ID: 458184
Cookbook: browseurl.jbs
Time: 00:10:01
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

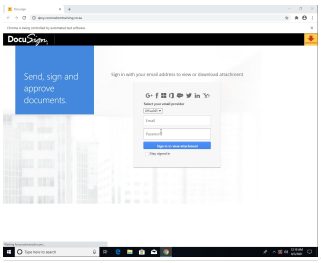
Windows Analysis Report http://axxy.coronationtraining…

Overview

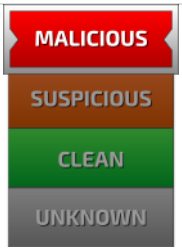
General Information

Sample URL:	http://axxy.coronationtraining.co.za/
Analysis ID:	458184
Infos:	

Most interesting Screenshot:



Detection



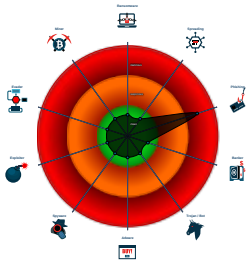
HTMLPhisher

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Phishing site detected (based on fav…
- Yara detected HtmlPhish7
- HTML body contains low number of …
- HTML title does not match URL
- None HTTPS page querying sensitiv…

Classification



Process Tree

- **System is w10x64**
- chrome.exe (PID: 4580 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --start-maximized --enable-automation 'http://axxy.coronationtraining.co.za/' MD5: C139654B5C1438A95B321BB01AD63EF6)
  - chrome.exe (PID: 464 cmdline: 'C:\Program Files\Google\Chrome\Application\chrome.exe' --type=utility --utility-sub-type=network.mojom.NetworkService --field-trial-handle=1644,5355613373542644251,6732772637902819495,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /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

Multi AV Scanner detection for submitted file

Phishing:

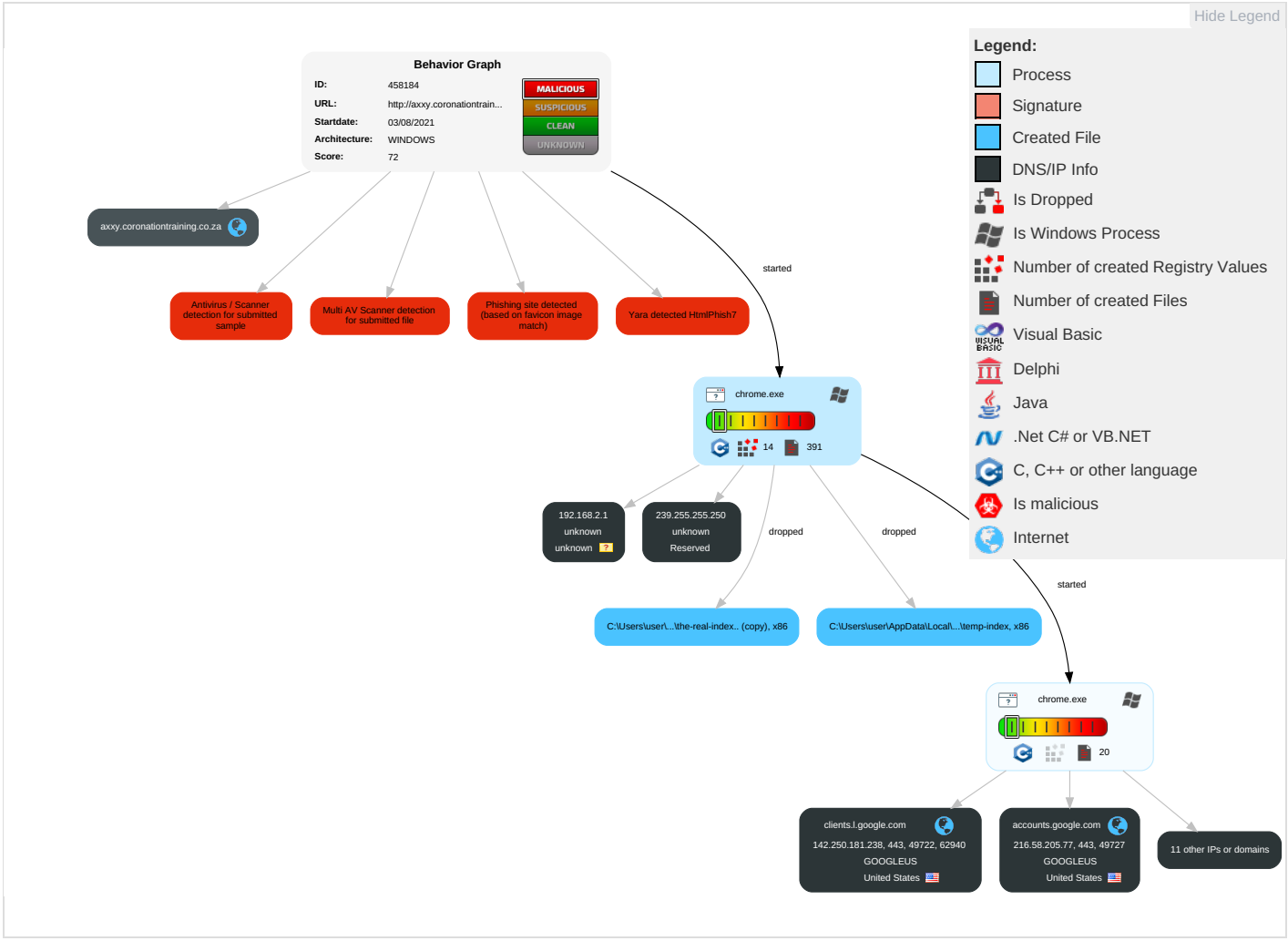
Phishing site detected (based on favicon image match)

Yara detected HtmlPhish7

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	Impa
Valid Accounts	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 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 3	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 4	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 3	SIM Card Swap		Carri Billin Fraud

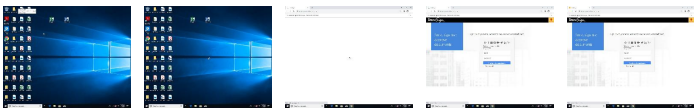
Behavior Graph

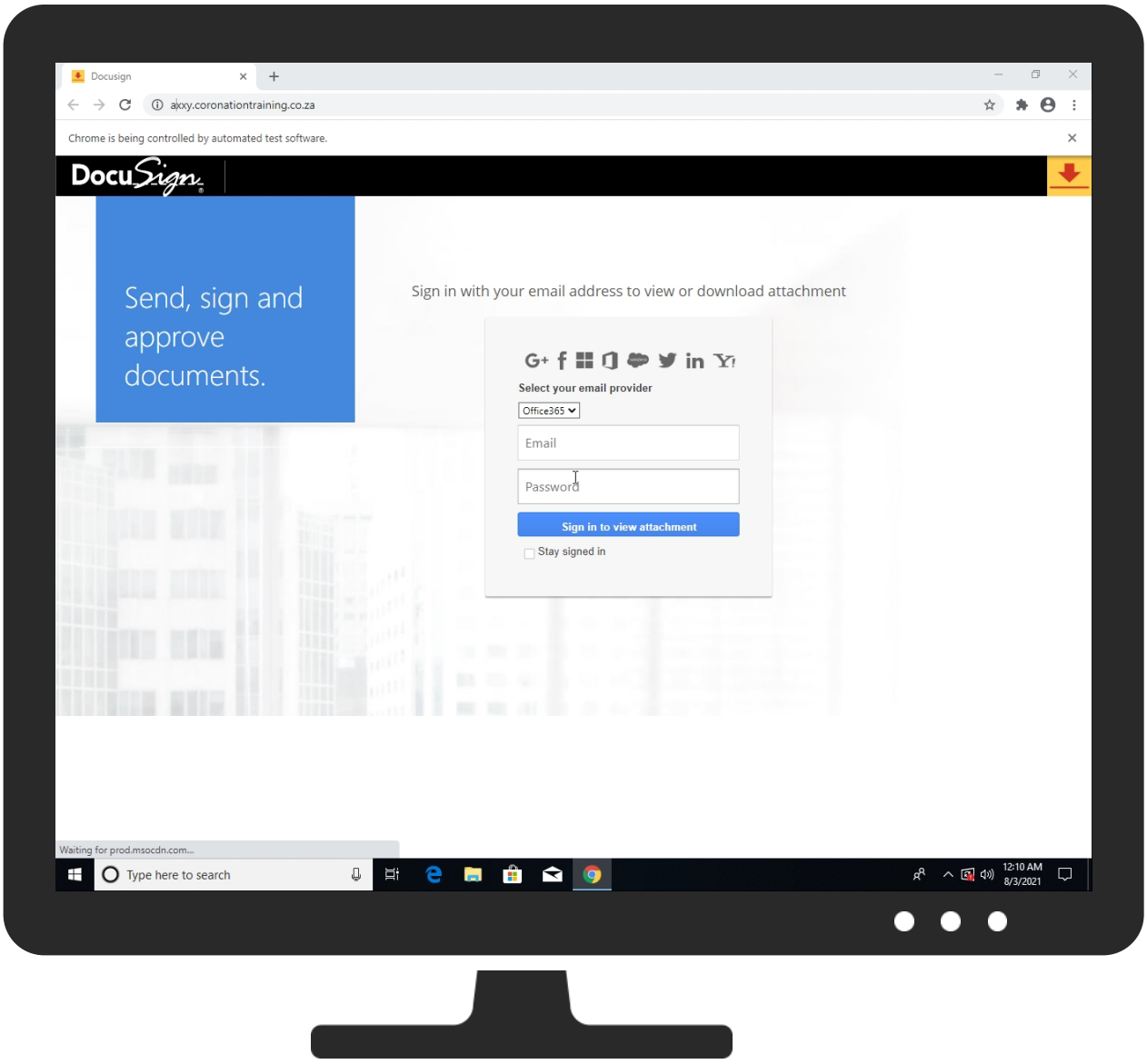


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://axxy.coronationtraining.co.za/	10%	Virustotal		Browse
http://axxy.coronationtraining.co.za/	100%	Avira URL Cloud	phishing	
http://axxy.coronationtraining.co.za/	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
prod.msocdn.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://dns.google	0%	URL Reputation	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/IdentityListAccountsHttp/external	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
accounts.google.com	216.58.205.77	true	false		high
clients.l.google.com	142.250.181.238	true	false		high
axxy.coronationtraining.co.za	154.0.167.80	true	false		high
googlehosted.l.googleusercontent.com	216.58.208.129	true	false		high
clients2.googleusercontent.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
g.microsoftonline.com	unknown	unknown	false		high
prod.msocdn.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
portal.office.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://axxy.coronationtraining.co.za/assets/cJZKeOuBrn4kERxqtaUH3T8E0i7KZn-EPnyo3HZu7kw.woff	false		high
http://axxy.coronationtraining.co.za/css/shellg2corecss_11377998.css	false		high
http://axxy.coronationtraining.co.za/css/shellg2coremincss_ba45585d.css	false		high
http://axxy.coronationtraining.co.za/assets/SpryValidationTextField.css	false		high
http://axxy.coronationtraining.co.za/css/GeminiHomeV2.css	false		high
http://axxy.coronationtraining.co.za/assets/jquery.ddslick.min.js	false		high
http://axxy.coronationtraining.co.za/assets/SpryValidationPassword.js	false		high
http://axxy.coronationtraining.co.za/css/AppTile.css	false		high
http://axxy.coronationtraining.co.za/css/shellttficons_9739c58c.ttf	false		high
http://axxy.coronationtraining.co.za/16.00.1279.006/en-US/css/Fabric/0.10.3/fonts/office365icons.woff?	false		high
http://axxy.coronationtraining.co.za/css/shellg2pluscss_baae2042.css	false		high
http://axxy.coronationtraining.co.za/images/apple-touch-icon-72x72.png	false		high
http://axxy.coronationtraining.co.za/assets/jquery.min.js	false		high
http://axxy.coronationtraining.co.za/assets/SpryValidationPassword.css	false		high
http://axxy.coronationtraining.co.za/css/conciergehelper.css	false		high
http://axxy.coronationtraining.co.za/css/data.css	false		high
http://axxy.coronationtraining.co.za/assets/SpryValidationTextField.js	false		high
http://axxy.coronationtraining.co.za/css/shellwofficons_f991c945.woff	false		high
http://axxy.coronationtraining.co.za/	false		high
http://axxy.coronationtraining.co.za/css/home_bkgd_1.png	false		high
http://axxy.coronationtraining.co.za/images/social_auth_providers.png	false		high
http://axxy.coronationtraining.co.za/css/MasterStyles15.css	false		high
http://axxy.coronationtraining.co.za/images/favicon.ico	false		high
http://axxy.coronationtraining.co.za/css/MasterStyles15MVC.css	false		high
http://axxy.coronationtraining.co.za/images/docusign.png	false		high
http://axxy.coronationtraining.co.za/	false		high
http://axxy.coronationtraining.co.za/16.00.1279.006/en-US/css/Fabric/0.10.3/fonts/office365icons.ttf?	false		high
http://axxy.coronationtraining.co.za/css/EmbeddedFonts.css	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.0.167.80	axxy.coronationtraining.co.za	South Africa		37611	AfrihostZA	false
216.58.205.77	accounts.google.com	United States		15169	GOOGLEUS	false
142.250.181.238	clients.l.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
216.58.208.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458184
Start date:	03.08.2021
Start time:	00:10:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://axxy.coronationtraining.co.za/
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.phis.win@28/205@8/7
Cookbook Comments:	• Adjust boot time • Enable AMSI
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\2a523636-3ce8-4d79-af25-721cc5ebe05f.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):	174256
Entropy (8bit):	6.079376785388877
Encrypted:	false
SSDEEP:	3072:SRoicfpuYAZ20//XkjhbEkzrw7zFcbXafIB0u1GOJmA3iuRJ:wolpUubUVaqfIlUOoSiuRJ
MD5:	3DE851B02D497DA656CBD877098C2D5C
SHA1:	A7553DC974ADFF392CA013DCC6405478BBB77214
SHA-256:	D2F047C783D326BF83A880146D35BB162363B7FE3AC1BA17622FF71A6CAF6701
SHA-512:	BB598F0CE0EA4CC30D9AACF0490BB0BE771011500105727731D7685639E8FC7DF1CA8D8A634A3A9968ACECCB2CAC88317813299DEFC6F15C64BBFC9DEC9FBC75
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":1.627974651143864e+12,"network":1.627942253e+12,"ticks":3985466743.0,"uncertainty":4717828.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016056515"},"plugins":{"metadata":{"adobe-flash-player":{"dis

C:\Users\user\AppData\Local\Google\Chrome\User Data\6752cf58-07ea-463f-acdf-30e7aeaca323.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):	174256
Entropy (8bit):	6.079376465747441
Encrypted:	false
SSDEEP:	3072:LRoicfpuYAZ20//XkjhbEkzrw7zFcbXafIB0u1GOJmA3iuRJ:NolpUubUVaqfIlUOoSiuRJ
MD5:	56C0A2FE1226666CD6CAD3C528317762
SHA1:	AC5E93EBFC3EF48C96ED03E42E0E339761DC91C0
SHA-256:	D1BE8C4F6EB9BDB68F7F761F6503157A0451A75784784C494709206441CC5934
SHA-512:	EC4254601BB9DD391894720D9CD9A2CE4C62DF9A3062ECCEC09B094957905FDF49FA4C2C8372DE447DFF54E60F54DEE2537E65234D9BB547776076EAD608AB0
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":1.627974651143864e+12,"network":1.627942253e+12,"ticks":3985466743.0,"uncertainty":4717828.0}},"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\9f01bc24-fd4c-4c68-ae6d-913e211e187e.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):	174256
Entropy (8bit):	6.079376924394296
Encrypted:	false
SSDEEP:	3072:LcHicfpuYAZ20//XkjhbEkzrw7zFcbXafIB0u1GOJmA3iuRJ:4HlpUubUVaqfIlUOoSiuRJ
MD5:	A6CEAFC31BC0925EE7C9098C49BA0070
SHA1:	966C4836B82D717B533862D2CF3FE434662D6E26
SHA-256:	A7BF5C1D06CE682AB51F654505E2222C01D243BE3FBAE15983E4BC665D192DD9
SHA-512:	673C32EFCAC5595FABBF5D0A7F30CE5FE797D4E3323B7B819A52B1FCCFFA79ECDE0F6BB59DD1D6079C39BC7D44D5D352F54A9DFB70460901E67C95D65816B35
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":1.627974651143864e+12,"network":1.627942253e+12,"ticks":3985466743.0,"uncertainty":4717828.0}},"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\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:	4184302DEB5009D767FECFC150F580DD57D5CF9CF3BFEB7E52C9F3340E5E6499251B9F0DFF37F0454411FED9046880E0A9204312D0212942563 72C916B8155AC
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\255b2b67-81fd-44a5-94e7-fede39dd6cc9.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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\255b2b67-81fd-44a5-94e7-fede39dd6cc9.tmp	
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\44152eb8-71a9-40c3-9fdb-554731b819fb.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):	5178
Entropy (8bit):	4.98490028910346
Encrypted:	false
SSDEEP:	96:n0C6XXMpcKILok0JCKL84nlkB1ybOTQVuwn:n0CUMpcs4KLlkBy
MD5:	CA42B8AF0D6E228B61B95166A8ECCF9F
SHA1:	F8482572AD27C83529FECA0AD7248C74D9C2C2FC
SHA-256:	B618FD238424A5688F653E720006B0AEDF829996FE64EC7D05D4D80F86E39694
SHA-512:	D88163E0CC458EC9F295A9C332DFDF68C410B37A216B795272C22DC3BA8F9CA6810FE21911100378BF519AE2A408D607699357071B7D97A9DE70DC06C98A019
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272448248367751","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\517f0c3d-f8d1-4938-a985-d7e27c28ee0d.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:L:L
MD5:	5058F1AF8388633F609CADB75A75DC9D
SHA1:	3A52CE780950D4D969792A2559CD519D7EE8C727
SHA-256:	CDB4EE2AEA69CC6A83331BBE96DC2CAA9A299D21329EFB0336FC02A82E1839A8
SHA-512:	0B61241D7C17BCBB1BAEE7094D14B7C451EFECC7FFCBD92598A0F13D313CC9EBC2A07E61F007BAF58FBF94FF9A8695BDD5CAE7CE03BBF1E94E93613A00F25 F21
Malicious:	false
Reputation:	low
Preview:	.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cdca899-913d-4fb7-a0bb-7322d94951d5.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):	5774
Entropy (8bit):	5.18349312351112
Encrypted:	false
SSDEEP:	96:n0C6kJM93I4TNSNcKILok0JCKL84nlkB1ybOTQVuwn:n0CtMxWNcs4KLlkBy
MD5:	9DD3EE4CDEDB024C12940448940002ED
SHA1:	64C32EB526A8A73A28F2E1CB38118377A76EDE10
SHA-256:	550A103FFD028F5AC76AB8D909281739587BBFEA29973DC980CBC8481D3CB936

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\6cdca899-913d-4fb7-a0bb-7322d94951d5.tmp	
SHA-512:	4F3A5F48A06574B9EC192E237B06B9365BFD6F0ADC9F713C77834B7BBCDC7214F9AA98D1070EDCC96A5916ADE43DAC773FE718C1260651D5FC987C83BF6601 8
Malicious:	false
Reputation:	low
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272448248367751","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\952f7ae2-06ae-470d-8287-196abb1be347.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:	modified
Size (bytes):	22596
Entropy (8bit):	5.536297525407854
Encrypted:	false
SSDEEP:	384:n2ngtbLl+D1Xf1kXqKf/pUZNCgVLH2HfDbrUldHG5nTj2nSJ4F:hLlif1kXqKf/pUZNCgVLH2HfXrUlBG5W
MD5:	D298FE3CE5C13E4A44BD47014294538D
SHA1:	14A394086F030704DDD78B8C184FDE01D77F618A
SHA-256:	901822E71E28B1D8E64C52AA09D29B2C940A335481AC06123E8CEF12BA4EA592
SHA-512:	21CE54057E3400ED9E796DC8AE0984379127EE75A663A3BA764177C9F54A90207FFEE4C6CE79DEB7B8E18EAFE16E47936ADA5FB4E584490823AD2CCDCA4DB(BB
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":"13272448248078036","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):	5.198686529864705
Encrypted:	false
SSDEEP:	6:mDBQKADM+q2PWXp+N23iKKdK9RXXTZIFUtpOBQyWAgZmwPOBQOADMVkwOWXp+N2v:bKADM+va5Kk7XT2FUtpryWAg/PrOADMX
MD5:	F59074C1CD9C7099E5DAF718927FFF92
SHA1:	0DD88EB3F5DA399A0AF0CB7058C430B3C4A0B043
SHA-256:	E674E7E7DC47EB8D171476F60CFEF471420158C1B1543D17E5FFB8882FE0D9C2
SHA-512:	8D4664E4ED3144AB5D25B508D4800F9720EEF73C367A23022C3B035718F37AC87E9A016EA0DCD22D45C90919D3289F07C5DB353C0885A909AA2757B2982EE15/
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.652 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-00:11:04.655 1a8c Recovering log #3.2021/08/03-00:11:04.656 1a8c 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):	5.198686529864705
Encrypted:	false
SSDEEP:	6:mDBQKADM+q2PWXp+N23iKKdK9RXXTZIFUtpOBQyWAgZmwPOBQOADMVkwOWXp+N2v:bKADM+va5Kk7XT2FUtpryWAg/PrOADMX
MD5:	F59074C1CD9C7099E5DAF718927FFF92
SHA1:	0DD88EB3F5DA399A0AF0CB7058C430B3C4A0B043
SHA-256:	E674E7E7DC47EB8D171476F60CFEF471420158C1B1543D17E5FFB8882FE0D9C2
SHA-512:	8D4664E4ED3144AB5D25B508D4800F9720EEF73C367A23022C3B035718F37AC87E9A016EA0DCD22D45C90919D3289F07C5DB353C0885A909AA2757B2982EE15/
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase\LOG.old (copy)	
Preview:	2021/08/03-00:11:04.652 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\AutofillStrikeDatabase/MANIFEST-000001.2021/08/03-00:11:04.655 1a8c Recovering log #3.2021/08/03-00:11:04.656 1a8c 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):	5.153722215067492
Encrypted:	false
SSDEEP:	6:mDBJADM+q2PWXp+N23iKKdKyDZIFUtpOBDEAgZmwPOBDEADMVkwOWXp+N23iKKdn:yADM+va5Kk02FUtpXAg/PXADMV5f5Kky
MD5:	26C929E9F1FBFF3928B8F678A1CC0CC2
SHA1:	F5BAAABAE76AE93882465AA5F43ED1400CA0457A
SHA-256:	DCEAEB5EA04939B35AC7AA932640B409417588C8946552299749EDC82F258CE5
SHA-512:	07F0C9944F9F96D7D7CAB14F87BB029333B527A7A57EA7078960352C059D41ECD459334FFF342D732D5F258F1195132B46212C5AF9AB88B6D8F160ADF9782270
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.641 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-00:11:04.642 1a8c Recovering log #3.2021/08/03-00:11:04.642 1a8c 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):	5.153722215067492
Encrypted:	false
SSDEEP:	6:mDBJADM+q2PWXp+N23iKKdKyDZIFUtpOBDEAgZmwPOBDEADMVkwOWXp+N23iKKdn:yADM+va5Kk02FUtpXAg/PXADMV5f5Kky
MD5:	26C929E9F1FBFF3928B8F678A1CC0CC2
SHA1:	F5BAAABAE76AE93882465AA5F43ED1400CA0457A
SHA-256:	DCEAEB5EA04939B35AC7AA932640B409417588C8946552299749EDC82F258CE5
SHA-512:	07F0C9944F9F96D7D7CAB14F87BB029333B527A7A57EA7078960352C059D41ECD459334FFF342D732D5F258F1195132B46212C5AF9AB88B6D8F160ADF9782270
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.641 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\BudgetDatabase/MANIFEST-000001.2021/08/03-00:11:04.642 1a8c Recovering log #3.2021/08/03-00:11:04.642 1a8c 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\1b2a36c9f1aba763_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.355888526248517
Encrypted:	false
SSDEEP:	6:mt1/Vnp3/PL1GQQWQCtN1bIA4/PL1GQQ1lSQovAhXK6t:llpnjvN1AjXo
MD5:	E76A783A67F85217077C11CEDB15EBE4
SHA1:	9EAF3CCD157B9236A708FDDC985DEFB9E64DC0AD
SHA-256:	2C88D2D8EE95A23C4F588F62AEC7EF0C2B4382ED9CB4A6179DE8E19AA99545D0
SHA-512:	138DF9D51A83AB572C6EF97EB2DB2684621BB7B8D752D0C961D464FD4706661C936CEB2F1E837B6FCC4875C1248BA02E35312E90C9B7F1D7619AC60A8FD6302
Malicious:	false
Reputation:	low
Preview:	0\r..m.....g.....Q...._keyhttp://axxy.coronationtraining.co.za/assets/jquery.ddslick.min.js .http://coronationtraining.co.za/..u.8'/.....].....e$.0.!.q...S...a..C.s<i..2..*.A..Eo.....es.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cd6e16b90a01c4c_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	240
Entropy (8bit):	5.395467438965584
Encrypted:	false

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\3cd6e16b90a01c4c_0	
SSDEEP:	6:mA7ZVnp3/PL1GQQWQtE4MdrIA4/PL1GQlISwEYZD4bhK6t:lZNpnjd4rjVBdl
MD5:	3942F40B647563C0CDCD1395CF0615A4
SHA1:	71F7020FF32BD68A71DEFBFFD9E0FAE092D3CF76
SHA-256:	5BFDBB3915E32B92240642D7B27B2C6520F5E0E0C7568117FE04826F41AFB5CA
SHA-512:	09443071E5BB7063F53A7D46F83C59348B138595CECDCFE17DB99C1122D28D9E07D2C6F3E5F4BF7EE756028607D6447960502F6E83A41AAB3F312C4331117587
Malicious:	false
Reputation:	low
Preview:	0\r..m.....l....._keyhttp://axxy.coronationtraining.co.za/assets/SpryValidationTextField.js .http://coronationtraining.co.za/.ex.8'/.....c.....d\...ud.3.bs.+".v>..hW.E..... .A..Eo.....Zs.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\64aa39824a44e548_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	227
Entropy (8bit):	5.3411369138511855
Encrypted:	false
SSDEEP:	6:mYbnp3/PL1GQQWQC3IA4/PL1GQI+lSuY4jM/lO8WnDUK6t:FDpnjujIsYMM/lTMm
MD5:	0AC831076B55A42278AEEC7D9795C0D7
SHA1:	05CBA56CDD69773DB66A48DAE1FC696B04D1B248
SHA-256:	4091C3A059EA61503FB48761C2B170445DDD53EBD95B9DDA3F76964D429307C1
SHA-512:	5B7986F5B904EA12C877F0218CCB460D3B50E0A0F04BF30A64D9707EEE46F9DF7140931FF80BBB9BC35CCED0BE599150BC5329425D3E905EE3FFB75FD8BAFB 2
Malicious:	false
Reputation:	low
Preview:	0\r..m....._....`...._keyhttp://axxy.coronationtraining.co.za/assets/jquery.min.js .http://coronationtraining.co.za/..u.8'/.....U.....~....5]o...i}.i..A.y.....0m...A..Eo..... ...M.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\a3a519bb973cf14d_0	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	239
Entropy (8bit):	5.418085737682363
Encrypted:	false
SSDEEP:	6:mU3lVnp3/PL1GQQWQtE4MVXIA4/PL1GQC+vlSI80EqIIzrnrHjron+/bK6t:p4Npnjd4hjvlDBHnnro+1
MD5:	A2DA3C2A9CAA6F702402FD3298296134
SHA1:	BDA13B248F2729B631742DFEC471CFC9DBC2EF5F
SHA-256:	7EC6648A2DCD4869329221EE800D0E0984A8D96E2E1FEF988B93CBEF78732E90
SHA-512:	D657BB4EA30E3391D62483DA9B1FCE01D3C5F4AB77414EB3D7C492BFA60182BEB8A1F87F80E06D77FBDC36FBAB8E7E41D599A801C4330A2ADFD2F6AD0EAE2 EDD
Malicious:	false
Reputation:	low
Preview:	0\r..m.....k.....}...._keyhttp://axxy.coronationtraining.co.za/assets/SpryValidationPassword.js .http://coronationtraining.co.za/.x.8'/.....k.....{...dk....I.I....4).N.....g^i..A ..Eo.....-.....A..Eo.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\temp-index	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	x86 executable not stripped
Category:	dropped
Size (bytes):	336
Entropy (8bit):	4.883406820348537
Encrypted:	false
SSDEEP:	6:7BngGLhZZmEG0eazQ3zbn3pHkQ+IRwHicE:7LLhZZmE1eazyz7V4hc
MD5:	01F732EF36EEC9EA4CE15F6301CEA0A5
SHA1:	905869D4EB59FCA51D91252606DCBB67337CA398
SHA-256:	0FF9EC27E885B47F937554B0A6B56C63A7BA9B2AD8E461F8094CF4852DDA92AF
SHA-512:	39ADA9738F08D7F9739FAB1D9E1CDD7FF834B4099CCD0933D2257FD65422ED81E6EA62CE2AED9F533DFB544B1C3FEAF0E2FC4729EEEE595755699F1653FCEF 5F
Malicious:	false
Reputation:	low
Preview:	H....g.oy retne.....M.<.....@yk.8'/.....L...k..<@yk.8'/.....c....6*.@yk.8'/.....H.DJ.9.d@yk.8'/.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../..... .....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../.....y.8'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Code Cache\js\index-dir\the-real-index.. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	x86 executable not stripped
Category:	dropped
Size (bytes):	336
Entropy (8bit):	4.883406820348537
Encrypted:	false
SSDEEP:	6:7BngGLhZZmEG0eazQ3zbn3pHkQ+IRwHicE:7LLhZZmE1eazyz7V4hc
MD5:	01F732EF36EEC9EA4CE15F6301CEA0A5
SHA1:	905869D4EB59FCA51D91252606DCBB67337CA398
SHA-256:	0FF9EC27E885B47F937554B0A6B56C63A7BA9B2AD8E461F8094CF4852DDA92AF
SHA-512:	39ADA9738F08D7F9739FAB1D9E1CDD7FF834B4099CCD0933D2257FD65422ED81E6EA62CE2AED9F533DFB544B1C3FEAF0E2FC4729EEEE595755699F1653FCEF 5F
Malicious:	false
Reputation:	low
Preview:	H....g.oy retne.....M.<.....@yk.8'/.....L...k..<@yk.8'/.....c....6*.@yk.8'/.....H.DJ.9.d@yk.8'/.....^}.Np..@ikt../.....-..0..x@ikt../...../...3.KPu../..... .....KPu../.....&<..\.O$.KPu../.....p..(....KPu../.....q....._.KPu../.....+<P|...X.KPu../.....y.8'/.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	0.6863571317626186
Encrypted:	false
SSDEEP:	12:TLyen4ufFdbXGwcFOaOndOtJRbGMNmt2SH/+eVpUHFxOUwae6:TLyqJLbXaFpEO5bNmISHn06Uwd
MD5:	1C0EAEEE6463CAE33B7A7CD9D9DF4DA5
SHA1:	FBC6A28A1501E40154FDC0A9D0C2F34A5F88AA65
SHA-256:	ED8AE7C5E6885874A39F4E86258F552670352A18D29BE1FF4D372A2F4CD06C8A
SHA-512:	355D19828609971998B09B36E7C7D304B7FB88C7A726670BEBF5CF2E2710F8E71B0F9DEF6FE9712B484C1EB122AEEEFDECF31D13E02C4539C399DFB86EC7619 F
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12836
Entropy (8bit):	0.9692845116501877
Encrypted:	false
SSDEEP:	24:zcLgAZOZD/0WqLbJLbXaFpEO5bNmISHn06Uwst8:z8NOZ3q5LLOpEO5J/Kn7Urt8
MD5:	8ED326456FA6368FA6C2CBF5BB101A7D
SHA1:	B0E5B0A03F18594E2E0B963551E12791055DE87A
SHA-256:	0EB80B4D498FAA08EE0B79C6FD3B281DDAF7D0EC2AFA0FDA1102FC70F49AB171
SHA-512:	B1D94E7EC63B7AA31242B0CAF4437E3DC6EFF22EBDCBDAF3D0B44C3913770022790C970FFEFAAFCAC90D38C87900672F329656A96E416A8F60A9B0A4DEB33C 13
Malicious:	false
Reputation:	low
Preview:	.....+..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1325
Entropy (8bit):	3.14704919987102
Encrypted:	false
SSDEEP:	24:34SFI63jFlrlAnnjpPV1XNMLqenjBP93lLlL:34ETfxenldGqenVP9VRL

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Current Session	
MD5:	787F3BEAD65088E840EF44749B06766E
SHA1:	4A59F38DEE14318A402CE083C47771EA69679E4A
SHA-256:	E2BF5DC868D8BBCE3CFFE6B77467C5112A7E90555C926772C9A2E4445AC3C6D2
SHA-512:	F74E4CCE6A6D2537F64F44B9B0E486BEFA9B198A6F894499A85221A585DA06F1E6C67FA1E4C1783F1994BCC98977A8AA61112FC5AEB7C421F20BC5B886513F6
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...3e507014_76f1_4590_9ac8_6c52434d60b8.....`a.....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....%...http://axxy.coronationtraining.co.za/.....D.o.c.u.s.i.g.n.....h.....`.....a..b....b..b....@.....X.....R...%...h.t.t.p.:././.a.x.x.y...c.o.r.o.n.a.t.i.o.n.t.r.a.i.n.i.n.g...c.o...z.a./.....8.....0.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....N.o. . o.w.n.e.r.....1.....f.i.l.e.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	164
Entropy (8bit):	4.391736045892206
Encrypted:	false
SSDEEP:	3:FQxlXayz/t2Hmwg0EOZL7Ao4uhFkEuRLKyC5Ei5+Gg:qT5z/t2qoEwhXeLKB
MD5:	0A906A9A542CDF08FF50DAAF1D1E596E
SHA1:	B97D6274196F40874A368C265799F5FA78C52893
SHA-256:	EB9CABBF5FDA1AD535300B0110EAA4068A083248BA928A631C9278545935426D
SHA-512:	8795E905B711ADE6B1C4B402D50AF491B64D157AA738669482DDBFC30E857DF970BFFB774A925F3F4A0802BD27AFAF939CE140894FF09B67FB9C0BB83ED4491A
Malicious:	false
Reputation:	low
Preview:	.f.5.....i.Wd.....Sgdaefkejpgkiemlaofpalmlakkmbjdnl.declarative_rules.declarativeContent.onPageChanged.[]..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.160820948539291
Encrypted:	false
SSDEEP:	6:mDOTFFq2PWXp+N23iKKdK8aPrqIFUtpOORFA9ZmwPOORFAPkwOWXp+N23iKKdK8h:fTXva5KkL3FUtpPjA9/PPjAP5f5KkQJ
MD5:	3FC2A6023325BCAB386359F1B0E81EC7
SHA1:	818F20CBDA104EF9CB8B345BD476DF381E188B8E
SHA-256:	121D755BE0EF70855A01BB3406BAC2FB5BCFA25B353C579F6A3C658CB0FCB1F3
SHA-512:	992DA4F70A8157EA9A20C913BF77321FC840B64C7E199B029DD9249AA219C188F8E424D6E75A90D651A60D7806C539251E0E3FD3911222E0A2EA62DF7F8388F4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.390 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-00:10:48.392 10d4 Recovering log #3.2021/08/03-00:10:48.392 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.160820948539291
Encrypted:	false
SSDEEP:	6:mDOTFFq2PWXp+N23iKKdK8aPrqIFUtpOORFA9ZmwPOORFAPkwOWXp+N23iKKdK8h:fTXva5KkL3FUtpPjA9/PPjAP5f5KkQJ
MD5:	3FC2A6023325BCAB386359F1B0E81EC7
SHA1:	818F20CBDA104EF9CB8B345BD476DF381E188B8E
SHA-256:	121D755BE0EF70855A01BB3406BAC2FB5BCFA25B353C579F6A3C658CB0FCB1F3
SHA-512:	992DA4F70A8157EA9A20C913BF77321FC840B64C7E199B029DD9249AA219C188F8E424D6E75A90D651A60D7806C539251E0E3FD3911222E0A2EA62DF7F8388F4
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.390 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/MANIFEST-000001.2021/08/03-00:10:48.392 10d4 Recovering log #3.2021/08/03-00:10:48.392 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Rules/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	570
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	6:qTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCTCT:qWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW
MD5:	D4BA0AE0BB0B9FAFF3DA6F35FDBC3C8A
SHA1:	FB3E9DEC7F35A9B1D94E54A5659DD0DE484055E7
SHA-256:	99DEF1B557F19F04C1AFFC6F247D0451F33FC10EC42E73792223C3215AC98BE6
SHA-512:	86FD07C34B9ABD4C52BA19EAE291936F92BC6D38A75C021EDC1DEDBC15617669876180CD99F959C62476D82EC6BB9F5FE4C6CB4D82CB037EFB76D99A4D3D9 51
Malicious:	false
Reputation:	low
Preview:	.f.5...............

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.141982759429901
Encrypted:	false
SSDEEP:	6:mDt6Xq2PWXp+N23iKKdK8NIFUtpOtGZmwPOt8KFkwOWXp+N23iKKdK8+eLJ:Lva5KkpFUtpV/PVG5f5KkqJ
MD5:	BDE7F2A6BCE2A25B69C8FCCBB1432886
SHA1:	629A1B499BE875E202874C329134FB7A3AE48F95
SHA-256:	865971095488BB6570B97171018C60CA0B86D4136CC3E1AA4E3D1B95719F51D8
SHA-512:	53965E63B7F533BBE903ED383BD2F57027A47BDFF928ADACB69D27D15614ECC29B6EA1398EC6AF67C4529D09420BC2377D9B733D634A9F7654E2FBB3228E49A E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:50.542 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-00:10:50.543 10d4 Recovering log #3.2021/08/03-00:10:50.544 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.oldT (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.141982759429901
Encrypted:	false
SSDEEP:	6:mDt6Xq2PWXp+N23iKKdK8NIFUtpOtGZmwPOt8KFkwOWXp+N23iKKdK8+eLJ:Lva5KkpFUtpV/PVG5f5KkqJ
MD5:	BDE7F2A6BCE2A25B69C8FCCBB1432886

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State\LOG.oldT (copy)	
SHA1:	629A1B499BE875E202874C329134FB7A3AE48F95
SHA-256:	865971095488BB6570B97171018C60CA0B86D4136CC3E1AA4E3D1B95719F51D8
SHA-512:	53965E63B7F533BBE903ED383BD2F57027A47BDFF928ADACB69D27D15614ECC29B6EA1398EC6AF67C4529D09420BC2377D9B733D634A9F7654E2FBB3228E49A E
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:50.542 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/MANIFEST-000001.2021/08/03-0 0:10:50.543 10d4 Recovering log #3.2021/08/03-00:10:50.544 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension State/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpiccmgmieda\1.0.0.6_0_metadata\comput ed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	11217
Entropy (8bit):	6.069602775336632
Encrypted:	false
SSDEEP:	192:GbylJnlTwGB7V9Hne4qasKxXItmLG48gcLg/PkI:Gb+nldByaFx4toj8VEPT
MD5:	90F880064A42B29CCFF51FE5425BF1A3
SHA1:	6A3CAE3996E9FFF653A1DDF731CED32B2BE2ACBF
SHA-256:	965203D541E442C107DBC6D5B395168123D0397559774BEAE4E5B9ABC44EF268
SHA-512:	D9CBFCD865356F19A57954F8FD952CAF3D31B354112766C41892D1EF40BD2533682D4EC3F4DA0E59A5397364F67A484B45091BA94E6C69ED18AB681403DFD3F
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["A+1PYW3V6CJbBuQ7aqrgYhyH3bT8PKyBXp3hN2slpI0=","WSOpQRkYTHjPSlG9Zif2a7TNhy43NDcG1Zg5Nv0UbH0=","jDctR8ImG5KZ rQKm4kDjUB7FokSJfjo/pmvFowRVlaY=","LPxhhJiuU0lprt0T6flpS7TkaDg7MocrbmzO65xH6RI=","nZ9zLb2By96AkKXALRM+C0Eu11XUjPiMXEKjiCPdtHE=","wifibc1QfMB N2jrtUtLgsCefvuceTpAatmLvul11RJA=","dHjWlSIIdjj7MWqg3T8MG58RuuqRXk32vqi/13JqEgA=","zd3DV7dbvfNvx1hdhU01fW5ily52DLN0CFL/ADaEeTI=","DpjXcO85FF FY9KJFPkGNfFUtdQlOsGwO5jUckiUwY14=","gqid6l1+mk/6yWgUECRofI9lMipXgXh2jEN2+CxmPE0=","prDB91X2Mmfg/M/txVMITWBmEGbOGjqBTP7CMjYqdHs=", "yLPAqV4gqoyS/zFkEt3Cn2j0q2v9QOSthVFfWn8EzCM=","EPQ3jzdrLkAHyvf3920B5Y3aAkO1IJdn/UtbnAmq6T0=","+oOc6ca+ChKUpTu+oa2ZRxRE+wG3QJmuYWE vYCs40NI=","3mBGNAiRlTANEQkqzU3TEi+5wJ0ubR5uwtS4/9OOM7w=","1A9NNawxuhu95H5eThvf1rewJ4QQWhhPNxJXO1C/n68=","E3vWLQxzmj+e5QxYbUsclIJ5 n0ITpw5JBHV1Kph3/KM=","i3I8ghdTF9c1ZXNBZmvsID+DV4gxBVN27rj9wsMtRpg=","R8B8qYabnMSlLPhrtu0hGYrHn3llsMHqBbi70gkljEE=","rhlzuEvv2KRAF Mms896xFwkNgPrw6WvmgPn6xrBSa2Y=","LAMXv6sRb0VZrY34aVXF3Fftxs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extensions\pkedcjkdefgpdelpbcmbmeomcjbeemfm\8520.615.0.5_1_metadata\c omputed_hashes.json	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	23474
Entropy (8bit):	6.059847580419268
Encrypted:	false
SSDEEP:	384:7dNc1NC6IcafusK4H1IIGRlhKlkIALQWdynQh2RX4K6M1tVztzr7XSNyzH:7dOscSRKc1nGRSkIhEw6M1tf7SNyb
MD5:	6AE2135EA4583C2F06CDEBEA4AE70FA4
SHA1:	DCEB26C7F02D53B5F214305F4C75B4A33A79CDC2
SHA-256:	03AA1944CB3C4F39E20B6361571BC45DFBEBD3FFDA3D8F148CC6ECB29958F903
SHA-512:	B5945E67D9F73DD1982D687E5C6D9B5D6B3886C8050363A259755C76AC0F93651F3425FA7C21AA6A13977AC1C8C9322F998F131648CB8909096058D4F0D23312
Malicious:	false
Reputation:	low
Preview:	{"file_hashes":[{"block_hashes":["DOZdV3jFvk12AM2JNDYKo3KZrlVRprmJ+sVGWkqqE4Q=","rVElW3Hu3T52SzDDUqGT5YiJTBGUv2h3pNuBKFlhZ1U=","X/ 3fg4KZxgQ1jBr5QGq0F5JnflgE27UErd88mrxTcxs=","VibLbpy0ig+5INMOU71fTYN76iaka2XVpmm1qAKYsX8=","EChCwCbQHbHQ7oDdGT2qNyiRJ0yck2YC2emNGq 4whtE="],"block_size":4096,"path":"_locales/iw/messages.json"},{"block_hashes":["xklkoZ7iSU1+7cd6DAtEmUC5lPFd+EgcbnzxkOiFwlk=","3KbsvoxKY/3AwqgF2aAdVQ RpMhsNVRkQ3rx2A6Z2Z+Y=","o9+tsohquaCMj+70zeinRG/hBhA2uLoDl/WoC1uokME=","xV/K8xucyWJELVT8Cqn+ugFjobBVmg8pnmACF+2PP4Y=","p/mvJm2wuCl 32Rx3it654MljKAsMe3S9IDEabc1A8mE=","j8mPrTb5oOsBTj2Fer78JE6xG6+kR64Cvu2SW8d3j/k=","nqSRpGQ3USU2bZJsZ+AzBmFOyann8omwJrhEWFZDTXc="," eTcQyJUuNuF9yCga/fXGyFCj/pysSceanhBzksdx23s=","Wj7faqnspeIXKMvnduxHn1XUBG8TEOqyns7/oUihekM=","VtBwXoadI3EP336rAiL33Gz19KGqtN+RYdKn MKAXoLw=","iDgLXQqXJp8nCZxgLuC9LXM45DGfufvGnXvmHsn18wc=","g+RfdDfrWTUK0Pkcsbot7NJ4SC9wVRV/dVVMuHAtEj8=","2oC4HcCuXu3VjFf6wnKlznt9u qQNaebcuWpm/mWj69U=","aMUIpuFqPMiieSaWhIktCK62v2P3OZQAWupWsYzCnvk=","L

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.517663567756539
Encrypted:	false
SSDEEP:	48:yBmw6fUTnvnlxBP/3hwdOhzlUaTR6s7s/nnCnV:yBCQnvnlxJpJUaTMs7WnCnV
MD5:	161B6D8C974A83D33D5D4BCC61FE9D23

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons	
SHA1:	12F5D0609CE49845D9793953694A0669F32522F5
SHA-256:	B47AEE66A46AF5565425F4022EFA38A6646D7E2BBA237E4B23245BE63C61C0E6
SHA-512:	417C704AE9ACAFD7AA4539643C7077C9D23C53991CAD4A52BBEBB057B0A65A019BAB77CA21AEE3C718217574FF13E29FD5485E44D9C38A8E073950E69D1451 2
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C.....g....._.c...~.2..... ....s...;+...indexfavicon_bitmaps_icon_idfavico

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Favicons-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	16972
Entropy (8bit):	0.7757824458256173
Encrypted:	false
SSDEEP:	24:IUfyLiXxh0GY/l1rWR1PmCx9fZjsBX+T6Uw53n:IedBmw6fU23n
MD5:	137E68A7956D3E0415493EF47DFCBF52
SHA1:	726944DA0C2A79FB2FF80160F3FAC545A13086FC
SHA-256:	27C8EF66C89977945B1A4FDCD281610CBAE61391181E54E615C37DEAFBBE3C11
SHA-512:	9889D66074A9239E6330ED390A652545CDFB1BA19EDF63C297104D4F464DE24AB79514F0956A3463F3A40BCD43115789BA61E36F40C2A7BA19EA4A8F9556D360
Malicious:	false
Reputation:	low
Preview:	.....T..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.8784775129881184
Encrypted:	false
SSDEEP:	3:FQxlX:qT
MD5:	0407B455F23E3655661BA46A574CFCA4
SHA1:	855CB7CC8EAC30458B4207614D046CB09EE3A591
SHA-256:	AB5C71347D95F319781DF230012713C7819AC0D69373E8C9A7302CAE3F9A04B7
SHA-512:	3020F7C87DC5201589FA43E03B1591ED8BEB64523B37EB3736557F3AB7D654980FB42284115A69D91DE44204CEFAB751B60466C0EF677608467DE43D41BFB939
Malicious:	false
Reputation:	low
Preview:	.f.5.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.215352755174993
Encrypted:	false
SSDEEP:	6:mDBUKADM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpOBUQsAgZmwPOBUQsADMVkwOx:fKADM+va5KkTXfchI3FUtpvQsAg/PvQ1
MD5:	18BD6EA4E2F3931AD0E0128B1E9D09F0
SHA1:	830048DFC695A301DC7ECF939892577173022589
SHA-256:	2F3037EB13C06C4D8185F64D662CC5484303F6ACD25972BEB936FF25A1AF3A15
SHA-512:	77AB81A4A78D9863F52AF778072E799FC0EC8488D8F3211B28B9E70E89C441D8DDA865E8A1BD8D890800DC235944295D0CCC39BFE79E5F3F6CDAEF7BF86F1E 2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.612 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MA NIFEST-000001.2021/08/03-00:11:04.615 1a8c Recovering log #3.2021/08/03-00:11:04.615 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB\LOG.old.7 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	372
Entropy (8bit):	5.215352755174993
Encrypted:	false
SSDEEP:	6:mDBUKADM+q2PWXp+N23iKKdK25+Xqx8chI+IFUtpOBUQsAgZmwPOBUQsADMVkwOx:fKADM+va5KkTXfchI3FUtpvQsAg/PvQ1
MD5:	18BD6EA4E2F3931AD0E0128B1E9D09F0
SHA1:	830048DFC695A301DC7ECF939892577173022589
SHA-256:	2F3037EB13C06C4D8185F64D662CC5484303F6ACD25972BEB936FF25A1AF3A15
SHA-512:	77AB81A4A78D9863F52AF778072E799FC0EC8488D8F3211B28B9E70E89C441D8DDA865E8A1BD8D890800DC235944295D0CCC39BFE79E5F3F6CDAEF7BF86F1E2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.612 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/MANIFEST-000001.2021/08/03-00:11:04.615 1a8c Recovering log #3.2021/08/03-00:11:04.615 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\AvailabilityDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.164971776705023
Encrypted:	false
SSDEEP:	6:mDBN/NADM+q2PWXp+N23iKKdK25+XuoIFUtpOBRAgZmwPOBRADMVkwOWXp+N23iM:SNADM+va5KkTXYFUtpyAg/PyADMV5f5X
MD5:	D24A9B5375D43BC3C412A0103C057B65
SHA1:	EA694D70FE0191D2D7C05B7A925260D55A0C66DB
SHA-256:	A777BCB0DD5A75F12D855252E4880C0DE5B61E52329F986B354F5F76DBCBE36A
SHA-512:	7A4080B9A64890DB36FEFF3AC767BC20F72469F717680D9ECC678EEDF9BAF30093F3904C9F04464EBCA89ED0E46C3EFB174ECCD217FF497B0656266A4FA82D2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.603 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-00:11:04.605 1a8c Recovering log #3.2021/08/03-00:11:04.605 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.164971776705023
Encrypted:	false
SSDEEP:	6:mDBN/NADM+q2PWXp+N23iKKdK25+XuoIFUtpOBRAgZmwPOBRADMVkwOWXp+N23iM:SNADM+va5KkTXYFUtpyAg/PyADMV5f5X
MD5:	D24A9B5375D43BC3C412A0103C057B65
SHA1:	EA694D70FE0191D2D7C05B7A925260D55A0C66DB
SHA-256:	A777BCB0DD5A75F12D855252E4880C0DE5B61E52329F986B354F5F76DBCBE36A
SHA-512:	7A4080B9A64890DB36FEFF3AC767BC20F72469F717680D9ECC678EEDF9BAF30093F3904C9F04464EBCA89ED0E46C3EFB174ECCD217FF497B0656266A4FA82D2
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.603 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/MANIFEST-000001.2021/08/03-00:11:04.605 1a8c Recovering log #3.2021/08/03-00:11:04.605 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Feature Engagement Tracker\EventDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.208272160232888
Encrypted:	false
SSDEEP:	6:mDVEADM+q2PWXp+N23iKKdKWT5g1IdqIFUtpOnAgZmwPOTWADMVkwOWXp+N23iKN:eEADM+va5Kkg5gSRFUtp6Ag/PvADMV5b
MD5:	9C85719C109B47FA336B511C7843893C

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG	
SHA1:	C29D7FB389840FC8E5C0F41CF08AE95351C037BF
SHA-256:	DC732C1AD1CC78CF1DEBAC926E1A1F07AB213307547F394F37A391D017A7DA94
SHA-512:	AC41EAFB90017ADBD3D513E9363979FF5EFCF081AB8CA829185180D20B2CFFCCFDE9EA01397DD7E57C207BF47CC9D6736BF4E182C69B3A14B40A980C491074AF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.589 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-00:11:04.591 1a8c Recovering log #3.2021/08/03-00:11:04.592 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	330
Entropy (8bit):	5.208272160232888
Encrypted:	false
SSDEEP:	6:mDVEADM+q2PWXp+N23iKKdKWT5g1IdqIFUtpOnAgZmwPOTWADMVkwOWXp+N23iKN:eEADM+va5Kkg5gSRFUtp6Ag/PvADMV5b
MD5:	9C85719C109B47FA336B511C7843893C
SHA1:	C29D7FB389840FC8E5C0F41CF08AE95351C037BF
SHA-256:	DC732C1AD1CC78CF1DEBAC926E1A1F07AB213307547F394F37A391D017A7DA94
SHA-512:	AC41EAFB90017ADBD3D513E9363979FF5EFCF081AB8CA829185180D20B2CFFCCFDE9EA01397DD7E57C207BF47CC9D6736BF4E182C69B3A14B40A980C491074AF
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.589 1a8c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/MANIFEST-000001.2021/08/03-00:11:04.591 1a8c Recovering log #3.2021/08/03-00:11:04.592 1a8c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\GCM Store\Encryption/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09931266207216792
Encrypted:	false
SSDEEP:	6:l9bNFlqQCNa/lvQfGrp3/PL1GQsLnwHOo/lCxthiZcGCxC+/eriUn0rp3/PL1GQr:TL+A/oGrpnjssNuQmGI/FMGpnjr
MD5:	C446F1F22F81502D382F63D4625EF07D
SHA1:	4C20C0862B34059B465144A7F159BFF281037D7B
SHA-256:	20C1AAE9CC978B88E00D97794BE7FA67D673DF6AA1773914230E8F3562B2119E
SHA-512:	FDBBE63F2B4B9FBF0D76E4187941E63AA51610480789F5318F1195BCB32051BEB6079D2DBEC1BA66A2EFEF7FD5E2552D1422B3C8DFD4159B5A1CAF1807119505
Malicious:	false
Reputation:	low
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	467
Entropy (8bit):	5.0783284700187155
Encrypted:	false
SSDEEP:	12:qbHUAn1g6u7H10PnTdtNBk778B/xgsbpnjUPfXzn:u0Aq6ub10rdVY78BJgs9njWj
MD5:	219ED50064C41C2A0CB650762D22F7A8
SHA1:	9B4C295258EB8717ABDEE8E454B7EDA9E6056BD9
SHA-256:	727B69455CEB5AC246B0FB92E923EDE69AAD46094FAE7042FD55EF180769D2F9
SHA-512:	6A5C6B0368CF22E0C97E52AFDE7A2AC70CD31352F56E87D45BDD5A08F09A70FEEFA2BB275E11F22151CA58F4698F07FD7FE8C729030398C1D8E6579741B9B22A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History Provider Cache	
Preview:	.....".4....axxy..co..coronationtraining..docusign..http..za*L.....axxy.....co.....coronationtraining.....docusign.....http.....za..2.....a.....c.....d.....g.....h.....i.... .....n.....o.....p.....r.....s.....t.....u.....x.....y.....z...:8.....BU...Q..... .....*%http://axxy.coronationtraining.co.za/2.Docusign :.....J....." ...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\History-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	33356
Entropy (8bit):	0.047390988727990205
Encrypted:	false
SSDEEP:	3:f2n3llu/fll/2HNll/2ofll/2SNll/2RtFll/2Mfll/2jtFll/2BMRgSWbNFl/lJ:enJ0oup7MXjm6g9bNFlWCj/l10el3n
MD5:	0CD2B02EE2A706E2FA7E0452F01C1D30
SHA1:	0E1A04CE3E90E37F6C17E7954897C71916EE4C01
SHA-256:	D78A32F701E5DF41156613B73AFA814462705A55EA02AB26B302E9E1EAC5F474
SHA-512:	076AC64345156C37B8CD4FCE9DE19EEAFFC575457E827E75803433FC3D1D3F3E73F787C12CC3231A0ACC29F6E44C4F28F68FC83D6BFBB927308BA5037500E15
Malicious:	false
Reputation:	low
Preview:	.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Last SessionQ. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	1325
Entropy (8bit):	3.14704919987102
Encrypted:	false
SSDEEP:	24:34SFI63jFlrlAnnjpPV1XNMLqenjBP93lLIL:34ETfxenldGqenVP9VRL
MD5:	787F3BEAD65088E840EF44749B06766E
SHA1:	4A59F38DEE14318A402CE083C47771EA69679E4A
SHA-256:	E2BF5DC868D8BBCE3CFFE6B77467C5112A7E90555C926772C9A2E4445AC3C6D2
SHA-512:	F74E4CCE6A6D2537F64F44B9B0E486BEFA9B198A6F894499A85221A585DA06F1E6C67FA1E4C1783F1994BCC98977A8AA61112FC5AEB7C421F20BC5B886513F6
Malicious:	false
Reputation:	low
Preview:	SNSS.....!.....1.,.....$...3e507014_76f1_4590_9ac8_6c52434d60b8.....`a..... .....5..0.....&...{524A03AB-861D-4591-9B4E-BDD69F9D425A}.....%...http://axxy.coronationtraining.co.za/.....D.o.c.u.s.i.g.n..... .....h.....`.....a..b....b..b....@.....X.....R...%...h.t.t.p.:././.a.x.x.y...c.o.r.o.n.a.t.i.o.n.t.r.a.i.n.i.n.g...c.o...z.a./..... .....8.....0.....h...0.....?.%. .B.l.i.n.k. .s.e.r.i.a.l.i.z.e.d. .f.o.r.m. .s.t.a.t.e. .v.e.r.s.i.o.n. .1.0. .....=.&.....N.o. . o.w.n.e.r.....1.....f.i.l.e.....

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	2955

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\000003.log	
Entropy (8bit):	5.457616349120036
Encrypted:	false
SSDEEP:	48:MFGLVeRa7FMQ8dbPGW3bQSefgGCNrS0U9RdiN9Qn:ua7FMLdbPGW3bQ5fgGOrS0Y
MD5:	E400B88591A2C8B35526ED09A7AEE314
SHA1:	1711903E4668465DD90CBDF21F87DA6F9F568F9A
SHA-256:	56F2197F8E9B37EE6C9893C3369D6D19B45EE70AC70BD4543146D07BF0F4FB0E
SHA-512:	C604D76D33DE7AAFE5EEB5FBFBE609777C06098D3FE40521B0B293EA24E04691013F448914A9FD2E3FE7C2EDA87B8476FC7002A28AAD3227AAC21C20B400A1(3
Malicious:	false
Reputation:	low
Preview:	..i...*.....8META:chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm.....Y_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.HangoutSinkDiscoveryService:.{"cache":{"sinks":{},"g":{},"h":null},"manualHangouts":{}}.a_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.IdGenerator.cast.RequestIdGenerator..120602000.H_chrome-extension://pkedcjkdefgpdelpbcmbmeomcjbeemfm..mr.temp.LogManager...["[2021-08-03 00:11:06.04][INFO][mr.Init] MR instance ID: 1346d865-4368-4dbb-84e8-bc9fc9809cf5\n","[2021-08-03 00:11:06.04][INFO][mr.Init] Native Cast MRP is disabled.\n","[2021-08-03 00:11:06.04][INFO][mr.Init] Native Mirroring Service is enabled.\n","[2021-08-03 00:11:06.04][INFO][mr.PersistentDataManager] removeTemporary_: 163 chars used\n","[2021-08-03 00:11:06.04][INFO][mr.PersistentDataManager] initialize: 163 chars used, 67 other chars\n","[2021-08-03 00:11:06.04][INFO][mr.CastProvider] Query enabled: true\n","[2021-08-03 00:11:06.04][INFO][mr.CloudProvider]

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.115048413644229
Encrypted:	false
SSDEEP:	6:mDOr+q2PWXp+N23iKKdK8a2jMGIFUtpOOHmXZmwPOOIGFNVkwOWXp+N23iKKdK8N:fr+va5Kk8EFUtpPHmX/PPIGFNV5f5Kkw
MD5:	5F45E523EE5EEC5CC0FB998EB598C46D
SHA1:	6EEDF14B65F79DFBB9114429166377EE5C1264EE
SHA-256:	D0A29F0137A06A8B9319F4CBB507495FC03D1AA6031584DDBC580F3E1663620B
SHA-512:	CAFF9D94B2B2DB0E512A4E198D377AC1C5BCAE0D90AEACCE12FFAD35EECCEAC83D1E8084CE555FF6C96C34428CA0CCF53417B338AC736BF2702D64C45D4I7691
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.118 cbc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:10:48.120 cbc Recovering log #3.2021/08/03-00:10:48.121 cbc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb\LOG.oldTM (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.115048413644229
Encrypted:	false
SSDEEP:	6:mDOr+q2PWXp+N23iKKdK8a2jMGIFUtpOOHmXZmwPOOIGFNVkwOWXp+N23iKKdK8N:fr+va5Kk8EFUtpPHmX/PPIGFNV5f5Kkw
MD5:	5F45E523EE5EEC5CC0FB998EB598C46D
SHA1:	6EEDF14B65F79DFBB9114429166377EE5C1264EE
SHA-256:	D0A29F0137A06A8B9319F4CBB507495FC03D1AA6031584DDBC580F3E1663620B
SHA-512:	CAFF9D94B2B2DB0E512A4E198D377AC1C5BCAE0D90AEACCE12FFAD35EECCEAC83D1E8084CE555FF6C96C34428CA0CCF53417B338AC736BF2702D64C45D4I7691
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.118 cbc Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:10:48.120 cbc Recovering log #3.2021/08/03-00:10:48.121 cbc Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statec9 (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	4219
Entropy (8bit):	4.871684703914691
Encrypted:	false
SSDEEP:	48:YXsJjMH+5s7YMHBKsvxMHVzspxMHbsIHt/soBDysKqnsllzMHpDCLsWJMHLsNuMg:RG+ZGJG+GTTD7IGpD+G7Gp2GnG4GVhH
MD5:	EDC4A4E22003A711AEF67FAED28DB603
SHA1:	977E551B9ED5F60D018C030B0B4AA2E33B954556

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network Persistent Statec9 (copy)	
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\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.170281852497513
Encrypted:	false
SSDEEP:	6:mDOqoIq2PWXp+N23iKKdKgXz4rRIFUtpOOo4vZZmwPOOo4vzkwOWXp+N23iKKdKt:fqoIva5KkgXiuFUtpP/vZ/PP/vz5f5K2
MD5:	07B79F963494B9B495D75E4116B2F9F2
SHA1:	923964FE1A2449B270A593F4D87AD809C5C5736F
SHA-256:	98ADFD4D8B6DC6CF739B43AA9E6EF1D8919470351FEE177D9D67B7B415DC856F
SHA-512:	180A392AA56C908099ADFC85405C5C3DF99CDB2BA6BE62E67D9B03C9C2A697BD6BD08D6A0B0D62C2ADD227DA668306C63BEB611CFD4D7D36ACEF8D80E0C291D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.430 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-00:10:48.432 1550 Recovering log #3.2021/08/03-00:10:48.432 1550 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications\LOG.old.} (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	334
Entropy (8bit):	5.170281852497513
Encrypted:	false
SSDEEP:	6:mDOqoIq2PWXp+N23iKKdKgXz4rRIFUtpOOo4vZZmwPOOo4vzkwOWXp+N23iKKdKt:fqoIva5KkgXiuFUtpP/vZ/PP/vz5f5K2
MD5:	07B79F963494B9B495D75E4116B2F9F2
SHA1:	923964FE1A2449B270A593F4D87AD809C5C5736F
SHA-256:	98ADFD4D8B6DC6CF739B43AA9E6EF1D8919470351FEE177D9D67B7B415DC856F
SHA-512:	180A392AA56C908099ADFC85405C5C3DF99CDB2BA6BE62E67D9B03C9C2A697BD6BD08D6A0B0D62C2ADD227DA668306C63BEB611CFD4D7D36ACEF8D80E0C291D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.430 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/MANIFEST-000001.2021/08/03-00:10:48.432 1550 Recovering log #3.2021/08/03-00:10:48.432 1550 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	5774
Entropy (8bit):	5.18349312351112
Encrypted:	false
SSDEEP:	96:n0C6kJM93I4TNSNcKILok0JCKL84nlkB1ybOTQVuwn:n0CtMxWNcs4KLlkBy
MD5:	9DD3EE4CDEDB024C12940448940002ED
SHA1:	64C32EB526A8A73A28F2E1CB38118377A76EDE10
SHA-256:	550A103FFD028F5AC76AB8D909281739587BBFEA29973DC980CBC8481D3CB936
SHA-512:	4F3A5F48A06574B9EC192E237B06B9365BFD6F0ADC9F713C77834B7BBCDC7214F9AA98D1070EDCC96A5916ADE43DAC773FE718C1260651D5FC987C83BF66018
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Preferences (copy)	
Preview:	{"account_id_migration_state":2,"account_tracker_service_last_update":"13272448248367751","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\Reporting and NEL	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	1.01134776751223
Encrypted:	false
SSDEEP:	48:TUIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUOoTRs2oTRsAoB:wIElwQF8mpcSJ2YR1
MD5:	BBCCB19BD88F77ABFEB439D2ECA16AAC
SHA1:	0D992DFFF7BB59C1C31F644FD655A0D0B49281A9
SHA-256:	616760EA7E4444B3B8782820A7BEF4C6937570E3FA42D9A57BC040B093CCC036
SHA-512:	C32245DB70DFB17F8163274AEC82349DC0B3B07BFA4AA4B21B85B8B4754F26CDE875DE84EF104E103EA9756A3140D4EA923347CFF059B101B12972FAC4980F2
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....C..........g...^.........j..

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Reporting and NEL-journal	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	21044
Entropy (8bit):	0.8265481291914679
Encrypted:	false
SSDEEP:	48:Z8qkIopK2rJNVr1GJmm8pF82phrJNVrdHX/cjrJN2yJ1n4n1GmhGUf6:Z8hIElwQF8mpcS2
MD5:	9FC9C3FF84F379E7FBA4D080187DA90A
SHA1:	1F990AB4AABAD94106C4B28D99892323B200F957
SHA-256:	10769245465BD262B7C79E46D97084C046BB669872E31A30508F84500C689F2E
SHA-512:	133CDA0710836E4EC5E87024252AD6A5359E092974146734EAF874D54B25FDE7B241DCF582792D9C60E4562376D3A9F06352B07FBBBBCA9581F353B8EBDC519
Malicious:	false
Reputation:	low
Preview:	.............W...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferences (copy)	
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):	5.536261251115225
Encrypted:	false
SSDEEP:	384:n2ngtbLl+D1Xf1kXqKf/pUZNCgVLH2HfDbrUldHGWnTj1PnSJ4r:hLlif1kXqKf/pUZNCgVLH2HfXrUlBGW5
MD5:	C30E09DADAD1750A9956CFC629CCFB6A
SHA1:	6D341322C51191170E9917CBDA5F0A1BFAD0876A
SHA-256:	FE611037179946675BC918A60C5068886DD7AC0DCF541A565F10A2373B762C0A
SHA-512:	C848ED4E4A2CAD20FB894FEB4930BF22C6452499ADAC768CDC56EEC0A45F0E951A51F81F7AAC34D90F0C7D8478F6D5B8147F89A31EC8FDCCAF01EEBEC291 DD2
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":"13272448248078036","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\Secure Preferences (copy)

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Secure Preferencest (copy)	
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):	22596
Entropy (8bit):	5.536297525407854
Encrypted:	false
SSDEEP:	384:n2ngtbLl+D1Xf1kXqKf/pUZNCgVLH2HfDbrUldHG5nTj2nSJ4F:hLlif1kXqKf/pUZNCgVLH2HfXrUlBG5W
MD5:	D298FE3CE5C13E4A44BD47014294538D
SHA1:	14A394086F030704DDD78B8C184FDE01D77F618A
SHA-256:	901822E71E28B1D8E64C52AA09D29B2C940A335481AC06123E8CEF12BA4EA592
SHA-512:	21CE54057E3400ED9E796DC8AE0984379127EE75A663A3BA764177C9F54A90207FFEE4C6CE79DEB7B8E18EAFE16E47936ADA5FB4E584490823AD2CCDCA4DBC BB
Malicious:	false
Reputation:	low
Preview:	{"extensions":{"settings":{"ahfgeienlihckogmohjhadlkjgocpleb":{"active_permissions":{"api":["management","system.display","system.storage","webstorePrivate","sy stem.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":"13272448248078036","location":5,"manifest":{"a pp":{"launch":{"web_url":"https://chrome.google.com/webstore"},"urls":["https://chrome.google.com/webstore"]},"description":"Discover great apps, games, extensions and themes for Google Chrome.","icons":{"128":"webstore_icon_128.png","16":"webstore_icon_16.png"},"key":"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt l3tO0osjuzRsf6xtD2SKxPlTfuoy7AWoObysitBPvH5fE1NaAA1/2JkPWkVDhdLBWLaIBPYeXbzlHp3y4Vv/4XG+aN5qFE3z+1RU/NqkzVYHtlpVScf3DjTYtKVL66mzVG ijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	114
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5ljljljljljl:5ljljljljljl
MD5:	1B4FA89099996CE3C9E5A0A9768230E8
SHA1:	9026E1E0906E3B3FE0E414EE814CC5A042807A04
SHA-256:	537818AAFD0902A8B2D58B483674391E33E762B5E1E8CD226D873098CCE9C8F9
SHA-512:	4279C9380ACC5AB329EC6BCDA10CCF0A7437CEF63845B63E741CE517042CFE83340D2D362DD6B9E039BF55E61F484CCF72B8FD8477D1D0292E0B879CB94946 B
Malicious:	false
Reputation:	low
Preview:	..&f.....&f.....&f.....&f.....&f.....&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.111301488265688
Encrypted:	false
SSDEEP:	6:mDOgIq2PWXp+N23iKKdKrQMxIFUtpOOhZmwPOO7kwOWXp+N23iKKdKrQMFLJ:fRva5KkCFUtpPh/PP75f5KktJ
MD5:	15CBC762F145FE89B3BF58403F8BFD04
SHA1:	3EB089DAB108D3B5E56A6550D2B296DB61CC6A0F
SHA-256:	CDB324F89E8580E337044CBA870D569FED2779DD2BB19885D2287E251184DED6
SHA-512:	320BCD568A18E41C7B7192F98D6D17DD6441CBF638C87DE293CEFDE53092430F8FBCE77F45AE35763E111CFCAC3B7AC447F32270A7FF0D526C7596A2C2C7A5 B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.307 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-0 0:10:48.308 1550 Recovering log #3.2021/08/03-00:10:48.308 1550 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session St orage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.111301488265688
Encrypted:	false
SSDEEP:	6:mDOgIq2PWXp+N23iKKdKrQMxIFUtpOOhZmwPOO7kwOWXp+N23iKKdKrQMFLJ:fRva5KkCFUtpPh/PP75f5KktJ
MD5:	15CBC762F145FE89B3BF58403F8BFD04
SHA1:	3EB089DAB108D3B5E56A6550D2B296DB61CC6A0F
SHA-256:	CDB324F89E8580E337044CBA870D569FED2779DD2BB19885D2287E251184DED6
SHA-512:	320BCD568A18E41C7B7192F98D6D17DD6441CBF638C87DE293CEFDE53092430F8FBCE77F45AE35763E111CFCAC3B7AC447F32270A7FF0D526C7596A2C2C7A5B
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.307 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/MANIFEST-000001.2021/08/03-00:10:48.308 1550 Recovering log #3.2021/08/03-00:10:48.308 1550 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.136322975304833
Encrypted:	false
SSDEEP:	6:mDOtc9yq2PWXp+N23iKKdK7Uh2ghZIFUtpOOjJI1ZmwPOOeQRkwOWXp+N23iKKdb:ftc9yva5KkIhHh2FUtpPc/PPJR5f5Kks
MD5:	C02B76E7AB318A92263764CA76EDFF20
SHA1:	1F7DDC18E7D8C2D3653F3F1AC4B7F465E2A3E721
SHA-256:	6C0266ADFF37E4C857A0FE8A05051B4D6003081E7DAD6A8A5140F40DBAC73F8C
SHA-512:	073CBF421821E49EB9F5B9547C72DCEB4C8832B1C3353614713B12827DC4B8A9E0A817227D6551F81D4F085ADF267BDFAA53268DFB8CB1B3649946D09BFD764
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.097 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-00:10:48.099 1570 Recovering log #3.2021/08/03-00:10:48.100 1570 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	348
Entropy (8bit):	5.136322975304833
Encrypted:	false
SSDEEP:	6:mDOtc9yq2PWXp+N23iKKdK7Uh2ghZIFUtpOOjJI1ZmwPOOeQRkwOWXp+N23iKKdb:ftc9yva5KkIhHh2FUtpPc/PPJR5f5Kks
MD5:	C02B76E7AB318A92263764CA76EDFF20
SHA1:	1F7DDC18E7D8C2D3653F3F1AC4B7F465E2A3E721
SHA-256:	6C0266ADFF37E4C857A0FE8A05051B4D6003081E7DAD6A8A5140F40DBAC73F8C
SHA-512:	073CBF421821E49EB9F5B9547C72DCEB4C8832B1C3353614713B12827DC4B8A9E0A817227D6551F81D4F085ADF267BDFAA53268DFB8CB1B3649946D09BFD764
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.097 1570 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/MANIFEST-000001.2021/08/03-00:10:48.099 1570 Recovering log #3.2021/08/03-00:10:48.100 1570 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Site Characteristics Database/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5a4b63d2-4f49-4e34-abf2-344c94643e82.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):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\5a4b63d2-4f49-4e34-abf2-344c94643e82.tmp	
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.240819290911859
Encrypted:	false
SSDEEP:	6:mDOUq2PWXp+N23iKKdKusNpV/2jMGIFUtpOOxK9ZmwPOOdPkwOWXp+N23iKKdKux:fUva5KkFFUtpPc9/PPdP5f5KkOJ
MD5:	2DB0FD6EC67F7862ACD270036240E374
SHA1:	B3A2A82CD67F7A161593E591C9FEC6A15A650942
SHA-256:	62D00FD350744900FA3322A7F2A43DE2E773BEC3D72A0B21C21AB03CCD11FE9C
SHA-512:	3D92211B268A4131106108E5B8469DFE1866589A78FDF3A464C2FD0E0D6500BA66DBF8EF90FA9A455FAB1D2B1357EE8EF02810678329F70D17F1FE3F7DF89C99
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.355 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:10:48.356 10d4 Recovering log #3.2021/08/03-00:10:48.357 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.240819290911859
Encrypted:	false
SSDEEP:	6:mDOUq2PWXp+N23iKKdKusNpV/2jMGIFUtpOOxK9ZmwPOOdPkwOWXp+N23iKKdKux:fUva5KkFFUtpPc9/PPdP5f5KkOJ
MD5:	2DB0FD6EC67F7862ACD270036240E374
SHA1:	B3A2A82CD67F7A161593E591C9FEC6A15A650942
SHA-256:	62D00FD350744900FA3322A7F2A43DE2E773BEC3D72A0B21C21AB03CCD11FE9C
SHA-512:	3D92211B268A4131106108E5B8469DFE1866589A78FDF3A464C2FD0E0D6500BA66DBF8EF90FA9A455FAB1D2B1357EE8EF02810678329F70D17F1FE3F7DF89C99
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.355 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:10:48.356 10d4 Recovering log #3.2021/08/03-00:10:48.357 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Network Persistent State (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.985305467053914
Encrypted:	false
SSDEEP:	6:YHpoNXR8+eq7JdV5qQlsDHF4xj70PpqQEsDHF4R8HLJ2AVQBR70S7PMVKJw1K3Ky:YHO8sdBsB6MAsBdLJlyH7E4f3K33y
MD5:	C401B619D9D8E0ADABC25A47EE49CFBA
SHA1:	C9D3B816DD3FBCD98E9C0A32CEC7B501EFC0BBDA
SHA-256:	8F5D75F5EF9876E8D30CE477509F735B50C4D87DBEDB433BE8EDBE6D4B3CB82F
SHA-512:	BC12F16CB95CB0AD708C6BBD005EF863A8552613E612F1084086E0F8262752E1B5144D044F0D141CE8462CC33343C36B517A5CC778751680485D8F88FB51B862
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543490879170","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543490879171","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.247402002188543
Encrypted:	false
SSDEEP:	6:mDOuXq2PWXp+N23iKKdKusNpqz4rRIFUtpOOiZmwPOOsaBRFkwOWXp+N23iKKdKr:fuXva5KkmiuFUtpPi/PPRP5f5Kkm2J
MD5:	49EE249B39104772C6EBA2DEEE351E52
SHA1:	E4DA1E839E3EE964B41D72EBE3ADB677CA9F3215
SHA-256:	864903E1B709DE6892461E953C7F1F18FB2592E6ED3458620CC6D64952CD4595
SHA-512:	521568137BCBFD4E91E4E6C9F081CFE51ECFE78BE273501E53D53B55643D99E233EFB53D93DE42403113539B3EAC9885F111BCD3B7D63D32C3B57982FA7808F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.434 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-00:10:48.435 10d4 Recovering log #3.2021/08/03-00:10:48.436 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	432
Entropy (8bit):	5.247402002188543
Encrypted:	false
SSDEEP:	6:mDOuXq2PWXp+N23iKKdKusNpqz4rRIFUtpOOiZmwPOOsaBRFkwOWXp+N23iKKdKr:fuXva5KkmiuFUtpPi/PPRP5f5Kkm2J
MD5:	49EE249B39104772C6EBA2DEEE351E52
SHA1:	E4DA1E839E3EE964B41D72EBE3ADB677CA9F3215
SHA-256:	864903E1B709DE6892461E953C7F1F18FB2592E6ED3458620CC6D64952CD4595
SHA-512:	521568137BCBFD4E91E4E6C9F081CFE51ECFE78BE273501E53D53B55643D99E233EFB53D93DE42403113539B3EAC9885F111BCD3B7D63D32C3B57982FA7808F
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.434 10d4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/MANIFEST-000001.2021/08/03-00:10:48.435 10d4 Recovering log #3.2021/08/03-00:10:48.436 10d4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\000003.log	
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.242800230649867
Encrypted:	false
SSDEEP:	6:mDt4Q+q2PWXp+N23iKKdKusNpZQMxIFUtpO5dWZmwPO5QVkwOWXp+N23iKKdKusx:XQ+va5KkMFUtpog/PoQV5f5KkTJ
MD5:	0DB6F5FBF642CD39F0E01BFF5B1896D5
SHA1:	6E13D4E4C14F26150729ECA4AA389D57BC656423
SHA-256:	E5DDE9CA3FB77958A95E54FEAFFA1B601912C87DDE25F3DB83515AC3AC125725
SHA-512:	8996D774C20FAAF9BFE6E2DCAF5A25266014AF054431EB8CA7ED06178C775991D595501570B6D98B19A9BE63680D5183C657828947E1D159554BEB9157643E1D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.556 30c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-00:11:04.557 30c Recovering log #3.2021/08/03-00:11:04.557 30c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.242800230649867
Encrypted:	false
SSDEEP:	6:mDt4Q+q2PWXp+N23iKKdKusNpZQMxIFUtpO5dWZmwPO5QVkwOWXp+N23iKKdKusx:XQ+va5KkMFUtpog/PoQV5f5KkTJ
MD5:	0DB6F5FBF642CD39F0E01BFF5B1896D5
SHA1:	6E13D4E4C14F26150729ECA4AA389D57BC656423
SHA-256:	E5DDE9CA3FB77958A95E54FEAFFA1B601912C87DDE25F3DB83515AC3AC125725
SHA-512:	8996D774C20FAAF9BFE6E2DCAF5A25266014AF054431EB8CA7ED06178C775991D595501570B6D98B19A9BE63680D5183C657828947E1D159554BEB9157643E1D
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.556 30c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/MANIFEST-000001.2021/08/03-00:11:04.557 30c Recovering log #3.2021/08/03-00:11:04.557 30c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\gfdkimpbcpahaombhbimeihdjnejgicl\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\62566084-2308-4792-a450-9e0f6a6a09bc.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):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\GPUCache\data_1

Category:	dropped
Size (bytes):	296
Entropy (8bit):	0.19535324365485862
Encrypted:	false
SSDEEP:	3:8E:8
MD5:	C4DF0FB10C4332150B2C336396CE1B66
SHA1:	780A76E101DE3DE2E68D23E64AB1A44D47A73207
SHA-256:	18FAB4D13CDA7E1DEE12DC091019A110A7304B6A65FC9A1F3E6173046BA38EF6
SHA-512:	51F0B463E97063A2357285D684FF159FDF6099E57C46F13C83E9D3F09D7A7CF03C1BA684BCCF36232FC50834F95953C3C68675C7B05AB4F84DEF1C566A5F3F5E
Malicious:	false
Reputation:	low
Preview:	.'..(..... .....

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.146783534649495
Encrypted:	false
SSDEEP:	12:AAva5KkkGHArBFUtp2/PK5f5KkkGHAryJ:Na5KkkGgPgvf5KkkGga
MD5:	FF8B4B24A96C8CED80A0D4419E11201F
SHA1:	3103F73A5B1894E2A5CB78A69FC8864A98F53F6D
SHA-256:	FF628EB87C7A6AADB0E53A7A833F4547FCEF291E9C1815F123E19BAA4717C1EB
SHA-512:	BB5B60FDCDBE9A4D2544D8E249A4355980610D9D74E8974D49A983A03529811B51B7E6D9E6C57058A58BC17E066C2F2D71B969177B92B52BC92B4AE469F44F6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:05.037 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:11:05.039 1550 Recovering log #3.2021/08/03-00:11:05.039 1550 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

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

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	430
Entropy (8bit):	5.146783534649495
Encrypted:	false
SSDEEP:	12:AAva5KkkGHArBFUtp2/PK5f5KkkGHAryJ:Na5KkkGgPgvf5KkkGga
MD5:	FF8B4B24A96C8CED80A0D4419E11201F
SHA1:	3103F73A5B1894E2A5CB78A69FC8864A98F53F6D
SHA-256:	FF628EB87C7A6AADB0E53A7A833F4547FCEF291E9C1815F123E19BAA4717C1EB
SHA-512:	BB5B60FDCDBE9A4D2544D8E249A4355980610D9D74E8974D49A983A03529811B51B7E6D9E6C57058A58BC17E066C2F2D71B969177B92B52BC92B4AE469F44F6
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:05.037 1550 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda \def\Local Storage\leveldb/MANIFEST-000001.2021/08/03-00:11:05.039 1550 Recovering log #3.2021/08/03-00:11:05.039 1550 Reusing old log C:\Users\user\A ppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Local Storage\leveldb/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State.. (copy)

Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	420
Entropy (8bit):	4.954960881489904
Encrypted:	false
SSDEEP:	12:YHO8sdvBVSsB6M/BVSsBdLJlyH7E4f3K33y:YXsdvjX6gjXdL3yH7n/iy
MD5:	F4FEFEEEC722772F9DC0FCE1B52D79B5
SHA1:	00EECFA3B37113D30E7D43BE4383C540F3D93D4D
SHA-256:	D33E13C12004A700F246D8C73709114A881609D658E045D54DE36874728D07F0
SHA-512:	41E61EC89366800FD5F4DD704E53B47DE29411B9088B46349A0A350758D08569C14DCC70CF8D6A6FE6D049CB6D32F2B091153E8148A1B5857BD7AF13492071BE

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Network Persistent State.. (copy)	
Malicious:	false
Reputation:	low
Preview:	{"net":{"http_server_properties":{"servers":[{"alternative_service":[{"advertised_versions":[50],"expiration":"13248543498399332","port":443,"protocol_str":"quic"},{"advertised_versions":[73],"expiration":"13248543498399332","port":443,"protocol_str":"quic"}],"isolation":[],"server":"https://dns.google","supports_spdy":true}],"version":5},"network_qualities":{"CAASABiAgICA+P////8B":"4G","CAESABiAgICA+P////8B":"4G"}}}

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.160436200860847
Encrypted:	false
SSDEEP:	12:7va5KkkGHArqiuFUtpY/PhvD5f5KkkGHArq2J:ba5KkkGgCgCtf5KkkGg7
MD5:	CEBEA2366CB215011DF0A6AF8367CC1F
SHA1:	CD4282CC0D09041E49CF4972E1501E4D5A159DEA
SHA-256:	BD5A26F6885F2D74B45A20C5C72148B8C41D2F2B29DB576A1990FB481AEC417D
SHA-512:	3DDC87B4B4249047B5039883F3AE6D78343C54C797EC1843E4FE7F0B5F5C18DBA0A66BFD9F8F74CD3A440D2B508925754CF2B1FD0C98A4585C4CE6093FDB73A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:05.046 f50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-00:11:05.048 f50 Recovering log #3.2021/08/03-00:11:05.050 f50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	429
Entropy (8bit):	5.160436200860847
Encrypted:	false
SSDEEP:	12:7va5KkkGHArqiuFUtpY/PhvD5f5KkkGHArq2J:ba5KkkGgCgCtf5KkkGg7
MD5:	CEBEA2366CB215011DF0A6AF8367CC1F
SHA1:	CD4282CC0D09041E49CF4972E1501E4D5A159DEA
SHA-256:	BD5A26F6885F2D74B45A20C5C72148B8C41D2F2B29DB576A1990FB481AEC417D
SHA-512:	3DDC87B4B4249047B5039883F3AE6D78343C54C797EC1843E4FE7F0B5F5C18DBA0A66BFD9F8F74CD3A440D2B508925754CF2B1FD0C98A4585C4CE6093FDB73A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:05.046 f50 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/MANIFEST-000001.2021/08/03-00:11:05.048 f50 Recovering log #3.2021/08/03-00:11:05.050 f50 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Platform Notifications/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	19
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:5l:5l
MD5:	E556F26DF3E95C19DBAECA8F5DF0C341
SHA1:	247A89F0557FC3666B5173833DB198B188F3AA2E
SHA-256:	B0A7B19404285905663876774A2176939A6ED75EF3904E44283A125824BD0BF3
SHA-512:	055BC4AB12FEEDF3245EAAF0A0109036909C44E3B69916F8A01E6C8459785317FE75CA6B28F8B339316FC2310D3E5392CD15DBDB0F84016667F304D377444E2E
Malicious:	false
Reputation:	low
Preview:	..&f.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG	
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.136698651015327
Encrypted:	false
SSDEEP:	12:C20va5KkkGHArAFUtpS0/PS05f5KkkGHArfJ:C/a5KkkGgkgc7+f5KkkGgV
MD5:	90288086D5FD17A09144CF654FC42E89
SHA1:	CC16C0F830ECF65025DA5F73F639C75290AA0A5C
SHA-256:	A9FE2739C0FB25F7AB3E10D9E4E9EB647A1548AFF3C2FC1BAE5BC404C5412A48
SHA-512:	1FDD177F7047FF6C59EB58BD57393C1BA0BBE8096C670F2D95CE937E2ED18C010ED947F693B7D331F9E81FE047CA40A0657FBA06B3A9D54BD397D91C0E92AC3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:20.340 ff4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-00:11:20.342 ff4 Recovering log #3.2021/08/03-00:11:20.342 ff4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage\LOG.oldon (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	415
Entropy (8bit):	5.136698651015327
Encrypted:	false
SSDEEP:	12:C20va5KkkGHArAFUtpS0/PS05f5KkkGHArfJ:C/a5KkkGgkgc7+f5KkkGgV
MD5:	90288086D5FD17A09144CF654FC42E89
SHA1:	CC16C0F830ECF65025DA5F73F639C75290AA0A5C
SHA-256:	A9FE2739C0FB25F7AB3E10D9E4E9EB647A1548AFF3C2FC1BAE5BC404C5412A48
SHA-512:	1FDD177F7047FF6C59EB58BD57393C1BA0BBE8096C670F2D95CE937E2ED18C010ED947F693B7D331F9E81FE047CA40A0657FBA06B3A9D54BD397D91C0E92AC3
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:20.340 ff4 Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/MANIFEST-000001.2021/08/03-00:11:20.342 ff4 Recovering log #3.2021/08/03-00:11:20.342 ff4 Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Storage\ext\nmmhkkegccagdldgiimedpiccmgmieda\def\Session Storage/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\000003.log	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	38
Entropy (8bit):	1.9837406708828553
Encrypted:	false
SSDEEP:	3:sgGg:st
MD5:	45A8ECA4E5C4A6B1395080C1B728B6C9
SHA1:	8A97BB0E599775D9A10C0FC53C4EDB29AA4CEB4E
SHA-256:	DB320AB28DFF27CDA0A7F87B82F2F8E61B3178A6DE8503753D76F1172D32E08E
SHA-512:	8EE91A3A1E77459273553F6A776C423A8EE95DB9DCFA897771814B7AD13FD84F06BB2B859F22B6DDA384B39EAA91F1819F170BABED6DA16BDBCF5BCB06CF2124
Malicious:	false
Reputation:	low
Preview:	..F.....F.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.181045916464135
Encrypted:	false
SSDEEP:	6:mDOtgN+q2PWXp+N23iKKdKpIFUtpOOjxGAWZmwPOOjxG3VkwOWXp+N23iKKdKa/o:ftgN+va5KkmFUtpP8AW/PP83V5f5KkaQ
MD5:	43E757A4E1237F24016076689CE1855F
SHA1:	4571620DDA5DC0F03C36F27EFD0EDC70FF8BC71B
SHA-256:	4FFE5A2BEEFCFADDA2975BBAB361162DF66287F21FE2EE9A654582226908D786

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG	
SHA-512:	49AE2F01A502525FD44E0CC0AF8A89782E12ABE275729B0BC41D64FE5AD86BDDA7CC0F1422B65F49416F90C58F12C077DA67A1496B3B6FE6343FCE0E6947090A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.097 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-00:10:48.099 9ec Recovering log #3.2021/08/03-00:10:48.099 9ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	321
Entropy (8bit):	5.181045916464135
Encrypted:	false
SSDEEP:	6:mDOtgN+q2PWXp+N23iKKdKpIFUtpOOjxGAWZmwPOOjxG3VkwOWXp+N23iKKdKa/o:ftgN+va5KkmFUtpP8AW/PP83V5f5KkaQ
MD5:	43E757A4E1237F24016076689CE1855F
SHA1:	4571620DDA5DC0F03C36F27EFD0EDC70FF8BC71B
SHA-256:	4FFE5A2BEEFCFADDA2975BBAB361162DF66287F21FE2EE9A654582226908D786
SHA-512:	49AE2F01A502525FD44E0CC0AF8A89782E12ABE275729B0BC41D64FE5AD86BDDA7CC0F1422B65F49416F90C58F12C077DA67A1496B3B6FE6343FCE0E6947090A
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:10:48.097 9ec Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/MANIFEST-000001.2021/08/03-00:10:48.099 9ec Recovering log #3.2021/08/03-00:10:48.099 9ec Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Data\LevelDB/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.255241796509862
Encrypted:	false
SSDEEP:	6:mDwQ+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpOmgZmwPOmQVkwOWXp+N23iKKdKksp:I+va5KkkOrsFUtp2/PyV5f5KkkOrzJ
MD5:	0A9F289403725210F1BAD98BD6FAB9B9
SHA1:	CCB98AE2DEEB8F56D4AA50C52373FC2BB4F0F8E8
SHA-256:	46B2011335DC9291209685CE8CA3B7006E842F26BAEF7D3684E5A0B1683016AC
SHA-512:	9C087E4325DFBCC91D95C3BB1CE92C009F160EAA762D69D0F0152158A797A55E77E887EC22C4C470287242DE5CFA10C6BE1D801D53CBC41534ED4CBD8AF9A97
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:06.012 132c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-00:11:06.014 132c Recovering log #3.2021/08/03-00:11:06.014 132c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.255241796509862
Encrypted:	false
SSDEEP:	6:mDwQ+q2PWXp+N23iKKdKks8Y5JKKhdIFUtpOmgZmwPOmQVkwOWXp+N23iKKdKksp:I+va5KkkOrsFUtp2/PyV5f5KkkOrzJ
MD5:	0A9F289403725210F1BAD98BD6FAB9B9
SHA1:	CCB98AE2DEEB8F56D4AA50C52373FC2BB4F0F8E8
SHA-256:	46B2011335DC9291209685CE8CA3B7006E842F26BAEF7D3684E5A0B1683016AC
SHA-512:	9C087E4325DFBCC91D95C3BB1CE92C009F160EAA762D69D0F0152158A797A55E77E887EC22C4C470287242DE5CFA10C6BE1D801D53CBC41534ED4CBD8AF9A97
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:06.012 132c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/MANIFEST-000001.2021/08/03-00:11:06.014 132c Recovering log #3.2021/08/03-00:11:06.014 132c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Sync Extension Settings\pkedcjkdefgpdelpbcmbmeomcjbeemfm/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\TransportSecurity (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	1207
Entropy (8bit):	5.592315110932319
Encrypted:	false
SSDEEP:	24:YrtEOUTw6H0UhVsTG1KUerkq/HeUeXby2qUeXvRI7wUxsRUenHQ:YBBUTw6UUhVseKUewqPeUer2UefMwUxv
MD5:	E748F67ACD8F080AB68A55817E522E55
SHA1:	138DE8FB6A887C3BDA4807D80594BA6404D16FBC
SHA-256:	AF9BBE4F91953D66F21893A22693AD949267CBEF29FD512FE867F75918CE3FCD
SHA-512:	AA4DE335A9E7BD82BB137222DD1167B10EADA4DCD8216634FDBD497DFFE8181E32079FC96248CF1C266724D13FADE3F67B4A960BFEFBFD3141A05BBE89089A41
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659510654.223229,"host":"Jbx/EIZxfCXPwzgMaWQPj8yDM6WT6M+2Htvd0llGyTA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627974654.223239},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659510652.833422,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Visited Links	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	12
Entropy (8bit):	3.188721875540867
Encrypted:	false
SSDEEP:	3:20Z:fZ
MD5:	7B4D46344D3C3C778D65DF2A1B9BBCCF
SHA1:	0ADC2ADB467D32B335D1739ADF74E3247BF0C476
SHA-256:	3CCD7642C49B8A6EEC0C17C4BF8329ACA247E8F2B0765CA584C4963EFAAF973D
SHA-512:	DB80ABAE45159D381ABF50B16C56F1C3835DE704A28B92F475AC0D02B6DF5765BE7E73DC33BFD0EC17B7104F1B4AA8E270C77A95C6E6F480151F47BC83B03D1
Malicious:	false
Reputation:	low
Preview:	......{(?...

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a02659bc-e80b-4a27-8e64-3d8805ce564a.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):	5.536261251115225
Encrypted:	false
SSDEEP:	384:n2ngtbLl+D1Xf1kXqKf/pUZNCgVLH2HfDbrUldHGWnTj1PnSJ4r:hLlif1kXqKf/pUZNCgVLH2HfXrUlBGW5
MD5:	C30E09DADAD1750A9956CFC629CCFB6A
SHA1:	6D341322C51191170E9917CBDA5F0A1BFAD0876A
SHA-256:	FE611037179946675BC918A60C5068886DD7AC0DCF541A565F10A2373B762C0A
SHA-512:	C848ED4E4A2CAD20FB894FEB4930BF22C6452499ADAC768CDC56EEC0A45F0E951A51F81F7AAC34D90F0C7D8478F6D5B8147F89A31EC8FDCCAF01EEBEC2914DD2
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":"13272448248078036","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAIwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\a3614eb6-e803-45b7-b83a-2d58eddf2822.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\Default\a3614eb6-e803-45b7-b83a-2d58eddf2822.tmp	
Size (bytes):	1207
Entropy (8bit):	5.592315110932319
Encrypted:	false
SSDEEP:	24:YrtEOUTw6H0UhVsTG1KUerkq/HeUeXby2qUeXvRI7wUxsRUenHQ:YBBUTw6UUhVseKUewqPeUer2UefMwUxv
MD5:	E748F67ACD8F080AB68A55817E522E55
SHA1:	138DE8FB6A887C3BDA4807D80594BA6404D16FBC
SHA-256:	AF9BBE4F91953D66F21893A22693AD949267CBEF29FD512FE867F75918CE3FCD
SHA-512:	AA4DE335A9E7BD82BB137222DD1167B10EADA4DCD8216634FDBD497DFFE8181E32079FC96248CF1C266724D13FADE3F67B4A960BFEFBFD3141A05BBE89089A41
Malicious:	false
Reputation:	low
Preview:	{"expect_ct":[],"sts":[{"expiry":1659510654.223229,"host":"Jbx/EIZxfCXPwzgMaWQPj8yDM6WT6M+2Htvd0llGyTA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1627974654.223239},{"expiry":1633014077.350499,"host":"OuKlWsMW1dkkbI1X/oi6o0Y95ZNSWnSoeaIXAEYPlv4=","mode":"force-https","sts_include_subdomains":true,"sts_observed":1601478077.350503},{"expiry":1633014077.22511,"host":"nAuqgR4iEWti7SOdT3UHPl6rmZU/DeaIm38P2O2OkgA=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478077.225114},{"expiry":1633014092.4175,"host":"0J7rAWV0ouCFYJ9XrkDiKnAO1SshXJmLJE1SS3V8kDM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478092.417504},{"expiry":1633014091.91938,"host":"5EdUoB7YUY9zZV+2DkgVXgho8WUvp+D+6KpeUOhNQIM=","mode":"force-https","sts_include_subdomains":false,"sts_observed":1601478091.919383},{"expiry":1659510652.833422,"host":"8/RrMmQlCD2Gsp14wUCE1P8r7B2C5+yE0+g79IPyRsc=","mode":"force-https","sts_include_subdomains":false,"sts_obs

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\b6290c22-7ec6-452a-bf6e-7612d6afe964.tmp	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16745
Entropy (8bit):	5.577673408698438
Encrypted:	false
SSDEEP:	384:n2ngtaLl+D1Xf1kXqKf/pUZNCgVLH2HfDbrUUAnSJ4N:ALlif1kXqKf/pUZNCgVLH2HfXrUnSJ6
MD5:	B8EEAA9A1A40F8FC7DEF768C4DD31517
SHA1:	14046792AB501B91F8000173ED571E82513A2F03
SHA-256:	D09689F6E1DCD7F7627FF6AD352515452E994952F433C4A96962E8075B33C6C1
SHA-512:	38C32507BAB7ADAF25F9D81086C93BC2E75ED821B50FDF5AF79D1DDF2BA65193EE2AAD60822E148246D1807A9BBED9EFAFA7CFDF115DCD39F1E063E5A419A74A
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":"13272448248078036","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/NqkzVYHtlpVScf3DjTYtKVL66mzVGijSoAlwbFCC3LpGdaoe6Q1rSRDp76wR6jjFzsYwQIDAQAB","name":"Web Store","pe

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

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

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\CURRENT (copy)	
SSDEEP:	3:1sjgWIV//Rv:1qIFJ
MD5:	6752A1D65B201C13B62EA44016EB221F
SHA1:	58ECF154D01A62233ED7FB494ACE3C3D4FFCE08B
SHA-256:	0861415CADA612EA5834D56E2CF1055D3E63979B69EB71D32AE9AE394D8306CD
SHA-512:	9CFD838D3FB570B44FC3461623AB2296123404C6C8F576B0DE0AABD9A6020840D4C9125EB679ED384170DBCAAC2FA30DC7FA9EE5B77D6DF7C344A0AA030E03 89
Malicious:	false
Reputation:	low
Preview:	MANIFEST-000004.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.450883895246111
Encrypted:	false
SSDEEP:	3:tUK6pEVNAgZmwv3IpDW2dEFhVV8sIpDW/GbVWGv:mDiAgZmwPODW2dEbVVvODWaVtv
MD5:	BF755A82A9DE47F70BCE479D0250D710
SHA1:	CD2B432786AAC217D7B94293CA50BCCA05A6549E
SHA-256:	6CFE5E3D332AE7A6484CEBF1504E69132ACAFD4A5462E742FB960A244EF1C54A
SHA-512:	8F77E4D89972CBF30D40477291610AB65BFFAD8AF79F9ABEFBDBD1C500768BC4F1C09248B454D30ACDA48354629AA291B9A1AAA402064B432E1910EF3511131
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.354 1a8c Recovering log #3.2021/08/03-00:11:04.437 1a8c Delete type=0 #3.2021/08/03-00:11:04.438 1a8c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\LOG.old (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	139
Entropy (8bit):	4.450883895246111
Encrypted:	false
SSDEEP:	3:tUK6pEVNAgZmwv3IpDW2dEFhVV8sIpDW/GbVWGv:mDiAgZmwPODW2dEbVVvODWaVtv
MD5:	BF755A82A9DE47F70BCE479D0250D710
SHA1:	CD2B432786AAC217D7B94293CA50BCCA05A6549E
SHA-256:	6CFE5E3D332AE7A6484CEBF1504E69132ACAFD4A5462E742FB960A244EF1C54A
SHA-512:	8F77E4D89972CBF30D40477291610AB65BFFAD8AF79F9ABEFBDBD1C500768BC4F1C09248B454D30ACDA48354629AA291B9A1AAA402064B432E1910EF3511131
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.354 1a8c Recovering log #3.2021/08/03-00:11:04.437 1a8c Delete type=0 #3.2021/08/03-00:11:04.438 1a8c Delete type=3 #2.

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000004	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	MPEG-4 LOAS
Category:	dropped
Size (bytes):	50
Entropy (8bit):	5.028758439731456
Encrypted:	false
SSDEEP:	3:Ukk/vxQRDKlVmt+8jzn:oO7t8n
MD5:	031D6D1E28FE41A9BDCBD8A21DA92DF1
SHA1:	38CEE81CB035A60A23D6E045E5D72116F2A58683
SHA-256:	B51BC53F3C43A5B800A723623C4E56A836367D6E2787C57D71184DF5D24151DA
SHA-512:	E994CD3A8EE3E3CF6304C33DF5B7D6CC8207E0C08D568925AFA9D46D42F6F1A5BDD7261F0FD1FCDF4DF1A173EF4E159EE1DE8125E54EFEE488A1220CE85AF 04
Malicious:	false
Reputation:	low
Preview:	V.....leveldb.BytewiseComparator...#.....

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG	
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.1621575255210335
Encrypted:	false
SSDEEP:	6:mDBS6pQ+q2PWXp+N23iKKdKfrzAdIFUtpOBSKdWZmwPOBSC4QVkwOWXp+N23iKKF:gpQ+va5Kk9FUtp0g/PDQV5f5Kk2J
MD5:	2654DAF7337F7DFC5ECEC3D5EC62C78D
SHA1:	8C5E98C7BB64F385ACA2E2A50AD9605094CECD92
SHA-256:	D0C7544C478B731F9078EBFB8FB8B8CB0FB6D3B6595F8BD6EFC18EA9A8008F9A
SHA-512:	5AF083ED2896FACE9984D1442A31051B923E63F641282C6323EA8590BA801B895FBD3F021F811AE8463D93F1E3D996C542610DE6625DE55B58C2D2AA5F722303
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.670 30c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-00:11:04.672 30c Recovering log #3.2021/08/03-00:11:04.673 30c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata\LOG.oldL. (copy)	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	335
Entropy (8bit):	5.1621575255210335
Encrypted:	false
SSDEEP:	6:mDBS6pQ+q2PWXp+N23iKKdKfrzAdIFUtpOBSKdWZmwPOBSC4QVkwOWXp+N23iKKF:gpQ+va5Kk9FUtp0g/PDQV5f5Kk2J
MD5:	2654DAF7337F7DFC5ECEC3D5EC62C78D
SHA1:	8C5E98C7BB64F385ACA2E2A50AD9605094CECD92
SHA-256:	D0C7544C478B731F9078EBFB8FB8B8CB0FB6D3B6595F8BD6EFC18EA9A8008F9A
SHA-512:	5AF083ED2896FACE9984D1442A31051B923E63F641282C6323EA8590BA801B895FBD3F021F811AE8463D93F1E3D996C542610DE6625DE55B58C2D2AA5F722303
Malicious:	false
Reputation:	low
Preview:	2021/08/03-00:11:04.670 30c Reusing MANIFEST C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/MANIFEST-000001.2021/08/03-00:11:04.672 30c Recovering log #3.2021/08/03-00:11:04.673 30c Reusing old log C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\shared_proto_db\metadata/000003.log .

C:\Users\user\AppData\Local\Google\Chrome\User Data\Last Browser	
Process:	C:\Program Files\Google\Chrome\Application\chrome.exe
File Type:	data
Category:	dropped
Size (bytes):	106
Entropy (8bit):	3.138546519832722
Encrypted:	false
SSDEEP:	3:tblolIrJ5ldQxl7aXVdJiG6R0RlAl:tbdlrnQxZaHIGi0R6l
MD5:	DE9EF0C5BCC012A3A1131988DEE272D8
SHA1:	FA9CCBDC969AC9E1474FCE773234B28D50951CD8
SHA-256:	3615498FBEF408A96BF30E01C318DAC2D5451B054998119080E7FAAC5995F590
SHA-512:	CEA946EBEADFE6BE65E33EDFF6C68953A84EC2E2410884E12F406CAC1E6C8A0793180433A7EF7CE097B24EA78A1FDBB4E3B3D9CDF1A827AB6FF5605DA3691724
Malicious:	false
Reputation:	low
Preview:	C:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.G.o.o.g.l.e.\.C.h.r.o.m.e.\.A.p.p.l.i.c.a.t.i.o.n.\.c.h.r.o.m.e...e.x.e.

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
Aug 3, 2021 00:10:53.459619999 CEST	192.168.2.3	8.8.8.8	0x916a	Standard query (0)	clients2.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:53.464632988 CEST	192.168.2.3	8.8.8.8	0x237b	Standard query (0)	axxy.coronationtraining.co.za	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:53.467102051 CEST	192.168.2.3	8.8.8.8	0x6b2a	Standard query (0)	accounts.google.com	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:54.021810055 CEST	192.168.2.3	8.8.8.8	0x218c	Standard query (0)	g.microsoftonline.com	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:54.022191048 CEST	192.168.2.3	8.8.8.8	0x73b5	Standard query (0)	portal.office.com	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:54.801466942 CEST	192.168.2.3	8.8.8.8	0x27a1	Standard query (0)	prod.msocdn.com	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:56.517283916 CEST	192.168.2.3	8.8.8.8	0xfb5a	Standard query (0)	axxy.coronationtraining.co.za	A (IP address)	IN (0x0001)
Aug 3, 2021 00:11:05.456279993 CEST	192.168.2.3	8.8.8.8	0xc24f	Standard query (0)	clients2.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 00:10:53.484055042 CEST	8.8.8.8	192.168.2.3	0x916a	No error (0)	clients2.google.com	clients.l.google.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:53.484055042 CEST	8.8.8.8	192.168.2.3	0x916a	No error (0)	clients.l.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:53.502990007 CEST	8.8.8.8	192.168.2.3	0x237b	No error (0)	axxy.coronationtraining.co.za		154.0.167.80	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:53.511568069 CEST	8.8.8.8	192.168.2.3	0x6b2a	No error (0)	accounts.google.com		216.58.205.77	A (IP address)	IN (0x0001)
Aug 3, 2021 00:10:54.054518938 CEST	8.8.8.8	192.168.2.3	0x73b5	No error (0)	portal.office.com	admin-portal.office.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:54.054518938 CEST	8.8.8.8	192.168.2.3	0x73b5	No error (0)	admin-portal.office.com	portal-office365-com.b-0004.b-msedge.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:54.090210915 CEST	8.8.8.8	192.168.2.3	0x218c	No error (0)	g.microsoftonline.com	g.live.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:54.090210915 CEST	8.8.8.8	192.168.2.3	0x218c	No error (0)	g.live.com	g.msn.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:54.090210915 CEST	8.8.8.8	192.168.2.3	0x218c	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:54.837379932 CEST	8.8.8.8	192.168.2.3	0x27a1	No error (0)	prod.msocdn.com	wildcard.msocdn.com.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:10:56.550080061 CEST	8.8.8.8	192.168.2.3	0xfb5a	No error (0)	axxy.coronationtraining.co.za		154.0.167.80	A (IP address)	IN (0x0001)
Aug 3, 2021 00:11:05.499445915 CEST	8.8.8.8	192.168.2.3	0xc24f	No error (0)	clients2.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 00:11:05.499445915 CEST	8.8.8.8	192.168.2.3	0xc24f	No error (0)	googlehosted.l.googleusercontent.com		216.58.208.129	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- axxy.coronationtraining.co.za

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49724	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:53.705657005 CEST	1184	OUT	GET / HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:53.908417940 CEST	1274	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:53 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 32 30 63 35 0d 0a 1f 8b 08 00 00 00 00 00 03 ed 3d 6b 77 db c6 95 9f d3 73 fa 1f 50 fa ec da ce 0a 7c 8a 7a 45 52 6b cb 76 e2 ad 5d 7b 6d 27 4d d3 d3 c3 33 04 86 24 22 10 40 00 50 94 d2 b3 fb db f7 de 79 00 33 c0 0c 00 52 72 9a ed 56 4c 2c 61 66 ee 9d 3b f7 3d 2f f0 fc 77 2f de 5d 7d fa cb fb 97 ce 2a 5f 87 97 bf fd cd 39 fe 76 6e d7 61 94 5d f4 56 79 9e 9c 0d 06 db ed b6 bf 9d f4 e3 74 39 18 9d 9e 9e 0e 6e b1 4d cf f1 83 f4 a2 17 e6 69 cf 09 49 b4 bc e8 d1 c8 fd f6 63 ef f2 7c 45 89 8f 98 d6 34 27 0e a2 70 e9 4f 9b e0 e6 a2 e7 c5 51 4e a3 dc cd ef 12 da 73 c4 d3 45 2f a7 b7 f9 00 51 7e e5 78 2b 92 66 34 bf f8 f6 d3 2b f7 a4 87 48 c2 20 ba 76 56 29 5d 5c f4 48 06 55 d9 e0 63 92 de 7d 47 c2 c0 27 79 10 47 9f 00 f8 55 40 43 bf ef 65 59 cf 49 69 78 d1 cb f2 bb 90 66 2b 4a f3 9e 83 7d 89 2e b0 41 17 94 ef a1 74 1b a7 bb 62 e4 0d 57 71 9a 7b 9b dc 09 60 78 3d d1 4b b0 26 4b 9a 0d 16 e4 06 4b fb f0 8f c4 c2 6a 06 b7 2e 6f 3d 28 70 55 fa a8 13 c1 11 43 dd e0 6b ba 0e a2 e0 9b 78 4d bf 1b f7 35 82 76 40 02 dd 7b 01 4d 97 74 45 c3 84 a6 7b e3 79 96 24 9f 82 90 ee 0d ff 72 3d a7 be 4f fd 57 a0 1b d9 de 58 de 92 2c a7 e9 47 56 37 9a 3e 10 9a b7 df 5d ed 8d 09 0a c2 70 39 f6 e2 14 85 05 25 b3 39 39 9c 4e 4f a6 be 8e d2 08 81 cd 47 a3 c9 f1 f1 e9 e9 09 57 c9 b6 9e 0b 7c 81 8f 1a 09 98 3e ad e8 9a be 81 a2 3a 70 d9 27 68 3f 31 eb bc 9d c0 24 dc 64 7c 3c 84 8e 87 87 e3 ee 04 e6 41 1e d2 cb 17 b1 b7 c9 82 65 74 3e e0 cf bf fd 0d 54 b1 96 f0 a7 c3 9c d2 81 33 8f fd 3b e7 ef f8 bc 00 bd 70 17 64 1d 84 77 67 ce b3 34 20 50 9b 91 28 73 33 9a 06 8b af b0 c9 9c 78 d7 cb 34 de 44 fe 99 f3 68 b1 e0 85 6b 92 2e 83 e8 cc 19 b2 a7 84 f8 7e 10 2d e5 e3 1c 6c 9d a6 45 65 9c 05 e8 05 ce 1c 32 cf e2 70 93 53 56 bc a2 c1 72 95 9f 39 a3 e1 f0 df 38 ca 20 72 b7 81 9f af 94 32 46 5e 16 fc 4c a1 6c 92 dc b2 32 2f 0e 63 40 fe e8 70 88 1f 56 04 8e 93 7a bc 0f 70 9f ac c8 dd d2 f9 75 00 ae 11 78 c6 30 b8 c4 ff 71 93 41 87 51 1c 71 0a fe 9b d1 ba c9 f3 38 3a c0 3f 83 28 d9 e4 7f 65 ac e6 a5 7f ab 16 67 9b f9 3a c8 ff d6 99 75 26 f2 59 af 84 61 26 67 ab f8 86 a6 e2 ef 9b 00 f8 44 7d 8e bc 18 e4 f8 78 41 7d 3e ee 4d 9a 61 59 12 07 e0 e7 f9 28 d9 e8 7c 0a 5a 4d f8 f0 f5 c1 89 0e 38 ca 5a 5b 90 28 4d 41 0b 15 80 d5 48 19 1b 27 7c 3c ac f0 7d 7c 84 1f 5d 0b e0 33 9a 8a 76 0c 76 2b a4 1b c5 e9 9a 84 4a 07 e3 5a 07 a3 c3 fb 74 30 8f 43 bf 44 af c8 8a ae 49 10 d6 24 18 6d c0 21 a6 b5 e2 44 44 a8 5a 45 4e eb 38 90 91 b5 c2 4d 1a 0a bd 70 d7 f1 cf 2e 49 12 4a 52 12 79 54 91 89 d4 49 63 a5 b1 d0 0f b2 24 24 a0 5f 41 84 82 72 e7 61 ec 5d 6b e6 33 39 12 5c 29 6d d0 39 11 45 ba 91 1a ed 58 9a ea 28 b9 75 c0 38 03 df 79 e4 9f e2 47 a9 75 f3 38 d1 5a 78 43 fc 7c 55 0c 76 1e df a2 2c 59 ef 02 04 8a b4 21 37 34 69 82 e6 d8 59 59 4a fc 60 93 31 3a 2a 98 8d d5 96 62 55 ef a6 15 bd 53 1c 8a 59 99 14 73 ad ab 94 b9 b2 50 2c 73 35 aa 97 ad 06 94 cc 5c 85 aa a6 1a b6 41 86 f3 53 fc 34 c9 90 0c f1 53 91 e1 8a f8 f1 16 95 0d 92 38 b4 38 68 3e 86 ff d3 e5 9c 3c 19 1e b0 4f 7f f4 b4 2e d8 1d e0 Data Ascii: 20c5=kwsP|zERkv]{m'M3$"@Py3RrVL,af;=/w/]}*_9vna]Vyt9nMiIc\|E4'pOQNsE/Q~x+f4+H vV)]\HUc}G' yGU@CeYIixf+J}.AtbWq{`x=K&KKj.o=(pUCkxM5v@{MtE{y$r=OWX,GV7>]p9%99NOGW|>:p'h?1$d\|<Aet>T3;pdwg4 P(s3x4Dhk.~-lEe2pSVr98 r2F^Ll2/c@pVzpux0qAQq8:?(eg:u&Ya&gD}xA}>MaY(\|ZM8Z[(MAH'\|<}\|]3vv+JZt0CDI$m !DDZEN8Mp.IJRyTIc$$_Ara]k39\)m9EX(u8yGu8ZxC|Uv,Y!74iYYJ`1:*bUSYsP,s5\AS4S88h><O.
Aug 3, 2021 00:10:53.970778942 CEST	1289	OUT	GET /assets/SpryValidationTextField.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.171333075 CEST	2025	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Tue, 15 Jul 2014 13:04:04 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 34 32 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 8d 56 4d 6f e3 36 10 3d af 01 ff 87 69 7a 49 02 59 49 fa b1 d8 ba 97 76 0d 08 cd 61 8b c5 c6 db 9e 69 69 64 11 91 48 95 a4 e3 08 8b fd ef 9d 21 2d 5b 92 65 3b 09 82 d8 c3 99 21 e7 cd 9b 47 fe 91 16 c2 58 74 70 f5 75 99 cc 3e 5c fd 3e 9d 4c 27 77 b7 f0 54 9b e6 1f 51 ca 4c 38 a9 d5 12 5f 5d 22 b1 cc e2 d4 5a 98 c1 0b 1a 4b 66 b8 8f 7f a1 6f ec 0b 9f 0d ce be 60 89 c2 22 3c c4 ef e3 07 b8 bd db e5 5a e8 ba 31 72 5d 38 b8 4e 6f e0 a7 fb fb f7 31 fc 99 e9 15 c2 53 63 1d 56 16 1e 55 aa 4d ad 8d 70 98 d1 5a 59 82 f7 b7 60 d0 a2 79 61 63 c8 e6 f3 2d 0b b2 82 30 08 ae 40 48 4b 61 2d 5a 10 75 5d 4a cc 80 8e c5 66 34 46 1b a8 d0 5a b1 46 3b 9d c0 2d 6c 0b 99 16 50 1b 7c 41 e5 d8 a9 82 dc e8 0a 56 28 d5 1a 32 69 eb 52 34 94 61 d5 40 86 b9 d8 94 2e e6 b8 3b 98 4e 62 47 08 e4 8c c0 17 fc 6f 23 0d 66 9f ec 3a ea 2d 3c aa 17 c6 2b d1 a6 12 ee 68 f5 93 54 04 e7 06 79 a1 67 17 af e3 76 a9 16 dc 99 11 ff 51 bb ef 15 19 e1 db 74 f2 6e 57 ca 1c 94 56 48 1d fd de 03 ce 52 97 52 a7 8d 05 ea bd 5a 07 14 b7 a2 d9 83 05 a5 d6 cf 84 16 06 24 b7 32 5b 13 41 a4 05 a9 08 5d 04 9d 77 10 b6 8e 9a 66 3d 50 bb fc 6d 43 98 55 a2 45 92 3a 49 c0 6a 93 a1 01 a1 32 48 75 49 c1 39 fd 1d 52 71 31 fb 44 21 71 48 06 d7 18 af 63 38 6e c2 13 fb dc f0 d1 06 dd 77 ba 9e 95 d4 e7 92 36 52 4e 48 85 87 cd 42 3d 91 df 88 8f e2 0a 8a e7 fa b5 2a 1b ef 61 6b 4c 65 2e d3 3e 89 20 15 8a b8 02 b6 d0 5b c5 24 a1 02 1d 33 87 43 76 90 13 bb 74 8d c6 51 1e 0d 57 52 95 b4 f3 55 60 d1 18 89 fc f9 47 ea 3a 4f ae 61 d4 db 98 37 8c ba c4 c8 23 ff 0b 4c 1d c9 7f 96 c1 23 f9 5b ff e9 a4 c7 e2 00 23 f1 f8 9d 67 cd 1c 7e 5c 2c 7e a6 1f b6 04 4a cd e1 a1 7e 05 ab 09 85 ce e2 f7 a0 18 2d f5 41 d1 56 d4 2c 83 08 6b a3 37 75 77 12 88 25 46 97 fb 51 f0 c2 a2 49 61 c8 a3 62 b5 b8 7e fc fb f3 d7 e5 8d 1f 0d 1a 10 f9 8c 97 07 24 8c c6 9c 68 96 eb 74 63 23 9a 81 d0 5e b8 23 4f df 33 fa 54 ed fa c0 1f 77 10 07 ab 47 23 58 c3 c7 08 42 4c 3b 22 66 27 82 5b dd a9 84 59 8e 82 74 ce ef 1e 31 0f 53 4d 7a 1d c6 82 5c 2b 9a 06 d8 58 4c 05 0f 69 7f 28 e6 3e f5 ac 57 55 c6 85 51 23 d2 de 74 c1 a9 e9 f2 38 bd 2d 8d 77 dd 23 2c 1d 15 91 c3 b5 db 17 a6 f4 40 c5 6f 76 83 c4 08 50 4f ff 1d 6d 00 1b 02 4e 41 41 0e 3b 15 82 74 82 5a 8f 14 b6 12 e9 33 93 80 e6 bf 23 1d d2 c5 83 49 f5 ba 1a a8 2a 55 bd 71 51 f8 37 ea c0 a4 3d e4 9d b5 64 fd f8 21 f9 f5 e3 43 47 86 c7 cf 4d e2 d2 92 62 fc e0 5e 41 cf 1e 7b 70 b4 9e ca 44 a7 e4 b3 ad eb 28 fc 58 73 a2 53 a2 73 3e 51 4f 81 a2 11 09 ba 10 de 15 a4 68 44 91 2e ee 7e d0 9b 68 44 a0 2e ee 7e 22 bc a7 63 3e ea 14 03 92 e4 37 fa 3d c3 00 6e b0 c1 14 25 3d 75 5a b1 18 b6 bf c1 b2 d4 db 37 13 37 e1 2c e7 88 db 71 38 79 ec 24 59 2c 7a ef 07 a2 Data Ascii: 42cVMo6=izIYIvaiidH!-[e;!GXtpu>\>L'wTQL8_]"ZKfo`"<Z1r]8No1ScVUMpZY`yac-0@HKa-Zu]Jf4FZF;-lP|AV(2iR4a@.;NbGo#f:-<+hTygvQtnWVHRRZ$2[A]wf=PmCUE:Ij2HuI9Rq1D!qHc8nw6RNHB=*akLe.> [$3Cvt QWRU`G:Oa7#L#[#g~\,~J~-AV,k7uw%FQIab~$htc#^#O3TwG#XBL;"f'[Yt1SMz\+XLi(>WUQ#t8-w#,@ovPOmNAA ;tZ3#I*UqQ7=d!CGMb^A{pD(XsSs>QOhD.~hD.~"c>7=n%=uZ77,q8y$Y,z
Aug 3, 2021 00:10:54.186908960 CEST	2030	OUT	GET /css/MasterStyles15.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.389544010 CEST	2037	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Mon, 13 Jun 2016 10:48:22 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 34 30 30 30 0d 0a 1f 8b 08 00 00 00 00 00 03 d4 bd 09 b3 a2 ca d2 28 fa 57 d6 3b 27 be b8 f7 5c 57 2f 91 49 ed 8e bb e3 01 e2 88 8a 22 38 dc f8 62 07 33 28 93 0c 22 76 f4 7f 7f 05 38 80 a2 6b f5 3e 43 bc bb 3b 7a b7 d6 90 95 95 99 95 95 99 95 55 fe af 9f 96 e9 a8 df 24 5f 15 77 df 83 d0 37 e5 f0 d7 87 db c0 42 51 b2 d4 f7 eb 27 f8 67 6c 2a a1 f1 bd 01 41 ff f5 c3 16 7d dd 74 be 49 6e 18 ba f6 77 04 f2 8e 3f 24 d7 57 54 ff 9b ec 5a 96 e8 05 ea f7 40 f5 44 5f 0c d5 4b 45 e0 89 b2 e9 e8 df 1b de f1 06 fe 2d 34 0a 23 80 6f 3f 35 d7 09 bf c5 aa a9 1b e1 77 c7 f5 6d d1 fa 11 1b 66 a8 66 fd 55 50 14 fb a2 f7 23 47 05 c6 fe eb 47 d6 3e 30 4f ea f7 c6 73 c8 6f a1 f2 d3 13 15 25 1d 1f f3 8e 6f 0d 18 20 7c 50 fd d0 94 45 eb 9b 68 99 ba f3 3d 74 bd 1f a1 7a 0c cf 5f 2d 55 0b 7f 19 68 4e 1b a3 88 cf 2f 03 ab 2c c5 ab 4a c5 ef 86 0b 06 fa 99 41 56 54 d9 05 24 31 5d e7 7b e4 00 9a a4 ed 7f c8 91 1f b8 fe 77 cf 35 9d 50 f5 7f 89 ff 47 31 83 14 67 e5 bf 7f 02 5a 82 9a b f e3 38 fe ff 98 b6 e7 fa a1 e8 84 c5 06 67 d8 67 08 8a aa 89 91 15 fe b8 1f ca 71 1d f5 97 f7 33 67 d9 f7 86 7a 7c 83 de b2 ff ff 32 6d fd e7 85 3b 61 62 a9 79 53 c3 3f 17 7e 0f 5c cb 54 de 00 59 df fe 8e 41 e9 9f 33 df bf b7 bc 14 48 f6 ff 5f 1f 1d df f5 14 37 76 18 33 00 e3 9e 71 7b ff 58 00 34 48 f7 78 2d f9 e9 a6 02 10 26 df 3f d0 1f 9a 69 81 b9 7e 17 2d cf 10 ff e7 b9 fc 7f a3 d0 3f 7e 55 0b c0 3d 5b 02 d5 52 e5 f0 fb 15 f2 99 4e 32 22 2b 0a fc 43 12 e5 9d ee bb 80 c2 df ce 15 9a a6 fd 78 9c 92 82 29 aa 0a ff 72 bd 94 4a 17 f1 f8 96 0e 00 64 1c 88 52 5e f1 64 94 5f 9a a9 5a 4a a0 86 15 b4 6a cb e9 9f 0b ad 52 58 29 c5 b3 7f 7e 5c a4 10 07 df 0a 7f 7f 59 aa ae 3a ca 95 49 a0 14 cb ba 61 69 9d 28 a9 d6 b9 2a c7 0f 50 fe 57 4a 14 11 ac d9 9f a9 0c 68 96 1b 7f 17 a3 d0 fd e1 ab d9 62 c8 38 29 45 60 79 3a ef a6 e3 45 e1 ff 09 13 4f fd df 7f cb 8b fe f6 df a5 42 d0 47 0d ef ca 82 48 b2 4d 50 78 5d 37 50 3a 89 6c 0e 36 40 e3 aa 0b c0 42 3a 4b 7c a6 05 ae c8 1c cc c0 04 64 fb 55 80 29 1b aa bc 93 dc e3 7f 5f 69 5a 1c d1 17 15 d3 bd 55 fd ac 94 11 18 fb c7 8f 6f b6 7b fa 76 15 26 18 fb 01 a4 45 da 99 61 b9 cc 0e 4a df 0b 9f 7f b9 d6 7b 74 a1 67 36 2d a8 c0 98 bb ef 39 bd 61 d5 fe a5 dc 77 f9 a5 28 e5 92 b4 d5 87 27 61 57 59 3a ab c7 94 87 a0 bc f1 50 d1 c8 6b 2c ac 2c 7d e7 52 18 2a 17 c3 50 0e 07 85 ee e1 a0 79 4d 58 e8 01 b4 d9 b9 83 e3 9e cb 6e 9c 2c 68 93 0f c9 72 e5 dd 4f 40 75 cf 12 93 ef d9 b7 b4 4f aa 65 7f 3e 2a de 5f 1f 36 76 99 74 86 a6 2d 35 a0 8b 68 5e 66 95 0d 6b 5f cb 2f 05 d6 ad e5 6d 91 7d d8 29 d6 e7 e2 1b d2 e4 74 f5 ad 6b b9 62 c8 80 96 73 d5 02 9a ec a0 fe d4 d2 92 5c 05 dc 5a cc 53 e1 bb 6b e2 a7 65 79 9b 54 0d 11 a9 ea 28 41 ba d7 28 e5 a6 65 90 85 b6 05 b8 9d Data Ascii: 4000(W;'\W/I"8b3("v8k>C;zU$_w7BQ'gl*A}tlnw?$WTZ@D_KE-4#o?5wmffUP#GG>0Oso%o |PEh=tz_-UhN/ ,JAVT$1]{w5PG1gZ8ggq3gz|2m;abyS?~\TYA3H_7v3q{X4Hx-&?i~-?~U=[RN2"+Cx)rJdR^d_ZJjRX)~\Y:Iai(*PWJhb8)E`y :EOBGHMPx]7P:l6@B:K|dU)_iZUo{v&EaJ{tg6-9aw('aWY:Pk,,}R*PyMXn,hrO@uOe>*_6vt-5h^fk_/m})tkbs\ZSkeyT(A(e
Aug 3, 2021 00:10:54.597409964 CEST	2074	OUT	GET /assets/SpryValidationTextField.js HTTP/1.1 Host: axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.801476955 CEST	2104	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Tue, 15 Jul 2014 13:04:04 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 34 34 34 31 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ed 7d f9 57 1b 49 92 f0 cf f4 7b fe 1f d2 da 9e 41 32 42 07 60 6c a3 a6 3d 32 e0 36 3b 18 bc 80 fb 58 a0 fd 0a a9 80 6a 4b 2a b5 aa 04 66 da 7c 7f fb 17 47 9e 55 59 3a 80 9e 99 dd b7 b4 1b a4 cc c8 c8 88 c8 c8 c8 c8 c8 ab 5e 17 47 c3 d1 ed 8f 41 2f ea 06 69 14 0f 8e c3 2f e9 db 28 ec 75 6b bf 25 62 59 5c 87 a3 04 52 45 a3 b6 fa 12 be 22 ac f8 30 0a 97 0f c3 5e 18 24 a1 68 d6 d6 6b cd 27 df d4 eb f8 bf d8 8a 87 b7 a3 e8 f2 2a 15 e5 4e 45 ac 34 1a eb 35 d1 ee c6 e7 a1 38 ba 4d d2 b0 9f 88 dd 41 27 1e 0d e3 51 90 86 dd 1a 95 69 f7 7a 82 ca 24 62 14 26 e1 e8 5a 66 50 e6 61 d8 8d 92 74 14 9d 8f 91 36 11 0c ba 62 0c b5 46 03 91 c4 e3 51 27 a4 94 f3 68 10 00 59 17 f1 a8 9f 54 c5 4d 94 5e 89 78 44 7f e3 71 4a 68 fa 71 37 ba 88 3a c4 60 55 04 a3 50 0c c3 51 3f 4a 81 08 31 1c c5 d7 51 17 3e a4 57 41 0a bf 42 40 d4 eb c5 37 d1 e0 52 74 e2 41 37 c2 42 09 15 ea 87 e9 86 26 4d 88 67 19 f2 12 11 5f 28 ba 3a 71 17 e0 c7 49 0a 4c a5 01 d0 8b 88 83 f3 f8 1a b3 94 90 06 71 1a 75 c2 aa 44 27 00 26 4a 44 0f 30 22 22 bb ee 41 37 43 18 54 db e9 05 51 3f 1c d5 0a 89 81 4a 2d c9 28 62 80 dd ee 18 08 fc b3 e8 11 92 d7 6e dc 19 f7 c3 41 4a 32 d7 18 a1 64 1d da 26 06 88 91 e8 83 12 8c a2 a0 97 98 36 a0 c6 a3 e2 16 2b 86 c5 fd 30 a2 92 08 31 08 fa 21 d2 55 ac 5f c0 8f 01 a5 c6 89 d2 44 93 02 fc 70 0d f1 28 01 52 6e 05 60 01 dd 02 ce 62 11 0e ba 90 1a a2 1a 01 69 fd 38 0d 05 cb 0d 94 b4 0b 34 83 8e 8a 0b c8 20 09 69 8c 49 7c 91 de a0 9e 48 d5 13 c9 30 ec a0 de 41 e1 08 35 72 84 1a 37 60 dd 4b 12 c5 19 95 3f 7e b7 7b 24 8e 0e de 1e ff d4 3e dc 11 f0 f9 c3 e1 c1 8f bb db 3b db e2 cd 2f 90 b9 23 b6 0e 3e fc 72 b8 fb c3 bb 63 f1 ee 60 6f 7b e7 f0 48 b4 f7 b7 21 75 ff f8 70 f7 cd c7 e3 03 48 28 b5 8f a0 64 89 7b 15 64 b6 f7 7f 11 3b 3f 7f 38 dc 39 3a 12 07 87 62 f7 fd 87 bd 5d 40 08 35 1c b6 f7 8f 77 77 8e aa 62 77 7f 6b ef e3 f6 ee fe 0f 55 01 48 c4 fe c1 b1 d8 db 7d bf 7b 0c 60 c7 07 55 ac 98 b0 e5 8b 8a 83 b7 e2 fd ce e1 d6 3b f8 da 7e b3 bb b7 7b fc 0b d5 f9 76 f7 78 1f eb 7b 0b 15 b6 c5 87 f6 e1 f1 ee d6 c7 bd f6 a1 f8 f0 f1 f0 c3 c1 11 a3 43 16 b7 77 8f b6 f6 da bb ef 77 b6 6b 40 05 d4 2c 76 7e dc d9 3f 16 47 ef da 7b 7b 19 8e 0f 7e da df 39 44 16 1c 76 df 30 b2 bd dd f6 9b bd 1d ae 10 18 de de 3d dc d9 3a 46 ce cc a7 2d 10 24 90 b9 57 15 47 1f 76 b6 76 f1 c3 ce cf 3b c0 53 fb f0 97 2a e0 65 db 75 b0 7f b4 f3 5f 1f 01 10 00 c4 76 fb 7d fb 07 60 b3 3c 45 42 d0 4c 5b 1f 0f 77 de 23 e9 07 6f 09 d1 d1 c7 37 47 c7 bb c7 1f 8f 77 c4 0f 07 07 db 24 fb a3 9d c3 1f 77 b7 76 8e 5a 62 ef e0 88 84 f7 f1 68 a7 0a b5 1c b7 91 00 44 03 92 83 6c f8 fc e6 e3 d1 2e ca 90 25 bf 7f bc 73 78 Data Ascii: 4441}Wl{A2B`l=26;XjK*f|GUY:^GA/i/(uk%bY\RE"0^$hk'*NE458MA'Qiz$b&ZfPat6bFQ'hYTM^xDqJhq7:`UPQ?J1Q>WAB@7RtA7B&Mg_(:qILquD'&JD0""A7CTQ?J-(bnAJ2d&6+01!U_Dp(Rn`bi84 iI|H0A5r7`K?~{$>;/#>rc`o{H!upH(d{d;?89:b]@5wwbwkUH}{`U;~{vx{Cwwk@,v~?G{{~9Dv0=:F-$WGvv;S*eu_v}`<EBL[w#o7Gw$wvZbhDl.%sx
Aug 3, 2021 00:10:54.805401087 CEST	2122	OUT	GET /16.00.1279.006/en-US/css/Fabric/0.10.3/fonts/office365icons.woff? HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive Origin: http://axxy.coronationtraining.co.za User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: */* Referer: http://axxy.coronationtraining.co.za/css/EmbeddedFonts.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:55.016778946 CEST	2181	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:53.973807096 CEST	1290	OUT	GET /assets/SpryValidationPassword.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.179171085 CEST	2029	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Tue, 15 Jul 2014 13:06:16 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 33 36 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 8d 96 51 4f db 30 10 c7 9f a9 d4 ef 70 ea 5e 00 a5 01 36 0d b1 ee 65 a3 52 25 1e 98 10 05 f6 ec 3a d7 c4 c2 b5 33 db a5 54 d3 be fb ce 76 53 92 34 2d 50 a1 94 cb f9 7c f7 bf df 9d f8 c1 0b 66 2c 3a 18 3c 3e 4c 86 57 83 ef fd de d9 29 4c 4b b3 7e 62 52 64 cc 09 ad ee 98 b5 2b 6d b2 94 5b 0b 43 78 41 63 c9 0a e7 e9 05 fd e5 5d e1 ce e0 f0 1e 25 32 8b 70 91 5e d2 8b d3 b3 10 68 ac cb b5 11 79 e1 e0 98 9f c0 e7 f3 f3 cb 14 7e 66 7a 86 30 5d 5b 87 0b 0b 37 8a 6b 53 6a c3 1c 66 f4 4e 4a 08 fe 16 0c 5a 34 2f de e8 63 f9 0f c5 7b 28 c8 0a cc 20 b8 02 81 4b ca 0c 2d b0 b2 94 02 33 a0 a4 bc 19 8d d1 06 16 68 2d cb d1 f6 7b 70 0a ab 42 f0 02 4a 83 2f a8 9c 77 5a c0 dc e8 05 cc 50 a8 1c 32 61 4b c9 d6 14 61 b6 86 0c e7 6c 29 5d ea cf 9d 41 bf 97 96 9b f2 ef f1 cf 52 18 cc 6e 6d 9e d4 ed 37 ea c5 4b 35 75 06 55 ee 8a f6 eb 5b a1 c6 5e 63 6f af 9b d9 6b 97 79 bc b4 4e 2f 5a c6 d0 0a b2 c1 df 7e ef 68 93 ec 08 94 56 48 ed fa d7 90 c6 52 17 b8 d3 c6 02 35 56 e5 51 a7 15 5b 6f e5 00 a9 f5 33 e9 81 51 ab 95 c8 72 ea be b0 20 14 e9 87 a0 e7 35 0d ad a3 b6 d8 20 c5 26 7e 25 b9 47 86 55 5a 51 af 48 3a 4a 14 0d 30 95 01 d7 92 0e cf e9 f7 2d 94 c3 57 b7 0d 14 03 c7 60 70 8c 69 9e c2 8e cc 53 ef 72 e2 33 6b b5 d7 e9 72 28 a9 91 92 ee 51 8e 09 85 6f 77 c5 72 92 70 8f cf c4 15 74 de 97 af 95 5c 07 0f 5b 22 17 73 c1 9b 94 00 67 8a 60 00 5b e8 95 f2 14 50 7d ce a3 e1 8f 6c 14 27 7c 74 89 c6 51 1c 0d 03 a1 24 dd 3c 88 98 74 50 12 d2 df ad aa 4d c1 06 8e 96 f7 3b cc b4 bd bb 51 6a 71 d9 3a d4 41 ed 0e 86 ad 23 5b 36 fb bd 06 88 51 0a 42 f1 28 34 7e 04 9f c6 e3 2f f4 e3 2d 91 8a 11 5c 94 af 60 35 5d 58 7b 59 23 17 14 e1 41 62 1b 44 c8 8d 5e 96 75 90 a9 cb 46 cb 2d c9 61 f2 35 ad 00 f2 58 f8 71 3e be f9 75 f7 f8 70 12 c8 26 be c5 33 be cf 77 24 7b 44 98 cc 35 5f da 84 10 8e 0d 82 33 f2 0c d2 40 a5 0d 99 16 42 d1 10 2e d1 7f 65 af d5 57 1e 04 d9 fa 27 10 9f 15 e5 66 b3 a9 56 ba 56 8d 27 15 19 2d a3 90 41 e2 59 e2 9a 56 6a 44 9b 5c 17 44 34 2c 2d 72 e6 e7 ac 09 f6 28 84 1e 36 2a cb 7c 71 d4 08 de 98 10 d8 37 21 41 ab 8f 85 09 ae 5b 95 85 a3 22 e6 70 ec b6 85 29 dd 5a b5 27 9b 61 a0 07 b5 f5 77 67 0f bc 21 ca 14 77 c0 db 45 05 a3 51 a7 ee 23 1d 9b 31 fe ec 39 a0 11 ae 4d bf 70 69 73 d8 9e 22 c2 3e 8e 50 e5 d2 25 f1 d1 f5 de 13 fb 16 75 58 91 7a 7d 35 f9 7a 7d 51 83 b1 3b 6b da 0e 55 97 bb d3 0e 1b f0 60 d2 cd cc 1a 6b 22 d9 b3 fd aa a2 da 87 bb 26 3b d9 3b da 07 43 35 16 50 b2 bb 81 0e 1e ae 6d 89 a4 bd 26 0e df 5a 5f 64 c9 ee 26 ab 1d de d7 b8 c9 e4 1b 7d 0e 34 ce f7 c5 20 47 41 ff 43 54 43 de ee da 1a a5 d4 ab 8f d2 36 f1 41 0e d0 56 7b bf 37 e9 c9 64 3c 8e 49 ff 07 00 25 eb 69 7a 09 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 36eQO0p^6eR%:3TvS4-P|f,:<>LW)LK~bRd+m[CxAc]%2p^hy~fz0][7kSjfNJZ4/c{(K-3h-{pBJ/wZP2aKal)]ARnm7K5uU[^cokyN/Z~hVHR5VQ[o3Qr 5 &~%GUZQH:J0-W`piSr3kr(Qowrpt\["sg`[P}l'|tQ$<tPM;Qjq:A#[6QB(4~/-\` 5]X{Y#AbD^uF-a5Xq>up&3w${D5_3@B.eW'fVV'-AYVjD\D4,-r(6*|q7!A["p)Z'awg!wEQ#19Mpis">P%uXz}5z}Q;kU`k"&;; C5Pm&Z_d&}4 GACTC6AV{7d<l%iz0
Aug 3, 2021 00:10:54.194547892 CEST	2031	OUT	GET /css/shellg2coremincss_ba45585d.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.399143934 CEST	2057	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sat, 11 Jun 2016 21:43:38 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 31 39 34 63 0d 0a 1f 8b 08 00 00 00 00 00 00 03 dd 3d 69 73 dc c8 75 7f 65 c2 ad 14 45 8b a0 30 f7 55 eb ec 90 14 29 6a 49 f1 a6 44 6d 6d 52 18 a0 31 03 12 c7 08 c0 1c 14 8b 55 2b 66 bd 96 64 25 15 c7 d9 4d 9c 2f 6b c7 76 52 e5 f2 07 c7 d7 da fe 51 f9 0d e9 6e 5c dd c0 c3 31 14 b5 eb b5 58 22 67 ba 5f bf 7e fd ae 7e fd ba 1b 58 b1 aa 8d 7a 7f ec ba 96 79 d9 97 e4 f3 81 6d 8d 4d 45 90 2d dd b2 3b ae 2d 99 ce 48 b2 91 e9 5e 7d a0 5a a6 2b a8 92 8c 2e fd 4f 86 a6 5f 74 16 49 fb 2d d9 32 9d c5 ae 63 cb 9d b1 ad df 59 74 86 48 d7 91 e5 6a a4 fc 1f 50 ab 26 57 ca 7d 75 05 97 fc dd 7b 1a 52 b5 d9 e2 52 49 b5 6c 43 72 ef 2c 22 a3 8f 14 05 29 82 35 c2 dd 5c 8c d0 e2 d2 72 84 64 6a a9 aa 87 45 6d b7 cb 72 bb 56 5f 21 45 4c 7b ef 2b d3 c4 75 fd 16 ed 66 b5 2d d7 5b f2 0a 2e 61 1a b8 f6 18 25 fa 71 26 03 bf 9b 66 a3 52 ad b4 eb 2b b8 e4 bd 29 ea 33 0d 71 c9 e2 52 97 0e 7e 8a b4 c1 d0 ed 98 a4 46 f7 8a 1c f7 42 47 7e c9 d5 0a e1 8a ec 08 7d c9 41 a5 8f 64 5d 72 9c bf 7f 7f c1 70 04 c2 29 41 58 f8 b8 d3 47 18 2d 5a 06 00 bf f3 fe 42 29 09 c9 31 7d 61 97 70 05 05 9c 5f 58 5e 08 a5 b0 90 a4 06 22 d9 19 21 e9 1c 7f 31 51 57 d1 9c 91 2e 5d 74 34 53 d7 4c 24 f4 75 4b 3e ef ba 68 e6 0a 0a 92 2d 5b 72 35 cb c4 95 43 64 6b ae 57 2e e9 da c0 ec c8 58 5c c8 f6 90 4f 24 5b 93 cc 10 3b 85 a2 ca 43 78 e7 75 43 91 0f 3d 22 ca dd a9 a6 b8 c3 8e 34 76 ad ae 21 d9 03 cd 14 74 a4 ba 1d 31 f8 66 53 38 31 9f 91 05 38 78 09 8e 90 a3 e7 6a 05 c3 13 05 10 e8 70 64 cd 96 31 fb 7c ce f7 2d 5b 41 b6 cf 52 c7 d2 35 a5 eb 17 d9 92 a2 8d 9d 4e 19 19 3c ba 95 72 bd 8b 19 de 3f d7 5c a1 6f cd 04 47 7b ae 99 83 8e df 0a 97 74 e1 52 c1 b0 9e a7 34 18 49 8a 42 8a 56 70 67 57 1f 18 48 d1 a4 92 23 db 08 99 25 c9 54 4a 77 82 ee 0c cc 3c 05 4d b0 76 08 23 6d 86 74 81 0a b0 23 2e 5d 66 0d 91 67 46 8c 1b 98 18 24 b4 2e c3 cf 9d d6 68 f6 37 9a 31 b2 6c 17 cb 1c 02 2e 97 19 e8 72 39 17 bc c2 82 57 72 c1 6b 2c 78 2d 17 9c 25 bd 9c 4b 7b 45 64 c0 2b 62 2e 38 4b 7b 25 97 f6 4a 9d 05 af e7 82 37 58 f0 46 1e 78 95 c5 5e e5 b1 7f a4 48 ae 44 1b 84 2e 05 7f 76 b1 11 77 24 d7 b5 ef 84 d5 4b 14 b3 67 3c 9e 96 6c 68 ba 1e 6f b3 f8 7f 9f bc 58 64 20 47 3a 36 84 24 cc a7 2c cc b3 31 72 a8 37 49 c2 7d c6 e1 42 b6 03 42 bd 4c 42 f5 14 25 09 78 cd a1 33 24 0d 22 ff 15 0b a3 99 aa b5 c6 99 04 03 f9 9a 85 94 74 64 bb 00 d0 0f 58 a0 59 2a ae 37 2c 58 1f 81 8c fd 17 16 46 c6 1d 9a 8a 64 03 70 3f 64 e1 1c 79 88 94 b1 4e dd 46 02 f2 5f 59 48 34 21 a5 49 a0 1f b1 40 d8 65 2b b6 36 81 86 f0 05 47 de 50 82 70 fd 3b 27 00 64 8e 01 98 9f b0 30 aa 34 b1 f0 04 83 20 25 fa 2f 4e ec 43 4c 1a 00 f4 33 8e 2a e2 e2 93 40 9f 7e 8f 23 4b 33 35 c9 1d db 60 9f bf 64 21 07 08 e4 ff ef 39 fe e3 99 19 5d 00 50 7f e0 a0 30 26 Data Ascii: 194c=isueE0U)jIDmmR1U+fd%M/kvRQn\1X"g_~~XzymME-;-H^}Z+.O_tl-2cYtHjP&W}u{RRIlCr,")5\rdjEm rV_!EL{+uf-[.a%q&fR+)3qR~FBG~}Ad]rp)AXG-ZB)1}ap_X^"!1QW.]t4SL$uK>h-[r5CdkW.X\O$[;CxuC="4v!t1fS818xjpd1|-[AR5N<r?\oG{tR4IBVpgWH#%TJw<Mv#mt#.]fgF$.h71l.r9Wrk,x-%K{Ed+b.8K{%J7XFx^HD.vw$Kg<lhoXd G:6$,1r7I }BBLB%x3$"tdXY*7,XFdp?dyNF_YH4!I@e+6GPp;'d04 %/NCL3*@~#K35`d!9]P0&
Aug 3, 2021 00:10:54.420039892 CEST	2065	OUT	GET /assets/jquery.ddslick.min.js HTTP/1.1 Host: axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.623928070 CEST	2092	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Wed, 23 Apr 2014 01:03:00 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 39 34 34 0d 0a 1f 8b 08 00 00 00 00 00 03 b5 59 cd 8e dc b8 11 7e 15 5a 83 ec a8 e1 91 dc 63 af 8d 40 3d d3 8b 60 7d d8 04 d9 78 03 3b c8 c1 f0 81 a2 a8 6e 7a 24 51 91 d8 f3 b3 bd 03 e4 9e 47 ca 21 ef 92 17 c8 2b a4 aa 48 76 53 3f d3 76 10 2c 0c d8 2d b2 58 2c d6 ef 57 e5 ff fc f3 5f 71 b9 6b 84 51 ba 61 31 5f b0 3d 3b 7c 6e 62 7e c1 72 5c ba e5 1d 13 ec 9a f1 b4 e0 86 c7 51 51 f4 95 12 37 d1 62 45 5b 05 6d 95 aa 29 e2 28 2d 8a a4 97 95 14 46 16 d1 e2 82 49 d8 2b d2 5e e5 95 6a 36 fd 70 3f b9 e5 d5 4e 22 55 39 e2 a0 5b 94 a0 c7 ad cd 0c 83 56 ab c6 c8 0e b7 b7 b3 27 a3 45 2a ff 16 e7 b0 7f 03 fb db 54 54 ba 97 bd 89 a3 4a e1 a1 0a 16 45 da 4b 63 90 e7 05 ab 07 df f4 c8 8f f9 a7 d5 3c e3 4e d6 fa 56 7e 5f f1 be 47 4d b8 8d e0 d1 2b b8 90 17 c5 49 0a bc cd 7e fd be 29 e4 3d dc 9f 0f 16 8d 44 99 6e c2 b5 b7 20 15 ac d5 2b a6 4a 16 57 69 bf d5 77 ef dd de 0f 1f 7e fc 23 1a aa 48 b7 a6 ae e2 b8 4e 55 cd 37 f2 7d 27 d8 77 ec fc 4a d5 1b 26 50 9c eb 28 54 3f d1 9c b3 e7 c8 8d 7e ff a4 7b 45 a6 bf be 66 51 a7 36 5b 13 c1 f9 88 15 8e 36 71 6b 19 8b a2 05 9c 3b 8f 58 df 89 eb 08 79 04 57 d2 c6 8b f5 f9 81 0e e4 31 f2 de 90 2c 15 cf 65 35 27 0d 52 44 6b cb 8a a8 9f b3 e8 ea 05 91 af a3 90 55 21 7b d1 29 d2 29 71 ec 6b 5e cd 72 0c 09 0b fb e9 5e 6b 3a 70 72 6e e4 db 01 2b 7a e8 dc e9 c4 d3 17 83 b7 3b 61 c3 6b 48 66 12 c8 cb bc 60 8f 4c 56 bd f4 b6 b1 8f 03 17 90 29 b8 3f 7c 52 10 90 4b 68 50 af 6a 78 35 da 18 47 dd 05 13 b0 aa 20 5a 57 ec 33 fd 8d 0e 61 1e 5a a9 4b 56 a5 ba f1 5e 41 66 f4 e1 1c a1 7f 84 bb a9 00 29 63 b3 55 3d 32 04 29 1f 8f a1 bf 8d 07 71 9f 4f 82 1b a3 a8 b0 51 33 88 cc 20 70 25 6d 1f 0f 06 41 5b 52 4c 2b 38 93 dd 2a 64 20 31 26 b8 a5 13 f8 c8 44 97 65 42 51 0b 11 d7 68 13 17 8b 14 5e 5f c8 bf b4 f1 eb e5 91 f8 c0 74 12 96 6e 27 d9 b5 91 d3 50 69 23 c4 b3 89 4a de 9b 88 0c 71 ea ac 37 df e1 e8 5b 7d d7 84 87 07 a1 3e 3a 79 83 7a 0c f4 aa 6c 8a 9d 4d 75 a3 f7 cd 69 ee a4 a0 5f 7a c5 41 88 cf 56 08 34 6e 3e 9b b9 81 97 40 1e 5b 49 e1 ee b2 bc 78 22 cb 87 81 f2 a5 8a 60 d3 88 37 88 48 2b d9 6c cc 96 5d 5d b3 25 fb e6 1b d0 b0 5b 58 b3 e5 58 4f c3 3c e1 24 04 cf 93 3f 58 29 a9 54 0d 9c f8 c6 3a 71 3e 51 36 56 07 2e b6 41 e1 1b 14 39 8a 89 e0 21 62 4e 1b 63 ef 76 39 7e 46 17 e5 28 80 1c e5 40 13 72 ac 89 72 a4 89 99 ab 9e d4 43 41 7a c0 bf 40 7f 4d ea d2 06 48 71 7c af 40 9e 78 71 fe 51 7c c2 df 9d 34 bb ae 61 f8 99 f2 b6 ad 1e 5c 62 f8 5d d7 f1 87 b4 ed b4 d1 98 60 d0 47 85 b4 99 83 77 9b 5d 2d 1b 03 54 97 c7 2c 17 a4 22 50 26 26 20 9d 7f 46 9f 62 bf fc c2 9e 89 f0 ae 54 35 ca 0c 6e 3b b0 0c a2 8e a7 b2 eb 74 17 47 3f 4a b3 d5 05 24 e9 e7 0c 4b 0c 24 6b 2d 7b 06 b9 81 c9 7b d5 9b 3e Data Ascii: 944Y~Zc@=`}x;nz$QG!+HvS?v,-X,W_qkQa1_=;|nb~r\QQ7bE[m)(-FI+^j6p?N"U9[V'E*TTJEKc<NV~_GM+I~ )=Dn +JWiw~#HNU7}'wJ&P(T?~{EfQ6[6qk;XyW1,e5'RDkU!{})qk^r^k:prn+z;akHf`LV)?\|RKhPjx5G ZW3aZKV^Af)cU=2) qOQ3 p%mA[RL+8*d 1&DeBQh^_tn'Pi#Jq7[}>:yzlMui_zAV4n>@[lx"`7H+l]]%[XXO<$?X)T:q>Q6V.A9!bNcv9~F(@rrCAz@ MHq|@xqQ|4a\b]`Gw]-T,"P&& FbT5n;tG?JKk-{{>
Aug 3, 2021 00:10:54.632102966 CEST	2100	OUT	GET /images/apple-touch-icon-72x72.png HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.835850954 CEST	2160	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: image/png Content-Length: 1391 Connection: keep-alive Last-Modified: Fri, 10 Feb 2017 00:16:28 GMT Expires: Fri, 01 Oct 2021 22:10:54 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 48 00 00 00 48 08 03 00 00 00 62 33 43 75 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 00 00 01 fe 50 4c 54 45 fe cd 4d fe cd 4d fe cd 4d ff cf 4d ff cf 4e ff cf 4e fe cd 4d fd cb 4c f3 a8 44 ef 9c 40 ef 9d 41 fe cd 4d fc c6 4b dc 5d 31 d0 39 27 d1 3b 28 fe cd 4d fc c6 4b db 5b 30 cf 36 26 d0 38 27 fc c6 4b db 5b 30 cf 36 26 d0 38 27 db 5b 30 fe cd 4d fe ce 4d fe ce 4d fe ce 4d fc c6 4b db 5b 30 cf 36 26 db 5b 30 fe cd 4d fe cd 4d fc c7 4b fb c4 4b fb c4 4b fb c4 4b fb c5 4b f9 bd 49 da 59 30 cf 36 26 fe cd 4d fe ce 4d f3 aa 44 dd 60 31 da 57 2f da 58 2f da 58 2f da 58 2f d9 56 2f d2 40 29 d0 38 27 dd 60 31 f3 aa 44 fe cd 4d fd ca 4c ea 8d 3d d2 3e 29 cf 35 26 cf 36 27 cf 36 27 cf 36 27 cf 36 27 d0 38 27 fe cd 4d fe cd 4d fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 fe cc 4d eb 8f 3d d0 37 27 eb 8f 3d d2 40 29 d0 37 27 fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 fe cd 4d fe cc 4d d2 40 29 fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cc 4d eb 8f 3d fe cc 4d eb 8f 3d d2 40 29 d2 40 29 fe cc 4d d2 40 29 d0 37 27 eb 8f 3d d2 3f 29 fe cc 4d ec 92 3e fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe ce 4d fe ce 4d fe ce 4d fe cd 4d fe cc 4d fa c0 4a f9 bd 49 f9 bd 49 fe cd 4d fe cd 4d eb 91 3e d8 51 2d d7 4e 2d d7 4e 2d fe cd 4d fc c7 4b da 59 2f cf 34 26 cf 36 27 cf 36 27 cf 36 27 cf 34 26 fe cd 4d fd cb 4d e4 7a 38 d1 3d 28 d1 3b 28 d1 3b 28 d1 3d 28 fe ce 4d fb c4 4b f2 a6 43 ef 9c 41 ef 9d 41 ef 9d 41 ef 9c 41 f2 a5 43 fb c4 4b fe cd 4d fe ce 4d ff cf 4e ff cf 4e ff cf 4e ff ff 60 0f 32 8f 00 00 00 01 62 4b 47 44 a9 27 0f 06 04 00 00 00 07 74 49 4d 45 07 df 05 0b 09 39 24 0d 0b 5e cf 00 00 02 49 49 44 41 54 58 c3 63 60 18 05 a3 60 14 0c 30 60 64 62 66 61 45 02 2c cc 4c 8c 64 19 c4 c6 ce c1 c9 85 04 38 39 d8 d9 c8 32 88 9b 87 97 8f 1f 09 f0 f1 f2 70 93 65 90 80 a0 90 b0 08 12 10 16 12 14 20 cf 20 51 31 71 09 24 20 2e 29 3a 6a d0 a8 41 a3 06 31 48 49 cb 40 80 ac 9c bc 02 b2 41 0a 8a 72 b2 50 29 69 29 82 c6 28 29 ab a8 aa a9 83 81 86 a6 96 36 b2 41 da 5a 9a 1a 10 19 35 55 15 65 25 02 06 e9 e8 ea e9 1b 18 1a 81 80 b1 89 a9 19 b2 41 66 a6 26 c6 60 09 43 03 73 0b 5d 1d 42 4e b2 b4 b2 b6 b1 b5 b3 07 02 07 47 33 27 64 83 9c cc 1c 1d 40 e2 76 b6 36 d6 56 96 04 fd e6 ec e2 ea e6 ee 81 62 02 2a 70 f2 70 77 73 75 71 26 1c d8 ce 9e 5e de 3e b8 4d 72 f2 f0 f1 f6 f2 24 c2 1c 90 9b 7c fd dc fd 71 98 e4 e4 ef 1e e0 4b 8c 7b 20 26 79 b9 05 06 61 35 c9 29 28 d0 cd 8b 58 73 40 be 0b 0e 09 0d c3 62 92 53 58 68 48 30 Data Ascii: PNGIHDRHHb3CugAMAa cHRMz&u0`:pQ<PLTEMMMMNNMLD@AMK]19';(MK[06&8'K[06&8'[0MMMMK[06&[0MMKKKKKIY06&MMD`1W/X/X/X/V/@)8'`1DML=>)5&6'6'6'6'8'MMM=@)7'MM=@)M=7'=@)7'M=@)7'M@)7'MM=@)7'MM=@)MM@)M=@)7'M=M=@)@)M@)7'=?)M>MMMMMMMMMMMJIIMM>Q-N-N-MKY/4&6'6'6'4&MMz8=(;(;(=(MKCAAAACKMMNNNN`2bKGD'tIME9$^IIDATXc``0`dbfaE,Ld892pe  Q1q$ .):jA1HI@ArP)i)()6AZ5Ue%Af&`Cs]BNG3'd@v6Vb*ppwsuq&^>Mr$|qK{ &ya5)(Xs@bSXhH0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49728	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:53.974234104 CEST	1290	OUT	GET /css/GeminiHomeV2.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.172175884 CEST	2027	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sun, 12 Feb 2017 02:30:50 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 32 62 33 0d 0a 1f 8b 08 00 00 00 00 00 00 03 95 54 d1 6a db 30 14 fd 95 8c 3c 64 83 3a d8 4e 9a a5 f2 53 3b 18 14 fa 30 e8 ca 1e 83 1c 5d db 22 b2 24 24 b9 49 66 f2 ef bb 92 e3 c6 49 d3 c2 f0 93 af ae ef 39 f7 9c 23 8f 9f 2b 10 e2 41 b1 fd bd 64 3f 95 72 60 7e 28 e9 28 97 60 da 9c ae 37 a5 51 8d 64 11 af 69 09 a4 31 e2 eb a4 52 35 ac f2 4d c9 56 c9 54 cb 72 f2 2d 1b f4 59 fe 17 c8 5a bd 82 39 8c ed a6 59 49 5a c3 a8 4a da 02 87 46 05 ad b9 d8 93 67 28 15 bc 3c 46 4f bc ac b0 c8 25 15 37 93 50 1c bd 3c 8e 42 75 d2 17 fe fc ba 28 bc 3c 0e ce 26 37 bf 29 d2 a1 37 f7 86 e3 10 4b a5 8d 2c 18 5e 64 01 2f 90 99 2d f4 2e ab a9 29 b9 24 f1 68 76 8b 6f 6b 25 94 21 e3 a2 28 32 ad 2c 77 5c 49 42 73 ab 44 e3 20 cb 95 73 aa 26 b3 ef d8 e8 60 e7 22 bf 4c 21 d4 96 a0 50 5c 5b 6e b3 b7 4a c5 19 03 99 6d 39 73 15 49 6f 63 bd 3b 8c 05 14 6e 85 08 ed 1b 66 1a ea 8d b6 38 00 4f 7a 75 df 43 3b a5 49 ba c4 ee 6c 5b 71 07 91 d5 74 0d 44 2a 53 53 d1 af 30 c7 e3 d1 2c f4 74 a8 be 70 98 1e a7 07 9b 7a e4 c4 b7 c6 27 1f 3e 40 8c 33 c6 ad 16 74 4f b8 14 c8 2c ca 85 5a 6f b2 0a bc ee 3d 9f 80 35 f3 9b 0c dd 3e 0a 39 9f 2f 97 8c 5d 21 7d 18 87 b0 f8 9d 41 ba 2b f8 5e 2c 32 f7 2b 5c 27 d1 6d 12 79 9a 49 1c 64 d4 b8 e0 0a fb 54 e3 da 73 c0 ad a1 1a 97 75 d4 b8 95 e3 02 ec 51 87 a8 77 34 08 45 b5 b6 91 e0 d6 5d aa e4 7c 84 56 ba 31 eb 8a 5a f8 d4 a7 c0 fa 2e 5d fa 84 20 b3 40 ff 14 b8 64 e1 79 76 e3 7c 80 5a 4d 19 e3 b2 24 49 8a 48 c9 5d d8 a2 87 c1 5d 37 e7 0d 69 da 4f db 76 0e e4 4a b0 3e b2 71 1c 5f d1 1f a8 7f 7a b1 02 bb 68 7e 22 41 8d 51 db b6 b3 30 ee 7d 8d 4f d1 37 20 a8 e3 af 5d 1a 92 99 b7 58 19 06 a6 9b 94 e0 8d 19 e1 e2 9c 8d 9c c1 0b a6 a9 41 2f bf f0 5a 2b e3 a8 74 7d 33 7e 1c 75 18 fe 8b 61 d5 ba bd 00 12 46 74 d2 25 4b ef 84 54 4f 7c 0d d2 a2 d7 6a 77 e1 d5 22 3e ef 70 dc 09 68 af 45 64 d8 25 68 0e a2 1d 38 b1 3c 5d fd b4 b3 79 8a bf 3b cd c0 6e 22 0c 10 98 07 44 3e 77 ee 3c 72 1f e5 f2 bd 07 c5 dc 3f 97 f3 71 b3 23 f7 61 da 92 4b 2e 5c ca 4f b8 fc 1f 8f a2 b8 32 38 f2 09 18 4c 3b 4c c5 51 33 6a 2d 2f 65 0d 1e 57 87 f6 de 0a 13 72 e2 cd 3c fc 03 3d 26 c5 cc 26 06 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 2b3Tj0<d:NS;0]"$$lfl9#+Ad?r`~((`7Qdi1R5MVTr-YZ9YIZJFg(<FO%7P<Bu(<&7)7K,^d/-.)$hvok%!(2,w\IBsD s&`'"L!P\[nJm9sIoc;nf8OzuC;ll[qtD*SS0,tpz'>@3tO,Zo=5>9/]!}A+^,2+\'myIdTsuQw4E]|V1Z.] @dyv\|ZM$IH]]7iOvJ>q_ zh~"AQ0}O7]XA/Z+t}3~uaFt%KTO|jw">phEd%h8<]y;n"D>w<r?q#aK.\O28L;LQ3j-/eWr<=&&0
Aug 3, 2021 00:10:54.187165022 CEST	2031	OUT	GET /css/MasterStyles15MVC.css HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:54.398912907 CEST	2056	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:54.416644096 CEST	2065	OUT	GET /assets/jquery.min.js HTTP/1.1 Host: axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.619584084 CEST	2078	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Wed, 23 Apr 2014 01:03:00 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 38 34 36 34 0d 0a 1f 8b 08 00 00 00 00 00 03 c4 bd f9 96 db 46 96 37 f8 7f 9f d3 ef 90 84 d5 69 40 8c 64 26 65 bb bf 2e 30 21 8e ac a5 ec 6a 6f 5d 52 95 ab 9a 49 f9 60 23 09 26 b8 88 64 6a 71 92 fd 2c f3 2c f3 64 73 7f f7 46 04 02 20 98 76 d5 cc 37 e3 2a 25 81 40 ec 71 e3 c6 dd e3 f2 71 e7 6c fe 5f 77 f9 e6 d3 d9 fb 7e ef 7f f5 9e 9c cd df e1 ad 97 ae 16 67 7b f3 b2 da 4c 2f cb 22 cd 97 db fc ec f1 e5 bf fe 8b 3f b9 5b a6 bb 62 b5 f4 63 95 04 f7 e6 ed 2c fd e4 c7 c1 fd 26 df dd 6d 96 67 93 5e b1 fd b9 58 66 ab 0f 94 38 8c c3 b8 b7 5c 65 f9 9b 4f eb 3c 8a a2 3f 0c e3 5e 96 4f e2 bb 72 f7 d7 22 ff b0 df c7 bd 75 bc c9 97 3b 29 11 76 fa 87 aa d6 3b d4 5a 4c fc 4e 3a 1f c5 e3 e0 fe 7d bc 39 4b a2 b4 97 ac b2 4f 2a 8b 26 be 77 ed 75 e3 ae f7 d4 0b 7a f1 7a 9d 2f b3 37 2b 3f 09 54 1e 65 bd 74 bb f5 bd ac d8 ae cb f8 93 17 0c b2 de 26 5f ac de e7 7e 30 a0 0a d1 13 6f b9 5a e6 de 7e cf cf 5e 70 9f de ee f7 7e 7a 4b d5 a7 9b 3c de e5 2f cb 7c 41 fd f2 bd 62 b2 89 17 b9 17 a8 f4 b6 c7 8f 5f af 36 59 be 89 e8 f5 43 91 ed 66 78 98 e5 c5 74 b6 8b ae 02 95 e8 9e 3c 9f 15 65 46 f5 71 7b 9d b4 dc ef 3b 94 af 56 75 90 96 91 8f c4 d5 72 67 67 60 bf af 52 5e ac d2 3b ce d8 cb f4 93 4a cb de 87 4d b1 cb 7d 7f d2 db de ad d7 ab cd 8e a6 e3 e3 f7 34 c3 e5 d0 bb ee 50 c6 1d cd f4 d9 6c b7 28 9f 7a 21 0d ac eb 5d f3 cb 35 66 ed 29 86 51 f6 d2 72 b5 c5 54 64 11 5e 6a c3 8d 39 03 f2 d6 06 92 61 56 27 3c ab 99 aa e6 95 86 2b f3 6a 87 7b e0 b5 8a f2 83 86 06 7e 75 d6 74 27 a0 83 a5 4c a3 fb c3 60 d2 cb e3 74 e6 a7 6b 0c 3a 8d 77 68 b5 fc e4 8f c6 8a 92 b6 00 3e ff 8a 0a 04 ca 82 1e 2d d5 68 37 2b b6 e3 28 3e 04 03 d3 8c d3 c4 16 59 de 45 89 93 b4 a1 a4 6d be 7b 53 2c f2 d5 dd ce 4f b7 ea aa 2a fa 8e 06 b6 24 68 0d 9c 02 05 15 d8 6d 3e 19 98 5e e6 1f ce e2 de 33 fa f8 3e ff db 8f c9 3c a7 71 78 df 17 e9 66 b5 5d 4d 76 bd bf 7d ff dd 37 6f de fc e4 d1 e8 e3 1d 8d 86 06 78 70 2a 9b b5 55 86 32 bb dd fa cf 39 6d b5 ed ae bd 60 42 93 95 06 f7 b4 65 e2 5d fc aa 28 77 f9 e6 fc dc 4f 23 37 c1 4f 95 bc 62 87 05 c1 00 33 9b 45 55 d2 96 16 ee fe a0 a6 6a a6 0a da 17 65 be 9c ee 66 6a ae 6e a3 6c 74 35 56 a5 5a a8 a5 5a a9 f5 60 b2 da f8 d3 a8 3f 98 5e 17 83 69 b7 cb 3b 6f 4a 9b a3 1f e0 cb ec ac 58 52 af 69 91 de e7 1b 6a 76 1b 00 ce 56 93 b3 19 6d 9f ed 6e 53 2c a7 1e f5 2d 1f cd 7a bb d5 77 ab 0f f9 e6 79 0c 18 a3 55 72 0a 8d 66 e3 60 50 46 b7 dc fa 74 8c bd 71 8b fd f7 d8 0b 6e a3 72 90 97 84 68 28 ad ec 70 da f9 39 1e 6e 83 fb 45 54 76 bd 33 af 7b ab 96 51 3e 5a 8c 69 d7 8e bc c7 48 e0 2a 3a cb e0 7e 1d 25 3c 82 15 fa 99 07 f7 f3 68 d5 23 20 2d 68 9d ce 3c de 84 73 1a 2e b5 45 3b 51 3f a1 55 2a 97 8f e6 a3 fe 58 ea e7 ea Data Ascii: 8464F7i@d&e.0!jo]RI`#&djq,,dsF v7*%@qql_w~g{L/"?[bc,&mg^Xf8\eO<?^Or"u;)v;ZLN:}9KO*&wuzz/7+?Tet&_~0oZ~^p~zK</|Ab_6YCfxt<eFq{;Vurgg`R^;JM}4Pl(z!]5f)QrTd^j9aV'<+j{~ut'L`tk:wh>-h7+(>YEm{S,O*$hm>^3><qxf]Mv}7oxp*U29m`Be](wO#7Ob3EUjefjnlt5VZZ`?^i;oJXRijvVmnS,-zwyUrf`PFtqnrh(p9nETv3{Q>ZiH*:~%<h# -h<s.E;Q?U*X
Aug 3, 2021 00:10:54.821007013 CEST	2150	OUT	GET /css/home_bkgd_1.png HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/css/GeminiHomeV2.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:55.018441916 CEST	2182	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: image/png Content-Length: 22035 Connection: keep-alive Last-Modified: Sat, 11 Jun 2016 21:33:48 GMT Expires: Fri, 01 Oct 2021 22:10:54 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: ff d8 ff e1 00 18 45 78 69 66 00 00 49 49 2a 00 08 00 00 00 00 00 00 00 00 00 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 32 00 00 ff e1 03 31 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 35 2d 63 30 32 31 20 37 39 2e 31 35 35 37 37 32 2c 20 32 30 31 34 2f 30 31 2f 31 33 2d 31 39 3a 34 34 3a 30 30 20 20 20 20 20 20 20 20 20 20 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 34 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 34 42 43 43 44 42 46 39 30 41 42 36 31 31 45 34 42 41 37 30 41 31 35 44 37 44 31 39 32 36 44 43 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 34 42 43 43 44 42 46 41 30 41 42 36 31 31 45 34 42 41 37 30 41 31 35 44 37 44 31 39 32 36 44 43 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 34 42 43 43 44 42 46 37 30 41 42 36 31 31 45 34 42 41 37 30 41 31 35 44 37 44 31 39 32 36 44 43 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 34 42 43 43 44 42 46 38 30 41 42 36 31 31 45 34 42 41 37 30 41 31 35 44 37 44 31 39 32 36 44 43 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 3a 52 44 46 3e 20 3c 2f 78 3a 78 6d 70 6d 65 74 61 3e 20 3c 3f 78 70 61 63 6b 65 74 20 65 6e 64 3d 22 72 22 3f 3e ff ee 00 0e 41 64 6f 62 65 00 64 c0 00 00 00 01 ff db 00 84 00 08 06 06 06 06 06 08 06 06 08 0c 08 07 08 0c 0e 0a 08 08 0a 0e 10 0d 0d 0e 0d 0d 10 11 0c 0e 0d 0d 0e 0c Data Ascii: ExifII*Ducky21http://ns.adobe.com/xap/1.0/<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.5-c021 79.155772, 2014/01/13-19:44:00 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/ResourceRef#" xmp:CreatorTool="Adobe Photoshop CC 2014 (Macintosh)" xmpMM:InstanceID="xmp.iid:4BCCDBF90AB611E4BA70A15D7D1926DC" xmpMM:DocumentID="xmp.did:4BCCDBFA0AB611E4BA70A15D7D1926DC"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:4BCCDBF70AB611E4BA70A15D7D1926DC" stRef:documentID="xmp.did:4BCCDBF80AB611E4BA70A15D7D1926DC"/> </rdf:Description> </rdf:RDF> </x:xmpmeta> <?xpacket end="r"?>Adobed
Aug 3, 2021 00:10:55.037655115 CEST	2207	OUT	GET /16.00.1279.006/en-US/css/Fabric/0.10.3/fonts/office365icons.ttf? HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive Origin: http://axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/css/EmbeddedFonts.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:55.248713017 CEST	2233	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:55 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:55.270553112 CEST	2233	OUT	GET /css/shellwofficons_f991c945.woff HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive Origin: http://axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/css/shellg2coremincss_ba45585d.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:55.480139971 CEST	2244	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:55 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:55.504919052 CEST	2244	OUT	GET /css/shellttficons_9739c58c.ttf HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive Origin: http://axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/css/shellg2coremincss_ba45585d.css Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:55.714556932 CEST	2250	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:55 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:55.752334118 CEST	2250	OUT	GET /images/favicon.ico HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:55.949815035 CEST	2258	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:55 GMT Content-Type: image/x-icon Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Thu, 09 Feb 2017 12:49:08 GMT Expires: Fri, 01 Oct 2021 22:10:55 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: STALE X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 34 30 36 0d 0a 1f 8b 08 00 00 00 00 00 00 03 ed 97 49 6c 1b 65 18 86 5f 7b 6c 8f 77 cf 8c f7 7d 49 62 4f 48 42 43 03 a9 95 a4 51 d4 d0 25 8e 13 96 03 1c 90 10 12 02 ca 1d 21 28 1c e0 00 12 42 5c e0 88 c4 05 b1 1d e0 8a 10 88 b5 88 96 2d 0b b4 69 a1 6d 24 48 a0 54 95 10 01 44 9b 90 84 6f 7e db f1 b8 f1 d8 73 68 5a 21 cd 23 fd 1a ff ff fb 7e 33 63 7b e6 9d 6f 00 13 38 08 02 68 6b c7 61 2b 30 08 20 93 a9 cc df b4 03 af d0 5a 7f 7f 75 ee 05 0e d0 90 c9 23 28 3e 54 d6 19 26 d4 a9 7e be f5 ad 3f 51 fe e2 5f 14 f6 cc 62 ea eb 0d 94 3e 5e 45 cf c4 09 ec 7e e0 1c f2 83 33 28 7f b5 8e 02 6d 8b 4f 2e a3 7c 7c 1d f9 9b 67 30 f4 f4 af 18 7d e9 22 7a 27 4f 62 6a 66 03 e5 63 54 5f a4 fa 6f 36 b0 ef d5 3f 30 f8 c8 4f 98 f8 68 15 bd 53 0b 28 7f b9 8e 89 0f 2f 63 cf a3 3f 63 fc b5 15 94 3e 5b 43 6f f9 24 d5 d0 fa 07 97 b1 fb fe b3 e8 2d d1 7e be dd 80 81 81 c1 b5 c5 7f 25 b9 06 fc f6 50 5a 45 c8 6e f1 c4 54 78 2c 5c ca 44 88 2e 97 a8 6c 53 5c 65 27 02 85 8f 6a 9f 42 3c 9b 8d 0b aa a9 cf e1 f0 d5 17 02 56 5e 92 78 6b a0 3a 15 bd ce b0 d9 1c 76 7a c5 ea 42 8e b3 f1 bc 8d cb 6d ed 20 92 71 bb 33 91 ad a9 df 1e 4c 26 83 f6 fa dc 9f 88 46 13 aa 29 fb 52 fe a6 b4 fb 7d da 21 a3 92 b1 63 50 e5 ac 45 65 a8 e6 6c e9 93 55 ca ca 4d 4c d3 a8 e5 a1 92 9d 03 0f 2d 52 be ce a2 f8 c4 32 46 5f bc 88 be db 17 d0 73 f0 04 6e ba f7 0c cb 5f 25 7b a7 e7 36 71 f0 dd 7f 58 46 0e 3f 7b 1e a5 4f d7 58 e6 de 78 e7 29 96 b3 4a f6 4e 7e be 86 be db 16 30 f0 e0 39 d2 57 91 bf 65 06 87 de bb 84 e2 91 25 96 cb c3 cf 9c 47 cf 81 ef 59 d6 f7 dd 71 0a dd 63 f3 2c f3 95 5c 37 30 30 d8 59 d2 d7 1d b1 05 8a 1e d1 3e f9 08 55 27 dd 51 a7 06 51 77 52 14 e3 92 3d af 81 5d 8a d3 11 4c 2d 68 72 b2 db 96 1a 64 7a 4a b4 90 ad 21 9b 2d 64 6d 25 77 75 69 1b 14 39 1c d6 34 54 64 4d 43 4d d6 30 d4 e5 a6 06 91 8b 79 ea ba 27 c6 35 7e 4d 31 62 c9 66 5d 9d 15 b9 d3 95 cd 5a 22 8d 86 80 20 08 c9 14 af c8 7c 2a 49 93 40 ba 11 fa b3 7d 92 57 d1 bd 92 4f 6c fa 33 9b 6b ba b9 89 78 35 f4 4c c2 4b 24 32 1a ba c9 d1 11 24 3a 1c db 2f 8b 0a b9 ca 55 99 d3 90 6b 97 ba a6 7c 3d d0 be b9 ae 0d 32 8d 7e 1a f7 41 d5 a7 38 54 86 6a 9f a2 f4 28 c5 c7 97 58 9f 32 fe c6 0a f6 be 70 01 87 de bf 84 b1 97 7f 67 ef 7f dd fb be c3 0d 34 76 dd 75 1a f2 c8 1c 8a 8f 2d 61 fc f5 95 ad 5e a5 ff 9e 1f 31 f2 dc 6f ac 57 d9 ff ce df ec fd 51 1e 9d 47 37 8d 29 fa 5c 3c b2 0c 79 78 0e 03 0f 2f 62 e8 a9 5f 58 ef 32 f2 fc 05 d6 af 4c cf 6e b2 5e 65 d7 dd 3f 40 de 3b 0f 79 88 7c 87 17 b1 ff ed bf 68 ed 34 eb 57 26 8f ae c1 c0 c0 60 67 c8 18 5c 75 24 9d 54 ed bc ac 13 9e ed dc 1a 73 66 75 e1 8c 59 e9 10 e8 b2 17 12 ba 28 38 ba a0 9c 0e 67 d3 09 c7 4e 88 1e eb 66 5d 50 23 f0 3f 41 0a 5b 2c 61 29 a3 17 29 9c 0c 06 93 Data Ascii: 406lle_{lw}IbOHBCQ%!(B\-im$HTDo~shZ!#~3c{o8hka+0 Zu#(>T&~?Q_b>^E~3(mO.\|g0}"z'ObjfcT_o6? 0OhS(/c?c>[Co$-~%PZEnTx,\D.lS\e'jB<V^xk:vzBm q3L&F)R}!cPEelUML-R2F_sn_%{6qXF?{OXx)JN~09We%GYqc,\700Y >U'QQwR=]L-hrdzJ!-dm%wui94TdMCM0y'5~M1bf]Z" |*I@}WOl3kx5LK2:/Uk|=2~A8Tj(X2pg4vu-a^1oWQG7)\<yx/b_X2 Ln^e?@;y|h4W&`g\u$TsfuY(8gNf]P#?A[,a))

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49735	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.183208942 CEST	2029	OUT	GET /css/conciergehelper.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.385534048 CEST	2033	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sat, 11 Jun 2016 21:43:38 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 35 37 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 cd 58 eb 6e db 36 14 7e 15 0f 46 d1 16 b3 0c d9 49 dc 44 06 02 b4 4b 8b 61 d8 ba 02 01 f6 b7 a0 c5 23 8b 08 45 0a 14 9d 38 31 9c 7f 7b 87 3d df 9e 64 87 d4 8d 94 e4 5c da 14 58 84 04 f1 21 cf 77 ee 17 79 9a 28 00 4e 44 0c 41 4e 04 f0 20 e1 f2 66 97 11 b5 66 22 d0 32 8f 8e c2 7c bb bc 61 54 a7 d1 d1 dc fc bf 92 8a 82 0a 4a d2 ac 25 14 fa 96 43 54 48 ce 68 4d 52 84 b2 4d 11 9d e0 25 03 75 82 ec fb 69 57 60 2a 33 f8 01 02 73 59 30 cd a4 88 12 b6 05 fa 13 cb 72 a9 34 11 da 1c 58 3a 59 21 eb 46 03 f2 6a 2d b3 52 ee 61 35 a9 8c af 80 7e b7 a2 be 5a b5 ec 70 a9 d8 3a d5 25 64 c5 85 22 02 0e 89 76 8d 72 8e 2c 83 77 46 e2 ab b5 92 1b 41 83 58 72 a9 a2 71 92 24 cb bb 80 09 0a db 68 16 86 87 6c 0a 84 fc 60 71 9f 6e 5c f8 3f 33 ed 01 e3 8a 14 38 ff 75 28 c7 aa cf 46 91 68 fe 92 b1 b4 88 2f 6e ef e3 16 1e 0e e4 d3 4d 7d 56 64 7f bc a1 68 5a 6e 75 bb 23 ca dc 11 1a 84 de e5 84 52 26 d6 ad 7d 35 a1 35 b0 a6 94 c9 e7 91 2a f5 2d 8d b2 22 e7 e4 36 12 52 80 2b 37 63 82 65 ec 0e bd ab 99 e6 e0 49 3c fb 46 81 a7 8d df e7 61 e8 19 1f 8d e9 d9 d1 59 98 2c 9d ec 4e d0 d6 a0 40 15 a2 d9 91 df 8f 52 20 26 c6 1d f4 99 81 74 98 4e 7c 26 ca 08 97 eb c6 83 87 ec ae ae a5 68 04 37 86 ec aa e8 d9 a0 96 ca bf 6b 63 6a a9 03 6d d8 d2 2b 5b 80 9e d0 30 76 65 40 92 40 ac 8b 40 2b 22 8a 04 2d f1 12 70 de ad 35 8a f6 01 dd 13 07 61 b5 41 93 c5 a4 c0 32 e8 53 99 c8 37 ba 47 de f5 53 ad d4 cc f5 79 46 b6 75 c5 db 00 6a d8 ea 80 a0 23 44 14 a3 d7 40 0d 68 71 6e b4 18 56 a5 3c 7a 41 7d 30 2b ab cf c7 a6 7a 6e 52 a6 21 40 21 31 60 20 55 46 78 5f e3 ca 97 c6 ad 23 1b a3 91 75 7b 4e 14 1e ef a7 4c 70 26 e0 43 a9 12 8e 7e a2 23 9b c0 ce bc 74 7a 09 82 f4 0f aa 84 f7 8e 4a 25 4f 43 97 b8 9f 62 f2 c5 0c d4 1a 4c b3 ca c9 1a de d3 0f 5d 67 0c 94 c2 7e fc a9 76 de 17 d3 f7 7e 97 c4 24 fe a5 26 1a 2e d8 75 5d 08 d1 19 8a 1b d9 e1 3d 5e 69 f1 0b e1 fc 0f f8 53 7c 49 31 c5 27 3d ca dc 92 1a e0 4b 10 f4 63 46 18 3f 40 ee 5c 57 bf 49 26 7c d2 45 2d a6 65 de ac 32 a6 3f 01 50 63 9e 3d 7b 7f 8d 58 64 c5 a1 b9 64 d1 9f 96 0c 4d f0 17 6d c7 b5 05 3c 10 75 2f 36 61 df 21 47 bb 16 6e 16 b6 13 e1 b4 9d 16 65 25 f6 14 a3 47 e6 d9 8f f5 56 fb 46 7c 86 9b 8f db 7c 57 e2 9c 9d bc aa ab b8 e2 8b 4f cd d3 d7 64 64 8b 64 d8 eb 03 67 d6 f3 03 f4 8b 03 50 5e 0c da 0b 07 02 61 2f 34 09 75 8c f9 34 eb f8 7a ff 00 fc 57 ec aa 06 93 3e 0e d3 0c 9e 15 c7 21 ee f6 ed 79 95 bf 9e 65 1d e4 81 b1 79 6c 1e b7 41 78 b5 57 8f 22 33 74 4b 5d 2a 3e b2 30 cf 93 8c 7a 8a d4 85 93 3e 46 54 e8 cb e9 5a dd f6 9b fd 54 11 8d 0a 5e 40 11 2b 96 9b 65 63 d2 27 d9 86 5a b5 29 33 63 1a b3 a6 33 c8 46 f8 eb a7 a5 cd af cf 9b 6c 05 6a 72 e8 60 ee ee 4a 76 66 5e 83 d2 2c 26 3c 28 b0 Data Ascii: 57eXn6~FIDKa#E81{=d\X!wy(NDAN ff"2|aTJ%CTHhMRM%uiW`*3sY0r4X:Y!Fj-Ra5~Zp:%d"vr,wFAXrq$hl`qn\?38u(Fh/nM}VdhZnu#R&}55*-"6R+7ceI<FaY,N@R &tN\|&h7kcjm+[0ve@@@+"-p5aA2S7GSyFuj#D@hqnV<zA}0+znR!@!1`UFx_#u{NLp&C~#tzJ%OCbL]g~v~$&.u]=^iS|I1'=KcF?@\WI&|E-e2?Pc={XddMm<u/6a!Gne%GVF||WOdddgP^a/4u4zW>!yeylAxW"3tK]*>0z>FTZT^@+ec'Z)3c3Fljr`Jvf^,&<(
Aug 3, 2021 00:10:54.407202005 CEST	2063	OUT	GET /css/shellg2corecss_11377998.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:54.620759964 CEST	2091	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:54.626292944 CEST	2099	OUT	GET /images/docusign.png HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.827408075 CEST	2152	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: image/png Content-Length: 7635 Connection: keep-alive Last-Modified: Thu, 09 Feb 2017 23:58:20 GMT Expires: Fri, 01 Oct 2021 22:10:54 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 45 00 00 00 5c 08 06 00 00 00 f9 da a7 ba 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 73 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 36 33 64 39 36 62 62 32 2d 39 31 36 37 2d 34 63 63 63 2d 39 66 65 32 2d 63 33 63 65 65 36 31 61 38 35 33 64 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 44 35 31 39 46 45 37 30 38 44 31 46 31 31 45 33 39 36 43 42 38 32 30 36 45 42 33 31 41 41 32 35 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 44 35 31 39 46 45 36 46 38 44 31 46 31 31 45 33 39 36 43 42 38 32 30 36 45 42 33 31 41 41 32 35 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 30 63 30 34 37 37 39 2d 30 62 35 62 2d 34 66 31 37 2d 61 64 33 63 2d 31 35 66 39 35 61 66 39 62 39 38 36 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 36 33 64 39 36 62 62 32 2d 39 31 36 37 2d 34 63 63 63 2d 39 66 65 32 2d 63 33 63 65 65 36 31 61 38 35 33 64 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 Data Ascii: PNGIHDRE\tEXtSoftwareAdobe ImageReadyqe<siTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M 0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rd f:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:63d96bb2-9167-4ccc-9fe2-c3c ee61a853d" xmpMM:DocumentID="xmp.did:D519FE708D1F11E396CB8206EB31AA25" xmpMM:InstanceID="xmp.iid:D51 9FE6F8D1F11E396CB8206EB31AA25" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:20c04779-0b5b-4f17-ad3c-15f95af9b986" stRef:documentID="xmp.did:63d96bb2-9167-4ccc-9 fe2-c3cee61a853d"/> </rdf:Description> </rdf

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49733	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.183407068 CEST	2030	OUT	GET /css/AppTile.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.386991978 CEST	2035	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sun, 12 Jun 2016 10:08:00 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 32 30 62 0d 0a 1f 8b 08 00 00 00 00 00 00 03 8d 53 4d 6b db 40 10 3d c7 bf 42 a1 07 b7 a0 35 b2 69 5a b2 81 40 8f b9 15 92 90 a3 19 49 23 6b f0 6a 67 d9 5d 7f a5 f4 bf 77 57 b6 63 a9 b2 83 11 08 34 f3 e6 cd 9b 99 a7 c9 86 ed 52 31 94 73 f2 d8 24 7f 46 37 0d d8 05 69 99 25 d3 cc 6c f7 af ec 61 74 53 92 33 0a 76 92 b4 22 8d 22 57 5c 2c 43 b8 62 ed 45 05 0d a9 9d 1c 3f e3 82 31 79 7d 4a 9e 31 04 68 51 fb 71 7a 08 be fd 3e 13 7c 7d ea e4 c7 e9 0b d4 dc 40 fa cb 12 a8 d4 81 76 c2 a1 a5 ea d8 c5 d1 3b ca e9 cc 6c 43 40 6c 30 5f 92 17 de 06 18 79 62 2d 27 d3 d9 9d 4b 78 e5 a3 be 04 c1 a1 20 2d c2 77 ba cf f4 4a 2a b6 4d 17 13 29 1b 7e bf 8a af c5 ba ab a1 7c 2d f2 1a d8 35 b3 8c fe 8e 26 a7 ab 16 ac 4f 57 15 9e 8d 9c 65 ed 0a 0b 56 6c e5 97 aa aa 2e 5c b7 c7 a3 a1 c1 74 62 2c af c9 05 85 73 8f 5b 1f 79 0d 94 25 e9 45 b0 cb 7d cb 6a f8 30 02 e4 8e d5 ca e3 ff 9d 72 f6 9e 1b 79 d7 a2 db 66 35 46 53 c8 e9 f7 36 14 89 05 04 9f 68 a9 b0 8a 7b d9 d4 c1 9a c2 19 28 50 ea 30 2b a8 8e e0 a1 d2 7a 67 d0 06 e2 65 94 77 e4 9e ee 67 ee 55 75 d5 5a 54 e0 69 8d 7d 01 05 6a 8f 36 8a 86 62 b9 b0 bc d2 a5 28 14 19 19 96 ea 43 4e e4 bc 3d df 7b 5e f3 1a 6d 54 90 b3 2d d1 ca 60 db 24 2c 84 ca 87 8f 3f 4c 84 d8 85 6a 57 db c3 00 83 4b 4b 57 80 c2 af 93 fb 60 84 6f 3d db 9e cf ba 4f 92 7c 39 77 3e 11 e5 7e 78 20 9c 3d 81 76 c4 ce 76 f6 a7 46 88 cf 2d 35 86 ad 07 ed 07 75 43 83 1e 2a e1 47 7c 3e c1 47 23 46 fc f1 94 9a 35 0e e1 43 a3 f6 4e 7f 52 76 b2 67 96 fd 9c 15 83 ce 8f ed 84 c5 ca ba 80 29 b1 82 95 f2 fd b9 0e c1 37 2a 7d fd 42 aa 15 b7 89 1f 7b d7 05 c8 3f 53 e2 c8 66 64 05 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 20bSMk@=B5iZ@I#kjg]wWc4R1s$F7i%latS3v""W\,CbE?1y}J1hQqz>\|}@v;lC@l0_yb-'Kx -wJ*M)~\|-5&OWe Vl.\tb,s[y%E}j0ryf5FS6h{(P0+zgewgUuZTi}j6b(CN={^mT-`$,?LjWKKW`o=O|9w>~x =vvF-5uC*G|>G#F5CNRvg)7*}B{?Sfd0
Aug 3, 2021 00:10:54.408272028 CEST	2064	OUT	GET /css/data.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:54.611244917 CEST	2075	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sat, 11 Jun 2016 21:43:38 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 36 66 39 0d 0a 1f 8b 08 00 00 00 00 00 00 03 d5 9b dd 6e db 46 10 85 5f c5 40 6f 1a 40 34 64 d9 91 65 f5 aa 69 81 a2 40 0a 14 68 5e 80 3f 4b 89 30 bd 24 28 2a 72 10 f4 dd 2b 92 fa d9 9d 99 33 bb 8e af 0a 02 b6 64 ed 19 cf d1 f9 bc 0a 67 91 db e6 7e f9 31 df 25 59 ba 33 c9 d7 6a 57 65 55 5d f5 df be 5f 1f ae c7 87 b5 f9 37 6b 8a 6f 37 b7 2f bb a4 6c 6c ff 5b 53 37 5d d2 6f cd 8b f9 3d ed 9e 4d 37 bb be 9c d7 49 5f b8 3f 90 d6 27 db e6 ab e9 d6 e3 57 a6 4d b6 ec 05 b1 46 d9 e4 fb dd 7a fc ca 6b 94 d3 0b df f3 41 b6 fe 69 3e 7f c8 57 4f 57 17 d9 46 f1 90 6d 72 df 83 b0 5a 76 70 52 72 07 52 05 b1 ff 73 85 73 ff 59 9a 3f 6f ba 66 6f 8b 04 59 69 ba c2 74 9a 1d 1a 09 50 00 4b 28 14 54 45 b6 45 62 99 c4 c8 92 90 37 4d 58 85 43 c3 2b 8a 2e 8d 2d 8e d6 72 91 96 0a 5a 34 5c 85 0a 8d aa 08 a8 34 a4 54 a2 88 03 29 59 9a 65 00 04 0d a6 48 96 34 92 20 48 be 13 21 da 5f eb 9e 26 9a aa 2c 1c 05 1a 4f 69 14 50 43 11 85 a9 f4 cd 50 79 36 a6 84 d3 99 ba 5c 63 4b 30 21 96 50 f8 4a df 0b 98 ef 88 06 83 24 1a 67 92 2b 54 46 61 2d fd 31 d8 fe ee aa 97 b4 fb 46 a2 6e 21 26 a7 f5 0a 6b 6d 10 b5 73 0d 8c 5a cb 49 7b 5c 15 8f 80 34 e6 61 cc ba 9d a9 ab 15 d0 04 07 62 05 cc 59 ab 62 46 ac d0 b0 b9 1d 12 09 52 28 94 49 96 50 15 0c 59 0b 19 f3 2d 91 bc ff 31 79 63 0b 4e 99 9b 3a 50 28 9c ed 82 9c 5d ab 60 d2 76 94 b4 fb ec e9 d1 cc 01 69 82 93 31 6f 2f ff 78 1f 93 36 40 5b c0 c5 a9 06 e6 8d 19 a2 b9 4b a6 48 3c 58 a3 30 27 19 c3 75 30 75 3b 40 1d 35 46 d2 ff 62 ba be e2 d0 b9 9f ab b2 40 61 ae 0f 32 77 29 82 91 eb 29 72 4f 65 fe d1 3c 00 e4 b8 8d 31 71 ef 73 35 da c4 24 0d 00 a7 5b 38 95 c0 bc 31 37 34 73 c1 11 09 06 4a 14 da 24 57 b0 0c 86 ad 07 b0 51 57 24 f6 cf d5 66 4b ff c5 56 43 48 c6 d5 0a 66 75 10 b3 a9 02 66 ac a6 8c 15 b9 c9 4b 74 6b 49 ba 1f 23 ae 67 ca 5a 85 2e a1 77 41 8f d1 aa 15 b4 98 09 1a 30 35 42 62 90 d7 2b 50 49 66 e4 1a 98 a8 1a 10 45 cd 48 09 73 32 02 48 a8 43 8b 3a 3c b4 38 17 51 c8 62 53 8b f2 a1 7c 2a 0b 0d 2d 0e 89 4a 87 3a b7 90 4c 88 25 14 c4 b4 c1 05 73 23 e6 cd 49 09 22 a2 8e 2e 44 57 a8 8c c2 1a 9a 5d c4 ba e2 b7 37 75 a7 dd df 5c 65 aa b9 98 7b 1c a7 94 66 90 dd 84 c6 e0 c7 ef 43 7d 5b b2 44 a5 30 74 33 1a b4 73 2e f3 7e 14 ff 4f a1 e9 58 5e 77 a3 c3 b6 ea 8d bf f5 1c a4 5d 6b 5c 87 f7 bc 83 b6 e3 4d 5a b8 d5 1d 18 69 a5 30 eb 20 8d 0e b1 1e 66 f2 2a cc 93 d0 a6 af 84 08 1d 34 7e 4a 30 cd a0 3d fb 6f 2e 5b 89 29 91 fa 66 6a 08 c6 01 51 51 8a f3 8a ac 3e 3a f4 23 ca a4 58 c7 75 18 89 4c 43 62 d2 42 24 32 3e 97 10 6e 15 49 a3 43 4c d9 4c 5e 85 91 10 da f4 95 10 89 4c 41 c2 ef d7 89 8a f6 ec bf b9 6c 25 46 42 ea 9b a9 21 12 19 40 c2 eb fb 1a 97 35 fb be 4b 6b 3e 7a b7 e2 e8 dd 59 8e f9 b0 ea f0 dd 2d 01 31 b1 6c fc be b8 1b 2e 8e 8a Data Ascii: 6f9nF_@o@4dei@h^?K0$(*r+3dg~1%Y3jWeU]_7ko7/ll[S7]o=M7I_?'WMFzkAi>WOWFmrZvpRrRssY?ofoYitP K(TEEb7MXC+.-rZ4\4T)YeH4 H!_&,OiPCPy6\cK0!PJ$g+TFa-1Fn!&kmsZI{\4abYbFR(IPY-1ycN:P(]`vi1o/x6@[KH<X0'u 0u;@5Fb@a2w))rOe<1qs5$[8174sJ$WQW$fKVCHfufKtkI#gZ.wA05Bb+PIfEHs2HC:<8QbS|*-J:L%s#|".DW]7u\e{fC}[D0t3 s.~OX^w]k\MZi0 f*4~J0=o.[)fjQQ>:#XuLCbB$2>nICLL^LAl%FB!@5Kk>zY-1l.

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.614960909 CEST	2077	OUT	GET /assets/SpryValidationPassword.js HTTP/1.1 Host: axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:54.818362951 CEST	2145	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: application/javascript Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Tue, 15 Jul 2014 13:06:16 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 31 33 33 62 0d 0a 1f 8b 08 00 00 00 00 00 00 03 d5 3c 6b 73 1a 49 92 9f 3d 11 fe 0f 65 3e 8c 9a 31 02 6b 62 6e 23 c6 1a ec 40 08 d9 1d 81 40 cb c3 5e 9f ac 9b 68 41 81 da 6e ba 71 77 23 59 6b eb bf 5f 66 d6 a3 ab 5f d0 f8 71 b1 e7 d8 1d 43 55 be 33 2b 2b 2b ab 70 ab c5 c6 eb f0 fe 8d e3 b9 73 27 76 03 ff c2 89 a2 bb 20 9c 37 3f 44 ec 90 dd f2 30 82 41 f6 ac f9 07 7c 43 48 76 11 f2 c3 11 f7 b8 13 71 76 d4 fc 47 f3 e8 f1 2f ad 16 fe 9f 75 83 f5 7d e8 2e 6f 62 66 cd ea ec f7 67 cf fe d1 64 9d 79 70 cd d9 f8 3e 8a f9 2a 62 b6 3f 0b c2 75 10 3a 31 9f 37 09 a7 e3 79 8c 70 22 16 f2 88 87 b7 72 82 26 47 7c ee 46 71 e8 5e 6f 50 32 e6 f8 73 b6 01 ae ae cf a2 60 13 ce 38 8d 5c bb be 03 62 2d 82 70 15 35 d8 9d 1b df b0 20 a4 bf 83 4d 4c 64 56 c1 dc 5d b8 33 52 af c1 9c 90 b3 35 0f 57 6e 0c 42 b0 75 18 dc ba 73 f8 10 df 38 31 fc 87 03 21 cf 0b ee 5c 7f c9 66 81 3f 77 11 29 22 a4 15 8f 9f 6b d1 18 fb 2d 23 5e c4 82 85 92 6b 16 cc 01 7e 13 c5 a0 54 ec 80 bc 48 d8 b9 0e 6e 71 4a 19 c9 0f 62 77 c6 1b 92 1c 03 18 37 62 1e 50 44 42 26 6f 7f 9e 11 0c d8 ce 3c c7 5d f1 b0 59 2a 0c 30 35 2c a3 84 01 75 e7 1b 10 f0 67 c9 c3 a4 ae f3 60 b6 59 71 3f 26 9b 6b 8a 80 d9 02 df 04 00 11 b2 15 04 41 e8 3a 5e 94 f8 80 9c 47 e8 86 2a 89 8a 03 ee 12 26 42 f8 ce 8a a3 5c e5 f1 05 fa 24 a0 e4 1c 37 8e b4 28 a0 8f e0 10 84 11 88 72 cf 80 0a c4 16 68 16 30 ee cf 61 94 63 18 81 68 ab 20 e6 4c d8 0d 82 74 0e 32 43 8c b2 05 4c 90 85 34 c5 28 58 c4 77 18 27 32 f4 58 b4 e6 33 8c 3b 40 76 31 22 43 8c 38 5f c4 5e 14 29 cd 08 7f f2 da 1e b3 f1 f0 6c f2 b6 33 ea 31 f8 7c 31 1a be b1 4f 7b a7 ec e4 1d 4c f6 58 77 78 f1 6e 64 bf 7a 3d 61 af 87 fd d3 de 68 cc 3a 83 53 18 1d 4c 46 f6 c9 74 32 84 81 5a 67 0c 98 35 b1 aa 60 b2 33 78 c7 7a ff ba 18 f5 c6 63 36 1c 31 fb fc a2 6f 03 41 e0 30 ea 0c 26 76 6f dc 60 f6 a0 db 9f 9e da 83 57 0d 06 44 d8 60 38 61 7d fb dc 9e 00 d8 64 d8 40 c6 44 2d 8f ca 86 67 ec bc 37 ea be 86 af 9d 13 bb 6f 4f de 11 cf 33 7b 32 40 7e 67 c0 b0 c3 2e 3a a3 89 dd 9d f6 3b 23 76 31 1d 5d 0c c7 82 1c aa 78 6a 8f bb fd 8e 7d de 3b 6d 82 14 c0 99 f5 de f4 06 13 36 7e dd e9 f7 33 1a 0f df 0e 7a 23 54 21 a5 ee 89 20 d6 b7 3b 27 fd 9e 60 08 0a 9f da a3 5e 77 82 9a 25 9f ba 60 48 10 b3 df 60 e3 8b 5e d7 c6 0f bd 7f f5 40 a7 ce e8 5d 03 e8 8a dc 35 1c 8c 7b ff 9c 02 20 00 b0 d3 ce 79 e7 15 a8 69 ed b0 10 b8 a9 3b 1d f5 ce 51 f4 e1 19 11 1a 4f 4f c6 13 7b 32 9d f4 d8 ab e1 f0 94 6c 3f ee 8d de d8 dd de f8 98 f5 87 63 32 de 74 dc 6b 00 97 49 07 05 40 32 60 39 98 86 cf 27 d3 b1 8d 36 14 96 1f 4c 7a a3 d1 f4 62 62 0f 07 75 70 fd 5b b0 12 d8 a1 03 e8 a7 64 f0 e1 80 d4 06 83 0d 47 ef 90 30 da 83 fc d1 60 6f 5f f7 60 1c 3c 3f 50 1a 4e Data Ascii: 133b<ksI=e>1kbn#@@^hAnqw#Yk_f_qCU3+++ps'v 7?D0A|CHvqvG/u}.obfgdyp>*b?u:17yp"r&G|Fq^oP2s`8\b-p5 MLdV]3R5WnBus81!\f?w)"k-#^k~THnqJbw7bPDB&o<]Y*05,ug`Yq?&kA:^G*&B\$7(rh0ach Lt2CL4(Xw'2X3;@v1" C8_^)l31|1O{LXwxndz=ah:SLFt2Zg5`3xzc61oA0&vo`WD`8a}d@D-g7oO3{2@~g.:;#v1]xj};m6~3z#T! ;`^w%`H`^@]5{ yi;QOO{2l?c2tkI@2`9'6Lzbbup[dG0`o_`<?PN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49734	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.183556080 CEST	2030	OUT	GET /css/EmbeddedFonts.css HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.387576103 CEST	2036	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/css Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Last-Modified: Sat, 11 Jun 2016 21:43:38 GMT Expires: Wed, 01 Sep 2021 22:10:54 GMT Cache-Control: max-age=2592000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Content-Encoding: gzip Data Raw: 31 38 64 0d 0a 1f 8b 08 00 00 00 00 00 03 bd d2 d1 4a c3 30 18 86 e1 5b 11 76 d0 0d 6c b3 39 9c 58 0f 3a 3c 10 06 82 e2 d8 05 b4 e9 9f 2e 90 26 25 c9 9c 43 bc 77 5b 37 21 c6 a9 c3 f6 ef d1 ba b4 7c ef 46 9f 39 53 d2 86 2c a5 f0 7a b8 2a b9 d8 c5 c1 12 0a 05 ab 45 f8 04 c5 46 a4 3a 64 5c a6 22 b8 31 9a c6 1b 2d 86 c1 da da ca c4 84 54 5a e5 51 69 14 cd 65 44 55 49 26 b3 68 3c 8e 26 17 57 d7 f5 e7 8c 80 0c 57 4b 42 8d 21 5b c8 9a 80 21 47 97 23 50 36 18 a1 ce 27 1c 18 7f 09 46 67 4c e9 32 b5 c3 00 ca 0c f2 1c f2 50 55 20 ed ae 82 60 74 8e 12 df 2a c6 9c ee fe 2b 4e ca 5a b7 64 f5 06 30 ff 98 79 2e 06 f5 23 4e b1 3e a9 5f e3 87 24 63 77 02 62 d9 dc 10 fb 93 2d f0 62 6d 0f 47 6f f3 3f e4 2d a1 e4 b7 4a e4 08 f4 be 4e 77 6f ef fb 7e 9f f8 bc 3a aa 3e af 85 cd cf cb a1 fa bb 6f 1e 46 c0 e7 ec 76 2f cf 1b ef 93 9d 9b 46 35 e7 86 b0 c1 b9 2d 54 6d 8d 6c 2c 71 de 76 f7 ea 8e 04 fa 94 e7 e7 51 f5 f9 31 6c 81 7e 0f 45 e1 a3 d2 36 15 0b aa a4 e9 44 9e b3 d7 9d 36 6f b4 0f 61 6e 12 45 95 1b c0 92 e4 36 50 f4 3c 30 c6 29 4c 67 97 ad 01 dd a5 99 e6 94 d4 f7 c6 d1 94 ec 7f be fa 5c e7 9d 70 3a 2d 91 0c 4e d6 d5 2a d5 28 4a 7e 50 d5 6a b8 c6 94 fc a2 a9 d5 76 4d 26 f9 bf a2 77 2f 30 16 69 72 0e 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 18dJ0[vl9X:<.&%Cw[7!|F9S,z*EF:d\"1-TZQieDUI&h<&WWKB![!G#P6'FgL2PU `t*+NZd0y.#N>_$cwb-bmGo?-JNwo~:>oFv/F5-Tml,qvQ1l~E6D6oanE6P<0)Lg\p:-N*(J~PjvM&w/0ir0
Aug 3, 2021 00:10:54.412552118 CEST	2064	OUT	GET /css/shellg2pluscss_baae2042.css HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36 Accept: text/css,*/*;q=0.1 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9
Aug 3, 2021 00:10:54.629344940 CEST	2099	IN	HTTP/1.1 404 Not Found Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Encoding: gzip Data Raw: 65 65 0d 0a 1f 8b 08 00 00 00 00 00 03 55 90 41 4f c3 30 0c 85 ef fd 15 66 67 98 07 da 31 8a 04 6b 27 26 95 31 a1 ec c0 31 2c 86 44 ca 92 91 b8 4c fd f7 24 1d 12 70 f4 f3 f7 ec 67 8b ab f6 79 a5 5e 77 1d 3c aa a7 1e 76 fb 87 7e b3 82 d9 0d e2 a6 53 6b c4 56 b5 97 ce dd 7c 81 d8 6d 67 b2 11 96 8f 5e 0a 4b da 94 82 1d 7b 92 cb c5 12 b6 91 61 1d 87 60 04 5e c4 46 e0 04 89 b7 68 c6 ea bb 95 7f 98 52 35 e2 24 95 25 48 f4 39 50 66 32 b0 7f e9 e1 ac 33 84 c2 bd 57 0e 62 00 b6 2e 43 a6 f4 45 69 2e f0 34 d9 ee 8d 71 ec 62 d0 de 8f d7 a0 e1 5f 80 86 52 8a 69 1a 44 e1 50 14 a6 54 86 9f ad f3 04 9c 46 17 3e 80 23 0c 99 40 07 e8 2a dc c6 c3 70 a4 c0 55 b7 3a 98 0a fe 26 fb 59 8b d3 21 25 7a 7d 40 f3 0d 59 3c e4 fe 3b 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: eeUAO0fg1k'&11,DL$pgy^w<v~SkV\|mg^K{a`^FhR5$%H9Pf23Wb.CEi.4qb_RiDPTF>#@*pU:&Y!%z}@Y<;0
Aug 3, 2021 00:10:54.634207010 CEST	2100	OUT	GET /images/social_auth_providers.png HTTP/1.1 Host: axxy.coronationtraining.co.za 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 Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:54.837213039 CEST	2162	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:54 GMT Content-Type: image/png Content-Length: 4056 Connection: keep-alive Last-Modified: Thu, 09 Feb 2017 12:44:02 GMT Expires: Fri, 01 Oct 2021 22:10:54 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 64 00 00 00 24 08 06 00 00 00 be 34 40 f8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 78 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 30 36 37 20 37 39 2e 31 35 37 37 34 37 2c 20 32 30 31 35 2f 30 33 2f 33 30 2d 32 33 3a 34 30 3a 34 32 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 44 37 41 37 34 45 46 41 41 44 42 39 31 31 45 36 38 32 30 38 41 46 31 43 35 41 38 41 36 42 30 31 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 44 37 41 37 34 45 46 39 41 44 42 39 31 31 45 36 38 32 30 38 41 46 31 43 35 41 38 41 36 42 30 31 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 Data Ascii: PNGIHDRd$4@tEXtSoftwareAdobe ImageReadyqe<xiTXtXML:com.adobe.xmp<?xpacket begin="" id="W 5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Reso urceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:fb981994-92c4-4700-92f9-9 3c8e28d32dd" xmpMM:DocumentID="xmp.did:D7A74EFAADB911E68208AF1C5A8A6B01" xmpMM:InstanceID= "xmp.iid:D7A74EF9ADB911E68208AF1C5A8A6B01" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <x mpMM:DerivedFrom stRef:instanceID="xmp.iid:fb981994-92c4-4700-92f9-93c8e28d32dd" stRef:documentID="x mp.did:fb981994-92c4-4700-92f9-93c8e28d32dd"/> </rdf:Description>
Aug 3, 2021 00:10:54.924699068 CEST	2178	OUT	GET /assets/cJZKeOuBrn4kERxqtaUH3T8E0i7KZn-EPnyo3HZu7kw.woff HTTP/1.1 Host: axxy.coronationtraining.co.za Connection: keep-alive Origin: http://axxy.coronationtraining.co.za 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: */* Referer: http://axxy.coronationtraining.co.za/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:55.129216909 CEST	2216	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:55 GMT Content-Type: font/woff Content-Length: 21956 Connection: keep-alive Last-Modified: Wed, 23 Apr 2014 01:03:00 GMT Expires: Fri, 01 Oct 2021 22:10:55 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 77 4f 46 46 00 01 00 00 00 00 55 c4 00 10 00 00 00 00 8e 8c 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 46 46 54 4d 00 00 01 6c 00 00 00 1c 00 00 00 1c 5c ac 79 1d 4f 53 2f 32 00 00 01 88 00 00 00 5d 00 00 00 60 a1 3d bf 0e 63 6d 61 70 00 00 01 e8 00 00 01 68 00 00 01 b2 8c e8 dc 99 63 76 74 20 00 00 03 50 00 00 00 59 00 00 00 a2 0f 4d 18 a4 66 70 67 6d 00 00 03 ac 00 00 04 a9 00 00 07 b4 7e 61 b6 11 67 61 73 70 00 00 00 08 58 00 00 00 10 00 00 00 10 00 15 00 23 67 6c 79 66 00 00 08 68 00 00 35 bf 00 00 51 54 ac c1 ad b5 68 65 61 64 00 00 3e 28 00 00 00 33 00 00 00 36 f9 36 14 da 68 68 65 61 00 00 3e 5c 00 00 00 1f 00 00 00 24 0e b7 04 fa 68 6d 74 78 00 00 3e 7c 00 00 02 0f 00 00 03 58 98 77 57 02 6b 65 72 6e 00 00 40 8c 00 00 0e 14 00 00 23 04 0c 96 0f 09 6c 6f 63 61 00 00 4e a0 00 00 01 ae 00 00 01 ae 76 97 63 4c 6d 61 78 70 00 00 50 50 00 00 00 20 00 00 00 20 02 5d 01 4a 6e 61 6d 65 00 00 50 70 00 00 02 e3 00 00 06 09 de 88 72 c2 70 6f 73 74 00 00 53 54 00 00 01 78 00 00 01 f2 82 78 e9 d5 70 72 65 70 00 00 54 cc 00 00 00 f8 00 00 01 09 43 b7 96 a4 00 00 00 01 00 00 00 00 c9 89 6f 31 00 00 00 00 c9 35 31 8b 00 00 00 00 c9 ed d8 60 78 9c 63 60 66 f1 63 9c c0 c0 ca c0 c1 3a 8b d5 98 81 81 51 1e 42 33 5f 64 48 63 fc c8 c1 c4 c4 cd c6 c6 cc ca c2 c4 c4 f2 80 81 e9 bd 03 83 42 34 03 03 83 06 10 33 18 3a 06 3b 33 00 05 14 d6 b0 c9 ff 13 61 68 e1 e8 65 8a 50 60 60 9c 0f 92 63 f1 60 dd 06 a4 80 5c 00 af b7 0e 9f 00 00 00 78 9c 63 60 60 60 66 80 60 19 06 46 06 10 58 03 e4 31 82 f9 2c 0c 13 80 b4 02 10 b2 00 e9 3a 86 ff 8c 86 8c c1 4c c7 98 6e 31 dd 51 10 51 90 52 90 53 50 52 b0 52 70 51 28 51 58 f3 ff 3f 58 e5 02 a0 8a 20 a8 0a 61 05 09 05 19 a0 0a 4b 98 8a ff 8f ff 1f fa 3f f1 7f e1 df ff 7f df fc 7d fd 60 eb 83 4d 0f 36 3e 58 f7 60 c6 83 fe 07 09 0f 34 a1 b6 e3 05 8c 6c 0c 70 65 8c 4c 40 82 09 5d 01 d0 2b 2c ac 6c ec 1c 9c 5c dc 3c bc 7c fc 02 82 42 c2 22 a2 62 e2 12 92 52 d2 32 b2 72 f2 0a 8a 4a ca 2a aa 6a ea 1a 9a 5a da 3a ba 7a fa 06 86 46 c6 26 a6 66 e6 16 96 56 d6 36 b6 76 f6 0e 8e 4e ce 2e ae 6e ee 1e 9e 5e de 3e be 7e fe 01 81 41 c1 21 a1 61 e1 11 91 51 d1 31 b1 71 f1 09 89 0c 6d ed 9d dd 93 67 cc 5b bc 68 c9 b2 a5 cb 57 ae 5e b5 66 ed fa 75 1b 36 6e de ba 65 db 8e ed 7b 76 ef dd c7 50 94 92 9a 79 a1 62 61 41 36 43 59 16 43 c7 2c 86 62 06 86 f4 72 b0 eb 72 6a 18 56 ec 6a 4c ce 03 b1 73 6b 19 92 9a 5a a7 1f 3e 72 e2 e4 d9 73 a7 4e ef 64 38 c8 70 f9 ea c5 4b 40 99 ca 33 e7 19 5a 7a 9a 7b bb fa 27 4c ec 9b 3a 8d 61 ca 9c b9 b3 0f 1d 3d 5e c8 c0 70 ac 0a 28 0d 00 a7 4b 7b 8e 78 9c 63 13 61 10 67 f0 63 dd 06 24 4b 59 b7 b1 9e 65 40 01 2c 1e 0c 22 0c 13 19 18 fe bf 01 f1 10 e4 3f 11 10 09 d4 25 fc 67 ca ff b7 ff 5a ff bf fa b7 12 28 22 f1 6f 0f 03 59 80 03 42 75 33 34 32 dc 65 98 c1 d0 cf d0 c7 Data Ascii: wOFFUFFTMl\yOS/2]`=cmaphcvt PYMfpgm~agaspX#glyfh5QThead>(366hhea>\$hmtx>|XwWkern@#locaNv cLmaxpPP ]JnamePprpostSTxxprepTCo151`xc`fc:QB3_dHcB43:;3aheP``c`\xc```f`FX1,:Ln1QQRSPRRpQ(QX?X aK?} `M6>X`4lpeL@]+,l\<|B"bR2rJ*jZ:zF&fV6vN.n^>~A!aQ1qmg[hW^fu6ne{vPybaA6CYC,brrjVjLskZ>rsNd8pK@3Zz{'L:a= ^p(K{xcagc$KYe@,"?%gZ("oYBu342e

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49748	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:56.753168106 CEST	2266	OUT	GET /images/favicon.ico HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: axxy.coronationtraining.co.za

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Aug 3, 2021
00:10:56.956697941 CEST</td><td>2270</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Aug 2021 22:10:56 GMT
Content-Type: image/x-icon
Content-Length: 7406
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Thu, 09 Feb 2017 12:49:08 GMT
Expires: Fri, 01 Oct 2021 22:10:56 GMT
Cache-Control: max-age=5184000
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Nginx-Upstream-Cache-Status: HIT
X-Server-Powered-By: nginx-ah
Accept-Ranges: bytes
Data Raw: 00 00 01 00 03 00 10 10 00 00 01 00 08 00 68 05 00 00 36 00 00 00 20 20 00 00 01 00 08 00 a8 08 00 00 9e 05 00 00 30 30 00 00 01 00 08 00 a8 0e 00 00 46 0e 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 08 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 44 a9 f3 00 4c c7 fc 00 27 37 d0 00 4d cc fe 00 4a c0 fa 00 2b 49 d5 00 32 65 de 00 26 36 cf 00 4c cb fd 00 27 36 cf 00 38 7c e5 00 4c c9 fd 00 26 34 cf 00 3a 81 e7 00 3e 93 ec 00 2c 4b d6 00 4d cf fe 00 4c c8 fc 00 27 38 d0 00 4d cd fe 00 42 a3 f1 00 36 74 e2 00 49 bf fa 00 2c 4d d7 00 4c ca fd 00 49 be f9 00 37 76 e3 00 43 a5 f2 00 4a c3 fb 00 2c 4c d6 00 4c c8 fd 00 49 bc f9 00 32 63 dd 00 2c 4a d6 00 4d ce fe 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 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 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 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 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 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 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 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 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
Data Ascii: h6 00F(DL'7MJ+I2e&6L'68|L&4:>,KML'8MB6tI,MLI7vCJ,LLI2c,JM</td></tr>
<tr><td>Aug 3, 2021
00:10:56.959414005 CEST</td><td>2281</td><td>OUT</td><td>GET /images/apple-touch-icon-72x72.png HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36
Host: axxy.coronationtraining.co.za</td></tr>
<tr><td>Aug 3, 2021
00:10:57.158807039 CEST</td><td>2291</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Aug 2021 22:10:57 GMT
Content-Type: image/png
Content-Length: 1391
Connection: keep-alive
Last-Modified: Fri, 10 Feb 2017 00:16:28 GMT
Expires: Fri, 01 Oct 2021 22:10:57 GMT
Cache-Control: max-age=5184000
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Nginx-Upstream-Cache-Status: HIT
X-Server-Powered-By: nginx-ah
Accept-Ranges: bytes
Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 48 00 00 00 48 08 03 00 00 00 62 33 43 75 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 20 63 48 52 4d 00 00 7a 26 00 00 80 84 00 00 fa 00 00 00 80 e8 00 00 75 30 00 00 ea 60 00 00 3a 98 00 00 17 70 9c ba 51 3c 00 00 01 fe 50 4c 54 45 fe cd 4d fe cd 4d fe cd 4d ff cf 4d ff cf 4e ff cf 4e fe cd 4d fd cb 4c f3 a8 44 ef 9c 40 ef 9d 41 fe cd 4d fc c6 4b dc 5d 31 d0 39 27 d1 3b 28 fe cd 4d fc c6 4b db 5b 30 cf 36 26 d0 38 27 fc c6 4b db 5b 30 cf 36 26 d0 38 27 db 5b 30 fe cd 4d fe ce 4d fe ce 4d fe ce 4d fc c6 4b db 5b 30 cf 36 26 db 5b 30 fe cd 4d fe cd 4d fc c7 4b fb c4 4b fb c4 4b fb c4 4b fb c5 4b f9 bd 49 da 59 30 cf 36 26 fe cd 4d fe ce 4d f3 aa 44 dd 60 31 da 57 2f da 58 2f da 58 2f da 58 2f d9 56 2f d2 40 29 d0 38 27 dd 60 31 f3 aa 44 fe cd 4d fd ca 4c ea 8d 3d d2 3e 29 cf 35 26 cf 36 27 cf 36 27 cf 36 27 cf 36 27 d0 38 27 fe cd 4d fe cd 4d fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 fe cc 4d eb 8f 3d d0 37 27 eb 8f 3d d2 40 29 d0 37 27 fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cc 4d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cd 4d fe cc 4d eb 8f 3d d2 40 29 fe cd 4d fe cc 4d d2 40 29 fe cc 4d eb 8f 3d d2 40 29 d0 37 27 fe cc 4d eb 8f 3d fe cc 4d eb 8f 3d d2 40 29 d2 40 29 fe cc 4d d2 40 29 d0 37 27 eb 8f 3d d2 3f 29 fe cc 4d ec 92 3e fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe cd 4d fe ce 4d fe ce 4d fe ce 4d fe cd 4d fe cc 4d fa c0 4a f9 bd 49 f9 bd 49 fe cd 4d fe cd 4d eb 91 3e d8 51 2d d7 4e 2d d7 4e 2d fe cd 4d fc c7 4b da 59 2f cf 34 26 cf 36 27 cf 36 27 cf 36 27 cf 34 26 fe cd 4d fd cb 4d e4 7a 38 d1 3d 28 d1 3b 28 d1 3b 28 d1 3d 28 fe ce 4d fb c4 4b f2 a6 43 ef 9c 41 ef 9d 41 ef 9d 41 ef 9c 41 f2 a5 43 fb c4 4b fe cd 4d fe ce 4d ff cf 4e ff cf 4e ff cf 4e ff cf 4e ff ff ff 60 0f 32 8f 00 00 00 01 62 4b 47 44 a9 27 0f 06 04 00 00 00 07 74 49 4d 45 07 df 05 0b 09 39 24 0d 0b 5e cf 00 00 02 49 49 44 41 54 58 c3 63 60 18 05 a3 60 14 0c 30 60 64 62 66 61 45 02 2c cc 4c 8c 64 19 c4 c6 ce c1 c9 85 04 38 39 d8 d9 c8 32 88 9b 87 97 8f 1f 09 f0 f1 f2 70 93 65 90 80 a0 90 b0 08 12 10 16 12 14 20 cf 20 51 31 71 09 24 20 2e 29 3a 6a d0 a8 41 a3 06 31 48 49 cb 40 80 ac 9c bc 02 b2 41 0a 8a 72 b2 50 29 69 29 82 c6 28 29 ab a8 aa a9 83 81 86 a6 96 36 b2 41 da 5a 9a 1a 10 19 35 55 15 65 25 02 06 e9 e8 ea e9 1b 18 1a 81 80 b1 89 a9 19 b2 41 66 a6 26 c6 60 09 43 03 73 0b 5d 1d 42 4e b2 b4 b2 b6 b1 b5 b3 07 02 07 47 33 27 64 83 9c cc 1c 1d 40 e2 76 b6 36 d6 56 96 04 fd e6 ec e2 ea e6 ee 81 62 02 2a 70 f2 70 77 73 75 71 26 1c d8 ce 9e 5e de 3e b8 4d 72 f2 f0 f1 f6 f2 24 c2 1c 90 9b 7c fd dc fd 71 98 e4 e4 ef 1e e0 4b 8c 7b 20 26 79 b9 05 06 61 35 c9 29 28 d0 cd 8b 58 73 40 be 0b 0e 09 0d c3 62 92 53 58 68 48 30
Data Ascii: PNGIHDRHHb3CugAMAa cHRMz&u0`:pQ<PLTEMMMMNNMLD@AMK]19';(MK[06&8'K[06&8'[0MMMMK[06&[0MMKKKKKIY06&MMD`1W/X/X/X/V/@)8'`1DML=>)5&6'6'6'6'8'MMM=@)7'MM=@)M=7'=@)7'M=@)7'M@)7'MM=@)7'MM=@)MM@)M=@)7'M=M=@)@)M@)7'=?)M>MMMMMMMMMMMMJIIMM>Q-N-N-MKY/4&6'6'6'4&MMz8=(;(;(=(MKCAAAACKMMNNNN`2bKGD'tIME9$^IIDATXc``0`dbfaE,Ld892pe  Q1q$ .):jA1HI@ArP)i)()6AZ5Ue%Af&`Cs]BNG3'd@v6Vb*ppwsuq&^>Mr$|qK{ &ya5)(Xs@bSXhH0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49751	154.0.167.80	80	C:\Program Files\Google\Chrome\Application\chrome.exe

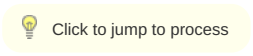
Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:56.784255028 CEST	2266	OUT	GET /images/docusign.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: axxy.coronationtraining.co.za
Aug 3, 2021 00:10:56.987759113 CEST	2283	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:56 GMT Content-Type: image/png Content-Length: 7635 Connection: keep-alive Last-Modified: Thu, 09 Feb 2017 23:58:20 GMT Expires: Fri, 01 Oct 2021 22:10:56 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 45 00 00 00 5c 08 06 00 00 00 f9 da a7 ba 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 73 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 33 2d 63 30 31 31 20 36 36 2e 31 34 35 36 36 31 2c 20 32 30 31 32 2f 30 32 2f 30 36 2d 31 34 3a 35 36 3a 32 37 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 36 33 64 39 36 62 62 32 2d 39 31 36 37 2d 34 63 63 2d 39 66 65 32 2d 63 33 63 65 65 36 31 61 38 35 33 64 22 20 78 6d 70 4d 4d 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 44 35 31 39 46 45 37 30 38 44 31 46 31 31 45 33 39 36 43 42 38 32 30 36 45 42 33 31 41 41 32 35 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 44 35 31 39 46 45 36 46 38 44 31 46 31 31 45 33 39 36 43 42 38 32 30 36 45 42 33 31 41 41 32 35 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 32 30 63 30 34 37 37 39 2d 30 62 35 62 2d 34 66 31 37 2d 61 64 33 63 2d 31 35 66 39 35 61 66 39 62 39 38 36 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 36 33 64 39 36 62 62 32 2d 39 31 36 37 2d 34 63 63 2d 39 66 65 32 2d 63 33 63 65 65 36 31 61 38 35 33 64 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 3c 2f 72 64 66 Data Ascii: PNGIHDRE\tEXtSoftwareAdobe ImageReadyqe<siTXtXML:com.adobe.xmp<?xpacket begin="" id="W5M 0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.3-c011 66.145661, 2012/02/06-14:56:27 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rd f:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Resour ceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:63d96bb2-9167-4ccc-9fe2-c3c ee61a853d" xmpMM:DocumentID="xmp.did:D519FE708D1F11E396CB8206EB31AA25" xmpMM:InstanceID="xmp.iid:D51 9FE6F8D1F11E396CB8206EB31AA25" xmp:CreatorTool="Adobe Photoshop CC (Macintosh)"> <xmpMM:DerivedFrom stRef:instanceID="xmp.iid:20c04779-0b5b-4f17-ad3c-15f95af9b986" stRef:documentID="xmp.did:63d96bb2-9167-4ccc-9 fe2-c3cee61a853d"/> </rdf:Description> </rdf
Aug 3, 2021 00:10:56.990794897 CEST	2290	OUT	GET /images/social_auth_providers.png HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Host: axxy.coronationtraining.co.za

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 00:10:57.194895983 CEST	2294	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 02 Aug 2021 22:10:57 GMT Content-Type: image/png Content-Length: 4056 Connection: keep-alive Last-Modified: Thu, 09 Feb 2017 12:44:02 GMT Expires: Fri, 01 Oct 2021 22:10:57 GMT Cache-Control: max-age=5184000 X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: HIT X-Server-Powered-By: nginx-ah Accept-Ranges: bytes Data Raw: 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 01 64 00 00 00 24 08 06 00 00 00 be 34 40 f8 00 00 00 19 74 45 58 74 53 6f 66 74 77 61 72 65 00 41 64 6f 62 65 20 49 6d 61 67 65 52 65 61 64 79 71 c9 65 3c 00 00 03 78 69 54 58 74 58 4d 4c 3a 63 6f 6d 2e 61 64 6f 62 65 2e 78 6d 70 00 00 00 00 00 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78 3a 78 6d 70 6d 65 74 61 20 78 6d 6c 6e 73 3a 78 3d 22 61 64 6f 62 65 3a 6e 73 3a 6d 65 74 61 2f 22 20 78 3a 78 6d 70 74 6b 3d 22 41 64 6f 62 65 20 58 4d 50 20 43 6f 72 65 20 35 2e 36 2d 63 30 36 37 20 37 39 2e 31 35 37 37 34 37 2c 20 32 30 31 35 2f 30 33 2f 33 30 2d 32 33 3a 34 30 3a 34 32 20 20 20 20 20 20 20 20 22 3e 20 3c 72 64 66 3a 52 44 46 20 78 6d 6c 6e 73 3a 72 64 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 30 32 2f 32 32 2d 72 64 66 2d 73 79 6e 74 61 78 2d 6e 73 23 22 3e 20 3c 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 20 72 64 66 3a 61 62 6f 75 74 3d 22 22 20 78 6d 6c 6e 73 3a 78 6d 70 4d 4d 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 6d 6d 2f 22 20 78 6d 6c 6e 73 3a 73 74 52 65 66 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 73 54 79 70 65 2f 52 65 73 6f 75 72 63 65 52 65 66 23 22 20 78 6d 6c 6e 73 3a 78 6d 70 3d 22 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 22 20 78 6d 70 4d 4d 3a 4f 72 69 67 69 6e 61 6c 44 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 64 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 20 78 6d 70 3a 44 6f 63 75 6d 65 6e 74 49 44 3d 22 41 44 42 45 31 31 45 36 38 32 30 38 41 46 31 43 35 41 38 41 36 42 30 31 22 20 78 6d 70 4d 4d 3a 49 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 44 37 41 37 34 45 46 41 41 44 42 39 31 31 45 36 38 32 30 38 41 46 31 43 35 41 38 41 36 42 30 31 22 20 78 6d 70 3a 43 72 65 61 74 6f 72 54 6f 6f 6c 3d 22 41 64 6f 62 65 20 50 68 6f 74 6f 73 68 6f 70 20 43 43 20 32 30 31 35 20 28 4d 61 63 69 6e 74 6f 73 68 29 22 3e 20 3c 78 6d 70 4d 4d 3a 44 65 72 69 76 65 64 46 72 6f 6d 20 73 74 52 65 66 3a 69 6e 73 74 61 6e 63 65 49 44 3d 22 78 6d 70 2e 69 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 20 73 74 52 65 66 3a 64 6f 63 75 6d 65 6e 74 49 44 3d 22 78 6d 70 2e 64 69 64 3a 66 62 39 38 31 39 39 34 2d 39 32 63 34 2d 34 37 30 30 2d 39 32 66 39 2d 39 33 63 38 65 32 38 64 33 32 64 64 22 2f 3e 20 3c 2f 72 64 66 3a 44 65 73 63 72 69 70 74 69 6f 6e 3e 20 Data Ascii: PNGIHDRd$4@tEXtSoftwareAdobe ImageReadyqe<xiTXtXML:com.adobe.xmp<?xpacket begin="" id="W 5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.6-c067 79.157747, 2015/03/30-23:40:42 "> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about="" xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/Reso urceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:fb981994-92c4-4700-92f9-9 3c8e28d32dd" xmpMM:DocumentID="xmp.did:D7A74EFAADB911E68208AF1C5A8A6B01" xmpMM:InstanceID= "xmp.iid:D7A74EF9ADB911E68208AF1C5A8A6B01" xmp:CreatorTool="Adobe Photoshop CC 2015 (Macintosh)"> <x mpMM:DerivedFrom stRef:instanceID="xmp.iid:fb981994-92c4-4700-92f9-93c8e28d32dd" stRef:documentID="x mp.did:fb981994-92c4-4700-92f9-93c8e28d32dd"/> </rdf:Description>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: chrome.exe PID: 4580 Parent PID: 4896

General

Start time:	00:10:47
Start date:	03/08/2021

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 'http://axxy.coronationtraining.co.za/'
Imagebase:	0x7ff77b960000
File size:	2150896 bytes
MD5 hash:	C139654B5C1438A95B321BB01AD63EF6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: chrome.exe PID: 464 Parent PID: 4580

General

Start time:	00:10:48
Start date:	03/08/2021
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=1644,535561337354264425 1,6732772637902819495,131072 --lang=en-US --service-sandbox-type=network --enable-audio-service-sandbox --mojo-platform-channel-handle=1720 /prefetch:8
Imagebase:	0x7ff77b960000
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

Disassembly