6c 54 79 70 65 3f 61 2e 61 64 64 69 74 69 6f 6e 61 6c 54 79 70 65 3a 22 63 6f 6e 74 65 6e 74 5f 74 79 70 65 22 3d 3d 3d 62 3f Data Ascii: oid 0,offers:{price:void 0,priceCurrency:void 0},productID:void 0},T=function(a,b,c){if(null==c)return a;var d=l()(a.offers);return{"@context":"http://schema.org","@type":"Product",additionalType:null!=a.additionalType?a.additionalType:"content_type"===b?
2021-09-27 18:34:07 UTC	1507	IN	Data Raw: 73 7d 28 61 2c 62 2c 63 2c 64 29 7d 29 3b 66 2e 65 6e 73 75 72 65 4d 6f 64 75 6c 65 52 65 67 69 73 74 65 72 65 64 28 22 53 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 50 69 78 65 6c 50 49 49 53 63 68 65 6d 61 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 2c 64 29 7b 76 61 72 20 65 3d 7b 65 78 70 6f 72 74 73 3a 7b 7d 7d 3b 65 2e 65 78 70 6f 72 74 73 3b 28 66 75 6e 63 74 69 6f 6e 28 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 65 2e 65 78 70 6f 72 74 73 3d 7b 65 6d 61 69 6c 3a 7b 74 79 70 65 3a 22 65 6d 61 69 6c 22 7d 2c 70 68 6f 6e 65 5f 6e 75 6d 62 65 72 22 7d 2c 66 6e 3a 7b 74 79 70 65 3a 22 73 74 72 69 6e 67 22 2c 74 79 70 65 50 61 72 61 6d 73 3a 7b 6c 6f 77 65 Data Ascii: s}(a,b,c,d)});f.ensureModuleRegistered("SignalsFBEventsPixelPIISchema",function(){return function(f,g,h,d){var e={exports:{}};e.exports;(function(){"use strict";e.exports={email:{type:"email"},phone:{type:"phone_number"},fn:{type:"string",typeParams:{lowe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1525	IN	Data Raw: 3f 65 28 61 29 3a 64 28 61 2c 7b 7d 29 7d 2c 67 65 74 74 65 72 46 6f 72 3a 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 62 29 7b 76 61 72 20 63 3b 69 66 28 21 67 28 62 29 7c 7c 28 63 3d 65 28 62 29 29 2e 74 79 70 65 21 3d 3d 61 29 74 68 72 6f 77 20 54 79 70 65 45 72 72 6f 72 28 22 49 6e 63 6f 6d 70 61 74 69 62 6c 65 20 72 65 63 65 69 76 65 72 2c 20 22 2b 61 2b 22 20 72 65 71 75 69 72 65 64 22 29 3b 72 65 74 75 72 6e 20 63 7d 7d 7d 2c 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 62 3d 63 28 37 34 29 3b 63 3d 63 28 36 29 2e 57 65 61 6b 4d 61 70 3b 61 2e 65 78 70 6f 72 74 73 3d 22 66 75 6e 63 74 69 6f 6e 22 3d 3d 74 79 70 65 6f 66 20 63 26 26 2f 6e 61 74 69 76 65 20 63 6f 64 65 2f 2e 74 65 73 74 28 62 2e 63 61 6c Data Ascii: ?e(a):d(a,{})},getterFor:function(a){return function(b){var c;if(!g(b)||(c=e(b)).type!==a)throw TypeError("Incompatible receiver, "+a+" required");return c}}}},function(a,b,c){b=c(74);c=c(6).WeakMap;a.exports="function"==typeof c&&/native code/.test(b.cal
2021-09-27 18:34:07 UTC	1541	IN	Data Raw: 3d 62 2e 70 61 72 65 6e 74 4e 6f 64 65 2c 21 61 7c 7c 21 62 29 72 65 74 75 72 6e 20 6e 75 6c 6c 7d 72 65 74 75 72 6e 20 61 26 26 62 26 26 61 2e 69 73 53 61 6d 65 4e 6f 64 65 28 62 29 26 26 64 2e 6c 65 6e 67 74 68 3e 30 3f 7b 70 61 72 65 6e 74 4e 6f 64 65 3a 61 2c 6e 6f 64 65 31 54 72 65 65 3a 64 2e 72 65 76 65 72 73 65 28 29 2c 6e 6f 64 65 32 54 72 65 65 3a 65 2e 72 65 76 65 72 73 65 28 29 7d 3a 6e 75 6c 6c 7d 28 61 2c 62 29 3b 69 66 28 21 61 29 72 65 74 75 72 6e 20 6e 75 6c 6c 3b 62 3d 66 75 6e 63 74 69 6f 6e 28 61 2c 62 2c 63 29 7b 66 6f 72 28 76 61 72 20 64 3d 5b 5d 2c 61 3d 61 2e 66 69 72 73 74 43 68 69 6c 64 3b 61 3b 29 61 2e 69 73 53 61 6d 65 4e 6f 64 65 28 62 2e 6e 6f 64 65 29 7c 7c 21 4d 28 62 2e Data Ascii: =b.parentNode,!a||!b)return null}return a&&b&&a.isSameNode(b)&&d.length>0?{parentNode:a,node1Tree:d.reverse(),node2Tree:e.reverse()}:null}(a,b);if(!a)return null;b=function(a,b,c){for(var d=[],a=a.firstChild;a;)a.isSameNode(b.node)||a.isSameNode(c)||!M(b.
2021-09-27 18:34:07 UTC	1557	IN	Data Raw: 62 5d 5d 3d 62 3b 72 65 74 75 72 6e 20 61 7d 2c 7b 7d 29 2c 72 3d 7b 63 74 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6a 28 67 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 2e 53 68 6f 70 69 66 79 2e 63 68 65 63 6b 6f 75 74 2e 62 69 6c 6c 69 6e 67 5f 61 64 64 72 65 73 73 2e 63 69 74 79 7d 29 7d 2c 65 6d 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6a 28 67 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 2e 53 68 6f 70 69 66 79 2e 63 68 65 63 6b 6f 75 74 2e 65 6d 61 69 6c 7d 29 7d 2c 66 6e 3a 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 6a 28 67 2c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 61 2e 53 68 6f 70 69 66 79 2e 63 68 65 63 6b 6f 75 74 2e 62 69 6c 6c 69 6e 67 5f 61 64 Data Ascii: b]]=b;return a},{}),r={ct:function(){return j(g,function(a){return a.Shopify.checkout.billing_address.city})},em:function(){return j(g,function(a){return a.Shopify.checkout.email})},fn:function(){return j(g,function(a){return a.Shopify.checkout.billing_ad
2021-09-27 18:34:07 UTC	1579	IN	Data Raw: 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 28 64 29 2c 65 29 3b 65 6c 73 65 20 72 65 74 75 72 6e 20 62 28 66 2c 64 2c 65 29 7d 66 75 6e 63 74 69 6f 6e 20 64 28 62 29 7b 62 3d 4a 53 4f 4e 2e 70 61 72 73 65 28 62 29 3b 76 61 72 20 63 3d 61 28 62 29 3b 62 3d 62 5b 63 5d 3b 69 66 28 63 3d 3d 22 65 76 65 6e 74 22 29 7b 76 61 72 20 65 3d 61 28 62 29 3b 69 66 28 65 3d 3d 22 65 71 22 29 72 65 74 75 72 6e 21 30 7d 69 66 28 63 3d 3d 22 61 6e 64 22 7c 7c 63 3d 3d 22 6f 72 22 29 7b 69 66 28 21 41 72 72 61 79 2e 69 73 41 72 72 61 79 28 62 29 29 72 65 74 75 72 6e 21 31 3b 66 6f 72 28 76 61 72 20 65 3d 30 3b 65 3c 62 2e 6c 65 6e 67 74 68 3b 65 2b 2b 29 7b 63 3d 64 28 4a 53 4f 4e 2e 73 74 72 69 6e 67 69 66 79 28 62 5b 65 5d 29 29 3b 69 66 28 63 29 72 65 74 75 Data Ascii: JSON.stringify(d),e);else return b(f,d,e)}function d(b){b=JSON.parse(b);var c=a(b);b=b[c];if(c==="event"){var e=a(b);if(e==="eq")return!0}if(c==="and"||c==="or"){if(!Array.isArray(b))return!1;for(var e=0;e<b.length;e++){c=d(JSON.stringify(b[e]));if(c)retu

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49817	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1175	OUT	GET /ca/restor/assets/fbevents.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1193	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "16e4e-5c26847e30180" Accept-Ranges: bytes Content-Length: 93774 Vary: Accept-Encoding Connection: close Content-Type: application/javascript
2021-09-27 18:34:06 UTC	1229	IN	Data Raw: 2f 2a 2a 0a 2a 20 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 32 30 31 37 2d 70 72 65 73 65 6e 74 2c 20 46 61 63 65 62 6f 6f 6b 2c 20 49 6e 63 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0a 2a 0a 2a 20 59 6f 75 20 61 72 65 20 68 65 72 65 62 79 20 67 72 61 6e 74 65 64 20 61 20 6e 6f 6e 2d 65 78 63 6c 75 73 69 76 65 2c 20 77 6f 72 6c 64 77 69 64 65 2c 20 72 6f 79 61 6c 74 79 2d 66 72 65 65 20 6c 69 63 65 6e 73 65 20 74 6f 20 75 73 65 2c 0a 2a 20 63 6f 70 79 2c 20 6d 6f 64 69 66 79 2c 20 61 6e 64 20 64 69 73 74 72 69 62 75 74 65 20 74 68 69 73 20 73 6f 66 74 77 61 72 65 20 69 6e 20 73 6f 75 72 63 65 20 63 6f 64 65 20 6f 72 20 62 69 6e 61 72 79 20 66 6f 72 6d 20 66 6f 72 20 75 73 65 0a 2a 20 69 6e 20 63 6f 6e 6e 65 63 74 69 6f 6e 20 77 69 Data Ascii: /*** Copyright (c) 2017-present, Facebook, Inc. All rights reserved.** You are hereby granted a non-exclusive, worldwide, royalty-free license to use,* copy, modify, and distribute this software in source code or binary form for use* in connection wi

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1262	IN	Data Raw: 79 70 65 22 2c 22 63 75 72 72 65 6e 63 79 22 2c 22 63 6f 6e 74 65 6e 74 73 22 2c 22 6e 75 6d 5f 69 74 65 6d 73 22 2c 22 6f 72 64 65 72 5f 69 64 22 2c 22 70 72 65 64 69 63 74 65 64 5f 6c 74 76 22 2c 22 73 65 61 72 63 68 5f 73 74 72 69 6e 67 22 2c 22 73 74 61 74 75 73 22 2c 22 73 75 62 73 63 72 69 70 74 69 6f 6e 5f 69 64 22 2c 22 76 61 6c 75 65 22 2c 22 69 64 22 2c 22 69 74 65 6d 5f 70 72 69 63 65 22 2c 22 71 75 61 6e 74 69 74 79 22 2c 22 63 74 22 2c 22 64 62 22 2c 22 65 6d 22 2c 22 65 78 74 65 72 6e 61 6c 5f 69 64 22 2c 22 66 6e 22 2c 22 67 65 22 2c 22 6c 6e 22 2c 22 6e 61 6d 65 73 70 61 63 65 22 2c 22 70 68 22 2c 22 73 74 22 2c 22 7a 70 22 5d 29 3b 66 75 6e 63 74 69 6f 6e 20 63 28 61 29 7b 72 65 74 75 72 6e 20 74 79 70 65 6f 66 20 61 3d 3d 3d 22 73 74 72 Data Ascii: ype","currency","contents","num_items","order_id","predicted_ltv","search_string","status","subscription_id","value","id","item_price","quantity","ct","db","em","external_id","fn","ge","ln","namespace","ph","st","zp"]);function c(a){return typeof a==="str
2021-09-27 18:34:06 UTC	1294	IN	Data Raw: 75 73 65 72 41 67 65 6e 74 2e 69 6e 64 65 78 4f 66 28 22 4d 65 73 73 65 6e 67 65 72 4c 69 74 65 46 6f 72 69 4f 53 22 29 3b 72 65 74 75 72 6e 20 62 21 3d 3d 6e 75 6c 6c 26 26 28 63 21 3d 2d 31 7c 7c 64 21 3d 2d 31 7c 7c 61 21 3d 2d 31 29 7d 76 61 72 20 62 3d 61 28 29 3b 66 75 6e 63 74 69 6f 6e 20 63 28 29 7b 72 65 74 75 72 6e 20 62 7d 6a 2e 65 78 70 6f 72 74 73 3d 63 7d 29 28 29 3b 72 65 74 75 72 6e 20 6a 2e 65 78 70 6f 72 74 73 7d 28 61 2c 62 2c 63 2c 64 29 7d 29 3b 66 2e 65 6e 73 75 72 65 4d 6f 64 75 6c 65 52 65 67 69 73 74 65 72 65 64 28 22 53 69 67 6e 61 6c 73 46 42 45 76 65 6e 74 73 47 65 74 49 57 4c 50 61 72 61 6d 65 74 65 72 73 45 76 65 6e 74 22 2c 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 67 2c 68 2c 6a 2c 6b Data Ascii: userAgent.indexOf("MessengerLiteForiOS");return b!==null&&(c!=-1||d!=-1||a!=-1)}var b=a();function c(){return b}j.exports=c})();return j.exports}(a,b,c,d)});f.ensureModuleRegistered("SignalsFBEventsGetIWLParametersEvent",function(){return function(g,h,j,k
2021-09-27 18:34:06 UTC	1339	IN	Data Raw: 6e 22 66 62 65 76 65 6e 74 73 2e 70 6c 75 67 69 6e 73 2e 22 2b 61 7d 66 75 6e 63 74 69 6f 6e 20 6b 28 61 2c 62 29 7b 69 66 28 61 3d 3d 3d 22 66 62 65 76 65 6e 74 73 22 29 72 65 74 75 72 6e 20 6e 65 77 20 67 28 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 29 3b 69 66 28 62 20 69 6e 73 74 61 6e 63 65 6f 66 20 67 29 72 65 74 75 72 6e 20 62 3b 69 66 28 62 3d 3d 6e 75 6c 6c 7c 7c 28 74 79 70 65 6f 66 20 62 3d 3d 3d 22 75 6e 64 65 66 69 6e 65 64 22 3f 22 75 6e 64 65 66 69 6e 65 64 22 3a 69 28 62 29 29 21 3d 3d 22 6f 62 6a 65 63 74 22 29 7b 65 28 6e 65 77 20 45 72 72 6f 72 28 22 49 6e 76 61 6c 69 64 20 70 6c 75 67 69 6e 20 72 65 67 69 73 74 65 72 65 64 20 22 2b 61 29 29 3b 72 65 74 75 72 6e 20 6e 65 77 20 67 28 66 75 6e 63 74 69 6f 6e 28 29 7b 7d 29 7d 76 61 72 20 63 3d Data Ascii: n"fbevents.plugins."+a}function k(a,b){if(a==="fbevents")return new g(function(){});if(b instanceof g)return b;if(b==null||(typeof b==="undefined"?"undefined":i(b))!=="object"){e(new Error("Invalid plugin registered "+a));return new g(function(){})}var c=
2021-09-27 18:34:06 UTC	1388	IN	Data Raw: 3b 69 66 28 6a 28 61 29 3d 3d 3d 21 31 29 72 65 74 75 72 6e 21 31 3b 72 65 74 75 72 6e 20 4f 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e 68 61 73 4f 77 6e 50 72 6f 70 65 72 74 79 2e 63 61 6c 6c 28 61 2c 22 69 73 50 72 6f 74 6f 74 79 70 65 4f 66 22 29 3d 3d 3d 21 31 3f 21 31 3a 21 30 7d 76 61 72 20 6d 3d 4e 75 6d 62 65 72 2e 69 73 49 6e 74 65 67 65 72 7c 7c 66 75 6e 63 74 69 6f 6e 28 61 29 7b 72 65 74 75 72 6e 20 74 79 70 65 6f 66 20 61 3d 3d 3d 22 6e 75 6d 62 65 72 22 26 26 69 73 46 69 6e 69 74 65 28 61 29 26 26 4d 61 74 68 2e 66 6c 6f 6f 72 28 61 29 3d 3d 3d 61 7d 3b 66 75 6e 63 74 69 6f 6e 20 6f 28 61 29 7b 72 65 74 75 72 6e 20 6d 28 61 29 26 26 61 3e 3d 30 26 26 61 3c 3d 4e 75 6d 62 65 72 2e 4d 41 58 5f 53 41 46 45 5f 49 4e 54 45 47 45 52 7d 66 75 Data Ascii: ;if(j(a)===!1)return!1;return Object.prototype.hasOwnProperty.call(a,"isPrototypeOf")===!1?!1:!0}var m=Number.isInteger||function(a){return typeof a==="number"&&isFinite(a)&&Math.floor(a)===a};function o(a){return m(a)&&a>=0&&a<=Number.MAX_SAFE_INTEGER}fu
2021-09-27 18:34:06 UTC	1409	IN	Data Raw: 21 66 29 7b 62 28 7b 61 63 74 69 6f 6e 3a 22 46 42 5f 4c 4f 47 22 2c 6c 6f 67 54 79 70 65 3a 22 46 61 63 65 62 6f 6f 6b 20 50 69 78 65 6c 20 45 72 72 6f 72 22 2c 6c 6f 67 4d 65 73 73 61 67 65 3a 22 50 69 78 65 6c 20 63 6f 64 65 20 69 73 20 6e 6f 74 20 69 6e 73 74 61 6c 6c 65 64 20 63 6f 72 72 65 63 74 6c 79 20 6f 6e 20 74 68 69 73 20 70 61 67 65 22 7d 2c 22 2a 22 29 3b 22 65 72 72 6f 72 22 69 6e 20 63 6f 6e 73 6f 6c 65 26 26 63 6f 6e 73 6f 6c 65 2e 65 72 72 6f 72 28 22 46 61 63 65 62 6f 6f 6b 20 50 69 78 65 6c 20 45 72 72 6f 72 3a 20 50 69 78 65 6c 20 63 6f 64 65 20 69 73 20 6e 6f 74 20 69 6e 73 74 61 6c 6c 65 64 20 63 6f 72 72 65 63 74 6c 79 20 6f 6e 20 74 68 69 73 20 70 61 67 65 22 29 3b 72 65 74 75 72 6e 21 31 7d 72 65 74 75 72 6e 21 30 7d 28 29 29 72 Data Ascii: !f){b({action:"FB_LOG",logType:"Facebook Pixel Error",logMessage:"Pixel code is not installed correctly on this page"},"*");"error"in console&&console.error("Facebook Pixel Error: Pixel code is not installed correctly on this page");return!1}return!0}())r

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49818	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1191	OUT	GET /ca/restor/assets/recaptcha__en.js.download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1245	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1245	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49819	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1193	OUT	GET /ca/restor/assets/insight.min.js(1).download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1245	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:06 UTC	1245	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49765	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	54	OUT	GET /ca/restor/assets/foundation.css HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:33:59 UTC	78	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "33543-5c26847e30180" Accept-Ranges: bytes Content-Length: 210243 Vary: Accept-Encoding Connection: close Content-Type: text/css

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	95	IN	Data Raw: 0a 6d 65 74 61 2e 66 6f 75 6e 64 61 74 69 6f 6e 2d 76 65 72 73 69 6f 6e 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 2f 35 2e 35 2e 31 2f 22 0a 7d 0a 0a 6d 65 74 61 2e 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 73 6d 61 6c 6c 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 2f 6f 6e 6c 79 20 73 63 72 65 65 6e 2f 22 3b 0a 20 20 77 69 64 74 68 3a 20 30 0a 7d 0a 0a 6d 65 74 61 2e 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 73 6d 61 6c 6c 2d 6f 6e 6c 79 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 2f 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 34 30 65 6d 29 2f 22 3b 0a 20 20 77 69 64 74 68 3a 20 30 0a 7d 0a 0a 6d 65 74 61 2e 66 6f 75 6e 64 61 74 69 6f 6e 2d 6d 71 2d 73 6d 61 6c 6c 2d 6d 65 64 69 75 6d 20 7b Data Ascii: meta.foundation-version { font-family: "/5.5.1/"}meta.foundation-mq-small { font-family: "/only screen/"; width: 0}meta.foundation-mq-small-only { font-family: "/only screen and (max-width: 40em)/"; width: 0}meta.foundation-mq-medium {
2021-09-27 18:33:59 UTC	175	IN	Data Raw: 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 31 30 20 7b 0a 20 20 20 20 77 69 64 74 68 3a 20 38 33 2e 33 33 33 33 33 33 25 0a 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 31 31 20 7b 0a 20 20 20 20 77 69 64 74 68 3a 20 39 31 2e 36 36 36 36 37 25 0a 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 31 32 20 7b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 0a 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 6f 66 66 73 65 74 2d 30 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 33 30 25 20 21 69 6d 70 6f 72 74 61 6e 74 0a 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 6f 66 66 73 65 74 2d 31 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 38 2e 33 33 33 33 33 25 20 21 69 6d 70 6f 72 74 61 6e 74 0a 20 20 7d 0a 20 20 2e 6c 61 72 67 65 2d 6f 66 66 73 65 74 2d 32 20 7b 0a 20 20 20 Data Ascii: } .large-10 { width: 83.33333% } .large-11 { width: 91.66667% } .large-12 { width: 100% } .large-offset-0 { margin-left: 0% !important } .large-offset-1 { margin-left: 8.33333% !important } .large-offset-2 {
2021-09-27 18:34:00 UTC	255	IN	Data Raw: 3a 20 32 2e 33 31 32 35 72 65 6d 3b 2a 2f 0a 2f 2a 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 2e 33 31 32 35 72 65 6d 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 2e 70 6f 73 74 66 69 78 2e 62 75 74 74 6f 6e 20 7b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 30 3b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 30 3b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 30 3b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 20 30 3b 2a 2f 0a 2f 2a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 2a 2f 0a 2f 2a 20 20 62 6f 72 64 65 72 3a 20 6e 6f 6e 65 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 2e 70 72 65 66 69 78 2e 62 75 74 74 6f 6e 20 7b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 Data Ascii: : 2.3125rem;*//* line-height: 2.3125rem*//*}*//*.postfix.button {*//* padding-left: 0;*//* padding-right: 0;*//* padding-top: 0;*//* padding-bottom: 0;*//* text-align: center;*//* border: none*//*}*//*.prefix.button {*//* padding-lef
2021-09-27 18:34:00 UTC	303	IN	Data Raw: 62 39 62 39 62 39 0a 7d 0a 0a 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e 20 75 6c 20 6c 69 3e 61 2e 62 75 74 74 6f 6e 2e 73 65 63 6f 6e 64 61 72 79 3a 68 6f 76 65 72 2c 0a 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e 20 75 6c 20 6c 69 3e 61 2e 62 75 74 74 6f 6e 2e 73 65 63 6f 6e 64 61 72 79 3a 66 6f 63 75 73 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 0a 7d 0a 0a 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e 20 75 6c 20 6c 69 3e 61 2e 62 75 74 74 6f 6e 2e 73 75 63 63 65 73 73 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 34 33 41 43 36 41 3b 0a 20 20 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 20 23 33 36 38 61 35 35 3b 0a 20 20 63 6f 6c 6f 72 3a 20 23 66 66 66 0a 7d 0a 0a 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e Data Ascii: b9b9b9}.top-bar-section ul li>a.button.secondary:hover,.top-bar-section ul li>a.button.secondary:focus { color: #333}.top-bar-section ul li>a.button.success { background-color: #43AC6A; border-color: #368a55; color: #fff}.top-bar-section
2021-09-27 18:34:00 UTC	368	IN	Data Raw: 0a 2f 2a 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 65 76 65 6e 2d 37 20 6c 69 3e 62 75 74 74 6f 6e 2c 2a 2f 0a 2f 2a 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 65 76 65 6e 2d 37 20 6c 69 20 2e 62 75 74 74 6f 6e 20 7b 2a 2f 0a 2f 2a 20 20 62 6f 72 64 65 72 2d 6c 65 66 74 3a 20 31 70 78 20 73 6f 6c 69 64 3b 2a 2f 0a 2f 2a 20 20 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 3a 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 35 29 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 65 76 65 6e 2d 37 20 6c 69 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 62 75 74 74 6f 6e 2c 2a 2f 0a 2f 2a 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 65 76 65 6e 2d 37 20 6c 69 3a 66 69 72 73 74 2d 63 68 69 6c 64 20 2e 62 75 74 74 6f 6e 20 7b 2a 2f 0a Data Ascii: /*.button-group.even-7 li>button,*//*.button-group.even-7 li .button {*//* border-left: 1px solid;*//* border-color: rgba(255, 255, 255, 0.5)*//*}*//*.button-group.even-7 li:first-child button,*//*.button-group.even-7 li:first-child .button {*/
2021-09-27 18:34:00 UTC	449	IN	Data Raw: 73 3a 20 31 72 65 6d 3b 2a 2f 0a 2f 2a 20 20 20 20 62 6f 72 64 65 72 2d 74 6f 70 2d 6c 65 66 74 2d 72 61 64 69 75 73 3a 20 31 72 65 6d 3b 2a 2f 0a 2f 2a 20 20 20 20 62 6f 72 64 65 72 2d 74 6f 70 2d 72 69 67 68 74 2d 72 61 64 69 75 73 3a 20 31 72 65 6d 2a 2f 0a 2f 2a 20 20 7d 2a 2f 0a 2f 2a 20 20 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 72 6f 75 6e 64 2e 73 74 61 63 6b 2d 66 6f 72 2d 73 6d 61 6c 6c 3e 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 2c 2a 2f 0a 2f 2a 20 20 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 72 6f 75 6e 64 2e 73 74 61 63 6b 2d 66 6f 72 2d 73 6d 61 6c 6c 3e 2a 3a 6c 61 73 74 2d 63 68 69 6c 64 3e 61 2c 2a 2f 0a 2f 2a 20 20 2e 62 75 74 74 6f 6e 2d 67 72 6f 75 70 2e 72 6f 75 6e 64 2e 73 74 61 63 6b 2d 66 6f 72 2d 73 6d 61 6c 6c 3e 2a 3a 6c 61 73 74 Data Ascii: s: 1rem;*//* border-top-left-radius: 1rem;*//* border-top-right-radius: 1rem*//* }*//* .button-group.round.stack-for-small>*:last-child,*//* .button-group.round.stack-for-small>*:last-child>a,*//* .button-group.round.stack-for-small>*:last
2021-09-27 18:34:00 UTC	526	IN	Data Raw: 68 3a 20 61 75 74 6f 3b 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 3a 20 61 75 74 6f 3b 2a 2f 0a 2f 2a 20 20 66 6c 6f 61 74 3a 20 6e 6f 6e 65 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 30 2e 30 36 33 65 6d 29 20 7b 2a 2f 0a 2f 2a 20 20 2e 69 63 6f 6e 2d 62 61 72 2e 6d 65 64 69 75 6d 2d 76 65 72 74 69 63 61 6c 20 7b 2a 2f 0a 2f 2a 20 20 20 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 2a 2f 0a 2f 2a 20 20 20 20 77 69 64 74 68 3a 20 61 75 74 6f 2a 2f 0a 2f 2a 20 20 7d 2a 2f 0a 2f 2a 20 20 2e 69 63 6f 6e 2d 62 61 72 2e 6d 65 64 69 75 6d 2d 76 65 72 74 69 63 61 6c 20 2e 69 74 65 6d 20 7b 2a 2f 0a 2f 2a 20 20 20 20 77 69 64 74 68 3a 20 61 75 74 6f 3b 2a 2f 0a 2f 2a 20 Data Ascii: h: auto;*//* margin: auto;*//* float: none*//*}*//*@media only screen and (min-width: 40.063em) {*//* .icon-bar.medium-vertical {*//* height: 100%;*//* width: auto*//* }*//* .icon-bar.medium-vertical .item {*//* width: auto;*//*
2021-09-27 18:34:00 UTC	574	IN	Data Raw: 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 2e 32 35 72 65 6d 3b 2a 2f 0a 2f 2a 20 20 6c 69 73 74 2d 73 74 79 6c 65 2d 70 6f 73 69 74 69 6f 6e 3a 20 6f 75 74 73 69 64 65 3b 2a 2f 0a 2f 2a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 69 6e 68 65 72 69 74 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 75 6c 20 7b 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 2e 31 72 65 6d 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 75 6c 2e 6e 6f 2d 62 75 6c 6c 65 74 20 7b 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 30 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 75 6c 2e 6e 6f 2d 62 75 6c 6c 65 74 20 6c 69 20 75 6c 2c 2a 2f 0a 2f 2a 75 6c 2e 6e 6f 2d 62 75 6c 6c 65 74 20 6c 69 20 6f 6c 20 7b 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 Data Ascii: *//* margin-bottom: 1.25rem;*//* list-style-position: outside;*//* font-family: inherit*//*}*//*ul {*//* margin-left: 1.1rem*//*}*//*ul.no-bullet {*//* margin-left: 0*//*}*//*ul.no-bullet li ul,*//*ul.no-bullet li ol {*//* margin-lef
2021-09-27 18:34:00 UTC	606	IN	Data Raw: 73 73 2e 72 6f 75 6e 64 20 7b 2a 2f 0a 2f 2a 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 31 30 30 30 70 78 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 2e 70 72 6f 67 72 65 73 73 2e 72 6f 75 6e 64 20 2e 6d 65 74 65 72 20 7b 2a 2f 0a 2f 2a 20 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 39 39 39 70 78 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 2e 73 75 62 2d 6e 61 76 20 7b 2a 2f 0a 2f 2a 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 2a 2f 0a 2f 2a 20 20 77 69 64 74 68 3a 20 61 75 74 6f 3b 2a 2f 0a 2f 2a 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 2a 2f 0a 2f 2a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 2d 30 2e 32 35 72 65 6d 20 30 20 31 2e 31 32 35 72 65 6d 3b 2a 2f 0a 2f 2a 20 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 30 2e 32 35 72 Data Ascii: ss.round {*//* border-radius: 1000px*//*}*//*.progress.round .meter {*//* border-radius: 999px*//*}*//*.sub-nav {*//* display: block;*//* width: auto;*//* overflow: hidden;*//* margin-bottom: -0.25rem 0 1.125rem;*//* padding-top: 0.25r

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	657	IN	Data Raw: 67 3a 20 74 6f 75 63 68 3b 2a 2f 0a 2f 2a 20 20 2d 6d 73 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 31 30 30 25 2c 20 30 29 3b 2a 2f 0a 2f 2a 20 20 2d 77 65 62 6b 69 74 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 33 64 28 2d 31 30 30 25 2c 20 30 2c 20 30 29 3b 2a 2f 0a 2f 2a 20 20 2d 6d 6f 7a 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 33 64 28 2d 31 30 30 25 2c 20 30 2c 20 30 29 3b 2a 2f 0a 2f 2a 20 20 2d 6d 73 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 33 64 28 2d 31 30 30 25 2c 20 30 2c 20 30 29 3b 2a 2f 0a 2f 2a 20 20 2d 6f 2d 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 33 64 28 2d 31 30 30 25 2c 20 30 2c 20 30 29 3b 2a 2f 0a 2f 2a 20 20 74 72 61 6e 73 Data Ascii: g: touch;*//* -ms-transform: translate(-100%, 0);*//* -webkit-transform: translate3d(-100%, 0, 0);*//* -moz-transform: translate3d(-100%, 0, 0);*//* -ms-transform: translate3d(-100%, 0, 0);*//* -o-transform: translate3d(-100%, 0, 0);*//* trans
2021-09-27 18:34:00 UTC	690	IN	Data Raw: 61 72 3a 20 62 6f 74 68 2a 2f 0a 2f 2a 20 20 7d 2a 2f 0a 2f 2a 7d 2a 2f 0a 0a 2f 2a 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 30 2e 30 36 33 65 6d 29 20 7b 2a 2f 0a 2f 2a 20 20 2e 6d 65 64 69 75 6d 2d 62 6c 6f 63 6b 2d 67 72 69 64 2d 31 3e 6c 69 20 7b 2a 2f 0a 2f 2a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 2a 2f 0a 2f 2a 20 20 20 20 6c 69 73 74 2d 73 74 79 6c 65 3a 20 6e 6f 6e 65 2a 2f 0a 2f 2a 20 20 7d 2a 2f 0a 2f 2a 20 20 2e 6d 65 64 69 75 6d 2d 62 6c 6f 63 6b 2d 67 72 69 64 2d 31 3e 6c 69 3a 6e 74 68 2d 6f 66 2d 74 79 70 65 28 31 6e 29 20 7b 2a 2f 0a 2f 2a 20 20 20 20 63 6c 65 61 72 3a 20 6e 6f 6e 65 2a 2f 0a 2f 2a 20 20 7d 2a 2f 0a 2f 2a 20 20 2e 6d 65 64 69 75 6d 2d 62 6c 6f 63 Data Ascii: ar: both*//* }*//*}*//*@media only screen and (min-width: 40.063em) {*//* .medium-block-grid-1>li {*//* width: 100%;*//* list-style: none*//* }*//* .medium-block-grid-1>li:nth-of-type(1n) {*//* clear: none*//* }*//* .medium-bloc
2021-09-27 18:34:01 UTC	707	IN	Data Raw: 6f 72 2d 6d 65 64 69 75 6d 2d 64 6f 77 6e 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 6c 61 72 67 65 2d 6f 6e 6c 79 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 6c 61 72 67 65 2d 75 70 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 6c 61 72 67 65 2c 0a 20 20 2e 68 69 64 65 2d 66 6f 72 2d 6c 61 72 67 65 2d 64 6f 77 6e 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2d 6f 6e 6c 79 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2c 0a 20 20 2e 68 69 64 65 2d 66 6f 72 2d 78 6c 61 72 67 65 2d 64 6f 77 6e 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 78 78 6c 61 72 67 65 2d 6f 6e 6c 79 2c 0a 20 20 2e 73 68 6f 77 2d 66 6f 72 2d 78 78 6c 61 72 67 65 2d 75 70 2c 0a 20 20 2e 73 68 6f 77 Data Ascii: or-medium-down, .show-for-large-only, .show-for-large-up, .show-for-large, .hide-for-large-down, .show-for-xlarge-only, .show-for-xlarge-up, .show-for-xlarge, .hide-for-xlarge-down, .show-for-xxlarge-only, .show-for-xxlarge-up, .show
2021-09-27 18:34:01 UTC	755	IN	Data Raw: 6f 72 2d 6c 61 72 67 65 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 68 69 64 65 2d 66 6f 72 2d 6c 61 72 67 65 2d 64 6f 77 6e 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2d 6f 6e 6c 79 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2d 75 70 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 73 68 6f 77 2d 66 6f 72 2d 78 6c 61 72 67 65 2d 64 6f 77 6e 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 68 69 64 65 2d 66 6f 72 2d 78 78 6c 61 72 67 65 2d 6f 6e 6c 79 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 68 69 64 65 2d 66 6f 72 2d 78 78 6c 61 72 67 65 2d 75 70 2c 2a 2f 0a 20 20 2f 2a 74 72 2e 68 69 64 65 2d 66 6f 72 2d 78 78 6c 61 72 67 65 2c 2a 2f 0a 20 20 2f 2a 74 72 2e Data Ascii: or-large,*/ /*tr.hide-for-large-down,*/ /*tr.show-for-xlarge-only,*/ /*tr.show-for-xlarge-up,*/ /*tr.show-for-xlarge,*/ /*tr.show-for-xlarge-down,*/ /*tr.hide-for-xxlarge-only,*/ /*tr.hide-for-xxlarge-up,*/ /*tr.hide-for-xxlarge,*/ /*tr.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49821	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1262	OUT	GET /ca/restor/assets/bframe.html HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap
2021-09-27 18:34:06 UTC	1327	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "2b99-5c26848200a80" Accept-Ranges: bytes Content-Length: 11161 Vary: Accept-Encoding Connection: close Content-Type: text/html
2021-09-27 18:34:06 UTC	1328	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 73 61 76 65 64 20 66 72 6f 6d 20 75 72 6c 3d 28 30 31 33 36 29 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 72 65 63 61 70 74 63 68 61 2f 61 70 69 32 2f 62 66 72 61 6d 65 3f 68 6c 3d 65 6e 26 76 3d 66 2d 62 6e 6e 4f 75 61 68 69 59 4b 75 65 69 37 64 6d 41 64 33 6b 67 76 26 6b 3d 36 4c 63 35 47 61 45 55 41 41 41 41 41 50 4f 72 39 36 43 50 35 54 63 4c 67 4a 34 37 71 36 47 4d 6b 6c 34 71 49 62 42 46 26 63 62 3d 71 30 6e 69 37 74 37 7a 7a 34 63 35 20 2d 2d 3e 0a 3c 68 74 6d 6c 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 65 6e 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d Data Ascii: <!DOCTYPE html>... saved from url=(0136)https://www.google.com/recaptcha/api2/bframe?hl=en&v=f-bnnOuahiYKuei7dmAd3kgv&k=6Lc5GaEUAAAAAPOr96CP5TcLgJ47q6GMkl4qIbBF&cb=q0ni7t7zz4c5 --><html dir="ltr" lang="en"><head><meta http-equiv="Content-Type" content=

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49822	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1310	OUT	GET /ca/restor/assets/saved_resource(2) HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap
2021-09-27 18:34:06 UTC	1371	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:06 UTC	1371	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49825	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1311	OUT	GET /ca/restor/assets/recaptcha__en.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/assets/anchor.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1371	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:06 UTC	1371	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49826	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1338	OUT	GET /ca/restor/assets/uwt.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:06 UTC	1404	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:06 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "1428-5c26847e30180" Accept-Ranges: bytes Content-Length: 5160 Vary: Accept-Encoding Connection: close Content-Type: application/javascript
2021-09-27 18:34:06 UTC	1404	IN	Data Raw: 74 77 74 74 72 3d 77 69 6e 64 6f 77 2e 74 77 74 74 72 7c 7c 7b 7d 2c 74 77 74 74 72 2e 63 6f 6e 76 65 72 73 69 6f 6e 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 66 75 6e 63 74 69 6f 6e 20 65 28 65 2c 74 29 7b 76 61 72 20 6e 3d 21 31 2c 69 3d 21 30 2c 72 3d 65 2e 64 6f 63 75 6d 65 6e 74 2c 6f 3d 72 2e 64 6f 63 75 6d 65 6e 74 45 6c 65 6d 65 6e 74 2c 61 3d 72 2e 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 2c 73 3d 61 3f 22 61 64 64 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 22 3a 22 61 74 74 61 63 68 45 76 65 6e 74 22 2c 75 3d 61 3f 22 72 65 6d 6f 76 65 45 76 65 6e 74 4c 69 73 74 65 6e 65 72 22 3a 22 64 65 74 61 63 68 45 76 65 6e 74 22 2c 63 3d 61 3f 22 22 3a 22 6f 6e 22 2c 64 3d 66 75 6e 63 74 69 6f 6e 28 69 29 7b 22 72 65 61 64 79 73 74 61 74 65 63 68 61 6e 67 65 Data Ascii: twttr=window.twttr||{},twttr.conversion=function(){function e(e,t){var n=!1,i=!0,r=e.document,o=r.documentElement,a=r.addEventListener,s=a?"addEventListener":"attachEvent",u=a?"removeEventListener":"detachEvent",c=a?"":"on",d=function(i){"readystatechange

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49830	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:06 UTC	1421	OUT	GET /ca/restor/assets/saved_resource(1).html HTTP/1.1 Host: www.joyeriasosa.com.py 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/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-Dest: iframe Referer: https://www.joyeriasosa.com.py/ca/restor/assets/anchor.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1438	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:26 GMT ETag: "95-5c26848200a80" Accept-Ranges: bytes Content-Length: 149 Vary: Accept-Encoding Connection: close Content-Type: text/html
2021-09-27 18:34:07 UTC	1439	IN	Data Raw: 0a 3c 21 2d 2d 20 73 61 76 65 64 20 66 72 6f 6d 20 75 72 6c 3d 28 30 30 31 31 29 61 62 6f 75 74 3a 62 6c 61 6e 6b 20 2d 2d 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: ... saved from url=(0011)about:blank --><html><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></head><body></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49834	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1437	OUT	GET /ca/restor/assets/recaptcha__en.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/assets/bframe.html Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1472	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1472	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49835	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1438	OUT	GET /ca/restor/assets/614267586032718(1) HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:07 UTC	1488	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1489	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49836	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1455	OUT	GET /ca/restor/assets/fbevents.js(1).download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap
2021-09-27 18:34:07 UTC	1489	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1489	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49837	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1455	OUT	GET /ca/restor/assets/recaptcha__en.js(1).download HTTP/1.1 Host: www.joyeriasosa.com.py Connection: keep-alive Origin: https://www.joyeriasosa.com.py 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: cors Sec-Fetch-Dest: script Referer: https://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1489	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1490	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49839	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1490	OUT	GET /ca/restor/assets/EXaf08311446b84717ae3ad026d3f43bdc-libraryCode_source.min.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1525	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1525	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49764	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	55	OUT	GET /ca/restor/assets/cwc.css HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:33:59 UTC	78	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "2fdaf-5c26847e30180" Accept-Ranges: bytes Content-Length: 196015 Vary: Accept-Encoding Connection: close Content-Type: text/css
2021-09-27 18:33:59 UTC	111	IN	Data Raw: 40 69 6d 70 6f 72 74 20 75 72 6c 28 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 52 6f 62 6f 74 6f 3a 33 30 30 2c 34 30 30 2c 35 30 30 2c 37 30 30 22 29 3b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 7b 2d 77 65 62 6b 69 74 2d 66 6f 6e 74 2d 73 6d 6f 6f 74 68 69 6e 67 3a 73 75 62 70 69 78 65 6c 2d 61 6e 74 69 61 6c 69 61 73 65 64 20 21 69 6d 70 6f 72 74 61 6e 74 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 69 6e 70 75 74 5b 74 79 70 65 3d 22 74 65 78 74 22 5d 2c 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 69 6e 70 75 74 5b 74 79 70 65 3d 22 70 61 73 73 77 6f 72 64 22 5d 2c 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 69 6e 70 75 74 5b 74 79 70 65 3d 22 64 61 74 65 22 5d 2c 2e Data Ascii: @import url("https://fonts.googleapis.com/css?family=Roboto:300,400,500,700");.cpc-component{-webkit-font-smoothing:subpixel-antialiased !important}.cpc-component input[type="text"],.cpc-component input[type="password"],.cpc-component input[type="date"],.
2021-09-27 18:33:59 UTC	191	IN	Data Raw: 6e 67 2d 72 69 67 68 74 3a 32 72 65 6d 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 34 30 2e 30 36 32 35 65 6d 29 7b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 23 6d 61 69 6e 2d 63 6f 6e 74 65 6e 74 3e 2e 72 6f 77 3e 2e 63 6f 6c 75 6d 6e 2c 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 23 6d 61 69 6e 2d 63 6f 6e 74 65 6e 74 3e 2e 72 6f 77 3e 2e 63 6f 6c 75 6d 6e 73 7b 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 33 2e 32 35 72 65 6d 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 33 2e 32 35 72 65 6d 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 36 34 2e 30 36 32 35 65 6d 29 7b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 23 6d 61 69 Data Ascii: ng-right:2rem}}@media only screen and (min-width: 40.0625em){.cpc-component #main-content>.row>.column,.cpc-component #main-content>.row>.columns{padding-left:3.25rem;padding-right:3.25rem}}@media only screen and (min-width: 64.0625em){.cpc-component #mai

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	271	IN	Data Raw: 5f 74 70 6c 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 73 6b 69 70 2d 6e 61 76 20 61 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 3b 74 6f 70 3a 2d 34 30 30 65 6d 3b 6c 65 66 74 3a 35 30 25 3b 74 72 61 6e 73 66 6f 72 6d 3a 74 72 61 6e 73 6c 61 74 65 58 28 2d 35 30 25 29 3b 70 61 64 64 69 6e 67 3a 31 2e 35 65 6d 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 66 66 66 3b 7a 2d 69 6e 64 65 78 3a 31 30 34 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 73 6b 69 70 2d 6e 61 76 20 61 3a 66 6f 63 75 73 7b 74 6f 70 3a 31 65 6d 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 73 6b 69 70 2d 73 69 64 65 6e 61 76 20 61 7b 70 6f 73 69 74 69 6f 6e 3a 66 69 78 65 64 3b 74 6f 70 3a 2d 34 30 Data Ascii: _tpl{display:none}.cpc-component .cpc-skip-nav a{position:fixed;top:-400em;left:50%;transform:translateX(-50%);padding:1.5em;background:#fff;z-index:104}.cpc-component .cpc-skip-nav a:focus{top:1em}.cpc-component .cpc-skip-sidenav a{position:fixed;top:-40
2021-09-27 18:34:00 UTC	335	IN	Data Raw: 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 74 6f 6c 62 61 72 2d 63 67 2f 66 69 6e 64 2d 70 6f 73 74 2d 6f 66 66 69 63 65 2e 73 76 67 27 29 7d 2e 73 74 67 31 34 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 74 62 2d 2d 6f 75 74 65 72 20 2e 63 70 63 2d 74 62 20 2e 63 70 63 2d 74 62 2d 2d 69 63 6f 6e 2e 69 63 6f 6e 2d 66 69 6e 64 2d 70 6f 73 74 2d 6f 66 66 69 63 65 2e 73 76 67 27 29 7d 2e 70 72 64 31 30 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 Data Ascii: sets/cpc/img/icons/toolbar-cg/find-post-office.svg')}.stg14 .cpc-component .cpc-tb--outer .cpc-tb .cpc-tb--icon.icon-find-po{background-image:url('https://stg14.canadapost.ca/cpc/assets/cpc/img/icons/toolbar-cg/find-post-office.svg')}.prd10 .cpc-component
2021-09-27 18:34:00 UTC	416	IN	Data Raw: 6f 6c 73 20 2e 63 70 63 2d 74 62 2d 2d 69 63 6f 6e 2e 63 70 63 2d 74 62 2d 2d 69 63 6f 6e 2d 65 78 70 61 6e 64 2d 74 6f 67 67 6c 65 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 73 74 67 31 30 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 74 6f 6f 6c 62 61 72 2d 63 67 2f 65 78 70 61 6e 64 2d 74 6f 6f 6c 62 61 72 2e 73 76 67 27 29 7d 2e 73 74 67 31 31 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 74 62 2d 2d 6f 75 74 65 72 20 2e 63 70 63 2d 74 62 2d 2d 62 6f 74 74 6f 6d 2d 74 6f 6f 6c 73 20 2e 63 70 63 2d 74 62 2d 2d 69 63 6f 6e 2e 63 70 63 2d 74 62 2d 2d 69 63 6f 6e 2d 65 78 70 61 6e 64 2d 74 6f 67 67 6c 65 7b 62 61 63 Data Ascii: ols .cpc-tb--icon.cpc-tb--icon-expand-toggle{background-image:url('https://stg10.canadapost.ca/cpc/assets/cpc/img/icons/toolbar-cg/expand-toolbar.svg')}.stg11 .cpc-component .cpc-tb--outer .cpc-tb--bottom-tools .cpc-tb--icon.cpc-tb--icon-expand-toggle{bac
2021-09-27 18:34:00 UTC	481	IN	Data Raw: 72 3a 23 33 33 33 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 61 63 6b 67 72 6f 75 6e 64 20 30 2e 33 73 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 6d 6f 62 69 6c 65 2d 63 6f 6e 74 61 69 6e 65 72 20 2e 6d 65 6e 75 2d 69 74 65 6d 2d 62 61 63 6b 3a 62 65 66 6f 72 65 7b 77 69 64 74 68 3a 31 2e 32 35 72 65 6d 3b 68 65 69 67 68 74 3a 31 2e 31 32 35 72 65 6d 3b 64 69 73 70 6c 61 79 3a 69 6e 6c 69 6e 65 2d 62 6c 6f 63 6b 3b 63 6f 6e 74 65 6e 74 3a 22 22 3b 66 6c 6f 61 74 3a 6c 65 66 74 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 63 68 65 76 72 6f 6e 2d 6c 65 66 74 2e 73 76 67 22 29 20 30 25 20 31 30 30 Data Ascii: r:#333;transition:background 0.3s}.cpc-component .mobile-container .menu-item-back:before{width:1.25rem;height:1.125rem;display:inline-block;content:"";float:left;background:url("https://www.canadapost.ca/cpc/assets/cpc/img/icons/chevron-left.svg") 0% 100
2021-09-27 18:34:00 UTC	510	IN	Data Raw: 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 36 34 2e 30 36 32 35 65 6d 29 7b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 66 6f 6f 74 65 72 20 2e 66 6f 6f 74 65 72 2d 6c 32 20 75 6c 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 7d 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 66 6f 6f 74 65 72 20 2e 66 6f 6f 74 65 72 2d 6c 32 20 75 6c 20 6c 69 7b 66 6c 6f 61 74 3a 6c 65 66 74 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 2e 37 35 72 65 6d 3b 62 6f 72 64 65 72 2d 72 69 67 68 74 3a 31 70 78 20 73 6f 6c 69 64 20 23 46 30 46 30 46 30 3b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 2e 37 35 72 65 6d 7d 40 6d 65 64 69 61 20 6f Data Ascii: media only screen and (min-width: 64.0625em){.cpc-component .cpc-footer .footer-l2 ul{margin-bottom:0}}.cpc-component .cpc-footer .footer-l2 ul li{float:left;margin-bottom:0;padding-right:.75rem;border-right:1px solid #F0F0F0;margin-bottom:.75rem}@media o
2021-09-27 18:34:00 UTC	558	IN	Data Raw: 63 70 63 2d 6e 61 76 20 2e 74 6f 70 2d 62 61 72 2e 6d 69 63 72 6f 2d 62 75 73 69 6e 65 73 73 2d 6e 61 76 20 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e 20 2e 75 73 65 72 2d 6e 61 76 2d 77 72 61 70 70 65 72 20 2e 73 73 6f 2d 73 69 67 6e 6f 75 74 3a 61 66 74 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 73 74 67 31 32 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 69 63 6f 6e 2d 6c 6f 63 6b 2e 73 76 67 27 29 7d 2e 73 74 67 31 33 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 6e 61 76 20 2e 74 6f 70 2d 62 61 72 2e 6d 69 63 72 6f 2d 62 75 73 69 6e 65 73 73 2d 6e 61 76 20 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f Data Ascii: cpc-nav .top-bar.micro-business-nav .top-bar-section .user-nav-wrapper .sso-signout:after{background-image:url('https://stg12.canadapost.ca/cpc/assets/cpc/img/icons/icon-lock.svg')}.stg13 .cpc-component .cpc-nav .top-bar.micro-business-nav .top-bar-sectio
2021-09-27 18:34:00 UTC	622	IN	Data Raw: 6d 67 2f 69 63 6f 6e 73 2f 61 72 72 6f 77 2d 64 6f 77 6e 2e 73 76 67 27 29 7d 2e 70 72 64 31 30 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 63 70 63 2d 6e 61 76 20 2e 6d 61 69 6e 2d 62 75 73 69 6e 65 73 73 2d 6e 61 76 20 2e 74 6f 70 2d 62 61 72 2d 73 65 63 74 69 6f 6e 20 75 6c 3e 6c 69 2e 68 61 73 2d 64 72 6f 70 64 6f 77 6e 3e 61 20 2e 63 70 63 2d 6e 61 76 2d 2d 70 72 69 6d 61 72 79 2d 63 68 65 76 72 6f 6e 3a 61 66 74 65 72 7b 62 61 63 6b 67 72 6f 75 6e 64 2d 69 6d 61 67 65 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 70 72 64 31 30 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 61 72 72 6f 77 2d 64 6f 77 6e 2e 73 76 67 27 29 7d 2e 70 72 64 31 31 20 2e 63 70 63 2d 63 6f 6d 70 Data Ascii: mg/icons/arrow-down.svg')}.prd10 .cpc-component .cpc-nav .main-business-nav .top-bar-section ul>li.has-dropdown>a .cpc-nav--primary-chevron:after{background-image:url('https://prd10.canadapost.ca/cpc/assets/cpc/img/icons/arrow-down.svg')}.prd11 .cpc-compo
2021-09-27 18:34:00 UTC	673	IN	Data Raw: 74 68 3a 20 34 30 2e 30 36 32 35 65 6d 29 7b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 67 64 70 72 2d 63 6f 6f 6b 69 65 2d 62 61 6e 6e 65 72 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 67 64 70 72 2d 63 6f 6f 6b 69 65 2d 62 61 6e 6e 65 72 5f 5f 70 6f 6c 69 63 79 2d 63 6f 6e 74 65 6e 74 7b 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 32 72 65 6d 7d 7d 40 6d 65 64 69 61 20 6f 6e 6c 79 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 69 6e 2d 77 69 64 74 68 3a 20 39 30 2e 30 36 32 35 65 6d 29 7b 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 67 64 70 72 2d 63 6f 6f 6b 69 65 2d 62 61 6e 6e 65 72 20 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 67 64 70 72 2d 63 6f 6f 6b 69 65 2d 62 61 6e 6e 65 72 5f 5f 70 6f 6c 69 63 79 2d 63 6f 6e 74 65 6e 74 7b 6d 61 72 Data Ascii: th: 40.0625em){.cpc-component .gdpr-cookie-banner .cpc-component .gdpr-cookie-banner__policy-content{margin-right:2rem}}@media only screen and (min-width: 90.0625em){.cpc-component .gdpr-cookie-banner .cpc-component .gdpr-cookie-banner__policy-content{mar

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:01 UTC	723	IN	Data Raw: 67 69 6e 2d 62 6f 74 74 6f 6d 3a 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 2e 38 37 35 72 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 72 65 6d 3b 63 6f 6c 6f 72 3a 23 36 36 36 7d 40 6d 65 64 69 61 20 73 63 72 65 65 6e 20 61 6e 64 20 28 6d 61 78 2d 77 69 64 74 68 3a 20 36 34 65 6d 29 7b 2e 73 69 67 6e 2d 69 6e 2d 6d 6f 64 61 6c 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 2e 73 68 69 70 70 69 6e 67 2d 6d 6f 64 61 6c 7b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 7d 7d 23 63 6f 6d 6d 65 72 63 69 61 6c 2e 73 69 67 6e 2d 69 6e 2d 6d 6f 64 61 6c 2e 63 70 63 2d 63 6f 6d 70 6f 6e 65 6e 74 20 2e 74 69 6e 67 6c 65 2d 6d 6f 64 61 6c 2d 62 6f 78 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 78 2d 77 69 64 74 68 3a 31 38 72 65 Data Ascii: gin-bottom:0;font-size:.875rem;line-height:1rem;color:#666}@media screen and (max-width: 64em){.sign-in-modal.cpc-component.shipping-modal{display:-ms-flexbox;display:flex}}#commercial.sign-in-modal.cpc-component .tingle-modal-box{padding:0;max-width:18re
2021-09-27 18:34:01 UTC	739	IN	Data Raw: 31 32 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 69 63 6f 6e 73 2d 73 65 61 72 63 68 2f 6c 6f 6f 6b 2d 75 70 2d 70 6f 73 74 61 6c 2d 63 6f 64 65 2e 73 76 67 27 29 20 6c 65 66 74 20 63 65 6e 74 65 72 20 6e 6f 2d 72 65 70 65 61 74 7d 2e 64 65 76 31 33 20 2e 73 65 61 72 63 68 2d 69 63 6f 6e 2e 6c 6f 6f 6b 2d 75 70 2d 70 6f 73 74 61 6c 2d 63 6f 64 65 7b 62 61 63 6b 67 72 6f 75 6e 64 3a 75 72 6c 28 27 68 74 74 70 73 3a 2f 2f 64 65 76 31 33 2e 63 61 6e 61 64 61 70 6f 73 74 2e 63 61 2f 63 70 63 2f 61 73 73 65 74 73 2f 63 70 63 2f 69 6d 67 2f 69 63 6f 6e 73 2f 69 63 6f 6e 73 2d 73 65 61 72 63 68 2f 6c 6f 6f 6b 2d 75 70 2d 70 6f 73 74 61 6c 2d 63 6f 64 65 2e 73 76 67 27 29 20 6c 65 66 74 Data Ascii: 12.canadapost.ca/cpc/assets/cpc/img/icons/icons-search/look-up-postal-code.svg') left center no-repeat}.dev13 .search-icon.look-up-postal-code{background:url('https://dev13.canadapost.ca/cpc/assets/cpc/img/icons/icons-search/look-up-postal-code.svg') left

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49840	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1523	OUT	GET /ca/restor/assets/js(1) HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1573	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1574	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
61	192.168.2.3	49841	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1523	OUT	GET /ca/restor/assets/cpc-logo.jpg HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1574	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Mon, 17 May 2021 01:14:26 GMT ETag: "f3c-5c27c50824080" Accept-Ranges: bytes Content-Length: 3900 Connection: close Content-Type: image/jpeg
2021-09-27 18:34:07 UTC	1574	IN	Data Raw: ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff fe 00 1f 43 6f 6d 70 72 65 73 73 65 64 20 62 79 20 6a 70 65 67 2d 72 65 63 6f 6d 70 72 65 73 73 ff db 00 84 00 02 02 02 02 02 02 02 02 02 02 03 03 03 03 03 04 04 04 04 04 04 07 05 05 05 05 05 07 0a 06 07 06 06 07 06 0a 09 0b 09 08 09 0b 09 10 0d 0b 0b 0d 10 13 10 0f 10 13 17 14 14 17 1d 1b 1d 25 25 32 01 02 02 02 02 02 02 02 02 02 03 03 03 03 03 04 04 04 04 04 04 07 05 05 05 05 05 07 0a 06 07 06 06 07 06 0a 09 0b 09 08 09 0b 09 10 0d 0b 0b 0d 10 13 10 0f 10 13 17 14 14 17 1d 1b 1d 25 25 32 ff c2 00 11 08 00 62 00 63 03 01 22 00 02 11 01 03 11 01 ff c4 00 1e 00 00 01 04 02 03 01 00 00 00 00 00 00 00 00 00 00 00 00 06 07 08 09 01 05 02 04 0a 03 ff da 00 08 01 01 00 00 00 00 bf c0 c6 95 84 d2 3b Data Ascii: JFIFCompressed by jpeg-recompress%%2%%2bc";

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
62	192.168.2.3	49842	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1524	OUT	GET /ca/restor/assets/search.png HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436
2021-09-27 18:34:07 UTC	1578	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 05:41:32 GMT ETag: "194-5c26bede43b00" Accept-Ranges: bytes Content-Length: 404 Connection: close Content-Type: image/png
2021-09-27 18:34:07 UTC	1578	IN	Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 18 00 00 00 18 08 03 00 00 00 d7 a9 cd ca 00 00 00 7e 50 4c 54 45 00 00 00 00 00 00 24 24 24 39 39 39 33 33 33 32 32 32 30 30 30 36 36 36 34 34 34 33 33 33 32 32 32 34 34 34 33 33 33 32 32 32 33 33 33 32 32 32 32 32 32 34 34 34 33 33 33 32 32 32 34 34 34 33 33 33 33 33 33 33 33 33 34 34 34 33 33 33 33 33 33 32 32 32 34 34 34 33 33 33 33 33 33 33 33 33 33 32 32 32 33 33 33 33 33 33 33 33 33 33 ff ff ff f2 31 88 e5 00 00 00 29 74 52 4e 53 00 01 07 09 0a 24 25 26 27 3c 3d 40 41 42 4b 4c 4d 4e 6e 70 71 72 73 74 8a 8c 8d 8e a3 a4 b4 ba bb bc c2 c3 c4 c5 e9 ea eb f0 4f 8e 25 00 00 00 01 62 4b 47 44 29 ca b7 85 24 00 00 00 8f 49 44 41 54 28 cf bd 90 c9 0e 82 30 14 45 Data Ascii: PNGIHDR~PLTE$$$999333222000666444333222444333222333222222444333222444333333333 444333333222444333333333222444333333333222333333331)tRNS$%&'<=@ABKLMNnpqrstO%bKGD)$IDAT(0E

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
63	192.168.2.3	49843	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1524	OUT	GET /ca/restor/assets/CoreModule.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9 Cookie: IV_JCT=%2Fpfe-pap; QSI_HistorySession=https%3A%2F%2Fwww.joyeriasosa.com.py%2Fca%2Frestor%2Findex.php%3Fid%3D40382411219~1632800046436

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:07 UTC	1593	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:07 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1
2021-09-27 18:34:07 UTC	1593	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
64	192.168.2.3	49847	198.33.200.21	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:08 UTC	1594	OUT	GET /pfe-pap/resources/registration/assets/favicon.ico?version= HTTP/1.1 Host: sso-osu.canadapost-postescanada.ca 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:08 UTC	1594	IN	HTTP/1.1 200 accept-ranges: bytes content-length: 15086 content-type: image/x-icon date: Mon, 27 Sep 2021 18:34:07 GMT last-modified: Thu, 26 Aug 2021 18:43:26 GMT p3p: CP="NON CUR OTPi OUR NOR UNI" vary: Origin, Access-Control-Request-Method, Access-Control-Request-Headers x-frame-options: SAMEORIGIN x-content-type-options: nosniff cache-control: private x-xss-protection: 1; mode=block x-permitted-cross-domain-policies: master-only content-security-policy: frame-ancestors 'self' referrer-policy: no-referrer-when-downgrade strict-transport-security: max-age=31536000; includeSubdomains; preload Set-Cookie: AMWEBJCT!%2Fpfe-pap!OWSPRD001PFE-PAP=pfe-pap_00305_s007ptom001; Path=/; Secure; HttpOnly Set-Cookie: PD_STATEFUL_cd469f1a-2d73-11e5-8331-74fe480683e1=%2Fpfe-pap; Path=/; Secure Set-Cookie: NSC_JOkwrm0hdmzqpdienhhvjoeqoeopfc1=ffffffff09eed61f45525d5f4f58455e445a4a42dcf5;path=/
2021-09-27 18:34:08 UTC	1595	IN	Data Raw: 00 00 01 00 03 00 30 30 00 00 01 00 20 00 a8 25 00 00 36 00 00 00 20 20 00 00 01 00 20 00 a8 10 00 00 de 25 00 00 10 10 00 00 01 00 20 00 68 04 00 00 86 36 00 00 28 00 00 00 30 00 00 00 60 00 00 00 01 00 20 00 00 00 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 25 c7 29 1b 25 cb 67 1a 25 ca 82 1a 25 c9 9d 1a 25 ca b8 1a 26 ca d2 1a 26 ca d2 1a 25 ca b8 1a 25 c9 9d 1a 25 ca 82 1b 25 cb 67 18 24 c8 2a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: 00 %6 % h6(0` $%)%g%%%&&%%%%g$*
2021-09-27 18:34:08 UTC	1596	IN	Data Raw: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 19 25 ca 3e 1a 26 c9 c8 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1b 26 ca ca 18 24 ca 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1c 1c c6 09 1b 26 c9 a2 1a 26 ca ff 1a 26 ca ff 1a 26 ca Data Ascii: %>&&&&&&&&&&&&&&&&&&&&&&&&$?&&&&
2021-09-27 18:34:08 UTC	1599	IN	Data Raw: 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 27 33 cd ff bc bf ef ff d9 db f6 ff e4 e5 f9 ff ef f0 fb ff fa fa fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff a3 a8 ea ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 24 cb 31 19 26 cb 66 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1e 2a cb ff 29 34 ce ff 34 3f d0 ff 3f 49 d3 ff 4a 53 d5 Data Ascii: &&&&&'3&&&&&&&&&&&&$1&f&&&&&&&&&&&&&&&&&&*)44??IJS

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:08 UTC	1606	IN	Data Raw: ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 84 8a e3 ff cf d1 f4 ff d9 db f6 ff e4 e5 f9 ff ef f0 fb ff fa fa fe ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff cc ce f3 ff 25 30 cc ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 27 ca c6 1a 26 c9 db 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 2a 35 ce ff 37 41 d1 ff 37 41 d1 ff 37 41 d1 ff 37 41 d1 ff 3b 45 d2 ff 45 4f d4 ff 50 59 d6 ff 5b 63 d9 ff 65 6d db ff 70 78 de ff 83 8a e2 ff f6 f6 fd ff ff ff ff ff c5 c8 f1 ff 22 2e cc ff 1a 26 ca ff 1a 26 ca ff Data Ascii: &&&&&&&&&%0&&&&'&&&&&&&&&&&&*57A7A7A7A;EEOPY[cempx".&&
2021-09-27 18:34:08 UTC	1607	IN	Data Raw: 1a 26 ca ff 1a 26 ca e2 1a 26 c9 db 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 36 40 d0 ff ec ed fb ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ef f0 fb ff a3 a8 ea ff 39 44 d1 ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca e2 1a 26 ca c2 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 24 2f cc ff d5 d7 f5 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f5 f6 fd ff ae b2 ec ff 5e 67 da ff 1e 2a cb ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca ff 1a 26 ca Data Ascii: &&&&&&&&&&&&&6@9D&&&&&&&&&&&&&&$/^g*&&&&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
65	192.168.2.3	49867	172.217.168.1	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1610	OUT	GET /crx/blobs/Acy1k0bLIjHsvnKaKN_oRpVaYYvFs25d7GKYF1WXrT6yizCMksBO0c_ggE0B6tx6HPRHe6q1GOEe3_NcIbSiGG8kXeLMUY0sAKVvC6R89zvKM13s5VqoAMZSmuUgjQL5vlygJuArQghXXE_qTL7NlQ/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
2021-09-27 18:34:12 UTC	1610	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycds491VljOyrSrIjta7u9xpRcUIq8wJEhMFNPFGTm5E6TZD4l4amtFPJunnHiTGZOIkBce96Crm3o7BpF4Pk6L7aSAyB0g Date: Mon, 27 Sep 2021 05:14:21 GMT ETag: 730d2491_a246e948_e80d9c94_d8b3f142_86eb8dd2 Expires: Tue, 27 Sep 2022 05:14:21 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: 47991 Cache-Control: public, max-age=31536000 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":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
2021-09-27 18:34:12 UTC	1611	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 b9 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[L|3>/u:T7(yM?V<?.1aO?dAH'MpBTmVn Ip>k|1n<Fbf*Q1s2{*6PpobM
2021-09-27 18:34:12 UTC	1612	IN	Data Raw: a8 02 0a a2 01 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 cd 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 Data Ascii: 00*H0Mbh=[O}+UKHF(n3\",gc6)(EU#ia:NPxO(mC;|5S{maEx[fPi`y5Rv$.l-mmni`WRpb++\kR$e~J\&c%dMjV%+1FDX\1c
2021-09-27 18:34:12 UTC	1613	IN	Data Raw: 8c 5f ae 3e 17 57 ff bc 38 68 04 57 0f 19 ac 3f 17 b7 b7 70 f1 a6 fc d7 fd a7 9b 72 f3 3c ce 08 06 5e 7d 78 7e fb f1 fa df 70 f1 7f ee ae bf bc b8 bd bf bc fc 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 Data Ascii: _>W8hW?pr<^}x~p;.XWj@FUi%2'`@T*Wa$$Y0,1dNE1KcMG;`%%01`\& @Wl7fJuO'E9pt8g?~|S|I~__W,bLO?7dNd|=Xx

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1614	IN	Data Raw: ad 05 64 e8 c5 c2 1d 97 6b ff e8 92 ca 4d fa c0 82 a0 9b cd 2a c5 b6 b8 32 0a bc d8 f0 a7 fd f9 1d 53 75 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 Data Ascii: dkM*2SuGb[1_4K;&G|O3i2syVitL-Q.g dkuY[md!`H;rzU[ou:(D}#wIm{r<}'!qf,nWB4}fHvRRRjmL<^P=Ut
2021-09-27 18:34:12 UTC	1615	IN	Data Raw: 22 ec 33 e1 aa 6d 2e 51 6d bb 18 e0 59 66 cf 0b 0c 0f 70 d9 d8 d4 a2 fb 54 a1 a3 e3 76 9c 26 87 3b e2 9e 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 d3 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 Data Ascii: "3m.QmYfpTv&;GiLz52x_{nzAesv{(Y&V~<8"5!4=i>V3;ONH=y,?bO|4O|<;Y&/]\K$b>9'Sgvp}Dh9i
2021-09-27 18:34:12 UTC	1617	IN	Data Raw: 50 92 d3 24 77 c0 7d 91 e5 5d 71 c8 19 ce cb 33 33 dc fd bc c3 19 b7 ce 2a 5d 70 65 ad 16 4c 73 b3 f3 a4 f7 79 e7 fd f2 e6 66 f1 7a 09 df 77 5e 7d 62 85 5a d4 9f a2 f9 54 b6 f9 14 cd 27 df b9 fb b9 b7 c3 05 97 4e 1b 67 85 11 d2 1a ed 04 a3 a8 08 e9 69 f5 9a 3f ba f9 2c 9a 7f 84 69 fe 51 f5 a7 74 cd 15 db 5d 97 bc fb 2e 16 c9 00 bf 2c 7c 25 2c d7 f5 d0 aa 9b e9 c4 99 ff 51 0f 2d a7 21 2e 0b 74 c3 73 28 fd 02 79 0f 2d 4d 75 4b 53 12 11 6f be f3 cb 20 0c 10 43 61 0d f0 c6 24 77 cc 68 52 16 66 95 48 20 6e d0 ac 11 97 fe a7 e7 cd 15 2f 16 e1 b9 f4 b3 2a 61 15 ec 61 01 13 5a 2e 0a 23 39 35 ad 94 88 a2 e9 ae b4 b2 c2 42 e4 48 94 97 dd 77 65 fd 84 5a 08 ae 58 61 a5 e4 30 2d 93 9a 9c 30 f0 d6 ec a9 64 f5 a7 f6 02 27 38 34 68 80 c6 77 77 7b dd f4 41 19 bc 1c 88 55 Data Ascii: P$w}]q33*]peLsyfzw^}bZT'Ngi?,iQt].,\|%,Q-!.ts(y-MuKSo Ca$whRfH n/*aaZ.#95BHweZXa0-0d'84hww{AU
2021-09-27 18:34:12 UTC	1618	IN	Data Raw: 8f 93 c9 a8 d0 11 b9 41 db 5d 27 d8 c3 46 11 a9 55 58 73 d1 8d 0e 1a e3 af 04 c9 62 08 91 86 3b b3 8b a4 4d 19 09 2e 0a e0 e5 a0 bd cf 2b f3 36 90 3c d5 7e 62 27 09 c5 c1 5c c8 54 99 d3 01 48 ef 23 03 72 71 56 89 38 c5 ce 33 48 36 17 d9 fd 62 43 86 be 9b 6a 30 21 d9 8b d5 5d 8f cb 54 5f a8 33 04 b2 4b ab 5f d8 13 04 7a c8 0e d9 79 0f dd 46 e2 6c 8d 5c d2 34 02 7b 58 ef 24 ae ac 98 8e ed 98 49 8b 2c 4d a2 a0 11 76 34 06 6e 78 9b 22 21 a0 a2 10 2e 75 44 a9 9d 88 a1 ec ea fe 46 da 9e 75 a6 58 b6 b8 34 18 c9 39 53 90 0c 4c 3a ac 79 c8 5b 8a d8 1e a3 9a e8 12 51 24 02 55 d6 b9 7b 9e 98 ff fe 85 96 8a d4 22 38 3b dd 2d 5a 49 5c 58 cd 09 3d 9a 22 da fe 02 2d 2d 08 11 61 78 29 b0 94 58 5b ca 49 b6 eb 9b 38 a7 74 58 e4 21 c2 88 4b b4 59 58 fb a3 ed cf 3a 13 aa 0a Data Ascii: A]'FUXsb;M.+6<~b'\TH#rqV83H6bCj0!]T_3K_zyFl\4{X$I,Mv4nx"!.uDFuX49SL:y[Q$U{"8;-Zl\X="--ax)X[I8tX!KYX:
2021-09-27 18:34:12 UTC	1619	IN	Data Raw: bd e6 67 38 d7 14 c8 c1 e1 56 52 d4 fb 23 8e 4e 6f 88 8b a8 8b 8b 9b a4 a1 14 8f f1 40 a4 13 6d 62 7c 8f 0a 70 79 f5 21 ed 4d a2 9a 86 ca 60 51 0e 16 dc db 86 ea 57 54 b2 33 dd ed 10 05 d3 fe 54 da 2c 0c e2 f5 2c 49 24 77 e2 9c 6a 38 01 17 1d 38 21 4a 0b 7f a9 3f b3 9d 3c 83 2b 77 ce 14 4c f0 ba 3e 0e 88 51 01 50 c8 5b 7e 1b 71 12 44 1b f3 de 7c c7 67 46 0c 07 7f 06 41 83 01 0c 07 67 c0 c0 db ac c1 36 1b dc fd 12 09 10 87 e1 a8 b0 93 ed f2 e1 5c e7 2c 16 3c 2a da ec b6 cb b6 45 5d 73 ac d3 5d ae 18 7d c6 66 cd 5e ad 56 13 be 07 e8 ec 8a 0d 5b c3 cf 6f 53 93 48 a5 b7 65 49 a2 0d 4a a0 97 12 20 ab 61 c6 d4 67 96 e0 0b 0d fb f0 49 75 02 e9 a5 67 d4 8d a9 cb 24 9a 83 c6 2b ae 00 11 53 67 bb ee d5 31 45 95 6d e6 42 80 06 64 d0 51 0d e8 12 a5 3c 51 e2 77 b1 be Data Ascii: g8VR#No@mb|py!M`QWT3T,,l$wj88!J?<+wL>QP[~qD\|gFAg6\,<*E]s]}f^V[oSHeIJ agIug$+Sg1EmBdQ<Qw
2021-09-27 18:34:12 UTC	1620	IN	Data Raw: 1c 1d 55 87 15 21 13 ea c0 32 45 6b 50 4d f6 fb e3 41 bd 53 07 d5 f8 b8 4f 99 22 f5 44 06 45 eb a0 1a 96 8d 7b 99 83 65 0f 89 e0 43 f5 44 29 42 0d 8d 4c 90 27 aa 7c 14 89 61 3f 85 5f e9 cb 1e a8 91 a3 e7 a9 8b 4f 1f 5e a6 46 8e cb da c1 12 7c 53 87 bc 29 02 99 e1 d4 43 ef b9 e1 8d a9 25 be 94 c8 29 b2 04 a8 f8 40 9d 7b ca 12 98 cc c0 52 53 6f 48 65 e5 14 8d 06 0f 3d 9d 1d ce 47 e3 79 59 03 9b 54 1d d3 07 6b b2 84 6a fd 1e 9d 96 29 10 26 de 73 95 25 72 50 f6 a7 33 88 55 35 e0 2b 09 af 9b 1e 5d cf 92 82 50 91 2a 35 f5 c0 7f 96 02 00 d7 df c0 fb 80 9d e6 82 17 f5 e6 09 8a 9c 8f 5f 6b fc 2a 71 b6 36 4f e7 60 5c 96 7f a4 c1 8c 7a 45 5b 9e 08 e5 9c 89 77 72 ac 21 30 86 bd 4a 19 49 0f f6 e6 49 fc 56 8e 9f a7 80 80 a8 7e e7 49 64 22 04 f5 44 c2 1a 22 44 84 a0 0e Data Ascii: U!2EkPMASO"DE{eCD)BL'|a?_O^F|S)C%)@{RSoHe=GyYTkj)&s%rP3U5+]P*5_k*q6O`\zE[wr!0JIIV~Id"D"D
2021-09-27 18:34:12 UTC	1622	IN	Data Raw: a8 48 d5 22 00 27 67 0b ab 0c dc b3 d0 4a 14 4e f2 a6 87 23 d5 e5 bd b7 4b 4c 2f 89 a7 f4 5b ec 8e 1b 42 17 cb 7a 84 3d 53 ab 7d cf b7 d6 18 f6 40 e5 ba 13 57 f1 c4 19 89 b0 27 8e cf f9 11 8f c3 06 a9 45 b0 c2 7b 65 82 92 92 0f 89 24 74 47 4f 58 44 2a c1 b8 42 80 e7 03 8f 5a 78 11 b4 61 a9 24 91 27 fe b7 89 e5 7b 74 7a 8d bf 55 2a c0 fd 44 80 58 6e 9d 52 70 47 02 d8 be 9d 82 e8 fb 07 7d 90 fd 64 bc fb e5 d3 d7 eb f9 a7 dd ab cb cb 9b c5 ed 73 d9 f9 55 7c ab 1d b2 c0 9b a9 3f 35 8d 40 0d 8b 77 bf ca ad d7 44 47 b8 7f af c1 46 76 be 0d 47 47 dd 41 ff ef e5 e8 ee ee 57 f5 e8 34 3b 58 fd 9b 35 21 4a 5c 36 6b 0b 42 ba b1 89 f9 dd d5 ed 87 c5 f5 cf e4 e8 7f 3b f7 91 29 46 9e e6 b4 fd dd 5d 73 d2 c6 40 c8 17 12 6c 43 41 64 75 82 c7 96 39 64 5b 85 22 25 a4 ee f4 Data Ascii: H"'gJN#KL/[Bz=S}@W'E{e$tGOXD*BZxa$'{tzU*DXnRpG}dsU|?5@wDGFvGGAW4;X5!J\6kB;)F]s@lCAdu9d["%
2021-09-27 18:34:12 UTC	1623	IN	Data Raw: 19 7a db b4 8a 9b 9c 54 f6 e4 db 32 ae 01 c7 13 0a 88 75 ce 14 c1 6a e3 79 db 5a 13 33 68 68 d8 2c ef a9 59 b0 42 02 5e 33 41 18 2b 8c 28 b4 5d 69 df ab 87 12 44 a4 a8 aa 41 09 0f d7 b9 50 08 61 1c 1b 09 55 ae bd 7e b1 c9 91 33 08 23 7e 91 64 e4 c9 a9 60 a8 96 cf 50 1b c2 4c e8 79 18 c6 6c 31 6b 1c 13 a8 ca 88 51 d1 92 03 a3 29 15 aa 26 af c9 77 b8 d2 1d c6 6a 99 82 5b ac d6 3c 14 16 6f 5b 26 e0 b2 b2 ad 23 e9 2e cd 35 18 8f 8d 33 a7 d4 3f 27 5a b3 3c 0e 22 a9 66 e0 ae 21 ed 58 19 a2 c2 26 f1 18 f7 f3 20 7b 0f 99 fb 58 31 d8 d1 76 f1 19 5b 5b 3d b7 b1 e5 a8 c6 ed f5 d5 d7 f3 4f 8b 9b 0f 57 57 b7 cd c8 86 55 90 dd c5 36 be d5 4e 43 d2 a1 7c 51 00 52 0f c2 ca f5 70 9d 66 96 28 65 68 83 5b a4 5e 58 5b 4d 37 d9 10 64 d5 c4 d8 a0 e1 96 ab db 7c ef c7 be ec 45 Data Ascii: zT2ujyZ3hh,YB^3A+(|iDAPaU~3#~d`PLyl1kQ)&wj[<o[&#.53?'Z<"f!X& {X1v[[=OWWU6NC|QRpf(eh[^X[M7d|E
2021-09-27 18:34:12 UTC	1624	IN	Data Raw: 12 ae 7e 19 80 87 e4 3c 84 e0 ea 52 26 90 97 2b 81 14 e9 2b b5 36 83 6f db d0 d5 75 d2 eb bd 97 da 89 c2 0a b3 a2 01 b4 45 86 98 cc c5 33 7e 69 0b 59 61 f5 61 e4 b6 fd 33 33 3f b7 ae c2 48 f8 e7 15 56 3c 78 90 0a 7c 7b ed 9c 0e c1 04 be aa 90 ab 4a 78 63 4d 30 85 91 c2 d7 85 52 f3 03 fc 7b 02 86 c9 b5 e9 5c 64 0b 89 97 55 08 3f 98 a2 cf 63 1c 14 e4 85 14 5b 14 73 9b 20 d1 08 c1 4a 2b 8d 07 68 a2 b5 f6 45 01 66 b8 e2 69 58 32 a2 d2 8a d2 6a e1 a5 0d 5a 04 e5 95 86 20 b0 aa 01 fe 50 27 f2 b0 97 d2 78 d0 cf 00 41 dc 49 69 85 a8 7c 0b db 8b 51 f4 24 b1 dc 31 06 f3 85 70 d5 94 9c 00 75 87 7f da 19 5e f1 b0 c1 62 cc 87 fb b5 b8 98 9d e4 ac 71 6b db a7 c7 b8 a8 b3 4d e1 b6 41 3d a1 ea cf 80 25 cb e0 61 7f c1 7b c7 77 ae 1e a1 8d b9 cd 4c 56 c3 9b 54 22 00 c2 70 Data Ascii: ~<R&++6ouE3~iYaa33?HV<x|{JxcM0R{\dU?c[s J+hEfiX2jZ P'xAIi|Q$1pu^bqkMA=%a{wLVT"p
2021-09-27 18:34:12 UTC	1626	IN	Data Raw: c8 0e 98 e7 a0 be 53 01 88 4a c4 c5 4c 33 b4 d7 9f 76 a7 63 b2 80 7b 05 e3 f7 05 c7 5d ea be 98 d7 69 b6 d7 8f cb 92 84 67 ae 84 df 5e 3f 1d 70 5b e0 9a b0 ed 8a b3 e1 f1 f4 84 ac e0 5e 7e 7e 77 f7 6f 50 4b 07 08 62 6e ee ba 6a 12 00 00 a8 61 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 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 62 6e 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 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 62 6e 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e cd 5c eb 6f db 48 92 ff 57 74 be f9 70 b3 c8 a3 df ec ce ed dc 40 b1 68 47 1b 5b f2 ea 91 20 8b 01 04 4a 96 92 c1 66 e2 9c ed 60 81 0b f2 bf 5f 91 dd 8c 8a aa 6a 4b ce 78 Data Ascii: SJL3vc{]ig^?p[^~~woPKbnjaPK*Q_locales/bn/PKPK)Q_locales/bn/messages.json\oHWtp@hG[Jf`_jKx

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1627	IN	Data Raw: c8 bd e0 48 35 c5 8c 38 d8 a8 04 e6 56 43 62 89 e2 5c 2e 16 79 f2 e4 49 da b6 86 bb 02 5c 5a d8 b6 04 ad 31 6c 6c b9 27 63 4b e1 9b 41 ac 8f a7 8a 89 08 88 ca 15 00 96 f0 37 00 7f 42 86 e9 49 87 b0 c7 dc 90 83 a5 ef 23 5d 03 5e 43 49 10 a9 0d 3a d4 26 c3 aa 44 27 65 c2 ac 5a a3 a8 2e 31 3a 09 d3 1a 25 0c 6c 17 52 28 a1 35 f0 87 17 66 e2 44 5a e3 20 75 86 68 09 8e ea 40 b1 00 20 d8 35 9d a8 01 a1 4a 2b 99 86 98 11 10 88 07 48 94 0a 50 2b c8 95 1c af ec be 93 df 27 14 f8 af 86 9a e0 25 df de f8 c7 67 ed 7d 6a c1 48 29 82 aa fd a6 e2 83 ff bd 21 32 cd a7 51 d2 95 92 71 ff 08 23 45 45 ae 45 f9 7e 4a 0a 14 86 d1 0d 41 a1 0d 02 15 cc 02 71 e0 6e 8e db b8 7e 49 0a 0e ed 06 e2 af 9d 8d fb ad e9 27 b2 31 47 ad 88 59 26 fb 5e a2 cf eb fd ba 9d b2 fd 44 08 69 0b ce Data Ascii: H58VCb\.yI\Z1Il'cKA7BI#]^CI:&D'eZ.1:%lR(5fDZ uh@ 5J+HP+'%g}jH)!2Qq#EEE~JAqn~I'1GY&^Di
2021-09-27 18:34:12 UTC	1628	IN	Data Raw: dc b7 64 ef 6d 1d 05 7d 55 e5 d8 d0 f9 fe e9 7c 72 76 df d3 e3 26 27 ee 50 6d 45 ed ad 53 42 42 2c a9 02 c4 45 2e f0 a3 ce 58 bc 34 c9 3f a8 3f 95 6f d0 c7 0e 2d 53 be a5 ad 20 54 a0 6d 65 f6 63 3c 88 0b a0 aa 3a 14 a0 bb 5e 58 01 d9 e2 43 a2 24 60 da c9 79 bc 51 01 59 15 d8 46 5d bb 01 15 50 c1 f2 23 9d c8 41 87 4b ac d9 f4 fb de f6 3f ed 6c 06 52 17 e4 e1 52 85 c4 86 ba c1 6f 25 58 29 64 77 5a 83 b1 de 3f d9 48 43 62 0d e0 2b e0 1a 78 38 6f 00 e5 24 ab 00 7f fe 6a 0b 66 65 ae 79 81 3d d7 65 2e d5 c9 76 46 f2 59 6d c3 49 27 c0 c7 49 08 0e 64 11 c0 90 c0 5d 10 4e a6 a4 fb 86 06 a2 07 16 22 51 d1 b5 b3 fc 01 1b 10 f7 ad 4e 77 a6 3e c9 94 10 d7 62 a0 c0 ea 20 be a9 07 f3 21 61 f2 f5 e8 b5 d3 24 4e f8 4b ce 35 e2 a4 12 4d 2c a6 c1 15 67 ea 27 42 94 b1 1a 3c Data Ascii: dm}U|rv&'PmESBB,E.X4??o-S Tmec<:^XC$`yQYF]P#AK?IRRo%X)dwZ?HCb+x8o$jfey=e.vFYmI'Id]N"QNw>b !a$NK5M,g'B<
2021-09-27 18:34:12 UTC	1629	IN	Data Raw: 1f 9e 2d 4e 86 e5 d9 60 97 10 f7 7c 66 9e d0 c9 78 72 be 18 94 d3 e3 c9 f0 82 3d 16 33 f4 94 a7 f6 a2 ec 0f ca c9 2e 0d ae 40 91 a7 71 31 19 9f 5f cc 08 7b 68 f7 20 4f 62 52 fe 7d 3e 9c 94 84 35 5c 73 23 4f 65 f6 e6 a2 bc 43 dc 74 0a 81 90 3a 1f 4e 26 e3 c9 70 74 da ea ee 62 3a 7f 5e f3 08 be 22 6a cc 44 cf 84 e0 a8 9c bd 1e 4f 5e 82 1e 9d 9c 94 93 5a 1d 5f 0f 4f 86 84 df 4c 02 9a 25 95 3b 20 f7 e6 ad 2c 91 69 ff bc 64 b7 c2 8d 9d 64 a9 bc ae 65 b6 b8 38 26 ac a1 01 29 a5 31 de 5d c5 3d 28 4d 96 5d 4c 86 af fa c7 6f 16 83 fe ac bf 98 4f fb a7 25 63 4e e4 31 64 42 66 5a e7 0d 3c b8 70 11 0a bf fe 6c 7c 4a e0 91 29 92 31 8b 67 f3 8b c5 ab e1 74 f8 7c d8 28 59 56 a4 cc cb 8b 28 b5 f1 c9 ec 75 7f 92 d7 7c 2e d2 21 54 e6 a3 97 a3 f1 6b b2 96 ab 84 92 b5 af 86 Data Ascii: -N`|fxr=3.@q1_{h ObR}>5\s#OeCt:N&ptb:^"jDO^Z_OL%; ,idde8&)1]=(M]LoO%cN1dBfZ<pl\J)1gt|(YV(u\.!Tk
2021-09-27 18:34:12 UTC	1631	IN	Data Raw: 5d db 31 79 98 4c cf 34 1c fb f0 fd 49 5c dc 3e bd ef aa 88 a8 ee 98 b6 e5 7a a6 e5 68 0e d9 f2 eb 3c ad ef db 97 2d d5 f0 1c 4b 45 f0 75 55 57 0d 97 4c 66 92 63 2b 1f e2 ba 88 15 c4 ad 77 57 e4 f7 71 c4 ca 0a cb 4a 8f 5f cd e6 fe 74 be 1c 86 a3 f7 af d8 26 4d 22 b6 db a9 8b 3c 5f a7 71 93 17 97 b0 79 15 8c fa cd 8b 6f 5b ab d9 c4 1f bd fa 51 fc bb f8 79 84 09 6d 52 16 c5 77 79 ba 8a 8b 52 cc 64 6b 25 fe 40 88 2b a4 16 9f d6 2b 4d 2c 60 6b 4c 1e eb e2 f1 d3 f4 c8 0b c6 de 0b 52 0f e6 d1 e3 63 47 8c 96 9b bb c3 30 fd 74 c6 fe f1 b9 8e 55 55 fd e9 ac dc b0 6c fb 07 53 ee 8a f8 f6 cd e7 a3 bb aa da 94 e7 67 67 65 bd d9 e4 45 75 ba 16 f1 39 8d f2 fb b3 68 17 d4 33 96 95 bf c5 c5 99 ee 89 aa fd 7c a4 54 ac 58 c7 15 ec 97 37 29 cb fe f9 f9 68 eb 98 0f a2 44 29 Data Ascii:]1yL4I\>zh<-KEuUWLfc+wWqJ_t&M"<_qyo[QymRwyRdk%@++M,`kLRcG0tUUlSggeEu9h3|TX7)hD)
2021-09-27 18:34:12 UTC	1632	IN	Data Raw: b1 2a f9 b8 d0 16 ba 63 98 9e 87 e6 c0 b2 80 c9 87 e3 86 59 82 c2 db 85 76 9d a0 8c 1a 5b 87 33 2c 26 6b e1 3f 86 03 b0 23 5b d8 46 24 db 86 a4 49 d5 c3 8c 38 55 04 45 b5 85 20 36 80 83 45 3b d1 3d 7a 02 ad 00 5a 91 30 60 79 cf 32 4c 97 04 69 76 98 03 08 d7 5e 51 0b 2f a0 7c d3 b0 4d 34 45 16 fa 22 c7 b0 68 ac 9f 75 38 96 aa f3 be c9 35 41 2b 10 4d aa 69 93 ec 0b d2 43 30 42 32 71 84 01 81 ed 21 4c 5b 80 1c 9e b1 e6 04 14 c0 4b 25 bf 81 f6 04 64 41 35 26 6d 14 5c cc 98 89 fc dd ee e8 1e 7e 09 84 38 8e ef 93 72 9f 38 76 49 76 c2 7f 96 75 ca ab 1e c9 b7 df 32 f5 30 37 0e ad c7 02 fc 9e 3a a4 d3 ff a6 15 7a a1 d7 d9 4a 68 49 e4 5e 6e 65 fe 64 f7 52 15 79 8d a0 40 52 03 4a 45 17 63 e9 86 bd d5 d0 16 04 1d 80 4a 77 1d 74 be 00 1a 4b 23 f9 e9 0b 78 64 db 8c 46 Data Ascii: *cYv[3,&k?#[F$I8UE 6E;=zZ0`y2Liv^Q/|M4E"hu85A+MiC0B2q!L[K%dA5&m\~8r8vIvu207:zJhI^nedRy@R JEcJwtK#xdF
2021-09-27 18:34:12 UTC	1633	IN	Data Raw: fd 88 7d d5 d0 7d e1 a7 0b b9 24 47 ec 7d d3 c6 52 43 93 8d aa b6 39 8a 58 fc 38 94 4c 65 0e f8 e1 47 75 20 bd dd 05 44 23 14 c5 e9 db 2a 2f 14 7e 66 00 d6 5d 61 86 c9 89 72 3d 19 9d 28 a2 80 6e f3 08 9c 0a 98 5b 17 ec 1e cf 78 1d 8c fc 59 a3 e8 f9 3d 87 a3 ba ae e1 42 ca f2 43 26 2a 9d b7 ea 81 13 75 e7 71 02 3d 65 d9 dd 14 f0 0b ae 55 13 a2 ab a0 1f fa cb e9 78 31 0f a6 4b bf df 0f e7 e1 78 e4 0f 97 bd f1 d5 55 30 9a cf 0e 87 96 5d 5c 51 3f 8b 7e 38 5e 7e 58 f8 c3 70 fe e9 d0 83 0c ac 88 87 9e 3f ea 05 c3 e5 bb c5 7c 3e 1e d1 39 d0 7b 21 ea 61 3c 9a 63 01 98 45 30 e3 6b 3a 74 22 6b c5 88 93 7e d8 5f 8e c6 f3 e5 7c 4a 96 21 d3 86 c4 7e 10 04 fd 77 7e ef fd 32 b8 f2 c3 e1 72 10 06 c3 fe a1 23 d9 c1 7b b7 a3 c1 78 7a b5 ec 07 b3 de 34 9c 48 97 25 39 a7 e9 Data Ascii: }}$G}RC9X8LeGu D#*/~f]ar=(n[xY=BC&*uq=eUx1KxU0]\Q?~8^~Xp?|>9{!a<cE0k:t"k~_|J!~w~2r#{xz4H%9
2021-09-27 18:34:12 UTC	1634	IN	Data Raw: 76 7d cf 70 0d d3 73 6d df d0 4e 05 6f 72 9a 32 89 a7 19 59 27 eb 28 23 2b fa 1c 97 2a fc 35 25 9b 6d 96 47 f3 e2 19 9f 42 fc a8 3b 7a 44 b2 f2 ea ac fc 6a ff 26 d6 c1 0a 8e e7 3a 96 a3 99 ba af b9 f6 e9 32 0f cf 11 97 e7 62 c9 86 5b b9 e2 ba 60 38 fb dd f6 f9 d7 1d 15 bf 73 e5 96 e1 59 d8 b8 03 bd 9e 6e 38 ae a9 9f 6a ef c7 db 55 11 27 59 4e 36 f0 43 c8 c5 6c c3 d0 2d cd f1 4c 53 87 b0 66 da b2 18 5f 34 5a 27 cf d5 8a 24 a3 f0 c0 6e 26 ec 89 e2 a4 41 1e 16 45 96 53 92 27 64 9d 26 62 f7 4b b2 5b 25 9b a2 21 96 b2 35 5f c3 5a 96 ab 6b 9e e1 f9 b6 a7 b6 90 fb 95 cb 38 a6 e3 78 8e 6b 31 bf 59 be 65 ba 8e 24 43 d3 27 ba c8 5f f9 c2 d3 e0 68 c3 b5 1c db f3 2d db d5 5d 29 12 ae e3 30 8b 72 f8 42 08 d8 9a e9 bb b6 86 73 31 34 43 33 3d c9 34 84 0e 5f 01 7b cc 36 Data Ascii: v}psmNor2Y'(#+*5%mGB;zDj&:2b[`8sYn8jU'YN6Cl-LSf_4Z'$n&AES'd&bK[%!5_Zk8xk1Ye$C'_h-])0rBs1 4C3=4_{6
2021-09-27 18:34:12 UTC	1636	IN	Data Raw: 39 9c 71 dc 41 db c1 28 69 52 cc 51 cf ab b5 45 5c 2e cf 09 df 2e 6e 58 27 31 15 47 cb 5a 00 41 49 c5 21 54 77 1d fa 97 c3 c2 d8 33 5b b4 40 e7 f3 ea 78 73 b2 80 1b e5 53 8b a3 c7 64 93 c4 95 c1 59 2c a4 60 76 e9 dc 7d e4 72 13 38 a8 59 68 da 4c 50 13 40 26 58 01 d2 d3 94 28 7b 6b 3e 65 3b 55 18 86 5c 4c 66 51 fe 9b d0 e4 a0 95 b1 4d 06 10 9a 61 9b 40 5f 59 d3 f6 91 b7 3f 96 81 52 84 de c7 72 3d 54 23 c7 d2 3d b9 bf 48 b8 f9 38 ba 0d 5d 20 0d cb 74 56 e2 f6 e3 36 66 cd a5 70 0f d0 a1 81 34 df 88 5b 23 f8 8f fb 7f 41 9f b1 8f 2a ec f7 6d d3 51 ab 64 d9 28 51 1e fa 50 a3 ec 19 6d 4f ae 72 b5 c5 e3 cf b4 66 8c 41 a2 26 f8 86 69 a3 68 d9 be 26 af d7 e5 ab ec e8 86 08 56 50 60 9d 18 d8 95 26 bb 75 b2 5b 85 39 5b 08 04 35 4d e2 82 6d 70 75 90 78 7b af a0 8d 86 Data Ascii: 9qA(iRQE\..nX'1GZAI!Tw3[@xsSdY,`v}r8YhLP@&X({k>e;U\LfQMa@_Y?Rr=T#=H8] tV6fp4[#A*mQd(QPmO rfA&ih&VP`&u[9[5Mmpux{
2021-09-27 18:34:12 UTC	1637	IN	Data Raw: fe 13 c4 62 9e 90 55 9e 71 43 d0 38 7a 9a a9 3b 06 0a 0c 1a 63 57 ae f6 12 35 23 bc 4a 3d ed 44 a7 85 28 af 62 99 ff c1 0f 25 4d 23 ef 57 a1 20 e5 0d 62 9c 5b e4 ea 7a 07 5d 36 fb fb 41 2c 8f 5e de b0 0c 10 0e b0 2c 13 c0 2a b7 39 fb 38 d9 8f 05 aa 66 b1 86 3a 21 b2 40 1e 53 1a 2e 4f 1f 8f 96 68 51 94 2b b3 ac 61 3d 96 0e 13 0c 03 04 d5 90 48 c4 43 b8 5e b1 d9 f6 be 91 44 c7 cd e8 06 98 47 c9 88 35 df 93 64 aa d1 72 c9 f4 b8 10 4a 87 ef fb 4e c9 58 2c cb d5 e5 bc 1e a5 f3 70 0f 70 df 5e cf 8a 15 64 c5 33 4b 10 f7 3c 50 29 47 73 d1 20 4a 79 df e7 48 5b 96 6b d1 5c 2e 4a cb 78 a2 9d 4e fd fe de 6a aa b0 ff ef 2b a7 e0 cb 26 c3 58 cf 74 c0 ad 7c cb 97 ca 99 8a e8 79 20 ac 20 c3 96 0e ba c3 b8 98 a5 ca 12 60 a8 38 3d fe 24 9c 2c c2 47 1a a3 10 9f a4 8f aa 99 Data Ascii: bUqC8z;cW5#J=D(b%M#W b[z]6A,^,*98f:!@S.OhQ+a=HC^DG5drJNX,pp^d3K<P)Gs JyH[k\.JxNj+&Xt|y `8=$,G

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1638	IN	Data Raw: bb 57 a0 2e 93 4e b7 89 b4 b9 97 2c 50 8d a5 95 e2 f7 c8 36 99 3a 29 de 11 52 48 8b 0e 40 6e 15 e5 67 9d 0a e9 51 67 74 1b 4c a4 c4 50 bc 04 7e 24 cc db 42 b4 2c 82 30 b4 9a 7d 86 62 d2 0e 14 0f fc f7 5a 40 51 25 77 29 86 fe d5 fd fd e6 78 28 09 a8 5e 92 dd 0b dc 36 65 f8 52 bc 5b 5c dd 3f 0c 02 a9 3c ab c6 7b d5 fd e3 ae 6a 0b aa 31 78 25 71 df bb 1d df 49 12 aa ff 3a f3 f2 f2 1f 50 4b 07 08 df 97 26 53 40 10 00 00 5d 35 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 64 61 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 64 61 2f 6d 65 73 73 61 67 65 73 2e Data Ascii: W.N,P6:)RH@ngQgtLP~$B,0}bZ@Q%w)x(^6eR[\?<{j1x%qI:PK&S@]5PK*Q_locales/da/PKPK)Q_locales/da/messages.
2021-09-27 18:34:12 UTC	1640	IN	Data Raw: 36 6b 8b 11 b8 8a e2 24 42 f6 14 e8 3e 3f 22 a2 2b f4 c5 9f de 37 d2 74 78 4d 53 3d 9d 2a 4e 17 3b 63 ef b9 5f 9d 80 5b 14 71 96 1e f3 1e 56 ff 42 74 24 db b2 3c 2a e3 87 e2 b1 28 d9 86 95 7c 01 53 ba 00 e6 13 34 f6 a2 8c 93 04 e9 c4 f2 4a 92 2d a9 d5 c6 0f 94 59 05 e8 42 09 a2 11 af 79 8e 15 5b f6 85 96 2a 45 b4 29 2b 2d 8b 18 e4 06 ac 22 2e 50 f5 49 b6 5a c6 09 85 1d 8b 09 52 77 69 bc 86 82 2c 2d d6 51 1a d1 13 da 90 52 a3 20 1d 80 5c 5e 4e ec 01 d0 b4 63 40 19 18 9b 3c f2 ec e6 e6 ec 94 9a 1f 81 4b e5 4a c4 8b 0f b5 8f 65 90 c0 26 1d a5 c7 52 58 d1 a4 99 02 62 b2 82 6e 1c 89 56 3f 1b 77 47 18 bf ad 68 07 14 a1 64 ef bf d4 8a e1 1c 6e 43 c4 cb 08 dc 0c 2b 97 bb 74 4d 56 83 d3 28 e0 75 05 19 d2 18 9e 2b 90 28 b2 94 1a c7 be b5 4d 41 33 42 78 ae 11 84 f0 Data Ascii: 6k$B>?"+7txMS=*N;c_[qVBt$<*(|S4J-YBy[*E)+-".PIZRwi,-QR \^Nc@<KJe&RXbnV?wGhdnC+tMV(u+(MA3Bx
2021-09-27 18:34:12 UTC	1641	IN	Data Raw: 29 3b ae bb b2 45 68 43 89 cc 59 75 83 71 9c 28 e3 c1 8a 9b 03 94 7a 66 d8 22 77 af f3 db 03 63 01 39 24 c2 0a 38 04 5d 14 2a 99 02 40 4c 87 ca ef 9e 25 65 bd 27 17 77 34 24 0c 6a 44 05 46 23 06 2a c2 29 e1 3c 65 dd d9 c1 3b 8e 01 9e d1 42 21 cf 14 eb 9a 17 ec 51 8f 4e a3 d5 b5 89 e3 51 df c4 a8 2f 0e b9 1c 2b f7 d9 43 1b 6e be 70 89 57 08 fa e7 d0 0a d1 ee ff 92 55 34 e5 80 50 18 c0 61 47 75 1c 9a db f1 83 d8 25 92 3a fe e8 78 c0 b5 65 5e dd 8d 38 0e 51 19 4b 43 14 31 ca 00 c7 c5 3b 88 1e bc 43 6d 8a 07 32 cd d6 08 02 dd 51 d1 d4 09 5c e7 a9 53 43 24 52 7e bd e3 e3 0d d8 21 20 91 55 f9 de 44 07 33 84 ab 1a 9a ad 03 73 31 f2 38 62 2b fb 3e 91 20 7e be 46 19 d0 80 2a d2 09 e5 c7 65 87 ad 8b 8e a2 1f 9b ca d9 f9 bf d1 57 21 c0 3b 30 d1 4a 8b fe f6 53 6d 0c Data Ascii:);EhCYuq(zf"wc9$8]*@L%e'w4$jDF#*)<e;B!QNQ/+CnpWU4PaGu%:xe^8QKC1;Cm2Q\SC$R~! UD3s18b+> ~F *eW!;0JSm
2021-09-27 18:34:12 UTC	1642	IN	Data Raw: 9f b5 b4 6a 00 71 fd 0d e8 83 3a 6d 6b 5e b2 6f 86 64 ea aa fe f5 06 ae 4a de 9e b5 eb e9 8f 83 e0 1f 62 33 93 7d 59 db ae 44 06 ce 92 0f a8 de 50 30 46 ac c4 83 88 2f f5 da 55 fc 16 8c 2f 44 42 20 b9 51 6a 57 d1 d2 21 64 2f 9e df 50 22 e9 10 b2 d7 41 ed 1a 2a 6a 22 b6 5d f1 93 dc 37 74 4c c1 37 c5 94 95 bd cf 6a 57 32 1b dc f8 d3 ee b9 2c c9 64 af 16 64 8a 3e 0d 67 98 d0 07 93 1b 49 f9 48 be 22 db 53 71 ee 0f ce 40 5d e6 e1 c0 47 d9 5c 0b 16 c8 2e 74 a5 e2 d7 a8 36 91 3a 49 be d1 90 48 d7 13 80 38 2a 8a af d5 24 d2 d3 70 7a 19 cc 85 c2 90 7c 48 b9 27 5c 8d 85 18 59 6a c2 d0 f5 47 84 62 c2 09 24 ef 80 9f b5 80 a2 0a ee 92 dc 9c 37 eb 47 fe 6c 22 08 c8 be c3 7b 16 b8 f4 45 f8 92 7c 7c d8 ac 9f 04 81 d0 9e 65 37 70 cd fa d9 40 76 04 d9 5d 74 23 71 3d bc 9c Data Ascii: jq:mk^odJb3}YDP0F/U/DB QjW!d/P"A*j"]7tL7jW2,dd>gIH"Sq@]G\.t6:IH8*$pz|H'\YjGb$7Gl"{E|e7p@v]t#q=
2021-09-27 18:34:12 UTC	1643	IN	Data Raw: fb 98 fe fd eb 9e e9 ba fe b7 8f d5 2e cd db 7f 52 0d 99 b0 fc e1 eb c9 ba ae 77 d5 a7 8f 1f ab fd 6e 57 94 f5 f9 8a db e7 fc a1 d8 7e 7c 78 35 e4 c7 34 af 90 29 1f cd 80 e7 ec d7 13 ad 4e cb 15 ab 21 3f 9b 6f d2 fc f1 eb 49 ab 98 26 d1 1e 36 69 55 e1 65 89 f0 ce 4a b6 38 6b 56 04 c1 7c 75 56 ad 8b 27 bc fc 53 5d ec ce ab fd 72 99 3d 64 d8 5c 9f b1 c5 3c 7d 20 55 dc 04 c8 01 c7 73 4c 1b 73 7a 96 a9 7b ae 21 05 d8 2f fb aa 49 9c e7 4d 46 11 fe b9 d8 6e a1 2a 2d d9 a7 ff d4 99 4a 5b 1b bf e5 0c b3 71 86 62 b1 4a 67 1c ba e0 ff d1 52 4e 60 58 7a e0 e8 be 6f da 81 69 18 12 60 84 f3 79 c9 60 a1 bc 11 08 6c d7 d3 91 88 c8 5e cf d7 03 cb 3e 16 f8 4c b9 a4 85 39 41 94 90 31 03 48 e8 01 a0 cd 71 4d 13 32 12 ec 7e 1b c2 4e f1 65 0c 43 4d c6 a7 bb cd be 4c 37 a7 c5 Data Ascii: .RwnW~|x54)N!?oI&6iUeJ8kV|uV'S]r=d\<} UsLsz{!/IMFn*-J[qbJgRN`Xzoi`y`I^>L9A1HqM2~NeCML7
2021-09-27 18:34:12 UTC	1644	IN	Data Raw: e3 a6 9f b9 c6 d4 ec fc ad 75 f9 bf 74 28 ef b4 20 2d a9 55 d8 eb fd 0e e3 3f 6c 2a ea b2 d8 63 c7 20 b9 45 2d 9a 0b c7 b4 dc 96 d5 3a a0 55 00 30 d3 f7 d0 99 02 79 1c 43 0a b5 f0 f1 99 ed 6a 70 9c 4d 23 e1 39 0e 35 99 4e 00 5e 84 ca 2b 93 9c 31 5b 97 da ea 8d d0 5d f7 1a 49 f0 1a cc 87 f6 d7 45 f9 07 4f 90 9b d9 4b 9e 58 07 cd e5 9c 71 cf e4 5a 45 e5 07 1e c3 16 a9 0b c9 b5 fb 9b 30 11 81 ed d8 b6 ae 63 51 20 5e d8 82 07 d6 26 d1 cb e6 b0 22 2c 6b 1e 05 af e9 b3 ca e6 dc e9 3f 36 8a a0 2a f0 c1 7a 1c 80 08 c8 85 a4 a7 07 fc 7e 8d 19 d2 34 e6 2c 20 dd 2f b2 42 54 5e 62 9e fc 4c 64 ab bd 1d 60 34 09 ba 87 fb 9b 84 17 25 ad 99 d5 45 93 69 83 c1 a1 9a 98 f4 24 d5 11 b1 7c 62 2e eb 74 03 a3 3c 3f 9d 03 a4 f8 96 a6 a3 1b 6d 9d 8a c8 05 00 f0 b5 d5 ed 76 40 c6 Data Ascii: ut(-U?l*c E-:U0yCjpM#95N^+1[]IEOKXqZE0cQ ^&",k?6*z~4, /BT^bLd`4%Ei$|b.t<?mv@
2021-09-27 18:34:12 UTC	1646	IN	Data Raw: 69 78 13 4f be 1c 6b 50 01 96 a4 e1 32 4c 2e a3 9b d9 c5 74 32 19 24 f2 1a e4 cb 1c 59 c3 20 99 60 03 58 45 34 a6 3d 1d 2b 51 f5 6d 92 92 5e dc 9b 25 83 c9 6c 32 92 b6 a1 22 9a 92 7c 3f 8a 7a 17 e1 e5 e7 59 74 1b c6 37 b3 7e 1c dd f4 8e 15 a9 ce d3 bb 15 f5 07 a3 db 59 2f 1a 5f 8e e2 a1 72 5b 8a 03 9c 6e 6d d7 51 d8 8b 46 c7 3a 54 74 aa 5b c7 70 34 b8 1d 4e 24 f3 c8 4d 4b b7 8a 51 f4 f3 34 1e 45 92 69 54 fd 52 b7 96 c9 97 61 f4 8e bb e5 53 06 49 d5 6d 3c 1a 0d 46 71 72 d5 c6 ee 6c 3c bd 20 1b e1 27 29 8c 15 e5 50 52 98 44 93 fb c1 e8 33 e2 a8 df 8f 46 14 8e f7 71 3f 96 ec ad a0 37 9d aa ba 36 a8 fa e6 a3 53 c9 38 bc 8d 94 4b 51 9d f2 74 6a b9 27 9f cd 86 97 92 69 e4 72 26 eb 18 1c 4b a9 6e ab 24 b1 e1 28 be 0b 2f bf cc 7a e1 24 9c 4d c7 e1 55 a4 48 27 e9 Data Ascii: ixOkP2L.t2$Y `XE4=+Qm^%l2"\|?zYt7~Y/_r[nmQF:Tt[p4N$MKQ4EiTRaSIm<Fqrl< ')PRD3Fq?76S8KQtj'i r&Kn$(/z$MUH'
2021-09-27 18:34:12 UTC	1647	IN	Data Raw: 2a 9c 96 2c 53 97 db 07 26 72 43 27 b3 70 e4 58 17 0a 89 8a 88 78 71 59 b3 60 95 92 46 14 5e 6b 09 8c 08 6d 79 16 90 0a 45 89 60 b1 3b f4 24 89 65 b1 42 2a 8d cf 57 23 9e d5 e3 cd 8a 80 c4 1d e5 16 b6 fb 8e ea a4 f1 36 ea 5d ae 91 58 56 f5 57 1f c7 ad 59 11 04 ec cd 38 29 bc f2 c1 fa 87 48 77 be ae a9 14 ba 28 7c e1 4c a5 3c 26 18 ed 0a d6 f8 6a bd 5c 6d d7 37 4a 5f d3 ad 69 79 01 3a a8 9c 29 ac 0f c6 3a e9 58 d7 e0 3d 39 32 89 a5 d6 a9 d9 db 4a 3e 9e 88 8d 0f b1 b0 29 67 05 a8 b9 12 aa 22 c7 6e 7b 49 4e 54 6e d9 9e a3 33 6e 04 bd c2 ba 65 5a bf fb c5 64 8f de 5e 5f fd b1 5e ce 6f 6e b1 56 20 8d 5d ac 3a 8f c6 93 ee 68 32 3b ed 0f 5e 3c 42 2a 52 a0 8d 4b 74 44 f5 71 e9 5a 06 9d 93 ab ab 37 ef d7 9d e7 f0 94 47 e5 a0 57 53 f9 ad a1 39 3e ef 0e 1e fd 79 f3 Data Ascii: *,S&rC'pXxqY`F^kmyE`;$eB*W#6]XVWY8)Hw(|L<&j\m7J_iy:):X=92J>)g"n{INTn3neZd^_^onV]:h2;^<B *RKtDqZ7GWS9>y
2021-09-27 18:34:12 UTC	1648	IN	Data Raw: a2 e3 e1 aa a4 f7 24 9b 04 62 63 20 90 a4 3f b8 a2 98 54 6b b1 aa e0 e7 d7 df a9 25 a7 e9 33 1b f8 be f9 07 d9 4f dc 6b c6 d2 92 58 d0 28 7f 3b 14 c6 da 8d ab 72 94 44 de e5 38 54 9b 8c 8e 78 81 04 7f d9 ca 66 ea 1f 1f 18 7e 52 a3 ae 8f 7e de 6e 65 54 12 4b 84 65 a9 57 99 e3 fa 73 02 4f c3 f6 09 8c 73 65 2c 2b e7 62 98 04 2c b1 81 43 9c a6 21 7c d2 60 d0 58 3c c4 51 3e fb dd 43 c6 f3 e5 24 42 83 22 86 6e b4 08 9d a8 06 2e 16 a3 be 01 76 c9 4d 18 62 b2 db 24 90 63 81 21 fb 64 c2 f2 0a eb 12 4d 31 90 03 89 b1 2c c5 08 88 9b 54 a5 f6 3f b8 8c 54 52 9e be d1 2d 1d e6 7c 2c 95 70 b6 9a 8b 33 e7 d0 c0 c4 58 79 45 14 b3 b5 64 c6 e7 7f 83 9f c4 a5 8b a4 b3 f4 15 ee 9a da 5d 54 0b 64 a9 f7 44 97 a4 33 e1 08 53 f7 3a ec af f3 84 f7 38 ec e5 1c ed 7b 95 59 d6 64 a7 Data Ascii: $bc ?Tk%3OkX(;rD8Txf~R~neTKeWsOse,+b,C!\|`X<Q>C$B"n.vMb$c!dM1,T?TR-|,p3XyEd]TdD3S:8{Yd
2021-09-27 18:34:12 UTC	1649	IN	Data Raw: 09 f5 a7 19 ee 97 b5 f2 17 a6 ba 93 a3 8c d5 00 4b 6c 61 f9 31 d9 bd ba 38 df 54 63 6e 51 73 3c 6e b4 fe d9 43 cc 54 3e 3f 6f 86 b9 b0 de 06 c0 ce 85 04 c0 08 11 1e 70 e3 9e 95 c4 c4 62 69 71 6c 9e 14 d5 b0 dc eb e7 16 d2 00 ae 08 52 39 e5 ad 16 8c fe 6d a8 38 a4 5f d8 87 61 f7 94 2b 5a ee 35 7f 9a bb 84 95 58 27 ce f7 91 6b 4b 71 5f bd af 00 b9 81 d3 3a 40 9a 00 6e ca 07 c1 2b 3b cd a4 71 36 48 83 f9 25 92 69 f2 ec a7 9b bd d4 17 58 b8 66 18 96 0d 9d 0f cb 0d 46 e0 22 4e d2 52 a4 73 68 78 38 8a 0e e9 25 1e 2a 3b 65 75 0f e6 c1 93 03 5f 7b 83 ee 27 8c 5c 61 51 a3 aa 1d 53 ec 48 42 46 d2 a5 6d 9d c3 49 80 01 76 8e a8 fa bb 4c 62 35 76 c9 08 de c7 c1 4e 5c b7 e0 e6 f4 1a 98 dd 0c 2f e4 d2 b8 64 60 da 6e 39 4d 46 00 b1 dd 18 b2 f8 db 86 a5 be b6 17 90 2f f6 Data Ascii: Kla18TcnQs<nCT>?opbiqlR9m8_a+Z5X'kKq_:@n+;q6H%iXfF"NRshx8%*;eu_{'\aQSHBFmIvLb5vN\d`n9MF/

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1651	IN	Data Raw: 99 cd ce 8f 88 68 28 2e a7 34 86 bb ab b8 37 69 90 65 e7 a3 fe 45 f7 e8 d5 ac d7 9d 74 67 d3 71 f7 a4 64 cc 89 bc ec 81 90 19 57 49 14 ef 5c 38 4c c4 af 3f 1d 9e 10 f7 c8 54 77 99 c5 93 e9 f9 ec a2 3f ee 3f eb 6f 94 2c 7b a4 cc 7b e8 28 b5 e1 f1 e4 65 77 94 d7 7c 0e 61 11 2a d3 c1 8b c1 f0 25 59 cb 15 ec c9 da 8b 7e af cc 7b 7b 26 ad c8 50 18 9f 0d 87 93 e7 83 72 4c a4 ca bd e5 91 10 79 55 d2 60 c5 bc c1 67 b3 6e 7c 32 3b 06 87 0c da 3b 19 42 ac 19 13 f7 c5 dd 38 6a 56 82 a4 c0 db f4 ca 41 9f 7a 2c ee f2 59 ba 6e d2 3f 2b 81 61 62 78 cc 10 50 b3 f0 6c 13 cd 06 e5 d1 24 72 4d e4 c3 bc 82 12 2d fe e2 21 eb b8 dc 3d 3a 2a cf 27 dd 67 a7 c4 76 b8 69 ae 3c 9d 93 e1 90 70 c2 65 a1 79 0a e7 e5 e8 18 76 45 b6 c3 bc 30 b2 85 c8 70 48 22 18 53 64 c8 13 98 0e fa 00 Data Ascii: h(.47ieEtgqdWI\8L?Tw??o,{{{ew|a*%Y~{{&PrLyU`gn|2;;B8jVAz,Yn?+abxPl$rM-!=:*'gvi<peyvE0pH"Sd
2021-09-27 18:34:12 UTC	1652	IN	Data Raw: 53 b0 bb f7 1f 8f 36 55 b5 2d df 9d 9e 96 bb ed 36 2f aa 93 b5 88 cf c9 32 bf 3f 5d 3e 47 f2 34 ce ca 07 56 9c ea 9e a8 b2 8f 47 4a 15 17 6b 56 c1 7e 71 9b c6 d9 a7 8f 47 ad 63 3e 89 b2 4c e3 b2 c4 8f 05 fb d7 2e 29 d8 ea 6d b3 22 18 66 eb b7 e5 26 7f c0 8f 7f a9 f2 ed 49 b9 bb bb 4b 96 09 36 37 60 6c 75 1b 2f b9 2b 11 02 e4 b5 e5 58 ba 89 39 1d 43 57 1d 5b 23 09 e6 af 56 09 4f ec 38 55 b0 de 7b 38 29 df fd e9 53 94 06 59 fb a3 53 d0 9b 53 90 ac 52 7a 0a fb b1 ff 1f 86 c8 f2 34 43 f5 2c d5 75 75 d3 d3 35 8d 56 7f 9c 2d 59 da 8c f6 4c db 51 51 7e a8 59 c7 55 3d c3 3c 1c 3d 3a f5 eb a1 ba 87 81 aa 07 3c b2 6c 5d c7 50 02 90 5f 26 88 4d d8 0b 11 9c 68 76 ac 6c d3 5d 11 a7 c7 40 cc bb 92 55 ef b4 f7 aa f2 e5 22 ce d6 f9 ae 7a 7a af 3d 7f 56 1e 92 6a a3 7c 19 Data Ascii: S6U-6/2?]>G4VGJkV~qGc>L.)m"f&IK67`lu/+X9CW[#VO8U{8)SYSSRz4C,uu5V-YLQQ~YU=<=:<l]P_&Mhvl]@U"zz=Vj|
2021-09-27 18:34:12 UTC	1653	IN	Data Raw: 8a 9e f9 39 b5 e2 a6 49 ab 51 15 f9 f1 53 e3 0f 1e 3d 17 42 c0 42 e9 83 7a 89 3b 9e 78 7b e4 1a ef 56 49 ce 93 90 57 7f 73 00 a8 38 b1 ea 84 e3 d7 0b 14 5b e8 30 55 c3 84 64 01 20 eb fc 13 81 62 b1 d6 26 39 4e e7 d3 4b 05 9a a7 5e e7 b2 9e b6 5d 25 84 07 a4 01 2a 1e d2 00 2a c8 23 22 98 eb 2d cc 7e 0b 3c 16 2c fd 1d 2a 44 34 22 2b b6 fa be 76 62 a3 65 d2 d0 a7 61 cb ae 6a a9 00 cf ee 13 c7 21 0e 86 b5 99 03 54 44 80 38 93 60 0f ba 67 91 5d 8c 97 58 6d dd fc cc aa 1d 24 41 4d 05 d0 4b 10 61 96 86 08 03 54 41 09 26 55 94 79 de 8e 45 4e a1 27 07 86 bb ae 89 43 d6 c8 0e 5f a3 0d 7e 18 b5 62 04 24 08 87 b6 8a 94 83 a2 85 58 f3 10 30 24 0d 71 38 07 16 20 45 1a 64 2f f9 a1 ae f9 3d 48 86 f3 bc 7d 14 59 d8 80 cf a4 61 fa 09 67 fa c7 76 02 d7 e6 f7 24 c0 42 97 df Data Ascii: 9IQS=BBz;x{VlWs8[0Ud b&9NK^]%**#"-~<,*D4"+vbeaj!TD8`g]Xm$AMKaTA&UyEN'C_~b$X0$q8 Ed/=H}Ya gv$B
2021-09-27 18:34:12 UTC	1654	IN	Data Raw: b3 f0 2c 14 49 d6 79 a4 92 27 e0 d4 db 78 10 5d fb d3 ee cc 97 31 15 f1 32 1f 7d 18 8d af 89 ad ac 99 21 b6 57 61 3f e8 46 7b 89 08 e8 f0 30 1b 8e c7 d1 c5 28 98 91 a8 ca de 8c 20 4e 6e 02 4a 56 92 87 70 c2 6e 76 be 18 00 90 91 bd d1 18 5c 33 23 f0 25 bb e0 6e 2d 11 29 a0 4d 3f 18 85 14 b1 64 97 f0 5f db 45 e1 30 c0 82 49 e1 49 ae 61 5a c3 a1 60 b3 51 d0 8b 9a 55 93 f8 48 de 00 d9 33 7e 46 c8 9a 97 fd 5e 2f 98 44 fe d9 25 a9 1d d9 45 55 b7 9f f3 f1 98 ac 44 a6 0f bb 3d 4c 82 e9 00 bb 22 db 91 bc 56 f2 8a 93 f1 98 30 98 44 1e 77 3b 98 8f 42 48 85 cb cb f0 3c 94 c4 44 f6 c4 40 e6 ab 1f ce 7a fe b4 cf 4f 6a 10 4e 87 be ac 14 65 8f 88 64 be 06 e1 28 10 f0 b2 40 65 8f 24 e4 23 bb 3d 91 39 12 3e 3a 48 5e d2 35 ca 5c 8c 7c 2a bf e8 3b 04 32 cb f1 07 0a f1 f4 59 Data Ascii: ,Iy'x]12}!Wa?F{0(NnJVpnv\3#%n-)M?d_E0IIaZ`QUH3~F^/D%EUD=L"V0Dw;BH<D@zOjNed(@e$#=9>:H^5\ |*;2Y
2021-09-27 18:34:12 UTC	1656	IN	Data Raw: 1a d2 69 cb 6a c8 af ee b2 24 ff e7 97 b3 4e 31 3d 44 5b a3 e0 2a fc 58 b2 5f 9a 14 05 f5 7d 6b 11 04 f3 ed f7 d5 43 f1 2b 7e fc 53 5d ec 2f aa e6 fe 3e 5d 53 5d 8e 18 db dc 25 6b 52 c5 5d 80 cc 77 3c c7 b4 f1 4c cf 32 75 cf 35 a4 64 1b c0 3c 4a ec b4 a8 b4 64 03 35 45 9e 64 ac 7a f7 5f 47 52 e9 68 e3 df 45 c2 6c 23 a1 b0 54 19 89 63 ff ff 3f ba c9 09 0c 4b 0f 1c dd f7 4d 3b 30 0d 43 c2 88 41 92 af 81 ac 65 bb 3e b0 5d 4f 47 3d a2 8a 3d 5f 0f 2c fb 74 fd 78 7e 39 1e 88 c5 66 80 a5 7a 00 fc 72 5c d3 c4 62 09 6d bf 4d e1 9f 78 10 c3 41 8b f9 f9 3e 6b ca 24 3b 2f ee ef 2b 56 bf 33 b4 1f f4 6f 1f 92 7c 5b 34 f5 d3 0f 46 f7 91 80 4a fb 36 99 5d 85 e3 f8 1f d1 ec e9 e9 07 b3 ef 27 ed ab 56 d4 65 a2 ed 11 2d 04 f7 a9 a8 1f 58 f9 ca e2 3f 77 2b 2b ad 6d 1d d5 d3 Data Ascii: ij$N1=D[*X_}kC+~S]/>]S]%kR]w<L2u5d<Jd5Edz_GRhEl#Tc?KM;0CAe>]OG==_,tx~9fzr\bmMxA>k$;/+V3o| [4FJ6]'Ve-X?w++m
2021-09-27 18:34:12 UTC	1657	IN	Data Raw: 42 ff 96 29 d3 08 d8 d1 f6 28 82 6c ed ed 87 96 2c 3a 16 98 12 1e 88 61 da 05 9f 00 fb 90 47 e3 01 32 48 1a 56 77 69 85 3e 02 f2 af 7d 4a bf 1f a5 42 99 6d eb 3a 4c 01 79 83 dd 1e 98 9f 44 56 3b 34 16 a5 af d5 e9 be cd 82 e7 89 88 b2 11 19 04 ff f1 cc 69 91 d9 b1 a1 3d f0 41 a8 1c 80 10 b8 8a a4 9a f7 dc a3 83 0c 28 a2 b2 d9 a5 75 c7 5e b4 a4 d9 a4 c5 31 25 b9 68 75 bb 98 49 6d 70 3f f4 12 93 3e f5 76 91 d6 ee 43 d6 a2 11 2c 67 d7 9c ab dc 11 67 69 a9 69 67 33 e8 1c 98 15 c0 07 cc 0a e4 32 90 c6 90 48 18 f6 92 b1 b0 fd 0b 56 f4 b6 64 dc 3f 68 ae 45 1b 35 17 03 ad 81 29 1a 4e f1 75 47 07 ec f7 a6 88 f6 76 74 d3 4a 79 00 70 78 90 ba 24 36 69 06 8e b4 cd 9b e2 b1 63 57 54 74 78 2e 7a 25 ed 12 91 e7 9c 51 28 0a 88 fd 3a 06 22 82 76 80 c6 67 4b 09 77 93 64 49 Data Ascii: B)(l,:aG2HVwi>}JBm:LyDV;4i=A(u^1%huImp?>vC,ggiig32HVd?hE5)NuGvtJypx$6icWTtx.z%Q(:"vgKwdI
2021-09-27 18:34:12 UTC	1658	IN	Data Raw: 54 27 f9 fd 8a 46 93 d9 cd 6a 18 cd 07 b3 78 aa dc 96 e2 68 a8 5f db 87 28 1c 46 b3 53 1d 2a fa d5 af 63 3a 9b dc 4c 17 92 7b e4 49 a7 5f c5 2c fa 69 19 cf 22 c9 35 aa 19 ab 5f cb e2 f3 34 7a 25 dc f2 d1 84 a4 ea 26 9e cd 26 b3 78 7c d5 e5 ee 6a be 7c 4f 3e c2 bf a4 34 56 34 48 49 e1 38 5a 7c 9a cc 3e 22 8f 46 a3 68 46 e9 f8 29 1e c5 92 bf 15 cc a6 57 55 df 06 55 2f 98 f4 2a 99 87 37 91 d2 14 d5 71 50 af 96 4f 14 b3 d5 74 20 b9 46 ee 6a b2 8e c9 a9 94 ea aa 4c 12 9b ce e2 db 70 f0 79 35 0c 17 e1 6a 39 0f af 22 45 39 49 b7 59 92 9a 39 51 0c 35 b8 a8 1a 88 5a fe 7a 72 25 c1 a3 62 be 50 08 2f 96 d3 d5 6d 3c 8f df c7 3c c9 7a 43 aa 78 af 44 d6 36 19 2d 3e 85 b3 fe cc 57 f5 35 49 cb 72 fc 71 3c f9 24 c9 aa 26 38 49 f6 36 1e 46 fd 68 af 60 11 3d 1a e6 37 93 c9 Data Ascii: T'Fjxh_(FS*c:L{I_,i"5_4z%&&x|j|O>4V4HI8Z|>"FhF)WUU/*7qPOt FjLpy5j9"E9IY9Q5Zzr%bP/m<<zCxD6->W5Irq<$&8I6Fh`=7
2021-09-27 18:34:12 UTC	1660	IN	Data Raw: fd ae 5d 4b 35 3c c7 52 11 61 5d d5 55 c3 25 6b bb 66 99 b2 ae e6 c2 51 2a e9 8a 29 17 8b 6d ba e2 f7 08 7a ac bc 19 47 fe 28 9a de 84 fd eb 37 5b b6 44 70 8a 8c 67 ca 65 9a ce 13 ae 5c 61 dc 9b a0 df a9 7e ff d4 8c 1e 0f fd fe 9b 9f cb 1f ca 8f 27 58 ca 26 61 f7 7c 91 26 33 be cd ca 35 34 66 e5 3f f7 e9 3a e7 eb 5c 2c e8 8d 56 2e bd 31 26 3f eb e5 cf cf cb 22 03 8c 83 01 52 0f e6 c9 d3 53 4b 74 a6 9b c5 71 80 7e 39 67 ff f8 56 70 55 55 7f 39 cf 36 6c dd fc c3 94 c5 96 3f 7c fc 76 b2 c8 f3 4d f6 e1 fc 3c 2b 36 9b 74 9b 9f cd cb d8 9c dd a7 ab f3 fb 7d 24 cf d9 3a fb 9d 6f cf 75 af ac cf 6f 27 4a ce b6 73 9e c3 7e 7a 87 bc 58 7e 3b 69 1c 8b 49 94 fb 84 65 19 7e dc f2 7f 15 f1 96 cf de d7 2b 82 e1 7a fe 3e 5b a4 bf e3 c7 9f f2 74 73 96 15 0f 0f f1 7d 8c cd Data Ascii:]K5<Ra]U%kfQ*)mzG(7[Dpge\a~'X&a|&354f?:\,V.1&?"RSKtq~9gVpUU96l?|vM<+6t}$:ouo'Js~zX~;iIe~+z>[ts}
2021-09-27 18:34:12 UTC	1661	IN	Data Raw: 53 8f 35 c4 1d 56 d0 ac 44 b2 14 cb 43 38 b8 00 59 2e 0a a2 1e b2 2e 04 8a 00 cd ae 0b 24 38 f4 41 ce 1b ac 2e 93 88 8b a4 c7 54 69 5e c1 57 a2 b0 bb f8 b4 2e 65 a1 e6 b0 1c fe a2 dd c0 ef 4b 60 0b a6 7e 6e 31 ce fe 9b 56 e2 95 5e a1 d1 a1 92 98 bd de 0a fc 45 f5 8f 24 2e 00 e3 d0 a5 69 5e 75 01 96 6e d8 8d 10 b5 a0 7f 00 46 ba eb a0 85 04 98 58 1a 49 c5 11 5b 14 a0 98 5d 3d de b1 2c d1 0a 5a 1e 84 0b c8 92 4a 91 71 51 6c f9 a6 c6 63 56 eb 10 e8 af ab 4e ed 01 22 04 b3 a2 5b b5 c1 d9 20 77 92 23 fe 76 27 8a f4 f1 b0 1f 54 d2 35 2a 61 05 6c fc 12 77 e3 f7 4d 4b 3f af d5 8a 65 9a aa 8a 95 41 23 61 17 0e b4 15 91 82 bd 38 ab 32 e6 e1 be fa bb 89 5f 60 7c 83 b9 35 6b 7f aa fd c2 b3 e7 42 b4 58 40 15 68 04 e2 f6 10 ae f8 4b da 86 88 8c ab 7c cd 4a c6 86 95 00 Data Ascii: S5VDC8Y..$8A.Ti^W.eK`~n1V^E$.i^unFXI[]=,ZJqQlcVN"[ w#v'T5*alwMK?eA#a82_`|5kBX@hK|J

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1662	IN	Data Raw: 83 0c ab 88 87 0b bf 7f 11 dc 4c 3f 4f a2 68 d0 a7 6b a0 cf 29 a8 87 41 3f c2 06 b0 8a 60 2c f6 74 ec 44 d6 e2 10 27 9d b0 33 ed 0f a2 69 34 22 db 90 69 3a 62 df 0d 82 ce 67 ff e2 7a 1a f4 fc f0 66 da 0d 83 9b ce b1 23 d9 35 71 bb a3 ee 60 d4 9b 76 82 f1 c5 28 1c 4a b7 25 b9 ec 68 f7 76 15 f8 9d 60 74 ec 43 a6 90 da 7d 0c 47 83 de 30 22 e1 a1 dd 41 bb 8b 51 f0 db 24 1c 05 24 34 b2 be a4 dd 4b f4 75 18 bc 72 dc b4 15 27 ae 7a e1 68 34 18 85 fd cb 26 77 a7 e3 c9 67 11 23 7c 45 d2 58 c2 85 c4 61 3f 88 be 0c 46 d7 c8 a3 6e 37 18 89 74 fc 12 76 43 12 6f 89 6e 69 75 d5 b6 41 d9 cb 0b ad 4e c6 7e 2f 90 2e 45 76 0f d2 ea e5 8b 38 b3 e9 f0 82 84 86 b2 18 f5 31 38 b6 92 3d 82 21 66 c3 51 78 eb 5f 7c 9d 76 fc c8 9f 4e c6 fe 65 20 29 27 f2 e4 84 b8 19 0b 49 21 07 17 Data Ascii: L?Ohk)A?`,tD'3i4"i:bgzf#5q`v(J%hv`tC}G0"AQ$$4Kur'zh4&wg#|EXa?Fn7tvConiuAN~/.Ev818=!fQx_|vNe)'I!
2021-09-27 18:34:12 UTC	1663	IN	Data Raw: b0 28 5a 1d e8 75 17 c2 7a fc 24 85 ff dd 4f a2 85 e0 8a 15 56 4a 0e 53 31 a9 c9 49 04 e6 b8 46 53 29 24 96 b0 12 81 45 88 34 c0 2f ab d5 e8 63 ff 5b f3 4d 62 3e f9 ff df 22 3e 85 bd 25 ca d6 ea 84 41 0a b4 ec 44 df 32 a3 b7 29 cf 96 19 c7 81 03 9a 39 a6 6a 72 9c 59 61 9d b6 fb b2 d9 8f 2f 64 51 d8 c2 a8 5a 2b 94 53 d2 14 e4 78 87 b9 86 8d d4 32 50 28 61 54 a1 ad 53 da 70 43 ba 08 85 b4 d6 9b 57 b4 bf 20 94 a0 45 81 b0 66 d2 19 cd 40 4f 05 13 4c 5a 62 63 a0 ef 7e 0c b2 d8 60 78 a9 51 60 2b 8a 55 2d d8 fe e0 fd dd ed 6f ab eb e5 fd 83 97 cc 0a dd 7f 43 98 f6 4d 50 8f 27 d3 59 7f 32 5b 9c 57 a3 97 4f 52 85 42 0e 2f f8 1d d3 3b bb bd 7d f7 71 d5 7b 01 d3 3d 29 47 c3 64 a8 40 6a 1f 2f d2 db 72 3b e5 f4 b2 3f 7a f2 e7 86 44 f3 ef 11 30 ee f3 c7 e5 f5 ea fd ed Data Ascii: (Zuz$OVJS1IFS)$E4/c[Mb>">%AD2)9jrYa/dQZ+Sx2P(aTSpCW Ef@OLZbc~`xQ`+U-oCMP'Y2[WORB/;}q{=)G d@j/r;?zD0
2021-09-27 18:34:12 UTC	1665	IN	Data Raw: f5 ad 56 9c b0 38 5a 1c 2a b1 b5 36 b9 97 e0 62 95 0c d5 13 7a 78 ae ca d3 3a 18 0c c9 0f 70 4c 44 9d 37 ef ab 76 38 10 24 59 89 78 44 78 ac d8 98 56 c8 36 62 30 81 38 72 80 e7 89 ab c4 1e 46 2b ae ac 84 4c 1e e0 3d 64 cf 00 b8 e4 8e 7a de 9a ef 19 55 8c 44 f8 cd dc 47 3e a7 de 4e 0c 5d 24 f6 26 39 bb 0f 05 70 c5 e1 46 ab 65 0d 5e 99 d0 12 f2 97 3c 80 c5 f1 24 32 0f 42 2e ad 2b f1 b3 08 48 4b ad 94 ca 58 c8 4c 61 c9 96 2c 08 b5 21 9f e6 5f 2b c3 14 b2 f8 a9 b0 e3 cf b7 21 28 4f b0 a3 6e 1d 0c d4 a2 0d c7 82 db a7 64 1d 2e e3 ca 3d 76 0e c1 dd ef 92 5c 50 4a 0d 59 ae 75 90 89 35 fd 0b 6d e9 04 3d 72 99 91 1b d8 2b 84 fc 6f 16 f8 eb 1a 1c 24 a2 4e 48 0d 39 b7 76 8c da 7b 9c fd ac bb 60 51 e5 25 9b 96 7c eb ee 37 26 c3 fa 99 f8 47 cc f5 75 6b e7 07 f2 d0 81 Data Ascii: V8Z*6bzx:pLD7v8$YxDxV6b08rF+L=dzUDG>N]$&9pFe^<$2B.+HKXLa,!_+!(Ond.=v\PJYu5m=r+o$NH9v{`Q% |7&Guk
2021-09-27 18:34:12 UTC	1666	IN	Data Raw: cf 67 6d 11 d6 66 bd e7 5b 7d c3 ba 63 d6 65 cd 59 b0 8f ca 41 df 07 d1 ff 3e 55 a1 94 b7 7b 16 85 da 50 0b ca 2b 01 f8 1b 66 4c 7d 1a 0e fe 21 81 74 f4 a0 88 46 9e 81 4a 03 3c 61 53 17 aa 34 07 b3 50 5c 41 5e 41 9d 17 5c 57 63 54 47 25 c8 61 b9 77 62 1f 09 2e 8d 69 84 63 c8 87 2e 9c a7 0b 3c 02 ef 1f 2f a1 88 fa 4a 41 dc d7 58 f4 39 67 12 8a 04 c1 46 ac 80 1c 4f f2 42 00 ee 57 bc 30 54 ca fb 43 6a 57 54 b9 6a 7b 3c d4 dd 44 b8 c9 a2 b8 af 72 79 fb 09 77 bd ed ae 47 e1 e9 a6 61 76 d1 5c be c1 f9 3b 8e 84 b8 90 8b cf ab b5 9d d8 e8 5c 9d ee 64 48 40 b2 1b 7d f0 1c 3f 05 41 99 c2 08 25 0a 80 a5 5a 49 80 c5 f4 f1 e8 ff aa f8 70 78 15 1d 87 d9 5d 95 aa 74 05 cd ce ea e8 52 77 9d 38 6c 51 08 69 b5 a0 cb 4b 18 87 44 d5 bc ed fe c0 32 5b d7 17 24 90 ad 0b be cc Data Ascii: gmf]}ceYA>U{P+fL}!tFJ<aS4P\A^A\WcTG%awb.ic.</JAX9gFOBW0TCjWTj{<DrywGav\;\dH@}?A%ZIpx]tRw 8lQiKD2[$
2021-09-27 18:34:12 UTC	1667	IN	Data Raw: a8 b7 80 50 e4 7c fc da e2 57 89 73 c3 79 3a a7 93 b2 fc 47 1a cc a8 37 ef e5 89 50 ce 99 78 33 ca 16 02 13 90 55 ba 91 f4 9c 72 9e c4 df ca c9 cb 14 10 10 85 ea 3c 89 4c 84 a0 1e 0c d9 42 84 88 10 d4 d1 bb 3c 05 0f 4d d2 b0 9b be 68 6d 0b 8d 19 e0 cd 54 65 a9 b3 87 79 22 f3 d1 ab fe 6c f0 82 52 32 ea c4 0e 45 e8 f5 78 0e 19 fa 68 fa 8a 30 1f e2 85 29 88 c4 8b fe e8 0c a0 cb a2 1a f5 c1 6c ae 92 15 50 cd 4e 72 f8 15 58 5b 0a 9d 88 a7 da 88 d1 21 03 48 53 c5 f4 cc 20 31 7a 56 cd ce cb 45 62 18 c4 db 9c d0 60 9f 16 42 ca 12 00 c3 a0 7f 59 7b b1 64 07 c4 e1 ef 35 15 80 a8 09 bb 88 a6 73 7b ff 65 7f 3e 4d 06 50 6f 87 59 0f 38 ef a7 ee 8b 78 9b 4f 7b ff b4 2c 93 f0 4c 55 83 db fb e7 23 6a 0b 54 b7 ac 1d 71 35 3e 9f 5f 24 23 a8 97 03 3e 3e fe 07 50 4b 07 08 44 Data Ascii: P|Wsy:G7Px3Ur<LB<MhmTey"lR2Exh0)lPNrX[!HS 1zVEb`BY{d5s{e>MPoY8xO{,LU#jTq5>_$#>>PKD
2021-09-27 18:34:12 UTC	1668	IN	Data Raw: 0d 15 36 e4 e9 9e 20 dc b8 88 05 bb 34 73 5e b3 25 2b f1 d7 82 f1 c0 e8 b6 f0 68 78 48 1b c7 b5 e0 51 43 84 4c 82 e0 d1 8a 29 5b 2c 96 55 38 9c d4 66 06 38 52 e7 5e 1c 0f 93 f1 24 d3 ee 23 9d eb 67 4d a4 be ae 61 a1 96 67 78 7c 03 69 50 e2 7c 11 ef 8a a3 b8 18 96 a9 ab 26 dc 83 99 55 c3 c0 0c c9 00 81 98 0a 7e 43 75 b9 f8 4f b7 11 40 cf 33 c8 0a ee aa 27 4d 15 d4 e8 81 b0 1d 84 11 9c 6d d3 dd 19 8b e8 09 b2 5a 67 60 a9 2c cf a0 38 94 1f b6 0c cc 99 56 ac fb e3 db c6 21 0f 82 a6 a9 9e ce 6b 55 a7 bc 5b b3 dd 05 d4 4a 0e 47 c9 b9 22 b4 cd ae 28 ea 21 9e ea ef 9b a7 38 2f e2 e5 aa fe 06 62 ac 2d ce 95 0e 22 7f c1 50 a8 75 f4 cf 95 75 9c f0 7d 84 1c 2a 94 bc cc 20 22 4a 4c 12 20 55 c0 3f 2f 9b 6d 02 57 49 2a a2 89 ea 61 fc 2f 89 f2 98 b0 2f 29 5f 50 b2 58 b0 Data Ascii: 6 4s^%+hxHQCL)[,U8f8R^$#gMagx|iP|&U~CuO@3'MmZg`,8V!kU[JG"(!8/b-"Puu}* "JL U?/mWI*a//)_PX
2021-09-27 18:34:12 UTC	1670	IN	Data Raw: 0d ea 14 a0 43 32 06 7b 8b 32 41 5a 8a 66 cf b6 35 34 78 ae 07 61 a1 43 e0 a9 92 9d 39 88 0a 56 e4 59 0d 6c e8 c9 0d a8 3b c3 03 6c 22 b5 5c 4f a5 e7 af 6c c3 e5 7e fe 56 f9 b8 e0 79 9a e4 42 bb 83 19 eb 6e 26 e3 2d d1 8b 04 42 ee 0a f4 b8 54 7c de 25 64 cb 98 3f 54 3f 0f 35 5d 35 51 2f 11 66 af a8 f7 08 53 c4 3c 29 b8 50 5e 55 a7 58 90 58 c0 53 be 59 c7 8d c3 91 f6 c2 5f b0 c2 aa 17 63 9b 0a f8 8e b5 bc 00 63 a2 8c c4 cf 69 8c c0 f0 16 47 a4 ba 07 b5 03 01 ca 85 32 70 13 92 94 36 c2 55 01 3d 1e 01 83 a3 21 55 50 24 2a 70 1d db a0 62 23 69 cb bd d9 64 5c a3 40 60 9d a3 51 38 e9 34 2a 79 d2 9c bd 60 ed 6b 36 2f ca b2 71 ee da 5c 3a 72 be d5 a0 a3 5e 39 83 10 4e 8f 55 48 85 ad e8 c0 b2 cd 13 2b f3 1a 64 0f 5a e4 18 6e ff 3f aa 84 4e ff 1b 45 49 53 16 d8 0e Data Ascii: C2{2AZf54xaC9VYl;l"\Ol~VyBn&-BT|%d?T?5]5Q/fS<)P^UXXSY_cciG2p6U=!UP$*pb#id\@`Q84*y`k6/q\: r^9NUH+dZn?NEIS
2021-09-27 18:34:12 UTC	1671	IN	Data Raw: 99 a1 b2 07 12 f2 91 1d 25 c9 1c 55 3e 5a 48 5e d2 cd ca 5c 0c 7c 2a bf e8 9b 3b 32 cb e8 8e 42 3c 7d 8d 41 66 39 0a 38 c0 4a d6 2d bb 97 93 39 68 31 97 bd 5a d2 66 5e 95 1a c1 52 89 54 6f 75 20 e3 07 d9 41 7d ab 83 f1 14 95 4a d1 50 d6 38 c9 7c 54 7a e8 fd f4 66 16 8d 66 01 17 36 34 1d e9 0d 75 ab 23 9e df d1 7d 40 85 b0 e4 ad d4 56 27 d7 81 3f 99 82 ab b8 e0 0b 24 a8 4b ef 3d 5b 5d 81 2a 68 52 cb 5e d9 69 f5 00 e1 fa 2b d0 07 75 da 46 5e b2 b7 a9 64 ee 6a fe 7a 05 57 25 d7 74 ed 7e ae 47 41 f0 4f 4a 66 b2 57 91 db 9d c8 c0 59 f2 5e d9 2b 0e 46 d8 2b ba 10 7a 59 d8 ee e2 d7 60 74 47 05 81 e4 3c aa dd 45 0b 43 c8 2e b9 5f 71 22 61 08 d9 b5 52 bb 87 5a 9a 50 da a5 af 30 bf e2 63 02 bd 49 53 56 76 3d d6 ee 64 3a f8 e0 4f 3a b7 b2 24 93 dd 4a c8 1c 7d 8c a6 Data Ascii: %U>ZH^|*;2B<}Af98J-9h1Zf^RTou A}JP8|Tzff64u#}@V'?$K=[]*hR^i+uF^djzW%t~GAOJfWY^+F+zY`tG< EC._q"aRZP0cISVv=d:O:$J}
2021-09-27 18:34:12 UTC	1672	IN	Data Raw: fa 9e 3d 02 c8 be bd fa af 87 d5 c5 26 ca fe c8 7a 40 7d 2d f2 58 39 c0 34 81 85 aa 86 b8 ea 80 2c 5b 25 a0 3e e0 a9 b7 62 4a 47 e9 dd f4 2a 19 24 83 aa a1 0d 78 70 99 67 d8 86 4e fc 7b c5 b6 f1 8a ad 38 92 8f b3 f4 1f d1 5d 11 a7 09 ff d7 8c 2d cf 7a 51 0e c4 dc 57 ba 5c b4 04 55 75 0c c3 81 2a dd 30 0c fd a5 ae 51 5a af d4 54 53 43 ff 70 3c b4 03 cd 01 78 bf 5c 19 76 90 fc 0f 62 b5 81 24 70 6d 5b b7 5d 53 53 0d 15 32 74 35 6f 82 7b b6 42 db 13 c8 fa b9 4e bc 6e b7 5b ab 30 3c 64 85 e3 5a 50 a1 61 cf 26 c1 67 ff 00 c8 f8 26 2d 2a 31 03 0d 0e a9 84 ff 7b 78 ba 27 b3 53 44 a0 5a 6d 22 b7 75 0d 7b b3 3c c3 e3 d1 20 fb c7 ae 58 99 57 3d c3 b0 4c 5d 35 a1 1a 2d 55 35 0c 58 47 94 8b 66 58 2f b6 41 09 00 a3 b0 c7 86 c3 3c cf 20 be bd 12 2b 4d 15 cd cd 43 9f 75 Data Ascii: =&z@}-X94,[%>bJG*$xpgN{8]-zQW\Uu*0QZTSCp<x\vb$pm[]SS2t5o{BNn[0<dZPa&g&-*1{x'SDZm"u{< XW= L]5-U5XGfX/A< +MCu

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1674	IN	Data Raw: b4 4c 39 17 e5 ad 87 67 59 2d 84 7c d4 61 2e aa ca 35 91 1d 1a 71 c3 21 82 9c 52 7f b3 c7 09 ad b6 8a 6c c5 78 00 96 eb c1 b5 48 39 7a 0e d6 50 46 4e c9 90 0f 75 87 c9 15 71 fe b5 c7 1f d0 be 6d bc e3 bf 8d 8f 79 cd b8 e2 35 2f a9 82 8d ba e4 67 5a 80 66 97 9f 11 d9 06 a9 94 9f 94 2b 71 cc 26 f8 64 dd 67 6c 93 1f ee e9 a6 85 f6 8e 84 b0 e8 30 cb 3b 1e 07 d5 07 b0 d8 3a 53 9f 43 f3 f7 9e fe a9 c9 df 6f f8 b7 2d d7 f2 00 65 b6 06 fc 40 01 02 46 da 0b 5e 34 df 4a cc d6 30 49 b9 1e b8 80 0e 06 a6 4a 82 d3 1c a7 ae c1 e7 ca 4d 5c 71 8b 34 cd ea 33 04 cc b6 06 38 98 e1 01 0f 91 5d ae a7 92 40 7d 60 4b 5e ab 1d 85 b7 d4 4e 94 b0 65 4d 4e 57 51 c1 b6 0f 6c 95 56 29 b7 65 1d 14 f2 df 9e 28 ed 8e 7f b7 ab 19 4d 53 e7 b9 18 cc 97 87 da e7 48 92 d6 b3 3a 47 a5 28 c9 Data Ascii: L9gY-|a.5q!RlxH9zPFNuqmy5/gZf+q&dgl0;:SCo-e@F^4J0IJM\q438]@)`K^NeMNWQlV)e(MSH:G(
2021-09-27 18:34:12 UTC	1675	IN	Data Raw: 43 8a 58 b2 eb 91 e7 72 b3 70 10 c0 60 52 78 92 53 a7 46 70 20 ba d9 30 38 9f d5 56 13 ff 48 5e 40 3a 12 3e 20 64 d5 97 fd f3 f3 60 3c f3 3f 5c 93 da 91 9d d5 b5 eb b9 18 8d 88 25 32 7a d9 ae 61 1c 4c fa d8 15 d9 8e e4 a5 a6 57 94 8c 46 a4 83 49 38 77 bb 82 f9 30 04 55 b8 be 0e 2f 42 89 4f 64 17 36 32 5d bd 70 7a ee 4f 7a 3c 52 fd 70 32 f0 65 a5 28 bb bc 93 e9 ea 87 c3 40 c0 cb 02 95 3d 94 34 1f d9 d9 8f 4c 91 d0 d1 d2 e4 25 33 aa 4c c5 d0 a7 f4 8b be bc 22 93 1c 5d 51 88 a7 d7 fd 32 c9 49 c0 01 56 Data Ascii: CXrp`RxSFp 08VH^@:> d`<?\%2zaLWFI8w0U/BOd62]pzOz<Rp2e(@=4L%3L"]Q2IV
2021-09-27 18:34:12 UTC	1675	IN	Data Raw: b2 6f d9 1d 98 4c 41 8b b8 ec 95 8b 36 71 51 6a 04 4b 25 d4 bc 55 81 ac 3f c8 ce d8 5b 15 4c e7 a8 54 8a 86 b2 59 49 a6 43 f0 a1 0f f3 8b c5 68 b2 08 38 b1 a1 e9 48 af 7f 5b 15 f1 fc 1e dd 04 94 08 4b 5e ba 6c 55 d2 0f fc d9 1c bd 8a 13 be 40 82 ba f4 22 b2 55 15 5a 05 4d 6a d9 9b 2d ad 1a 40 5c 7f 01 fa a0 4e db 9a 97 ec 35 22 99 ba aa 7f bd 82 ab 92 4b b2 76 3d fd 49 10 fc 46 9b 99 ec 05 dc 76 25 32 70 96 bc 49 f5 8a 82 09 62 45 37 42 2f ed da 55 fc 12 4c ae 28 21 90 1c 39 b5 ab 68 e9 10 b2 5b e7 57 94 48 3a 84 ec 6a a8 5d 43 45 4d 68 db a5 af ea be a2 63 06 be 49 53 56 76 c3 d5 ae 64 3e bc f5 67 e7 97 b2 24 93 dd 28 c8 14 7d 1c cd 31 a1 0f a7 b7 92 f2 91 bc 4f 76 a4 e2 d2 1f 5e 80 ba 2c c2 a1 8f b2 b9 21 16 c8 8e 72 a5 e2 37 a8 36 4a 9d 24 ef 64 48 a4 Data Ascii: oLA6qQjK%U?[LTYICh8H[K^lU@"UZMj-@\N5"Kv=IFv%2pIbE7B/UL(!9h[WH:j]CEMhcISVvd>g$(}1Ov^,!r76 J$dH
2021-09-27 18:34:12 UTC	1676	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 2c 69 5a cf 8e 6d ea 36 fc 82 a5 75 cb c2 ea 24 cf 13 f0 a7 18 eb 42 7e 00 6e 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$;\|W'&ZhEM&M=bt,Ms&C6@H^Z1<1lJw]mCtIXX9&~<{]p$.f@&uXAX,>!0I,iZm6u$B~nK{6AC pTD#]i
2021-09-27 18:34:12 UTC	1678	IN	Data Raw: c3 66 e0 c8 37 77 d0 03 c9 b6 95 21 14 f7 12 f6 87 87 f8 17 f8 89 26 82 a9 1e ee 30 a0 22 dd 31 90 46 10 0d 18 d6 96 ca f6 36 69 8e 49 5a b5 e3 51 dd 26 96 8e c3 e9 db a8 2a 43 8a cd 6f 60 e2 fc 32 61 39 2e 09 5f 5a d3 e1 30 d6 73 f0 04 bb 3a 8e 03 9a 24 48 fd 00 69 40 05 4b 93 8d 2f b9 d0 e1 7e e1 45 30 5e c5 74 99 70 79 9f 12 7a 5e 58 b6 7e 83 f4 a2 df 77 75 90 0b 24 a0 d7 87 20 08 9f 5e bb b9 96 74 3c ff c4 eb 67 fa 19 2c 98 d4 45 2a 1a 21 d7 a6 97 ab a6 ed 40 b4 a0 a6 1c f9 3a e0 c4 cb 55 42 55 b3 c4 10 2d 4a d3 ea 27 f9 b6 2c f8 22 7f ff 7b 15 79 2b bf df b5 8a eb f8 4e 00 78 75 0d a0 17 0e 3a 40 ec 7c e6 9f 28 74 24 29 ab 2a 26 60 84 8a e6 f6 ae 81 1e d4 0f 20 64 4c 48 4f 5d 91 c0 8e 9c 12 11 2f c9 7d 52 6e c5 4d 8d 1b 00 9d d1 d4 07 00 6a 54 a5 1f Data Ascii: f7w!&0"1F6iIZQ&*Co`2a9._Z0s:$Hi@K/~E0^tpyz^X~wu$ ^t<g,E*!@:UBU-J','{y+Nxu:@|(t$)*&` dLHO]/}RnMjT
2021-09-27 18:34:12 UTC	1679	IN	Data Raw: ed c7 d3 1b 09 1e 15 ad 8b c2 78 b9 9a ad ef e2 45 fc 36 66 45 d6 9b 52 c5 fb 40 b2 b7 e9 68 f9 21 9c f7 57 be 8a df 24 2f ab c9 fb c9 f4 83 64 ab 6a 1b 25 db bb 78 18 f5 a3 bd 42 6b f4 78 58 dc 4e a7 cb 77 93 68 21 45 55 f5 1a 99 e4 e4 63 24 93 95 e2 9d 00 66 b7 b8 59 8f 00 c8 a8 de e5 14 5c b3 90 e0 4b f5 8c a9 b5 44 a4 80 36 c3 68 12 cb 88 a5 7a 5e f6 dc 6e 19 df 46 58 b0 74 f0 14 d7 7b ad e1 2d 63 b3 49 34 58 8a 55 4b f1 51 bc 20 d7 31 3e 21 24 e7 e5 70 30 88 66 cb f0 ed 58 3a 3b aa 0b d2 7e 3f 37 d3 a9 b4 12 95 0e ed f7 30 8b e6 23 ec 4a da 8e e2 2d bb 17 9c 4c a7 12 83 29 84 7a bf 83 d5 24 86 54 18 8f e3 9b 58 11 13 d5 73 38 95 af 61 bc 18 84 f3 21 cd d4 28 9e df 86 aa a3 a8 7a ae ab f2 35 8a 27 11 83 97 35 4e f6 44 41 3e aa 5b 31 95 23 e6 a3 87 e4 Data Ascii: xE6fER@h!W$/dj%xBkxXNwh!EUc$fY\KD6hz^nFXt{-cI4XUKQ 1>!$p0fX:;~?70#J-L)z$TXs8a!(z5'5NDA>[1#
2021-09-27 18:34:12 UTC	1680	IN	Data Raw: 1f df 2d 6f ef 6a 6e 34 cb ae ff b3 b8 f9 74 bf fc 74 5f b1 e6 49 56 33 b1 19 4c 7e 96 f5 cf 6b ce 90 07 14 7a 80 a5 a0 8f be 7d 4b c8 69 f6 f9 c3 a6 a8 fe 72 52 fe f7 db 2f 4b 21 c4 5f 4e ee 3e 97 9f 9a ff 94 9d 0f b7 cb d5 af 6f 8f 3e dc df 7f be 7b 7e 72 72 f7 e5 f3 e7 9b db fb e3 f7 b5 a0 8e 17 37 bf 9f 2c 1e d8 7f 52 7e ba fb e7 f2 f6 44 fa 3a ee bc 3d ea dc 97 b7 ef 97 f7 30 7e 36 ff 58 7e fa 9f b7 47 0d e1 6a 92 ce e2 63 79 77 07 3f de 2e ff f7 cb 6f b7 cb 77 cf e2 8a 60 e0 a7 f7 cf ee 3e dc fc 13 7e fc d3 fd cd e7 e3 bb 2f ab d5 6f 8b df 60 73 67 cb e5 bb 79 b9 a8 48 d5 2c 00 ef 63 ac 91 1a e6 b4 4a 0a 9b 67 ac 7d 04 e1 97 16 d9 2c b6 15 ec f7 62 0c 59 6d 9a 7d f8 1c 7c 7e 0c 74 ea f9 c1 da c0 0a 2b db 25 4d 19 a5 c9 ec 96 95 26 96 e1 77 64 b5 f1 Data Ascii: -ojn4tt_IV3L~kz}KirR/K!_N>o>{~rr7,R~D:=0~6X~Gjcyw?.ow`>~/o`sgyH,cJg},bYm}|~t+%M&wd
2021-09-27 18:34:12 UTC	1681	IN	Data Raw: a3 29 3c 60 8d 2b d7 93 b7 5d 0b 7a e8 b1 e7 34 d8 d9 cf 3d 4a c1 63 24 51 d1 5e 8c 74 c2 79 48 bf eb 63 37 e3 12 b5 1d cc e5 16 26 3e 14 eb 1c 7c 6c d5 8c fe f7 3c b6 aa ca cc 4a 49 2f 95 f1 2e 37 5e 50 fe c5 8a 1c da 3d 53 87 6d f8 85 e2 42 e3 e5 d6 8a c1 39 41 82 ca d9 f2 ee 1f 64 1e 5d 62 34 60 9c 74 b5 22 1b c5 f3 3f 4e 02 1e 74 d7 2a ed bd 70 d2 18 99 b1 e5 29 47 61 2c 03 91 03 45 5b 15 4a 41 98 06 fe 28 2b 40 b8 3f b4 38 f7 63 2d e6 bb f3 7d 7b 29 b1 ed bc 36 4a 89 1a 1c 8d b7 10 cf 72 6d bd 51 da f1 27 1a 3b 32 bf 24 6a 40 3a b7 5f 1c a9 17 65 44 a6 55 ae bd d0 46 68 61 95 e1 5d e0 8e 93 63 23 64 75 6a ed b4 32 b9 b7 42 e8 7c 67 19 8d 03 4c 87 ea 14 4e 4c 1e cc 2d 82 c3 53 ee a4 37 2e 1a 05 9d 38 c3 1f 4a 8c e7 a8 22 da d4 55 98 fc ae a5 14 49 47 Data Ascii:)<`+]z4=Jc$Q^tyHc7&>\|<J\/.7^P=SmB9Ad]b4`t"?Nt*p)Ga,E[JA(+@?8c-}{)6JrmQ';2$j@:_eDUFha]c# duj2B|gLNL-S7.8J"UIG
2021-09-27 18:34:12 UTC	1683	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 ca 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: lG"zy__1w|KRwe#^&4zYN^2XION*).|{ITm[`>Z,v.C:2k c,tBY8T's<O^6k3NV9Z;j,\md,(|:<q.3^/Unx
2021-09-27 18:34:12 UTC	1684	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 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 00 02 00 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 00 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 68 69 2f 6d 65 73 73 61 67 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? lRo)%

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1685	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 4d d4 95 09 0d c1 bc d5 e0 25 24 03 60 ee e0 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,"YLWdfCM%$`o'.24tW`k@o[XlP\+yKb5p8/lG+JUd&yB,^ *yYO=+s+?&2A=bpq8&D7stS,lol! L$sElLx
2021-09-27 18:34:12 UTC	1686	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 <x3N2Ie@Y5ro'%!htw"vNRD8m#0=cd(9;$?x\Mb,rf}SFoa!j-}QhX'BV:5$9-$bR(@pXNY47%mqa8sn|B{*ib gG2R0p.0#$@Q5
2021-09-27 18:34:12 UTC	1688	IN	Data Raw: ad 02 a1 fa 8b 09 90 fe a0 3f 1f 8e a6 f3 e9 38 39 06 55 aa 4d d6 1f 95 65 ff 69 b7 f7 7c 5e 9e 76 07 27 f3 a3 41 79 d2 5f 05 44 3d 9c 97 07 74 34 1a 9f ce fb e5 a4 37 1e 9c 91 c7 22 26 91 f2 d0 9e 95 dd 7e 39 5e 85 41 95 3c f2 30 ce c6 a3 d3 b3 69 42 9e b4 cb 90 07 31 2e 7f 9b 0d c6 65 42 1a aa f1 91 87 32 7d 79 56 ae 61 77 3a 59 90 80 3a 1d 8c c7 a3 f1 60 78 dc c8 ee 7c 32 7b 5a d1 08 7e 4a c4 98 08 9d 13 80 c3 72 fa 62 34 7e 0e 72 74 74 54 8e 2b 71 7c 31 38 1a 24 f4 26 52 da 2c a8 dc 01 a9 57 14 65 81 4c ba a7 25 89 0a 35 3a 92 85 f2 a2 e2 d9 fc ac 97 90 26 0d 0b 53 18 a3 d5 55 d4 e3 b1 c9 b2 b3 f1 e0 bc db 7b 39 ef 77 a7 dd f9 6c d2 3d 2e 09 75 4a 9e 3b 4d c0 4c aa b8 9d 36 2e 54 60 41 af 3f 19 1d 27 e6 91 a8 ad 11 8b a7 b3 b3 f9 f9 60 32 78 3a a8 85 Data Ascii: ?89UMei|^v'Ay_D=t47"&~9^A<0iB1.eB2}yVaw:Y:`x|2{Z~Jrb4~rttT+q|18$&R,WeL%5:&SU{9wl=.uJ;ML6 .T`A?"`2x:
2021-09-27 18:34:12 UTC	1689	IN	Data Raw: 1f 38 fe a9 df ab 35 cb 57 a2 ba db b5 5c d7 77 3d 5b e6 c4 0e 6c cb 73 4f ef 1e b3 5d 5a 3d 8b 27 75 16 7c 1d 39 34 3d db 75 fc c0 76 3c c3 23 7b 8b 47 64 89 a8 36 a8 31 72 74 2b f0 1c 1d 69 37 75 53 b7 7c 12 d7 7d 3c 8f b1 9a 75 ac 65 3b b1 d4 ba 4f a9 d8 f0 47 86 14 16 da 9b f1 a4 33 9a cc 6e a3 fe cd 1b b6 5d c7 2b 86 4c c6 da 95 10 8b 35 d7 ae 71 e3 9b b0 df ab ae ff dc dc 3d 1e 76 fa 6f 7e 2c 2f 94 3f cf 10 c7 76 cd 1e f9 93 58 cf 79 9a 95 01 34 66 e5 3f 1e 45 92 f3 24 97 d1 bc 31 ca b8 1b 63 72 d9 2c 2f bf 84 45 6e b0 8e 6e 50 7a b0 cf 9e 9f 5b 52 33 db 3e 9d 66 e7 af 17 ec 6f 5f 0a ae eb fa 5f 2f b2 2d 4b 9a 7f 30 ed 29 e5 5f 7f fa 72 f6 94 e7 db ec fd c5 45 56 6c b7 22 cd cf 17 65 6e ce 1f c5 e6 e2 f1 90 ca 0b 96 64 bf f2 f4 c2 0c ca ee fc 72 a6 Data Ascii: 85W\w=[lsO]Z='u|94=uv<#{Gd61rt+i7uS|}<ue;OG3n]+L5q=vo~,/?vXy4f?E$1cr,/EnnPz[R3>fo__/-K0)_rEVl"endr
2021-09-27 18:34:12 UTC	1690	IN	Data Raw: 6c 45 c2 30 58 68 35 3d 32 b9 4c b1 5b f2 54 ee 58 75 29 3e 5e 15 7d 3e 34 8a e9 59 76 10 60 c4 70 1c 20 33 9d 1a e6 69 55 8e 6c 59 2d 0c 31 14 9b 35 b4 48 e5 c2 93 fc 8a d8 1d fc 61 79 80 43 b2 e3 af d1 4f 7b ae 76 6c 23 9a 60 6b 8e 02 bb 00 76 51 59 60 f7 c0 b1 6c 9f 64 eb a8 1a 8e a1 a2 02 7d 90 bb 6d b9 36 86 2a 07 73 95 67 39 34 db c7 33 92 a8 8d 4c 39 7c f9 36 08 06 a2 4b b7 5d 52 82 d7 3b 09 9e 88 17 29 3f ac 72 f3 3d 62 96 a8 98 b0 cd 77 7d bb 15 9b 1a 03 8a ef 1b 38 3f 0c 44 92 03 64 5a 36 f5 0c 26 57 96 36 05 50 cd dc 2f 80 99 69 fc 50 84 9b 17 18 29 ab 5d d4 e9 f0 e2 93 21 ec 11 3a 36 2d 2a 0c 69 9e f2 32 82 9d ff 37 a3 d6 2b b3 54 23 d3 15 69 7d 7d 54 fa 9d d3 51 9e 8a 02 49 81 6c 17 79 35 25 39 a6 e5 36 3a dd 81 b8 03 f0 99 be 87 d9 1a 60 e5 Data Ascii: lE0Xh5=2L[TXu)>^}>4Yv`p 3iUlY-15HayCO{vl#`kvQY`ld}m6*sg943L9|6K]R;)?r=bw}8?DdZ6&W6P/iP)]!:6-*i27+T#i}}TQlly5%96:`
2021-09-27 18:34:12 UTC	1692	IN	Data Raw: 88 fd 37 30 6d e1 a7 0f 69 f5 5b 54 52 65 6b 60 e2 46 bf bb 12 6a 1c 79 50 4a a2 f9 85 67 d5 f1 50 9c c8 73 de 52 a1 4b 7e 94 07 0f 19 7f 40 39 65 e2 6b be e3 a9 76 3f ec bf 93 e7 9b a9 f8 e7 bf 96 f2 14 94 61 4a db c7 f5 d9 54 bf 33 7e c7 2a 69 2f 5f 9c 78 ba ef 5b 3e 54 ac 3c a1 52 ab 65 a2 eb 92 38 2b 2a 8a 4e 78 cb b9 0b f8 3c 93 b0 5b a5 e6 2e ec 45 9d d9 68 30 9d 84 a3 59 a7 d7 8b 26 d1 a0 df b9 9d 75 07 77 77 61 7f 32 3e 7d aa ea 05 18 f5 33 ed 45 83 d9 df a7 9d db 68 f2 e9 d4 83 0a bd 88 87 6e a7 df 0d 6f 67 1f a6 93 c9 a0 4f 63 a0 ef 98 a8 87 41 7f 82 05 20 8a 70 2c d7 74 ea 44 35 88 11 27 bd a8 37 eb 0f 26 b3 c9 88 2c 43 25 24 89 fd 65 18 f6 3e 74 ba 37 b3 f0 ae 13 dd ce 2e a3 f0 b6 77 ea 48 75 10 df ee e8 72 30 ba 9b f5 c2 71 77 14 0d 95 cb 52 Data Ascii: 70mi[TRek`FjyPJgPsRK~@9ekv?aJT3~*i/_x[>T<Re8+*Nx<[.Eh0Y&uwwa2>}3EhnogOcA p,tD5'7&,C%$e>t 7.wHur0qwR
2021-09-27 18:34:12 UTC	1693	IN	Data Raw: 81 e3 05 be e9 99 96 ef 39 81 a9 1f 3f 1d 6e 35 92 7e 7b d6 75 6a 4c a7 09 59 6a 4b f6 61 ee 6e eb 1f 0f a9 b6 a2 e9 4b b2 d4 9e 68 9a d2 d5 36 d1 52 ba 78 ca a7 53 92 69 8f 5c ac 96 9e 5b 5b 52 f1 cf d5 af 62 6d ac ea fa 9e 6b bb ba 65 04 ba e7 1c 2f 1d 95 db 66 b1 39 4d e7 74 46 eb 45 69 50 72 05 b6 e9 db d8 a5 0b 59 df 30 5d cf 32 8e 35 dc 27 33 ca 57 d7 e6 79 fa 42 56 a4 ca cb 92 9b b1 20 5c 8b 63 9a 86 ad bb be 65 19 d0 a5 5b 8e a4 65 98 2c 69 51 d1 94 66 da 92 ac 1f ca 5c ec 68 c6 15 95 e7 da 67 6e 57 f1 c4 9d b2 3c d5 d6 05 7f 66 2a 7c f0 44 b4 fa 0f e4 a9 20 e7 62 61 47 0f 74 ac 6c 7b 86 ee 9b 7e e0 f8 c7 0b 77 77 36 73 09 d7 72 5d df f5 6c e6 36 3b b0 2d cf 3d 96 18 71 7f 2d b9 3d 29 ad a8 10 f5 75 38 db f4 6c d7 f1 03 db f1 0c 4f 4a 8b 6b 92 2d Data Ascii: 9?n5~{ujLYjKanKh6RxSi\[[Rbmke/f9MtFEiPrY0]25'3WyBV \ce[e,iQf\hgnW<f*|D baGtl{~ww6sr]l6;-=q-=)u8lOJk-
2021-09-27 18:34:12 UTC	1694	IN	Data Raw: ab e5 b9 16 2a 7c 78 64 d5 6e d7 c0 6d 7c 37 cf 17 64 f6 44 4e b5 c7 1c db 22 9a a0 8f 47 58 8d 6e c8 78 e7 b6 76 eb cc cd 34 f1 77 80 aa 26 ef 59 b2 81 2e 69 b5 d3 7d 56 51 e1 81 60 89 2d 35 66 9e 1d 86 a0 6a 06 98 12 95 73 14 b3 a6 42 8a 19 15 dc 1b 65 cf 79 be 8d 49 cc 02 cf 00 7c a2 c7 a3 54 2d 89 7a 47 ac 0b 24 aa 64 13 b3 92 0d ea 0f a0 b1 18 6e e8 a6 63 01 83 8f 75 dc 15 f9 a2 20 ab c7 64 4a 78 36 b0 df b8 b0 89 1e 86 f1 c6 f6 7c b4 31 d7 36 7c 19 27 b6 c2 79 d5 71 58 12 6d d9 e4 23 c6 3b 16 eb 8a 20 38 1b a2 1a 7a 04 ca 14 4f 79 a6 81 06 22 11 36 14 54 e3 14 bd ab 49 0f 44 22 29 85 a7 2b 69 4a 5a e6 db 4c 8c 47 b6 83 d6 e6 63 20 35 eb 41 d1 f1 15 0d b4 d5 6a 8d 01 67 c9 c6 36 f1 05 aa f9 ee bb 13 19 a3 8e 68 32 81 69 39 68 76 4e a0 2b 96 d4 de e7 Data Ascii: *|xdnm|7dDN"GXnxv4w&Y.i}VQ`-5fjsBeyI|T-zG$dncu dJx6|16|'yqXm#; 8zOy"6TID")+iJZLGc 5Ajg6h2i9hvN+
2021-09-27 18:34:12 UTC	1695	IN	Data Raw: 45 4c 31 5d fa ba 65 b8 26 7a 0b 86 6d 4f ee f3 7f 8e a6 35 61 15 a5 32 dd b3 17 66 78 1b 71 5b 72 ea a6 fd b4 4e cf 35 f3 d4 d6 ae ae b7 3b fd 0e fb f4 b3 30 db 73 3d d3 36 41 51 c0 bd 2c 40 b1 34 e5 d4 03 9f aa 0d ef a6 b8 3d a7 3a c8 cc 5a 3d 2b 1e 36 47 19 58 c7 34 c1 64 4d 89 59 a8 e3 2b 26 5d f1 89 08 65 3e 23 27 e0 29 35 91 d6 03 5f 79 03 a9 3e e5 f6 d1 72 82 20 70 6b 9e 63 db 9e 21 83 41 87 6f e2 81 ff 58 08 25 5c da aa a1 de f7 41 b4 5c dd c3 44 28 61 c1 48 60 cf d1 a1 a3 7c e8 ce 7f 6c 8e 46 b1 37 88 bf fc 8b 1b b2 62 7b 7f 5d 47 06 e5 b6 18 46 fb 96 0b 7e 16 d8 81 d4 19 0f 98 a3 0f 92 0b 1a 6d 1b e0 52 8c c6 d9 7f bc ca 36 8c 1e f2 0f 4b 5a 02 b9 f9 63 8b b7 65 f7 fd 89 c8 07 db 35 6c df 36 d0 d6 d1 db 3d 64 d7 b1 2d bf 1d 8c 7f 8c 2d f8 86 13 Data Ascii: EL1]e&zmO5a2fxq[rN5;0s=6AQ,@4=:Z=+6GX4dMY+&]e>#')5_y>r pkc!AoX%\A\D(aH`|F7b{]GF~mR6KZce 5l6=d--

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1697	IN	Data Raw: a3 9b 68 22 15 86 e2 3d f5 03 61 3e 16 62 64 11 84 e1 32 bc 63 28 26 ed 40 f1 92 c1 4e 0b 28 aa e4 2e c5 e5 44 f3 fc 5d 38 1e 4a 02 aa 97 85 77 02 37 a1 0c 5f 8a b7 a9 9b e7 87 51 24 b5 67 d5 f9 5f f3 fc b8 a7 da 82 ea fc bd 91 b8 ef df 8c 6f 25 09 d5 7f f3 79 7d fd 1f 50 4b 07 08 5d 1c 7c 4f 11 10 00 00 16 36 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 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 69 64 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 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 00 19 00 00 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 bd 5a db 72 db c8 11 fd 15 44 f1 c3 ee 16 4d e1 7e 71 d6 71 41 24 28 c1 e2 6d 49 50 2a a7 5c c5 1a 8a Data Ascii: h"=a>bd2c(&@N(.D]8Jw7_Q$g_o%y}PK]\|O6PK*Q_locales/id/PKPK)Q_locales/id/messages.jsonZrDM~ qqA$(mIP*\
2021-09-27 18:34:12 UTC	1698	IN	Data Raw: 59 dc 2a d2 76 93 3c 80 b1 d8 43 9c 14 03 53 c6 cb 2a 96 d6 c9 36 8f 4b de 62 5c 6a 2c a3 35 df 56 7e 99 86 0b d0 78 04 57 9b 90 eb 87 1d 04 4b e1 9c 8f dd e1 11 79 5c aa 96 82 20 77 11 08 52 ca e3 2c 5f c3 49 1a ee b3 ca 9f 04 94 48 db d2 a0 cc 13 2e 7a f0 c7 87 3c 2e 6e 97 e3 b9 de 29 a7 16 a5 3c a1 d8 06 b4 cb 27 bd 85 ba 62 18 c2 47 44 85 86 e1 46 f7 51 96 ef db 92 7f 98 cd 6e 1f 2d d8 52 34 ab 7a 31 2d 69 c1 cb 2f 0d b9 ac 91 50 4b 20 eb 34 ca f8 dc f2 fa af 19 4f 04 fc 40 d5 3f b2 56 1d 0e 08 b2 25 44 0d b6 20 4c 73 44 63 1d 2e a2 c7 e2 1e 9e fa 85 3f 7d cd b6 51 5b ea 96 68 b1 ad ea 82 0f d8 3e 2f b9 55 ab 88 f8 5b 98 e5 8f 39 44 20 5b 7d 65 b5 56 58 62 e6 59 61 5b 07 a6 b6 7d 5e 4a a1 1a 8f 43 f6 1c 90 0d c3 30 fc 5f ac 66 b7 4f 96 18 50 79 ae 42 Data Ascii: Y*v<CS*6Kb\j,5V~xWKy\ wR,_IH.z<.n)<'bGDFQn-R4z1-i/PK 4O@?V%D LsDc.?}Q[h>/U[9D]eVXbYa[} ^JC0_fOPyB
2021-09-27 18:34:12 UTC	1699	IN	Data Raw: f2 b0 8a 3f c4 b2 2d 6b 8a a9 02 0b a1 fb 2d ca 24 7f 98 9b 91 c1 0b 34 e4 d2 4f e0 2a b6 41 a2 4a 6a 4b 97 2e af fe 2d 7d 41 63 68 f0 ab 9f ab 87 a2 2d 51 d1 ae a3 78 a1 0c 00 1e 44 4b f6 b1 c7 41 cd 7b c5 f3 5f 1e 6f f3 2c e4 8a 54 81 2f 55 85 c0 50 29 05 e5 48 88 3a 98 68 10 38 51 81 b3 0a f5 22 3b 36 e5 df fa 18 c6 e5 e4 5e 5a 01 e4 1c c7 31 0b b2 43 17 af 08 aa 04 09 86 b6 96 65 6f cb ff 4a 3b ad 00 18 db 06 c1 9a b2 05 c5 4c 4a a5 5b 82 c2 f3 d9 cf 73 23 ff 83 a1 5c 30 d9 1f 87 e5 d0 43 1a 07 21 5b 33 c1 ca 8e ee d0 d3 c7 83 20 b0 a1 54 a0 76 74 05 fc ca b9 5b 17 a6 6a d9 9f af 19 ba 45 41 de 16 e9 5a 7a 83 0c 41 9f ac 2b 00 76 a0 bb 85 7d 26 8f 66 51 f5 64 10 86 ad 18 8e 86 e6 cb 86 e6 32 55 7a 8a 5c 6f e4 f3 ab 14 1b 51 75 50 58 a6 a2 18 b2 cc 93 Data Ascii: ?-k-$4O*AJjK.-}Ach-QxDKA{_o,T/UP)H:h8Q";6^Z1CeoJ;LJ[s#\0C![3 Tvt[jEAZzA+v}&fQd2Uz\oQuPX
2021-09-27 18:34:12 UTC	1700	IN	Data Raw: e0 9b b7 7a fc d4 f3 08 3d 8b ce e5 ea f1 b3 a1 68 09 a2 d3 e6 da e2 66 d4 9f 0d 88 85 e8 2b e5 a7 a7 ff 00 50 4b 07 08 db d0 86 a4 8f 0e 00 00 6b 2e 00 00 50 4b 03 04 14 00 08 08 08 00 2a 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 69 74 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 00 00 00 00 00 00 50 4b 03 04 14 00 08 08 08 00 29 8c 04 51 00 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 69 74 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e bd 5a 69 6f db 48 12 fd 2b 5c 6f 80 39 e0 d8 bc 8f 60 66 07 8c 44 d9 9c c8 92 47 87 83 2c 02 08 6d 89 96 1b 43 91 1a 1e ce 4e 02 ff f7 7d d5 24 6d 45 dd f4 ec 2c 76 e7 8b 2d 5b 5d d5 dd d5 55 ef bd 6a f2 cb 89 a1 1b 7e e0 db 8e 6b d8 be ef 98 ba 63 78 27 6f b4 2f Data Ascii: z=hf+PKk.PK*Q_locales/it/PKPK)Q_locales/it/messages.jsonZioH+\o9`fDG,mCN}$mE,v-[]Uj~kcx'o/
2021-09-27 18:34:12 UTC	1702	IN	Data Raw: 67 c3 d9 36 03 1f c2 86 6b 6b 96 21 63 e9 df 80 f5 3a e3 6b d6 64 2b 96 56 b0 2c cb 11 fd 07 ce 9a 53 68 a1 94 81 60 7f 43 9e 97 9c 95 f4 7f 52 21 ad 95 58 c9 9a 14 11 79 e4 d9 3a ad 05 11 97 f9 be 80 b6 f8 a5 c6 f2 9e b3 0d 92 25 81 51 5d f1 94 7f fe cc f0 0d b6 ae 41 c6 a0 48 01 6b 8c 18 9c 2a e8 36 4d 76 1c 3b d8 71 92 5a 05 fd 1f c1 bb ab 33 31 e9 99 16 6b 1b 5a 21 8c cb 5c ec a6 5d f3 29 2d 7a 97 6f 72 2d 29 f7 29 70 12 33 60 76 50 59 8d 8f a7 58 15 f6 57 01 14 52 32 2f 13 00 07 c6 a6 a4 88 ca aa a0 5f c5 ae 89 2c c3 32 f8 03 5b ff 8e c9 c8 37 8d fb ed 68 33 6c bd 16 e9 4a 31 68 55 04 2a a3 64 4f fb 2b d2 76 83 e9 d3 4e 5a f1 97 88 6d 62 0a fa b5 c9 c9 4b 8e f5 14 0f 10 9b 4d 41 da d0 b6 16 08 02 d5 0c 7c 46 aa 59 b2 54 aa 73 04 29 e5 3b 9e b1 46 fb Data Ascii: g6kk!c:kd+V,Sh`CR!Xy:%Q]AHk*6Mv;qZ31kZ!\])-zor-))p3`vPYXWR2/_,2[7h3lJ1hU*dO+vNZmbKMA|FYTs);F
2021-09-27 18:34:12 UTC	1703	IN	Data Raw: d4 2d 20 ad a7 7b 1e b5 c2 f8 20 61 d4 90 97 6d 66 09 be 6a cc 3c 52 1c 8e 81 d3 42 ef 01 98 96 5b 79 48 ba ac de 51 06 d1 45 07 2b aa 64 cd 51 85 88 3b a1 26 9a 58 ed b9 ca 90 33 da 8e 04 5e 26 c4 59 25 ee 62 d3 6f 3a 81 dd 4c 09 a1 ef eb 96 e1 9a 00 53 74 2b 9e cc 4d 3d 1a 80 98 9f 37 cc 8f b5 50 57 9d 68 df b2 0d da be 64 b7 07 01 9b a7 b6 76 71 f9 19 b6 0e fd fe ae 9d 0e 9d 94 69 9b a0 43 d0 ba 05 90 91 44 ee 98 ce 1d 6d f4 e1 05 72 c3 ec 5f 93 bd f0 47 39 4a ba d9 80 63 d3 84 9e 31 25 6a 9b 71 29 ce e8 74 88 06 c1 88 42 37 e9 81 af e6 f7 ee 4e e9 c0 12 18 19 04 81 2b e8 d4 b6 3d 43 ae 28 1c 2c e5 14 cf ea d6 c4 12 c8 e4 fb a0 6e 57 f7 20 ee a5 6a 1a b6 f0 21 3a fc a7 59 9f ef 11 fe 5a 22 50 2c f8 af 63 02 48 2e 8b f0 ca b7 5c d0 7c 60 07 12 3c 7f 25 Data Ascii: - { amfj<RB[yHQE+dQ;&X3^&Y%bo:LSt+M=7PWhdvqiCDmr_G9Jc1%jq)tB7N+=C(,nW j!:YZ"P,cH.|`<%
2021-09-27 18:34:12 UTC	1704	IN	Data Raw: 32 7f af 28 1f c5 eb 58 07 2e 2e c3 c9 05 a4 cb 2a 9e 84 28 9b 1b 69 05 aa bb 5c a5 f9 0d aa 4d 96 4e 8a b7 28 14 d6 6d 07 20 b7 8a f2 23 32 85 f5 22 5e 8c a3 95 54 18 8a 57 0d 0f 8c 9b b6 10 2d 4b 2b 18 06 e1 35 a1 98 b4 03 c5 c3 db 27 2f 90 a8 52 b8 14 37 e6 dd f8 eb 70 39 97 0c 54 6f b2 3d 19 8c 43 19 be 14 ef f1 75 e3 e7 51 24 d1 b3 ea 0a ae 1b bf 9c a8 b6 a0 ba 8b ee 2c 6e a6 e3 e5 95 64 a1 7a 17 fb f1 f1 df 50 4b 07 08 35 c9 27 78 2c 0f 00 00 5d 2f 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 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 69 77 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 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 00 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 69 Data Ascii: 2(X..*(i\MN(m #2"^TW-K+5'/R7p9To=CuQ$,ndzPK5'x,]/PK*Q_locales/iw/PKPK)Q_locales/i
2021-09-27 18:34:12 UTC	1706	IN	Data Raw: ec 9e a2 a1 4f cd d5 3c 24 44 ec 4b f5 39 af c9 4b 80 9a 10 2a e0 d3 02 fb 36 26 3a 72 ce c2 d4 2b 15 44 3f c1 41 75 da 4a 5b 1a 27 ad 68 85 9e ac d0 46 49 ad 04 53 f0 5c 40 be 4c 4a 10 91 7e b2 8b 7c 6e 4d 02 95 0c 24 6b e0 39 81 7d b2 56 6e b3 5e ac 0c c7 b9 62 80 03 2d c0 db 14 f6 0d 10 6e 12 31 11 ec 03 38 d8 36 d6 fd 03 ba 0b 81 2b 0f 1f 69 e4 1c 0e 49 fd f8 b2 e1 a2 54 3c e7 cc 8a 32 fa 0b 0a 99 36 fe ec 62 c7 3c a0 e9 c5 11 81 dd 0e 25 71 17 54 e6 ad 1a 2b ee c6 6f 40 d6 88 41 c0 79 e0 fb 94 2f d4 7f df c5 77 89 95 7f ae e1 89 2e 20 a1 5d 5c 03 6c 91 8d a3 f8 11 46 11 5c 4f 79 cb bc 48 84 22 8e 57 36 ba 22 ee 39 15 14 66 b3 89 21 38 af 61 d7 2b b0 2c 38 c7 f1 95 33 b9 5b 2f 43 6e 09 14 a6 31 87 b5 ab a7 a1 8d 63 6e 3d 87 77 3b 83 eb 50 7c dd f1 83 Data Ascii: O<$DK9K*6&:r+D?AuJ['hFIS\@LJ~\|nM$k9}Vn^b-n186+iIT<26b<%qT+o@Ay/w.]\lF\OyH"W6"9f!8a+,83[/Cn1cn=w;P|
2021-09-27 18:34:12 UTC	1707	IN	Data Raw: c6 4d f2 5a 13 8d 01 35 68 fc ae fe 3d c5 02 60 b4 82 5c de 33 5a 02 09 7c 4d db c5 2b c3 13 c8 64 e5 8c 0d 00 48 53 0e 85 24 32 c8 1d 3f 05 65 62 13 f9 6b 0a aa 9c c4 12 4a 43 d1 0a 5e aa 23 67 be b8 37 73 e9 c5 81 af 08 f3 de 96 9f 23 7b bc fc de e7 ec a1 d4 df ef 98 3d d1 46 5b c0 10 09 87 fc 0a 51 1c d2 ec 56 bf f7 a2 1a 8e 27 b5 e9 bb ad 4c b8 82 e4 60 a1 6c 13 46 4b 46 18 c3 66 c2 44 7b 20 41 71 d4 3b d8 ac 9f 68 01 b6 a4 52 5a 40 30 e0 77 c6 b2 4d 23 5e 09 b2 f8 06 5f ef b5 82 3f 06 87 5c fe Data Ascii: MZ5h=`\3Z|M+dHS$2?ebkJC^#g7s#{=F[QV'L`IFKFfD{ Aq;hRZ@0wM#^_?\
2021-09-27 18:34:12 UTC	1707	IN	Data Raw: 38 5e a4 11 7b e1 ba f1 f8 82 73 ee f6 96 54 f2 7c 16 1a c4 15 31 79 5c 47 78 ab c3 63 1c af 1d 49 1c 05 44 72 b0 1f 3c bc 4c 1c 3e 82 a8 a0 c2 16 b9 5b 88 52 a1 df d2 76 6d ea 36 2e 91 a8 ca 03 a9 c4 3b 50 09 9b 96 5e 23 57 62 5b 0c 5a ac 9e 2d fa 43 92 98 13 af e2 b6 c1 93 b6 f4 0c e3 e7 06 ce 60 5d a8 b5 36 4d 98 e0 65 13 11 70 98 82 bc fd cc 86 88 37 ba 50 0f f1 a5 1c 82 0e 04 6f 06 f0 15 7c 95 41 48 d8 8a f9 bd 21 d0 98 12 0a 94 6f 70 cb df ab 74 d7 c6 46 f7 50 4d fe ba 61 cf 24 65 ff a7 2c 9d b8 62 f4 41 f6 1a 5e 0b 6a cf cd 0e f7 cd 40 6d 55 a0 6e 87 6c 7f 4d 01 1b aa e7 99 f5 6b 93 02 c0 90 24 40 be 94 a5 69 79 f2 0f 5f 36 00 29 af 1f eb cc 27 2d 4b 67 cd c1 12 15 57 00 1c a9 19 07 b2 63 e9 35 26 71 68 08 c7 74 8a 70 94 c3 31 31 5f bf f5 a9 b5 bf Data Ascii: 8^{sT|1y\GxcIDr<L>[Rvm6.;P^#Wb[Z-C`]6Mep7Po|AH!optFPMa$e,bA^j@mUnlMk$@iy_6)'-KgWc5&qhtp11_

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1708	IN	Data Raw: 86 22 54 d1 88 24 79 a2 e5 44 91 18 74 42 f8 15 be f1 49 ad 1c be 0d 43 7c f8 f6 13 b5 72 94 95 01 96 90 9b 1a 2c a4 08 44 96 53 af b9 c5 96 57 ae 16 c4 52 a2 24 88 12 a0 f2 03 35 1a 11 25 30 9e 82 a7 86 d1 90 2a 54 29 1a 15 1e 7a 33 3d 98 0d 47 b3 ac 04 36 a1 39 86 93 d2 51 42 a5 7d 0f 4f b3 10 08 13 ff 67 22 4a a4 9f 75 26 53 c8 55 25 e0 cb 88 a8 1b ce 60 46 49 41 aa 08 8d 9a 7a 19 30 4a 01 80 eb 2f 10 7d c0 4f 63 c9 8b 7a d7 94 22 57 e7 af 0d 71 95 98 41 8b d3 e9 8f b2 ec b7 30 99 51 ff 4f 25 4e 84 0a ce c4 fb b7 1b 08 8c 60 af 42 41 c2 61 b8 38 89 5f b2 d1 db 10 10 10 5d d6 38 89 48 86 a0 06 69 37 10 21 32 04 35 40 13 a7 50 43 93 30 ed 86 ff d4 63 03 8d 09 e0 cd d0 64 a9 b1 a0 38 91 e9 e0 ac 33 e9 1e 52 46 46 8d 03 50 84 de 0d a7 50 a1 0f c6 67 84 fb Data Ascii: "T$yDtBIC|r,DSWR$5%0*T)z3=G69QB}Og"Ju&SU%`FIAz0J/}Ocz"WqA0QO%N`BAa8_]8Hi7!25@P C0cd83RFFPPg
2021-09-27 18:34:12 UTC	1710	IN	Data Raw: f2 9a 48 a9 98 42 43 68 ca 5a f2 2e 01 ca 90 a4 a1 56 c1 6a 62 21 4b 4b c5 18 ac 4f ea da e7 73 50 64 3e ca 41 93 8b f9 cf 9f 3e dc 5e 15 1f 7e be ac eb eb ea e6 19 1d fc 4a 3e 7b e3 d5 11 83 a4 cb 06 21 6f ae cd 97 5f e9 e7 cf d3 d9 c9 70 92 ff 91 cd be 0c ba 78 6f 32 71 5c 2c ef a4 c5 0e d2 22 34 38 db 80 0e dc 1f 65 f1 e0 0d 2e 6f de 55 57 f7 db e3 9f 5f bb c7 97 a0 7f 21 a0 36 10 0a fe c7 20 4d 2b 82 d4 db 2e b3 0f 1e 0f c6 17 e3 b0 10 3c 97 50 28 d3 16 cc 66 b9 e2 0c 31 3c 6c ed 57 86 c0 33 a2 ab dd a5 ed 80 47 00 24 01 9c b8 ec ad 98 95 ce 5d f4 16 48 48 b1 86 bf cd ba 6a 9c c6 40 45 27 44 73 ae 61 6b c6 39 67 d8 de 3b f5 88 19 4a 04 05 20 a0 2d 94 70 aa a1 16 22 f5 8c 9a 8d 43 03 0d 18 e1 e0 dd 46 29 a6 8c a0 04 6a 82 a5 c8 1a e0 d9 db a5 e0 1d a0 Data Ascii: HBChZ.Vjb!KKOsPd>A>^~J>{!o_pxo2q\,"48e.oUW_!6 M+.<P(f1<lW3G$]HHj@E'Dsak9g;J -p"CF)j
2021-09-27 18:34:12 UTC	1711	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]MqCH\nTK@V3W??IWs*' )DP^ir\bB;*4|.KR,p/TmJ,*Hcgp::= V(%P ATxZdrv:hTN [Pb,z`%xq
2021-09-27 18:34:12 UTC	1712	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 73 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]DCNgprqaOggq6sT,ll8f4lzvHol,KTM,^gRgl6wWs#*qcH%'t89w|KO@^"'YRyl:%IMJcZ,;x
2021-09-27 18:34:12 UTC	1713	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 47 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: g9GIn}i9dxs\z%{Yt+V$Z:sn70qV)iD-P^TTDJf*'?,rZKtJ*yF&H)~8 1IM]%(|L[&<wi<V#/@93X'#]+tpV+[Ghr|:~azqGt Z+Xe
2021-09-27 18:34:12 UTC	1715	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 af 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:_QkVHlU8D6WOwp}N2Sx?HxO>+f#d^'>eHPC*=4wL")jxE6yyTH_y $|3?#nl4.oW9R~RkS7]`BY9>{J
2021-09-27 18:34:12 UTC	1716	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 0e 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 a8 ff 42 79 e5 c3 54 67 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?<>5F|y!1$D tW%3s`3%JI86L/#Xn[V0."j#N'gLCU;iSt&7ByTg,0ly|x'kFliFl%XWz;,v
2021-09-27 18:34:12 UTC	1717	IN	Data Raw: d2 ef 93 08 c6 54 03 f2 04 c6 bd 2e 40 85 f3 f3 ee 59 97 e1 09 77 5f 0e 47 ab d3 1d 9e b4 07 9d 4a 52 a7 dd c1 45 9b 33 45 ee 46 52 8e d6 69 b7 57 d6 ee 65 02 96 dd 63 82 0f d7 f1 e7 08 d5 34 32 41 9e a9 9b 72 24 7a 6d 0a bf e8 53 e5 b8 95 fd 97 d4 c5 d3 87 04 71 2b 07 65 e5 60 99 73 73 37 27 71 04 32 cb b9 27 58 e5 96 d7 a6 46 7c 29 93 a0 64 09 70 f1 81 9b d1 cc 12 18 8e c1 52 a9 37 e4 aa 15 1c 8d 1a 0f 3d 1f 9f 4d fa 83 49 59 01 1b aa 8e f4 8e df 2c a1 4a bf fb af 4a 0a 84 99 87 03 67 89 9c 96 ed d1 18 62 55 05 f8 4a c6 eb d2 5b a3 b2 a4 20 54 50 a5 e6 9e b7 95 a5 00 c0 f5 6f e0 7d c0 4e 73 c1 8b 7b d0 1c 47 2e c6 af 2d 7e 95 b9 e3 21 4f e7 74 50 96 ff a0 c1 8c 7b 00 77 9e 08 e7 9c 99 47 f0 6d 21 30 00 59 d1 83 d0 5b 29 f2 24 fe 56 0e 5e 52 40 c0 d4 fb Data Ascii: T.@Yw_GJRE3EFRiWec42Ar$zmSq+e`ss7'q2'XF\)dpR7=MIY,JJgbUJ[TPo}Ns{G.-~!OtP{wGm!0Y[)$V^R@
2021-09-27 18:34:12 UTC	1718	IN	Data Raw: 7f cd 17 a2 f1 05 b1 56 d2 17 5d 0f fc 0f 0d a5 1d 97 cc 69 66 ad 50 4e 70 4e 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: V]ifPNpNUqm8DvT+,"BT <PKm2p?g9;_R!gl~6NW7zZObGK__*+p;Kg@MOqD0r0X]2o<ZBZMljWBgm1f4xRi

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1720	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=XRoaL3\thBug]6/d5?C:- ,6k@sFO{>+h'>*=;3e?|=QU`(4I8B3g\8>t+FZ(mYe"~(H7aMC &s0n"Dj`LC
2021-09-27 18:34:12 UTC	1721	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 e4 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:]/V$(WKi>jr:IM^U}*Y/rr)W+(1Mui%Op9\HHf]\(<ggIy$zGBx_Md.%fWyShYM_NgYOd&Gb6[D<+Y[OQf/PmtV ,_n9$s+xl
2021-09-27 18:34:12 UTC	1722	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: Ry\6bowm6iQrZ164}oVX??(-(5GOOmSud})T|wzZm^T'K|szs)x>*R,9dUIY"oMtVXlQbNn*9gz{!G2}Sfw^6~Lq3
2021-09-27 18:34:12 UTC	1724	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:s61Tj4E\NS*i.pYYL<_PYaO&[n"E}/vm?pm"m'ytimCLPR0;N!98h<%zB|ACYzDlikDs ~fH%p,
2021-09-27 18:34:12 UTC	1725	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 a1 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:S0H&lOJTf`2m$Yx~9j"H`t=EQ<TnK1 !{PPvV1 ~Hrs
2021-09-27 18:34:12 UTC	1726	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 9d 78 86 e7 db 9e ac fa a5 d2 8f b9 ec 52 c7 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='.{32KoX7oB(xc9}DqeqdFwXg0d=p\SDxHVq.6"g:piK89g\KqJ--|CyU1]pC`O\xRtq-fHLL(JbrllW w+Kr+]Q1
2021-09-27 18:34:12 UTC	1727	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 7d 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 87 79 d4 a8 86 42 db 93 db 52 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 f6 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: nV\Vm^Zxb*3kmGn@O0DL*oM7{>fGZ#9Lf3\\|K5,mL%mIJ1pom,Cp,rXY|/"a}F&XlHVD-<<|^?4Y6yBRg<vXJbD~ y/x<N{6&y"8NZ
2021-09-27 18:34:12 UTC	1729	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 64 59 ae 2e d7 83 f1 91 03 29 ce 52 3d b3 ea 02 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 2c 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@l*M|O*Z~|w*^dY.)R=zTUeLymldU38Vy,=bqKb<Rfr6Q"(t km"Q74yY:;Z
2021-09-27 18:34:12 UTC	1730	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 00 51 36 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 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 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 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~8C01FI+PJR1DP|)^dU;j]ZaKPKl9Q6PK*Q_locales/ml/PKPK)Q_locales/ml/messages.json][o;+ZOKv(V<8

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1731	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$X8g0Nq&tHwU1#:C/M1^`>0vd\$dj7`}nrNd@]A{K$GY"OT `_eE +LE&%pl[NI.?T{/1@WUK YWLFP
2021-09-27 18:34:12 UTC	1732	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 8c 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 af 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)Bkym4cee2kAd{)%SUN+'x3?'O.TH`5'pDbJ7$BCt\()UuL3-8<(kRns
2021-09-27 18:34:12 UTC	1734	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{SxEu])]1rCyeI'>WObsODu/N>)b2?g8tES)`8^m?^R gB?:(x!)0`0bZiUvxMiP7I<\'pXVQWM"A 1=OiUyj/2
2021-09-27 18:34:12 UTC	1735	IN	Data Raw: 59 fd 55 f6 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 0e 91 e8 7f 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/lXI_u%n%j50f5yJ^cpdc%"Q#:o'%VtX4cD.=JX,U^V8B*b;~QZB(pF1e9s%C
2021-09-27 18:34:12 UTC	1736	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 c8 c4 bf 42 96 4c e5 0d 55 2c 1b cb 99 1e f6 e5 51 c6 74 51 1e 03 9f e0 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 41 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 f6 0b e5 bc 9a 0b 69 68 8e f3 84 28 ad da ac 5d d8 69 53 Data Ascii: 6H E uWlU#Agu@wJd1i3RD=v]r5bBLU,QtQPEtA6Qh,:{'x-e[Fy'sYgkU -HA#!+d[jhX"{>&f9wDd$qC(Fih(]iS
2021-09-27 18:34:12 UTC	1738	IN	Data Raw: 12 c1 58 5a 32 21 c4 34 3b 58 65 0c 57 10 28 14 5c 58 e1 b4 64 84 ac 22 cd 45 eb 1f e1 60 10 22 99 54 39 4c 8b 99 02 42 7b 2b 65 01 51 3e 18 1f 57 30 5a c0 17 48 e2 50 c8 10 c6 93 3c 82 5f 67 34 71 f9 d1 b4 16 46 26 b3 22 4d 24 16 45 07 ad 1a 10 61 63 68 c5 e2 a6 d4 b6 18 80 50 ed ff f3 0b b3 d7 98 32 58 6d a8 4d ac 45 63 d9 c6 4f 34 0e 98 98 49 89 48 69 da 98 29 17 51 89 61 db bc d6 be 73 6b b8 bc b2 a9 e7 f7 b8 fa 3f 36 65 01 11 81 44 58 27 ea 15 f9 93 7c 89 6a 9f 09 b6 3d 26 22 70 41 7f 73 00 4f 14 df 02 0f 2f 91 94 24 53 50 cd 6e b9 ca 56 2e 68 21 fa 14 c8 a5 71 62 9e 8a 28 c7 43 4c 6c 0d 13 bc 6a 6a 42 12 a3 20 da dc 30 27 ba cb 2e 59 cb 67 39 18 7d 70 d5 0c 52 48 30 7d 0c 4c f2 fa 56 eb 35 d2 2d 65 40 1c 92 8b 48 16 2e 11 42 b1 d2 e3 73 8c 6e 1c ee Data Ascii: XZ2!4;XeW(\Xd"E`'T9LB{+eQ>W0ZHP<_g4qF&"M$EachP2XmMEcO4IHi)Qask?6eDX'lj=&"pAsO/$SPnV.h!qb (CLljjB 0'.Yg9}pRH0}LV5-e@H.Bsn
2021-09-27 18:34:12 UTC	1739	IN	Data Raw: 61 d9 9b 06 ac 13 fe 10 2f 31 43 8b bf 5a 48 ef 97 bb bd 5e 79 31 ed 3e 3f 4b 74 87 9a 3b c9 c3 39 1d 8d 12 4c a8 84 2f 0f e1 a2 1c 9f 00 55 09 39 c4 bb bf 36 00 19 8d 12 0f 46 24 e5 79 00 b3 e1 00 42 85 b3 b3 c1 e9 80 e0 09 75 0b 80 82 d5 1f 4c 7a dd 71 bf 3a a9 93 c1 f8 bc 4b a9 22 75 e9 8c 82 75 32 18 96 b5 79 99 83 66 0f 09 e7 43 75 41 29 40 35 8c 8c 93 27 ca 80 14 88 61 37 0d bf d2 77 14 51 2b 47 2f 53 13 9f be aa 83 5a 39 2e 2b 03 4b d0 4d dd 90 a0 00 64 96 53 6f 7d c9 2d af 55 2d b1 a5 44 fa Data Ascii: a/1CZH^y1>?Kt;9L/U96F$yBuLzq:K"uu2yfCuA)@5'a7wQ+G/SZ9.+KMdSo}-U-D
2021-09-27 18:34:12 UTC	1739	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 e3 21 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`|4U`czQ02Ef|UMokdAHzMzs^(pmv,:3y q&^!*%$S9~D]<"!K5CIvu0o"KNJq25>).j*@_q5X24UL'
2021-09-27 18:34:12 UTC	1740	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 1b aa 86 01 d3 88 72 d1 e0 cb 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: ^5tZ\`:@n~#+Wj8@]s+;Xk mkjBcUwfUV`xZa&mVMH6,X4Y*&Tr69p{wbCy\ViS(6#m%iie9W8#m~pG6Jk]/
2021-09-27 18:34:12 UTC	1742	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 3a 12 e6 0c 3d 7b a4 02 20 38 36 28 19 67 94 00 2d 90 34 f9 40 57 e8 16 22 8e 86 28 23 c5 55 40 27 1c a8 22 06 64 48 c7 66 33 b6 28 9b 3f 27 c8 c7 a7 b7 a0 8d f9 51 bf 3e 62 03 97 d5 0d 5c 9b 93 2d de cd 30 65 d3 19 b3 84 bb e3 c6 7e 02 7d 87 d6 fe 02 04 ff 3f 5d 9e 1a fc 1f 36 f9 2a 8f 11 02 03 c8 ea a8 8e c3 a7 65 7c 20 70 34 c0 08 Data Ascii: qmFkr-ek`BKBRfC3TltCJfNt+d=@Dr=_B"eq<rf>c_9G9@ Ov!A0=Gue?e| :={ 86(g-4@W"(#U@"'dHf3(?'Q>b\-0e~}?]6*e| p4

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1743	IN	Data Raw: d9 c3 27 99 82 1a 71 d9 5b 0c 75 e2 a2 d4 08 96 4a 28 79 ad 02 59 7f 90 9d 7f d7 2a 18 8e 51 a9 14 0d 65 93 92 4c 87 e0 43 d7 e3 9b 49 6f 30 09 38 b1 a1 e9 48 1f c2 d6 2a e2 f9 dd bb 0f 28 11 96 bc 83 58 ab a4 15 f8 a3 31 7a 15 27 7c 81 04 75 e9 33 c0 5a 55 68 15 34 a9 65 2f 8c d4 6a 00 71 fd 00 f4 41 9d d6 35 2f d9 1b 39 32 75 45 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 a3 84 40 72 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(yY*QeLCIo08H*(X1z'|u3ZUh4e/jqA5/92uEzW%A;mfRYF+}VC0@rTCD!dp5]+:F4eeOq+K21&AR>wTPIQ 6iTF]t9
2021-09-27 18:34:12 UTC	1744	IN	Data Raw: 72 03 cb b5 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 a0 ef 05 00 73 c3 03 e0 12 98 db 22 e7 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_t]y-iHntu,MLI=ms"AMb-]t}-Vt<gBma,]>C"Y{lyLvknw@@l{<ibL0@1{X:m"VhJ&-m<[H3`zvHb^.Bi !POtJZXSj
2021-09-27 18:34:12 UTC	1745	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 ab 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[VCNl).H*I@Uf"c5|nBQC(g{]SaUkf.|B{T.CW9(@R7 {5je{?
2021-09-27 18:34:12 UTC	1747	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 a9 7c 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 2b 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=P\GHh!yEr1,W}rqU[urbz\R,ouQxJP|=qv164m#a;NzQ8Ko[]*hR^1iuF^}T$v?qFLk8+^vz{EBo] P haNi]>4e
2021-09-27 18:34:12 UTC	1748	IN	Data Raw: f3 56 55 99 57 fd 4c 95 08 e9 ce 99 b2 41 02 b3 2c 7d ca ca 25 cb 5f b3 fe 7b 6d 91 3e 3d 55 5b 32 4d 60 9a aa 21 57 3a 90 c7 56 05 9c be c8 d8 4c 39 51 66 0f 15 b2 e9 c8 ae aa 01 d6 3d 44 c0 33 6c 43 17 22 76 07 08 5d 44 0f 6c f5 18 25 71 c9 e2 92 c3 74 19 dd e3 74 cc ce ee b7 39 8b b6 f4 b1 f2 e7 02 e9 55 d5 31 0c 07 ee 74 c3 30 f4 43 7f 1f a2 7a a4 a6 9a 1a 68 c1 f1 80 f0 9a 03 14 16 92 3b 2f 36 2c a9 73 6b 20 b9 ae 6d eb b6 6b 6a aa a1 c2 4a 18 df d4 8f 52 94 58 55 fa 79 0b ec b0 6b 63 c3 43 92 1d d7 82 b1 86 3d 9b 02 c6 7e c8 b6 8f 88 66 f9 98 65 79 b5 17 ac dd 76 74 f2 e1 78 98 d5 93 ad 30 e5 67 8d 8f 36 51 aa ba 86 5d 59 9e e1 51 22 84 9d f7 69 f4 7d ce 56 cd 96 2c 53 57 4d b8 07 4f aa 86 81 f5 09 13 f4 18 ab 87 da a0 73 e0 22 56 64 23 58 9e 67 08 Data Ascii: VUWLA,}%_{m>=U[2M`!W:VL9Qf=D3lC"v]Dl%qtt9U1t0Czh;/6,sk mkjJRXUykcC=~feyvtx0g6Q]YQ"i}V,SW MOs"Vd#Xg
2021-09-27 18:34:12 UTC	1749	IN	Data Raw: 57 44 c5 55 2d 15 50 dc 5e 0e c8 ed f9 75 65 e6 00 5d 11 43 62 2a ec 4b f7 2c 61 67 97 11 68 bb 54 8a 6c 5d a9 4d 68 41 e8 4c 4b 43 f4 81 ca 60 1c 53 28 a3 61 c2 c0 1f f5 68 d4 9a 8e 55 e1 a8 b8 26 f2 ae 09 5b fe c0 b8 b8 42 dc a2 67 f4 22 54 e4 c9 b9 67 8d 32 ae 72 61 ab 28 42 e8 77 48 51 0f 11 44 1d 09 0e 29 ef 35 95 f3 c4 d7 14 51 90 4f 9e 6b e4 1e 78 ad 44 b5 00 7c a1 2a f6 18 be 99 d0 b5 e9 26 09 10 ea d2 4d 8c 6d 08 e5 ff 93 72 0b 5c 8b eb ab 30 db a4 0b 33 dd b4 c0 c3 c8 b7 25 b6 8e 17 90 6e 5c cb bd 50 20 d9 e6 7b b7 d8 e2 4a bf 5f 87 6d 5b ae e5 01 90 6c 0d 18 80 33 05 28 90 32 ec 82 d5 24 5d 75 46 b6 ad a1 bf 71 3d 90 b3 0e 85 a4 4a b2 c1 cd 78 33 00 76 5e 91 5e ad a8 19 8d a6 01 71 64 78 80 33 54 91 eb a9 42 62 ee 60 05 ec db 3e e2 b4 bd 55 2e Data Ascii: WDU-P^ue]Cb*K,aghTl]MhALKC`S(ahU&[Bg"Tg2ra(BwHQD)5QOkxD|*&Mmr\03%n\P {J_m[l3(2$]uFq=Jx3v ^^qdx3TBb`>U.
2021-09-27 18:34:12 UTC	1750	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 dc 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 32 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: '$Hbr@F_t^("KQx`5zAgTZ=BVw:%Z~_XL4{;@8v^pu^\|uat)SE2pxd$#9>ZH^r|Q~~,E,dM2-QT[Av#`8IP|p=~|1
2021-09-27 18:34:12 UTC	1752	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 4f 59 b8 fd a8 29 3f a9 df 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: 6\dS40=)*CK7LU$3]&DcwQdvAvA2K."TMO4GZqh*v\3Lk&YD@o}(hhxY)['OOY)?>x]\o'%RaVY\z%'p/-:zYxg' 0#Ql#gWUCR@@[C|
2021-09-27 18:34:12 UTC	1753	IN	Data Raw: 96 b7 59 96 6e d8 b5 cc b7 a0 03 01 74 ba eb a0 5f 07 48 59 9a 90 c7 1d 82 95 6d 08 92 ab 32 c2 70 2c 8b 3a 70 cb 83 74 83 1c 10 55 58 89 ce c4 b8 db f8 20 43 3f 77 2a 6b 08 2f 3c d4 85 06 83 30 81 82 11 f2 e9 a6 d2 94 a8 de d7 0e 1c bb b4 45 26 67 6c 4d 7f a3 70 1a 29 0f d1 8f 57 55 4e 9b a6 aa 62 52 50 86 58 83 03 61 29 48 e2 5f 48 38 20 ad 00 ff 05 5b e4 c7 ca f0 6d 76 64 c5 cf 95 4f 78 f5 5c a8 32 0b b0 04 f1 23 b8 ec 9f 24 95 52 a1 cf ae f2 7b 28 01 2e 4a a0 7a c0 3f 34 0e 45 bd 55 92 c7 03 ed 44 3b 22 68 e2 b6 fd fa cd e9 50 1c e5 17 d5 64 6c 74 e4 26 34 27 88 49 a7 4f 02 25 d1 02 95 35 36 2a ad f5 cc e5 78 70 5b 51 a5 a9 9f 94 c0 be 5e 24 34 24 b6 07 f0 05 6d 07 51 eb 09 4d d8 43 c5 b5 ab 68 71 ac 7d c2 c7 7c 9e f0 6a fb ae 80 84 99 62 09 df 73 9f Data Ascii: Ynt_HYm2p,:ptUX C?w*k/<0E&glMp)WUNbRPXa)H_H8 [mvdOx\2#$R{(.Jz?4EUD;"hPdlt&4'IO%56*xp[Q^$ 4$mQMChq}|jbs

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1754	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 f4 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 e5 0f 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 6e 86 24 3d e4 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:]4;&}$E>?8!k>]$Gu]_B#kw[<\Aot(F'!%)8ytu(@D5jZMF'/xB#wj%2Fx%$\n$="mZGIG"1`|$k
2021-09-27 18:34:12 UTC	1756	IN	Data Raw: b4 64 f5 60 db b0 6d d7 76 4c 6e 20 d3 33 0d c7 3e 1d 3c 64 c5 92 a5 55 e3 2c 57 85 2d 75 c7 b4 2d d7 33 2d 47 73 88 6f 6f f3 f5 6e d3 48 77 2d d5 f0 1c 4b 85 dd 75 55 57 0d 97 a8 c2 f7 32 f7 14 18 ba ac ad 72 cf d6 0a cb b0 cf aa 48 0a 38 7c a7 f4 ee 8a 7c c3 e6 49 59 61 ab ca b3 f1 c4 1f 4d 66 d7 61 f4 fe 59 b2 dd 2a 57 79 be 5a 33 e5 1d 86 3c 0b a2 7e fd c3 9b 76 d8 78 e8 47 cf 7e 12 3f 88 c7 33 68 b5 5d 27 73 76 97 af 17 ac 28 85 3a ed 34 f1 07 5f 19 c6 e4 ba 3d d3 c4 2e da c9 e4 67 5d fc fc a8 0f 19 60 1c 0c 90 4a 30 cf 1e 1e 3a 0c 35 db de 9d da ea e7 cb e4 1f 9f 77 4c 55 d5 9f 2f cb 6d 92 b5 7f 24 ca 5d c1 96 af 3f 9f dd 55 d5 b6 7c 75 79 59 ee b6 db bc a8 2e 56 c2 36 17 f3 7c 73 39 df 1b f1 32 c9 ca af ac b8 d4 3d 91 a4 9f cf 94 2a 29 56 ac c2 fc Data Ascii: d`mvLn 3><dU,W-u-3-GsoonHw-KuUW2rH8|IYaMfaY*WyZ3<~vxG~?3h]'sv(:4_=.g]`J0:5wLU/m$]?U|uyY .V6|s92=*)V
2021-09-27 18:34:12 UTC	1757	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&[i]7M%FzwJf{xhGwtK#9m"L-&ZMi 0*y8o[Yz_/aEP
2021-09-27 18:34:12 UTC	1758	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 f7 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'?[~lSAnAxt3(J%9.Tq u/"Fi8idS
2021-09-27 18:34:12 UTC	1759	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 35 b1 48 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 ba 2a f7 65 5d 15 1e d6 1d 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: Il)UrAvKIE3aulVSx!te;9%e_2I7L5H&qIJt.4V5VIuTm04hTKK\PVJ(ElncLp@+5f.R:-S1hJmk;&scQ*e]\"&K-lX*6CWuplKW(DYg)Mg?/3
2021-09-27 18:34:12 UTC	1761	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 f9 2c 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: -MI6[-e[#=Af7a+_OX70t.N;J+;+9T4IQk;<#\qU%q$hO7,@2up+Oyk?rP#_c= Kc=,btVp[c8(:P;2Wg>GAq ~z#@!<0]Yz}P-
2021-09-27 18:34:12 UTC	1762	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 77 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 a8 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 e8 67 92 24 35 ce 57 a9 52 64 9b f2 33 73 Data Ascii: EdBoJ.Jr-du^R>rzA,wnTI;`zgTt=t*CY9u=diX-YuTES7LoUHT[*~Pk3NC#Y1b%kb;wYouflg$5WRd3s
2021-09-27 18:34:12 UTC	1763	IN	Data Raw: 72 75 2f 03 00 50 4b 07 08 00 00 00 00 02 00 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 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\{o*?.Kw=(QcKRdYJ&vj;8rf(!"kCr8;RH4Y%w^~4/T+?D_;w6NJz% XSD>>}kIR-4{u2ZQj.Ng0%F
2021-09-27 18:34:12 UTC	1764	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 08 79 70 a6 c1 20 bf 3d ec 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 Ii5<9HYBd"|\,5,h3xvj?!9R5?})Wq.vggyp =|!. ?&9%+]^c&!"b ypVq/jK: cA|KEMNfbbcpx::ZLHzJ3ATYe![s>M t8

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1766	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%r+Jjzb"CVg@& ~sezjO *POeDo(one!_.kL
2021-09-27 18:34:12 UTC	1767	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{\}\kiTg69'0_=LN{Q'-!3,\8?$3;VB<RSZ`=HK>c*^nH='(^1$\UG-bPNAzG}5C_S HMu)bqOFL1hWW
2021-09-27 18:34:12 UTC	1768	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}9}!QYbei^^|s1KWg{'!3$Z~dpVh3,jsubD0LP,/e]harAU.@;cxgRUNIO%7 r7/)VD1b
2021-09-27 18:34:12 UTC	1770	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>:QT8}67=V9mci/pWHQ1yERCw9h xKt/~OF3^wvWkY~):mcZn9(y(
2021-09-27 18:34:12 UTC	1771	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: !|t}XzZ}+]pt$3]MO[sWuH3>_x.+p;3D\Y5A\+h9\W&YkO$
2021-09-27 18:34:12 UTC	1771	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 4c 7b fd f1 74 3c 94 a6 a1 52 e8 92 fd 65 18 76 3e 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?i^vt4vgnJ*![vx;8=y1"9kL{t<Rev>7^v)h?vQ{(kF[pxRan0#}_0\8Q-IPw?
2021-09-27 18:34:12 UTC	1772	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 db 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 36 be 8e 24 9a 9e ed 3a 7e 60 3b 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\d|Qe\lDbjgien9+F|Jk|vDYdgcGtx=CM?p7M\u}eV<f$kT6$:~`;-LXbn#nO%\?ebX^T iKR{7M4~6Ib2.xLv~/QoDI
2021-09-27 18:34:12 UTC	1774	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?(!:Fi9i'y8}CzPI3yx-7Y*,;08`'\o2.k|=?L#{x ?w/HyE}:h:Tm[YM2o,t%ewU.:ux<,%08D3
2021-09-27 18:34:12 UTC	1775	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&O|59ix!MuZ&^=Fy~#x61bJvS1p#RhC)*GgJhu:0?@pIQo >xi4np0Y_M4r

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1776	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 e4 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[%,wZWyWadQk\U7Cw:"xU(`/TK`kC~o~X}t:NF:qq|tA_"a$8eeR!D"~<m6)s#x \acrNFu
2021-09-27 18:34:12 UTC	1777	IN	Data Raw: 9c 98 dd c7 53 a2 42 54 63 8d 13 43 95 4d ba a2 cc 61 4b 95 58 0a 7c ca fd 66 05 4a 28 9b ca 4f 34 7d 6d 51 0b 3b 20 5c 22 88 07 42 e2 fd 9d 54 4d 66 f7 b4 f9 d7 fe 2e 2b d7 a5 28 59 40 2c b9 c6 e6 a8 59 95 9c 1d d7 ab 70 71 63 91 9c 0c 5b 3c 54 6d c1 84 61 4a 20 80 25 e4 4d 09 8e b4 56 98 90 9d 30 a2 75 53 1d c4 fe 68 de 69 66 3f 47 ac 61 44 0b 5b 75 92 23 b3 c7 c7 6c b5 e8 29 5a 76 ba c8 e8 84 c5 07 c7 29 be c5 a4 d3 eb 3c 62 24 d2 e1 c3 e0 83 53 93 21 b2 ee 1e a5 7d 06 6f ba 45 c9 c0 e8 58 92 4a 0a 61 bb 3a c4 07 30 33 96 51 bd 8d 41 64 6a 72 12 aa fc 00 43 f2 d2 86 e3 43 5c 95 5e 30 52 95 54 83 24 fa 25 c5 ef 92 00 46 65 e8 44 0b b1 04 18 5c 4f c5 2a c2 d8 ee 86 b9 2a 71 0c 49 f5 6a b9 b0 c0 32 93 33 0d 09 e3 36 fb 04 bc 9a 5a d9 b4 96 b6 9f 10 09 1d Data Ascii: SBTcCMaKX|fJ(O4}mQ; \"BTMf.+(Y@,Ypqc[<TmaJ %MV0uShif?GaD[u#l)Zv)<b$S!}oEXJa:03QAdjrCC\^0 RT$%FeD\O**qlj236Z
2021-09-27 18:34:12 UTC	1779	IN	Data Raw: a4 5a c3 4c cd c7 cd 1a c8 a6 be 6c a2 8c d5 10 23 40 46 9f 19 b9 fc 33 9a 8c 38 6e c2 4d 64 a6 3a 82 85 30 1a da c7 9e 9c a5 84 7c bc c1 59 67 bd 0d 10 fa 3a 09 61 1e 38 60 88 f6 ee 1b 76 4d 84 9d c9 74 73 a5 8d ea 00 89 7f 53 77 76 4e 02 17 7d 90 aa 50 de 6a c1 08 27 da 3d a9 cc de d3 8d 49 cd 72 36 53 6b 4e 11 20 36 2f b4 0e 10 a6 83 a1 f1 41 b0 92 ac 34 41 b5 e0 6d 17 b2 88 4b 47 84 d4 0b 1f 1e 19 13 a6 99 58 31 75 6f 3c c3 81 2d 70 20 eb b6 0a 23 f0 9c 02 52 ca f6 f8 ff f9 e3 01 49 1b 60 e0 14 26 73 ed 2c 6d cc 33 74 ca 32 39 17 fd d9 0e c4 7d 4f 89 96 27 66 86 b6 90 98 39 b9 24 b8 42 97 6b b8 e0 83 6e f1 3b 2d 19 53 58 46 3e 68 cb b2 03 62 70 32 ed 84 87 a9 ee a9 51 a7 9a 94 14 76 70 eb 1e 63 c3 94 b8 91 1b 6e 59 9f 29 ec a4 53 50 f8 08 4c 28 db 21 Data Ascii: ZLl#@F38nMd:0|Yg:a8`vMtsSwvN}Pj'=Ir6SkN 6/A4AmKGX1uo<-p #RI`&s,m3t29}O'f9$Bkn;-SXF>hbp2Q vpcnY)SPL(!
2021-09-27 18:34:12 UTC	1780	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 66 83 f2 70 12 4f 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|Mr}+Iy2r/#@Y1X Nk|qG@)6rOK80Q<fh]xfpOM-n!=<,&'Dw)<`EapH<S*Mk^|jNG]N|\hq>\qLY1[9|EM<}WrT
2021-09-27 18:34:12 UTC	1781	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 f7 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'$JwbC7+8fwcYvVoHRQ\ pypi.xeZQUpY:arETWE.MAm*o~OOW,`jeSV>D) >PPc)O}hv&
2021-09-27 18:34:12 UTC	1782	IN	Data Raw: ac 32 91 ff 00 15 02 ad 4b 11 4a b3 d7 15 a3 02 32 26 f8 43 f2 75 33 3b ae 27 b3 d0 fb 19 a0 5d 28 08 1a 7f 92 95 02 6e 35 30 36 12 93 9a 88 58 01 e9 5b fe 2a 65 bf 45 77 77 35 d9 a9 66 01 3c 37 4b 01 9f c2 26 00 60 40 75 c0 ee 5c 42 f4 47 0d ac 3c 67 00 e7 2f 45 cd 42 7e c8 23 d1 8d 21 ee c3 e2 47 a1 d4 42 eb a8 a2 5f 85 9f 1c c5 54 80 ea ed 91 d3 04 41 f7 5a c8 da 40 69 b8 96 97 3c 2c 56 73 4d b2 dc 8b b0 da 8d 98 37 a3 82 6a 83 16 82 6c 9a 2a b6 05 f8 8e c2 65 90 c0 eb d4 8e 89 17 b5 04 22 54 83 81 48 30 c7 40 60 a8 64 dd ed 25 ee 2e e2 cc 98 3b b1 da 4f b1 4f 96 82 a0 05 8f 07 35 75 e1 47 44 1a d1 e8 bd 30 06 ee 42 7e 14 55 d7 97 82 e5 20 7d dc 83 fc c7 86 26 ec 13 96 7a 1e c7 e2 27 49 40 5d 87 1f c0 58 3a c9 92 9f 58 ff 8e f3 ab 32 cb e3 a2 46 5f cb Data Ascii: 2KJ2&Cu3;'](n506X[*eEww5f<7K&`@u\BG<g/EB~#!GB_TAZ@i<,VsM7jl*e"TH0@`d%.;OO5uGD0B~U }&z'I@]X:X2F_
2021-09-27 18:34:12 UTC	1784	IN	Data Raw: f6 a6 93 91 77 ee 4b d2 89 5c e2 10 35 23 4e 36 e4 e0 22 2b 22 72 f9 ab fe 39 81 47 49 3b 21 11 1e 4f 06 d3 9b 60 14 9c 06 55 90 b5 6e a9 e4 7b 08 aa ad df 1d df 7a c3 f6 c8 97 95 37 a2 65 d2 bb ec f5 6f 89 ac ac 49 23 b2 37 41 c7 6f 47 7b 09 8b 68 d1 30 ba ee f7 c7 17 3d 7f 44 bc 2a fb 8a 86 28 f9 ec d3 62 25 b9 8a ad e4 46 e7 d3 2e 00 19 d1 3b ee a3 d6 8c 08 7c c9 6e 24 1a 49 78 0a 68 d3 f1 7b 01 45 2c d9 15 ca 6b b9 71 70 ed c3 60 92 78 92 83 a9 46 f0 ba aa 66 3d ff 6c 5c 5b 4d fc 23 f9 46 68 47 f8 19 21 45 5d f6 ce ce fc c1 d8 3b bd 22 b9 23 3b c0 6b d7 73 de ef 13 4b 64 fc b2 5d c3 c0 1f 76 b1 2a b2 1c c9 37 46 6f 28 e9 f7 49 05 93 90 f1 76 05 93 5e 00 aa 70 75 15 9c 07 12 9f c8 ee 71 64 ba 3a c1 e8 cc 1b 76 f8 4e 75 83 e1 b5 27 4b 45 d9 f5 9e 4c 57 Data Ascii: wK\5#N6"+"r9GI;!O`Un{z7eoI#7AoG{h0=D*(b%F.;|n$Ixh{E,kqp`xFf=l\[M#FhG!E];"#;ksKd]v*7Fo(Iv^puqd:vNu' KELW
2021-09-27 18:34:12 UTC	1785	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 86 fd 7f 18 1d cb d3 0c d5 b3 54 d7 d5 4d 4f d7 34 86 01 17 13 01 e8 28 46 7b a6 ed a8 28 3f 14 ac e3 aa 9e 61 1e 8f be 14 f1 26 9d c7 d3 c2 40 f7 30 5c f5 00 53 96 ad eb 30 60 c0 f9 e3 1a 11 0a ea 01 42 d4 ef 9d 2e 67 e9 4a cc 4e 93 87 87 75 b4 f9 a0 29 1f d5 1f 97 62 31 4e d2 cd d3 47 ad fc a8 a0 56 7f 74 ba 17 b5 30 f8 e6 77 9f 9e 3e ea Data Ascii: u\&8}2??\,hu{Y~?Q6b56btLQgbiFp1~$[\|M<[}5ht'UXg::R-EQb$>Ww t^TMO4(F{(?a&@0\S0`B.gJNu)b1NGVt0w>
2021-09-27 18:34:12 UTC	1786	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 44 83 cb 6c 7f 97 a2 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*$6De"q:F`Dl$!\M4\F]+&jP7uVyBbmiy'm|1,:Rta,S

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1788	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*{'9s\3fvaw5=_40%Yxm>&OrPT36z5yVZND=\&V#yy'c0v0HV+$1]z|5^mN5n&+E5W3 ^PB>G
2021-09-27 18:34:12 UTC	1789	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 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 57 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{/rO+!_>.>TYt~}O?]ooW_wx_cnA~qvu|}P.^z/oW'qF0'wn_O^;Y,W5Z**u0X :
2021-09-27 18:34:12 UTC	1790	IN	Data Raw: 85 4e 31 10 4a c8 4f 33 f0 a9 55 56 5b e5 9c 22 27 b2 cd e8 1d f5 ed c7 09 06 bf 34 1a c6 7e 4d b3 25 4a fb b5 78 10 f7 52 e0 bc 03 13 d2 2f 0d 19 fd 86 52 fa fe 35 5e 63 95 17 3e 28 a1 d6 cd 01 d6 f3 b9 e4 7d 64 e4 8f 54 e2 2e 0a 45 5a ab a0 b4 0d de d9 20 e8 f2 63 1a 1f c7 e6 18 a9 8a 0d 4b 1e 10 e2 7c 3b 5e 35 cf 8c e9 4f 21 4e 97 d6 85 ff b3 82 19 40 24 33 6d 42 10 5e 59 ab 24 9f cf 2e 27 8d a3 16 26 6d 4d 13 2b 78 f5 ad d8 5c 4e 2a 2b 0a 37 20 27 16 fe e8 4c 80 dc 7c e7 12 c0 7f 9f 32 b5 2d 48 18 30 2a 21 03 4f e8 4c 16 ac 36 be c1 b0 b4 8a e2 13 b0 a5 e6 6a e2 d7 cb ed 3d e6 fc c7 7a 96 56 48 a3 9d 09 c2 58 61 44 a6 2d 6f ff f6 6e 3c b1 42 15 1d 33 de 68 eb 42 26 84 71 bc ef 6d ef 1a 77 d5 dd 2b 18 da db ea 02 79 34 e6 6d 97 e8 68 cc 92 a4 a5 a5 96 Data Ascii: N1JO3UV["'4~M%JxR/R5^c>(}dT.EZ cK|;^5O!N@$3mB^Y$.'&mM+x\N*+7 'L|2-H0*!OL6j=zVHXaD-on<B3h B&qmw+y4mh
2021-09-27 18:34:12 UTC	1791	IN	Data Raw: c9 f7 ce a6 97 1a ec 57 47 e8 c5 ab a3 8e 3a 32 a7 cf ff 1f 2f 0b 99 f8 1a 3a 8e 72 d3 b1 f0 fb 1f 23 7f 33 97 29 a3 1c 04 25 d6 68 08 8a 48 a1 f6 eb 61 90 7d 4e 95 a6 72 d7 0f cc 1d 96 e1 6f e1 76 8a c2 b2 84 59 2b a5 bd 55 2d ae 1d 68 01 d3 a3 8e 7a e1 8b 4c 9b 06 b2 45 31 48 04 cf e7 dc 5a 24 d0 f7 39 86 e9 21 2c 0d 21 b8 75 ba cf 98 4c f2 ae 1f 63 a4 5a cb 40 eb 0a 46 2d 67 e7 f5 3a fa f3 de 4b ed 44 66 85 e1 4f ce 62 27 f7 88 23 3c 0d 0c 69 8c c8 1a b2 18 bf 6f f6 80 e1 d7 ef 97 3e f0 46 eb 02 1a 7a ed 9c 0e c1 04 36 28 de 91 5f f5 c6 9a 60 32 23 85 5f e7 06 0d b1 a4 d1 2e d1 cb 56 52 21 c1 4e 53 87 c5 ee 61 36 ef 70 87 b9 de e8 df 03 a6 54 f2 c5 4a 2b 8d 37 32 d3 5a fb 2c 03 5d 4c 17 90 b8 33 e4 91 8a 16 5e da a0 45 50 5e 69 30 a8 6c 66 e5 51 57 ed Data Ascii: WG:2/:r#3)%hHa}NrovY+U-hzLE1HZ$9!,!uLcZ@F-g:KDfOb'#<io>Fz6(_`2#_.VR!NSa6pTJ+72Z,]L3^EP^i0lfQW
2021-09-27 18:34:12 UTC	1793	IN	Data Raw: d3 b3 7c 4e 14 83 b9 c5 15 0d 2e c3 42 08 59 22 60 e8 75 2f 0a 2b 46 56 c0 9c fe f8 4a 05 20 2a 61 17 53 72 ae 7e 7f d1 9d 4d c8 00 ee 5a c7 af 03 ce ba d4 7c 31 f7 74 56 bf 9f e4 39 71 cf 5c 1e b9 fa fd 6c c8 2d 81 2b c9 55 23 2e 47 67 b3 73 32 82 bb 3b fc cb 97 7f 03 50 4b 07 08 8b 4a 75 50 bd 11 00 00 7e 61 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 00 0c 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 74 65 2f 03 00 50 4b 07 08 00 00 00 00 02 00 00 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 00 19 00 00 00 5f 6c 6f 63 61 6c 65 73 2f 74 65 2f 6d 65 73 73 61 67 65 73 2e 6a 73 6f 6e dd 5c 5b 73 13 4b 92 fe 2b 5a 2f 0f 73 26 c0 d4 bd aa d9 39 7b 42 58 6d a3 c1 96 3c 92 0c c1 c4 89 50 Data Ascii: |N.BY"`u/+FVJ *aSr~MZ|1tV9q\l-+U#.Ggs2;PKJuP~aPK*Q_locales/te/PKPK)Q_locales/te/messages.json\[sK+ Z/s&9{BXm<P
2021-09-27 18:34:12 UTC	1794	IN	Data Raw: 0e c7 d4 69 b0 df 91 4b bd 72 2e ee 72 ab 06 a9 23 c0 6e 1f a1 aa 00 f1 b2 10 5e 6b 0f 7b 54 5a 6b 95 c7 ef a8 c7 d8 51 47 1b 0f 52 18 09 81 b7 2f 20 dc 95 1e a2 b8 7c ec 9f c4 94 7e 3d 34 69 c0 a6 e0 9c 72 c1 48 a1 05 90 67 09 47 f7 72 89 e4 49 63 f8 25 91 10 8d 35 ae 10 ab a3 96 2d d0 9e a3 0a 53 fd df df df 8f eb d5 05 c0 9c 0f 16 d6 2b 41 81 cc da 58 ad d7 e9 43 34 b5 66 61 7e 75 91 a2 89 48 40 3a ce 03 86 c2 67 01 2c 29 32 7c a6 86 d8 8e 37 e0 46 94 04 69 d9 42 17 95 c5 b0 d2 c6 96 28 2f 90 0e e6 e5 64 8d 12 06 96 05 79 98 d0 1a 38 c0 2e ac 15 7a c7 ba a8 40 d5 08 f0 71 01 fe 51 0e f4 a7 28 74 be 3e 10 35 de d7 23 8d 80 00 bf 80 34 cb 83 aa 40 a6 e5 32 0a ec 11 df 1d 5e 3f 86 9b de 9f ea 5d 0a b4 d7 c6 4c cf bb df 36 26 2b d4 2f cf da f9 2b 89 48 29 Data Ascii: iKr.r#n^k{TZkQGR/ |~=4irHgGrIc%5-S+AXC4fa~uH@:g,)2|7FiB(/dy8.z@qQ(t>5#4@2^?]L6&+/+H)
2021-09-27 18:34:12 UTC	1795	IN	Data Raw: bb 0e b0 46 0f b1 91 fa de eb f7 4f 0e df a3 c8 ef be 0d b0 c4 e6 b2 cd ba 49 49 bd d9 a6 31 42 00 ff 94 0b 20 31 2f 8c 5c d3 13 c0 a5 e1 31 7d 46 35 02 1c 2b 30 e9 de 8f 28 f1 a0 58 0b eb ce 7d 2b 12 bf 45 56 00 33 8a a0 e1 5f 88 e3 a5 28 58 4e ec 70 0e 26 90 ab a1 4e 2e ad 12 7d 7f 92 b5 5d c5 3e df 5b dc b1 94 71 88 b4 63 aa e5 6f a6 e2 d0 96 79 ac 71 56 68 e3 00 92 44 d5 db 67 dc 8e 65 1e 8c e0 89 1b 75 e4 c9 e5 d3 b3 c9 31 51 96 7b b2 f6 7b 75 29 58 a7 84 84 00 5f 15 10 9c ba 82 6f ba 97 dd b6 b3 85 9c f5 e7 6d 8c 1a a5 5d 19 cd 81 3d 56 db 18 d8 d3 62 10 d3 a1 8a d5 6c 43 31 e5 97 66 e7 ae 00 e3 d1 85 07 6b 0a c2 0a ab f8 5c eb 87 39 01 80 ec c3 93 66 6a 0f 19 38 d8 6f 55 4b 04 4d 53 85 65 75 2d 82 11 13 32 76 fb 5b ff 6d 12 17 45 21 a1 43 91 b6 7a Data Ascii: FOII1B 1/\1}F5+0(X}+EV3_(XNp&N.}]>[qcoyqVhDgeu1Q{{u)X_om]=VblC1fk\9fj8oUKMSeu-2v[mE!Cz
2021-09-27 18:34:12 UTC	1796	IN	Data Raw: 23 ce 3b 7a f4 d6 16 f7 be 9b 7c a9 69 d4 9f e2 76 97 25 a2 9f e0 c6 2a fd d5 e8 92 bd 33 26 56 74 e1 1b 09 72 d4 cd 2c 97 29 0e 31 8d ed d5 cb 39 bc 08 41 07 05 c8 0d 10 be f6 98 ee e1 9b 20 29 33 69 f8 82 53 9a ef ec b1 c5 ef 7e 20 ee 21 49 6f 7e 5a 7f ec 49 39 18 f6 e7 93 f1 d9 ac 9c cc fb 83 c1 70 36 1c 8f fa c7 f3 83 f1 c9 49 39 9a 4d 57 c5 c3 bd d1 86 d2 39 1b 0c c7 f3 bf 9d f5 8f 87 b3 37 ab 14 b8 c8 95 50 38 e8 8f 0e ca e3 f9 f3 b3 d9 6c 3c a2 6b a0 2f 7c a1 14 c6 a3 19 6c 00 56 51 4e ab 3d ad 12 e1 ba 13 08 91 c1 70 30 1f 8d 67 f3 d9 84 6c 83 3b 81 20 e3 0f cb 72 f0 bc 7f f0 72 5e 9e f4 87 c7 f3 c3 61 79 3c 58 25 c4 5d d1 cf 13 3a 1c 4f 4e e6 83 72 7a 30 19 9e b2 db 62 5a 45 f3 d4 5e 94 fd 41 39 59 a5 c1 95 d6 f2 34 4e 27 e3 93 d3 19 61 0f 3d 91 Data Ascii: #;z|iv%*3&Vtr,)19A)3iS~ !lo~ZI9p6I9MW97P8l<k/|lVQN=p0gl; rr^ay<X%]:ONrz0bZE^A9Y4N'a=
2021-09-27 18:34:12 UTC	1798	IN	Data Raw: 60 d7 ab 76 bd 7a 5d ff ad ab 4f 59 d3 95 b6 fe c6 a3 5f e3 f7 af ea cf 78 57 bb 4d 41 d6 d7 eb 78 e5 ba e5 4c c5 7b 89 96 6f 55 df 4b bb 76 6d e2 c7 6f af 8a df a7 6b 5c 4b 41 d7 57 4a 8d 78 43 12 89 7f 47 0e a5 43 dc c6 1d ad 11 05 93 a4 06 f2 2a bc 2b 4c 21 b4 0c c2 59 56 68 12 b1 a7 b7 d5 10 c5 a2 5e a1 6b 5e a3 1b bd 6a 29 c4 b5 89 f9 f3 c8 80 51 de 80 c6 0b b8 b7 97 aa 70 5a e6 d5 ae 1c ba 47 a4 68 5b 81 c6 4d 46 6e a2 68 22 4f f1 1a 2a d0 44 0d 09 31 09 2b 5d 19 f9 b3 4a 49 23 0a af b5 04 2e 85 b6 3c 7f 44 42 49 ed eb 6d fe 22 07 91 7b 6a 6e 0a 1b 97 6c e9 e0 9d 28 37 68 d9 8c e2 55 c8 86 d3 45 78 a3 af db cd 45 46 3b d6 28 db 5b 36 be 64 ad 08 02 76 6d 9c 14 5e f9 60 3d b7 e9 b4 5e b5 76 8f ed bb 51 47 a4 58 e8 a2 f0 85 33 95 b1 99 60 b4 2b 58 8a Data Ascii: `vz]OY_xWMAxL{oUKvmok\KAWJxCGC*+L!YVh^k^j)QpZGh[MFnh"O*D1+]JI#.<DBIm"{jnl(7hUExEF;([6dvm ^`=^vQGX3`+X

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:12 UTC	1799	IN	Data Raw: 31 24 b9 66 cc 8e 29 f0 d7 db 57 e2 22 2c 59 92 42 08 e4 7b d0 3c 6d 4c 61 bf e9 84 51 8a fe 29 eb 77 14 5f b4 9a 14 fa 5e b7 1c c6 bd 50 a5 76 c4 ed b6 e9 e0 a6 04 76 9a f4 3d f2 6f 79 81 76 2d 5a 0e 19 cb da 25 1a 2a c2 56 12 2e ea 9a 45 95 08 d4 67 c1 dd 43 53 0c 90 d9 f4 86 55 1a ad 14 32 2d a6 16 40 5a 4a 06 89 35 ac 5a 26 b0 49 27 29 9a 56 0f 71 15 0e 15 0a 4b 17 05 b8 fe 7a 04 cb 3b 46 90 64 29 8a 84 6d da 82 a0 2a 66 22 1b 6a 1b 4a 9c 5f b0 7f 5a b4 0a c5 08 83 70 32 ed c7 e6 dc 2d 39 05 71 ae ac 5d a0 d8 9b 10 10 45 e0 28 e0 35 a2 d9 21 73 fd 88 88 90 fc 70 dd ae c5 5d d0 8e 65 51 6b 45 1b 53 a8 93 8b 55 d8 a5 33 48 2d a9 f6 9e 78 1f 1d 45 d7 a1 9c c6 a8 ef 97 c1 4e 2d f4 de 48 78 e7 88 54 c3 01 dc 03 48 40 5f 20 0a 71 d7 a8 de ca 79 60 a7 a5 ca Data Ascii: 1$f)W",YB{<mLaQ)w_^Pvv=oyv-Z%*V.EgCSU2-@ZJ5Z&I')VqKz;Fd)m*f"jJ_Zp2-9q]E(5!sp]eQkESU3H-xEN-HxTH@_ qy`
2021-09-27 18:34:12 UTC	1800	IN	Data Raw: 65 94 d6 c2 b9 47 1d f0 ec b1 99 07 0e be 20 98 9d 7b e6 bb 9c 45 d9 5d 86 09 08 e0 c1 0d 66 99 39 07 75 4f 7d 48 7a fc 05 03 9c ce 21 a6 dc 14 77 87 c9 f0 4e e2 cb e0 f1 8e ff f6 77 3f 50 e9 40 93 a1 48 59 21 04 57 08 25 ab b1 0b 40 6a 03 e8 6a c7 68 92 95 4b 4d d7 49 08 8b 90 cc 04 14 26 10 48 04 04 ad 3c 30 a2 33 6c 46 0f a4 57 24 1d f9 06 9f 85 29 b6 25 d1 ed 03 f1 26 fa 7d ed 12 dc f8 6a a4 e0 8b aa d9 5c 95 f0 d2 08 fe 9c 5c d7 40 b6 db 23 7f 26 cc 8f 9e 45 f8 2a fa ff 31 bd 17 2a d1 1d 5b 2f 4d fa 04 6b d7 50 3d 38 e1 5c 75 e6 10 fe 60 b1 29 13 bf fb 9f 23 71 ae ea 06 59 09 6e 64 a4 81 da 24 73 92 13 1d b9 48 73 c6 b0 6d e4 74 78 d0 d1 05 3e 89 97 fa 25 5d 5c cc 38 2b 1e 8a 93 22 1b 17 5f cc 51 17 7c 60 0f 55 02 a9 ce c2 5c 62 f7 43 29 29 45 7c d9 Data Ascii: eG {E]f9uO}Hz!wNw?P@HY!W%@jjhKMI&H<03lFW$)%&}j\\@#&E*1*[/MkP=8\u`)#qYnd$sHsmtx>%]\8+"_Q| `U\bC))E|
2021-09-27 18:34:12 UTC	1802	IN	Data Raw: 9c 7b d9 42 6e 79 ed 6a 24 96 32 05 47 96 00 97 1f b8 13 4f 59 02 f3 25 78 2a 8d 86 5c 1d cf d1 a8 f1 d0 93 e5 d1 6a 3a 5b 95 15 b0 a1 e6 48 1f 36 ca 12 aa ec 7b 7a 56 52 20 cc bc 68 2d 4b e4 b0 1c 2e 96 90 ab 2a c0 57 32 51 97 1e 7f cf 92 82 54 41 8d 9a 7b 8d 44 96 02 00 d7 7f 40 f4 01 3f cd 25 2f ee cd 27 1c b9 98 bf 7a e2 2a 73 54 35 4f e7 70 56 96 ff a2 c9 8c 7b 8d 60 9e 08 17 9c 99 37 c0 f4 10 98 81 ae e8 46 e8 69 d9 3c 89 7f 94 b3 67 14 10 30 7d e3 3c 89 4c 86 e0 1e 5f e8 21 c2 64 08 ee c0 5a 9e 42 84 26 34 ed d2 97 c9 f5 d0 58 00 de a4 26 cb 9d e6 cb 13 59 4e 9e 0f 17 07 4f 39 23 e3 4e ac 70 84 5e 4c 97 50 a1 4f e6 cf 19 f7 61 de f7 82 48 3c 1d 4e 8e 00 ba ac c6 93 21 b8 cd 19 e1 80 1b fd b1 cb cf c0 db 28 74 62 1e f9 62 56 a7 0a 80 96 8a f4 a8 1d Data Ascii: {Bnyj$2GOY%x*\j:[H6{zVR h-K.*W2QTA{D@?%/'z*sT5OpV{`7Fi<g0}<L_!dZB&4X&YNO9#Np^LPOaH<N!(tbbV
2021-09-27 18:34:12 UTC	1803	IN	Data Raw: 5d 9c cb b6 51 ff a8 01 77 99 a8 4b 2e 55 20 40 d8 0c 68 f2 23 e9 df f6 85 10 9c 4c 0d a0 46 00 53 04 96 6b 99 8a dd a6 2c 5d b1 d3 9b b8 8c 45 45 2b 2b f1 49 c6 c5 fa 6f 2c 2d 51 63 72 72 15 67 49 c5 4a 51 ea 4c 1f 90 42 a9 67 59 1e 74 9a 96 65 99 4a 64 7f 65 95 7c d6 a0 b6 01 04 f2 02 c0 86 e1 a1 78 1f 3e 5b 83 4d fd b0 05 37 fb ae 6b ba be 6d 50 8b 42 44 79 f8 82 15 09 41 e5 5b 26 45 b2 6a 6a 61 8e c4 10 c5 f0 e4 e4 44 6a b2 02 b8 df f3 1d 68 32 60 04 5b a9 c6 77 0d ca 56 fb f8 2d e4 2d 20 26 82 Data Ascii:]QwK.U @h#LFSk,]EE++Io,-QcrrgIJQLBgYteJde|x>[M7kmPBDyA[&EjjaDjh2`[wV-- &
2021-09-27 18:34:12 UTC	1803	IN	Data Raw: 07 ff 06 d8 4d a0 d9 76 7f e7 37 21 61 c3 f6 a6 81 e3 3a 81 15 70 67 29 46 e9 23 ce d2 ac 39 ab 63 9b d4 86 7e 00 35 b5 2c ec 55 59 e1 32 de 8a 3d c9 15 f0 0c f2 c6 c7 87 e9 c2 92 41 60 1d 4a cc 00 1a ab fa 61 9b 02 ee 02 60 b5 07 9b 02 ae 5d 8d 8f 7e 7c 59 97 55 4c fe 90 94 15 93 67 91 48 0d f0 16 2b ff f0 a9 d1 c6 ad 61 18 34 30 79 0a 9a 2a 90 de 6d d2 06 dd 97 31 59 c6 cf 49 46 58 b5 02 3c 92 92 6b a7 cc ab a4 c5 38 f8 11 19 65 2b ee cc 27 ce 8a 18 61 29 f8 40 0c 1b 11 81 94 a4 14 cf 14 f2 51 09 ed 12 78 8f 89 cc 95 8c 55 08 85 92 9f 62 55 e3 6a ae 17 3c 26 12 63 7b 40 04 12 6f e3 22 6b 76 dc f8 fe 98 6c 81 14 32 2c 56 31 79 61 c5 e3 ba 58 ed 7e 47 b0 48 5c e1 9f 24 c5 8e eb 73 20 83 13 be 03 99 b7 2b 92 c6 79 2c ad 47 84 5d 9d c7 e7 a4 24 0d 33 c9 24 Data Ascii: Mv7!a:pg)F#9c~5,UY2=A`Ja`]~|YULgH+a40y*m1YIFX<k8e+'a)@QxUbUj<&c{@o"kvl2,V1yaX~GH\$s +y,G]3
2021-09-27 18:34:12 UTC	1804	IN	Data Raw: ea 62 bb 11 02 36 9f 32 9b b6 03 56 83 b8 71 d4 31 47 1b b2 f7 19 64 3d 20 bc 47 c7 08 a6 f4 84 df e4 bf f5 84 48 dd fc 6f 37 20 72 1d df 09 50 1c 5d 03 55 08 79 8c 62 a4 34 d3 92 f6 88 76 d7 75 0d 74 dc 7e 00 16 63 82 80 52 8d 6b 04 2b 78 ad e9 52 d2 c4 b3 1b a0 96 7a 96 15 a0 ac 22 a2 fc 80 2a 2e 9a 6f 1b e4 fc 44 c2 6d 03 a2 d5 5e 7a 28 19 0e 26 be 6d 18 18 ab 52 10 2d 12 7e d1 5f 08 e8 aa 03 72 97 d7 23 7c 13 54 b9 35 23 7a 86 75 e3 72 d7 57 21 44 b2 4d dd 08 70 0a d0 0e 27 94 ca e6 21 d4 3b 10 e1 9a f8 72 6c 68 d5 9d 15 ab c9 3c 7a 9c 06 af 1f e2 ba 19 d4 b5 3a 9c 8d d4 a4 1f 5d 85 64 8e a8 50 9e 0b fa cc f9 3e 6a 2f 08 b5 52 0f 22 2e b1 6c d2 3a 93 0e f3 0c 84 14 12 8a 02 0a e0 31 0a 87 2b cc aa d5 ad f3 c9 db b6 e1 db ef b5 61 82 d7 ae 60 a6 34 dd Data Ascii: b62Vq1Gd= GHo7 rP]Uyb4vut~cRk+xRz"*.oDm^z(&mR-~_r#|T5#zurW!DMp'!;rlh<z:]dP>j/R".l:1+a`4
2021-09-27 18:34:12 UTC	1806	IN	Data Raw: b7 82 f9 70 00 aa 70 7d 3d b8 18 68 6c a2 bb 8d d3 e9 ea 0f a6 bd 70 d2 e7 9e 3a 1f 4c 6e 42 5d 2a ea 2e 7c 75 ba ce 07 c3 a8 2e 2f 0b 64 f6 50 03 3e ba 41 99 4e 51 ad a3 03 e4 35 9d b1 4e c5 30 54 e9 97 fa f6 97 4e 72 74 a5 96 78 f5 9d 19 9d e4 24 e2 05 56 73 6e dd bd a6 4e 41 87 b8 ee 8d a6 2e f1 3a d5 94 5a aa 61 e7 9d 0a 74 f8 a0 bb b1 e8 54 30 9d 23 53 d5 6a a8 eb b9 74 3a 6a 3e 74 36 bf 58 8c 26 8b 88 13 1b 35 1c d5 17 04 3a 15 f1 f8 1e dd 46 2a 11 d6 bc 0c dd a9 e4 3c 0a 67 73 60 15 27 7c 91 a6 ea aa 37 cb 9d aa 00 15 6a 50 eb 5e 14 eb d4 00 e2 fa 17 54 1f e4 69 17 78 e9 de d7 d3 a9 13 f8 f5 4e 5d d5 dc 4f 76 eb 39 9f 44 d1 2f 2a 98 e9 5e 98 ef 56 a2 2b ce 9a 77 16 df 51 30 81 af d4 83 a8 77 a4 dd 2a fe 12 4d ae 54 42 a0 99 6c 75 ab e8 40 08 dd eb Data Ascii: pp}=hlp:LnB]*.|u./dP>ANQ5N0TNrtx$VsnNA.:ZatT0#Sjt:j>t6X&5:F*<gs`|7jP^TixN]Ov9D/*^V+wQ0w*MTBlu@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49766	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	55	OUT	GET /ca/restor/assets/styles.css HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	79	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:20:22 GMT ETag: "7e64-5c26847e30180" Accept-Ranges: bytes Content-Length: 32356 Vary: Accept-Encoding Connection: close Content-Type: text/css
2021-09-27 18:33:59 UTC	127	IN	Data Raw: 2a 2c 3a 61 66 74 65 72 2c 3a 62 65 66 6f 72 65 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 69 6e 68 65 72 69 74 7d 68 74 6d 6c 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 7d 62 6f 64 79 2c 68 74 6d 6c 7b 68 65 69 67 68 74 3a 31 30 30 25 7d 2e 67 2d 72 6f 77 2c 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 7d 2e 67 2d 72 6f 77 7b 77 69 64 74 68 3a 31 30 30 25 3b 6d 61 78 2d 77 69 64 74 68 3a 6e 6f 6e 65 7d 2e 67 2d 72 6f 77 3a 61 66 74 65 72 2c 2e 67 2d 72 6f 77 3a 62 65 66 6f 72 65 7b 63 6f 6e 74 65 6e 74 3a 22 22 3b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 7d 2e 67 2d 72 6f 77 3a 61 66 74 65 72 7b 63 6c 65 61 72 3a 62 6f 74 68 7d 2e 67 2d 72 6f 77 20 2e 67 2d 72 6f 77 7b 6d 61 72 67 69 6e 3a 30 20 2d 31 36 70 78 3b 77 69 64 74 68 3a 61 75 74 6f 7d Data Ascii: *,:after,:before{box-sizing:inherit}html{box-sizing:border-box}body,html{height:100%}.g-row,body{margin:0}.g-row{width:100%;max-width:none}.g-row:after,.g-row:before{content:"";display:table}.g-row:after{clear:both}.g-row .g-row{margin:0 -16px;width:auto}
2021-09-27 18:33:59 UTC	208	IN	Data Raw: 2d 74 6f 70 3a 32 70 78 20 73 6f 6c 69 64 20 74 72 61 6e 73 70 61 72 65 6e 74 7d 2e 74 61 62 2d 6c 69 73 74 5f 5f 69 74 65 6d 20 2e 62 75 74 74 6f 6e 7b 77 69 64 74 68 3a 31 30 30 25 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 33 2e 37 35 72 65 6d 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 32 35 72 65 6d 7d 2e 74 61 62 2d 6c 69 73 74 5f 5f 69 74 65 6d 2d 2d 61 63 74 69 76 65 7b 62 6f 72 64 65 72 2d 74 6f 70 3a 32 70 78 20 73 6f 6c 69 64 20 23 63 61 32 36 31 61 7d 2e 74 61 62 2d 6c 69 73 74 5f 5f 69 74 65 6d 2d 2d 61 63 74 69 76 65 20 2e 62 75 74 74 6f 6e 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 35 30 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 7d 40 2d 77 65 62 6b 69 74 2d 6b 65 79 66 72 61 6d 65 73 20 74 61 62 2d 70 61 6e 65 6c Data Ascii: -top:2px solid transparent}.tab-list__item .button{width:100%;line-height:3.75rem;font-size:1.25rem}.tab-list__item--active{border-top:2px solid #ca261a}.tab-list__item--active .button{font-weight:500;text-decoration:underline}@-webkit-keyframes tab-panel

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49767	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	56	OUT	GET /ca/restor/assets/jquery.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:33:59 UTC	79	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 18:33:59 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Sun, 16 May 2021 01:30:50 GMT ETag: "1b16c-5c2686d518680" Accept-Ranges: bytes Content-Length: 110956 Vary: Accept-Encoding Connection: close Content-Type: application/javascript
2021-09-27 18:33:59 UTC	143	IN	Data Raw: 2f 2a 21 20 6a 51 75 65 72 79 20 76 33 2e 35 2e 31 20 7c 20 28 63 29 20 4a 53 20 46 6f 75 6e 64 61 74 69 6f 6e 20 61 6e 64 20 6f 74 68 65 72 20 63 6f 6e 74 72 69 62 75 74 6f 72 73 20 7c 20 6a 71 75 65 72 79 2e 6f 72 67 2f 6c 69 63 65 6e 73 65 20 2a 2f 0a 21 66 75 6e 63 74 69 6f 6e 28 65 2c 74 29 7b 22 75 73 65 20 73 74 72 69 63 74 22 3b 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 26 26 22 6f 62 6a 65 63 74 22 3d 3d 74 79 70 65 6f 66 20 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3f 6d 6f 64 75 6c 65 2e 65 78 70 6f 72 74 73 3d 65 2e 64 6f 63 75 6d 65 6e 74 3f 74 28 65 2c 21 30 29 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 69 66 28 21 65 2e 64 6f 63 75 6d 65 6e 74 29 74 68 72 6f 77 20 6e 65 77 20 45 72 72 6f 72 28 22 6a 51 75 65 72 79 20 Data Ascii: /*! jQuery v3.5.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery
2021-09-27 18:33:59 UTC	223	IN	Data Raw: 61 3d 65 29 5b 53 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 61 2e 75 6e 69 71 75 65 49 44 5d 7c 7c 28 6f 5b 61 2e 75 6e 69 71 75 65 49 44 5d 3d 7b 7d 29 29 5b 68 5d 7c 7c 5b 5d 29 5b 30 5d 3d 3d 3d 6b 26 26 72 5b 31 5d 29 2c 21 31 3d 3d 3d 64 29 77 68 69 6c 65 28 61 3d 2b 2b 73 26 26 61 26 26 61 5b 6c 5d 7c 7c 28 64 3d 73 3d 30 29 7c 7c 75 2e 70 6f 70 28 29 29 69 66 28 28 78 3f 61 2e 6e 6f 64 65 4e 61 6d 65 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 3d 3d 66 3a 31 3d 3d 3d 61 2e 6e 6f 64 65 54 79 70 65 29 26 26 2b 2b 64 26 26 28 70 26 26 28 28 69 3d 28 6f 3d 61 5b 5d 7c 7c 28 61 5b 53 5d 3d 7b 7d 29 29 5b 68 5d 3d 5b 6b 2c 64 5d 29 2c 61 3d 3d 3d 65 29 Data Ascii: a=e)[S]||(a[S]={}))[a.uniqueID]||(o[a.uniqueID]={}))[h]||[])[0]===k&&r[1]),!1===d)while(a=++s&&a&&a[l]||(d=s=0)||u.pop())if((x?a.nodeName.toLowerCase()===f:1===a.nodeType)&&++d&&(p&&((i=(o=a[S]||(a[S]={}))[a.uniqueID]||(o[a.uniqueID]={}))[h]=[k,d]),a===e)

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	287	IN	Data Raw: 7b 72 65 74 75 72 6e 20 31 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 39 3d 3d 3d 65 2e 6e 6f 64 65 54 79 70 65 7c 7c 21 2b 65 2e 6e 6f 64 65 54 79 70 65 7d 3b 66 75 6e 63 74 69 6f 6e 20 47 28 29 7b 74 68 69 73 2e 65 78 70 61 6e 64 6f 3d 53 2e 65 78 70 61 6e 64 6f 2b 47 2e 75 69 64 2b 2b 7d 47 2e 75 69 64 3d 31 2c 47 2e 70 72 6f 74 6f 74 79 70 65 3d 7b 63 61 63 68 65 3a 66 75 6e 63 74 69 6f 6e 28 65 29 7b 76 61 72 20 74 3d 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3b 72 65 74 75 72 6e 20 74 7c 7c 28 74 3d 7b 7d 2c 56 28 65 29 26 26 28 65 2e 6e 6f 64 65 54 79 70 65 3f 65 5b 74 68 69 73 2e 65 78 70 61 6e 64 6f 5d 3d 74 3a 4f 62 6a 65 63 74 2e 64 65 66 69 6e 65 50 72 6f 70 65 72 74 79 28 65 2c 74 68 69 73 2e 65 78 70 61 6e 64 6f 2c 7b 76 61 6c 75 65 3a Data Ascii: {return 1===e.nodeType||9===e.nodeType||!+e.nodeType};function G(){this.expando=S.expando+G.uid++}G.uid=1,G.prototype={cache:function(e){var t=e[this.expando];return t||(t={},V(e)&&(e.nodeType?e[this.expando]=t:Object.defineProperty(e,this.expando,{value:
2021-09-27 18:34:00 UTC	352	IN	Data Raw: 28 73 2e 74 79 70 65 29 3f 75 2e 63 68 65 63 6b 65 64 3d 73 2e 63 68 65 63 6b 65 64 3a 22 69 6e 70 75 74 22 21 3d 3d 6c 26 26 22 74 65 78 74 61 72 65 61 22 21 3d 3d 6c 7c 7c 28 75 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 3d 73 2e 64 65 66 61 75 6c 74 56 61 6c 75 65 29 3b 69 66 28 74 29 69 66 28 6e 29 66 6f 72 28 6f 3d 6f 7c 7c 76 65 28 65 29 2c 61 3d 61 7c 7c 76 65 28 63 29 2c 72 3d 30 2c 69 3d 6f 2e 6c 65 6e 67 74 68 3b 72 3c 69 3b 72 2b 2b 29 4f 65 28 6f 5b 72 5d 2c 61 5b 72 5d 29 3b 65 6c 73 65 20 4f 65 28 65 2c 63 29 3b 72 65 74 75 72 6e 20 30 3c 28 61 3d 76 65 28 63 2c 22 73 63 72 69 70 74 22 29 29 2e 6c 65 6e 67 74 68 26 26 79 65 28 61 2c 21 66 26 26 76 65 28 65 2c 22 73 63 72 69 70 74 22 29 29 2c 63 7d 2c 63 6c 65 61 6e 44 61 74 61 3a 66 75 6e 63 74 Data Ascii: (s.type)?u.checked=s.checked:"input"!==l&&"textarea"!==l||(u.defaultValue=s.defaultValue);if(t)if(n)for(o=o||ve(e),a=a||ve(c),r=0,i=o.length;r<i;r++)Oe(o[r],a[r]);else Oe(e,c);return 0<(a=ve(c,"script")).length&&ye(a,!f&&ve(e,"script")),c},cleanData:funct
2021-09-27 18:34:00 UTC	400	IN	Data Raw: 6e 64 28 7b 61 74 74 72 3a 66 75 6e 63 74 69 6f 6e 28 65 2c 74 2c 6e 29 7b 76 61 72 20 72 2c 69 2c 6f 3d 65 2e 6e 6f 64 65 54 79 70 65 3b 69 66 28 33 21 3d 3d 6f 26 26 38 21 3d 3d 6f 26 26 32 21 3d 3d 6f 29 72 65 74 75 72 6e 22 75 6e 64 65 66 69 6e 65 64 22 3d 3d 74 79 70 65 6f 66 20 65 2e 67 65 74 41 74 74 72 69 62 75 74 65 3f 53 2e 70 72 6f 70 28 65 2c 74 2c 6e 29 3a 28 31 3d 3d 3d 6f 26 26 53 2e 69 73 58 4d 4c 44 6f 63 28 65 29 7c 7c 28 69 3d 53 2e 61 74 74 72 48 6f 6f 6b 73 5b 74 2e 74 6f 4c 6f 77 65 72 43 61 73 65 28 29 5d 7c 7c 28 53 2e 65 78 70 72 2e 6d 61 74 63 68 2e 62 6f 6f 6c 2e 74 65 73 74 28 74 29 3f 70 74 3a 76 6f 69 64 20 30 29 29 2c 76 6f 69 64 20 30 21 3d 3d 6e 3f 6e 75 6c 6c 3d 3d 3d 6e 3f 76 6f 69 64 20 53 2e 72 65 6d 6f 76 65 41 74 74 Data Ascii: nd({attr:function(e,t,n){var r,i,o=e.nodeType;if(3!==o&&8!==o&&2!==o)return"undefined"==typeof e.getAttribute?S.prop(e,t,n):(1===o&&S.isXMLDoc(e)||(i=S.attrHooks[t.toLowerCase()]||(S.expr.match.bool.test(t)?pt:void 0)),void 0!==n?null===n?void S.removeAtt
2021-09-27 18:34:00 UTC	432	IN	Data Raw: 20 69 2e 78 68 72 46 69 65 6c 64 73 29 72 5b 6e 5d 3d 69 2e 78 68 72 46 69 65 6c 64 73 5b 6e 5d 3b 66 6f 72 28 6e 20 69 6e 20 69 2e 6d 69 6d 65 54 79 70 65 26 26 72 2e 6f 76 65 72 72 69 64 65 4d 69 6d 65 54 79 70 65 26 26 72 2e 6f 76 65 72 72 69 64 65 4d 69 6d 65 54 79 70 65 28 69 2e 6d 69 6d 65 54 79 70 65 29 2c 69 2e 63 72 6f 73 73 44 6f 6d 61 69 6e 7c 65 5b 22 58 2d 52 65 71 75 65 73 74 65 64 2d 57 69 74 68 22 5d 7c 7c 28 65 5b 22 58 2d 52 65 71 75 65 73 74 65 64 2d 57 69 74 68 22 5d 3d 22 58 4d 4c 48 74 74 70 52 65 71 75 65 73 74 22 29 2c 65 29 72 2e 73 65 74 52 65 71 75 65 73 74 48 65 61 64 65 72 28 6e 2c 65 5b 6e 5d 29 3b 6f 3d 66 75 6e 63 74 69 6f 6e 28 65 29 7b 72 65 74 75 72 6e 20 66 75 6e 63 74 69 6f 6e 28 29 7b 6f 26 26 28 6f 3d 61 3d 72 2e Data Ascii: i.xhrFields)r[n]=i.xhrFields[n];for(n in i.mimeType&&r.overrideMimeType&&r.overrideMimeType(i.mimeType),i.crossDomain||e["X-Requested-With"]||(e["X-Requested-With"]="XMLHttpRequest"),e)r.setRequestHeader(n,e[n]);o=function(e){return function(){o&&(o=a=r.
2021-09-27 18:34:00 UTC	497	IN	Data Raw: 61 74 65 64 22 29 7d 7d 3b 76 61 72 20 4d 3d 61 2e 66 6e 2e 61 6e 64 53 65 6c 66 7c 7c 61 2e 66 6e 2e 61 64 64 42 61 63 6b 2c 4e 3d 61 2e 66 6e 2e 66 69 6e 64 3b 69 66 28 61 2e 66 6e 2e 61 6e 64 53 65 6c 66 3d 66 75 6e 63 74 69 6f 6e 28 29 7b 72 65 74 75 72 6e 20 64 28 22 6a 51 75 65 72 79 2e 66 6e 2e 61 6e 64 53 65 6c 66 28 29 20 72 65 70 6c 61 63 65 64 20 62 79 20 6a 51 75 65 72 79 2e 66 6e 2e 61 64 64 42 61 63 6b 28 29 22 29 2c 4d 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 7d 2c 61 2e 66 6e 2e 66 69 6e 64 3d 66 75 6e 63 74 69 6f 6e 28 61 29 7b 76 61 72 20 62 3d 4e 2e 61 70 70 6c 79 28 74 68 69 73 2c 61 72 67 75 6d 65 6e 74 73 29 3b 72 65 74 75 72 6e 20 62 2e 63 6f 6e 74 65 78 74 3d 74 68 69 73 2e 63 6f 6e 74 65 78 74 2c 62 2e 73 Data Ascii: ated")}};var M=a.fn.andSelf||a.fn.addBack,N=a.fn.find;if(a.fn.andSelf=function(){return d("jQuery.fn.andSelf() replaced by jQuery.fn.addBack()"),M.apply(this,arguments)},a.fn.find=function(a){var b=N.apply(this,arguments);return b.context=this.context,b.s

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49768	167.172.159.206	443	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:33:59 UTC	207	OUT	GET /ca/restor/assets/api.js.download HTTP/1.1 Host: www.joyeriasosa.com.py 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://www.joyeriasosa.com.py/ca/restor/index.php?id=40382411219 Accept-Encoding: gzip, deflate, br Accept-Language: en-US,en;q=0.9
2021-09-27 18:34:00 UTC	351	IN	HTTP/1.1 404 Not Found Date: Mon, 27 Sep 2021 18:34:00 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 285 Connection: close Content-Type: text/html; charset=iso-8859-1

Timestamp	kBytes transferred	Direction	Data
2021-09-27 18:34:00 UTC	352	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6a 6f 79 65 72 69 61 73 6f 73 61 2e 63 6f 6d 2e 70 79 20 50 6f 72 74 Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.joyeriasosa.com.py Port

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: chrome.exe PID: 6316 Parent PID: 488

General

Start time:	20:33:53
Start date:	27/09/2021
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://www.joyeriasosa.com.py/ca/'
Imagebase:	0x7ff68b0a0000
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

Key Value Modified

Analysis Process: chrome.exe PID: 2964 Parent PID: 6316

General

Start time:	20:33:54
Start date:	27/09/2021

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=1616,3579062385751043411,7070705701747647181,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1676 /prefetch:8
Imagebase:	0x7ff68b0a0000
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

Analysis Process: chrome.exe PID: 7096 Parent PID: 6316

General

Start time:	20:35:05
Start date:	27/09/2021
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=audio.mojom.AudioService --field-trial-handle=1616,3579062385751043411,707075701747647181,131072 --lang=en-US --service-sandbox-type=audio --enable-audio-service-sandbox --mojo-platform-channel-handle=6564 /prefetch:8
Imagebase:	0x7ff68b0a0000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: chrome.exe PID: 8184 Parent PID: 6316

General

Start time:	20:35:06
Start date:	27/09/2021
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=video_capture.mojom.VideoCaptureService --field-trial-handle=1616,3579062385751043411,707075701747647181,131072 --lang=en-US --service-sandbox-type=video_capture --enable-audio-service-sandbox --mojo-platform-channel-handle=6112 /prefetch:8
Imagebase:	0x7ff68b0a0000
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