

Browser Forensic Tools

With the help of Browser Forensics and with the assistance of forensics tools one can extract sensitive data and chosen keywords from most web browsers. One can retrieve deleted data and keywords, check whether history was cleared, retrieve artifacts like Cookies, Downloads data, History, Saved Password, websites visited etc. Also, it helps a lot to understand how an attack on a system was conducted, helping in finding the source of Malwares/ Adware / Spywares, Malicious Emails and Phishing Websites etc.

1. Chrome-Cache-View-

Chrome Cache View is a small utility that reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.

Usage/advantages-

- Information for cache file are displayed as - URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, and more.
- You can select and export one or more cache files from the list,
- Copy the URL list and the entire table of cache files to excel spreadsheet.
- You can also extract and save the actual files from the cache.

The Location of Chrome Cache Folder-

The cache folder of Google Chrome –

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

Download chrome-cache-view from –

https://www.nirsoft.net/utils/chrome_cache_view.html

Copy the executable file (ChromeCacheView.exe) to the destination folder and run it.

```

Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HP>cd Downloads/chromecacheview

C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe

C:\Users\HP\Downloads\chromecacheview>

```

The main window displays the list of files currently stored in the cache of the default Google Chrome user.

Filename	URL	Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expires Time	Server Name	Server Response	Web Site	Frame	Content	Cache Name	Ca
a3632c32f102ee...	https://static.site24x7rum...	application/avas...	22,443	29-Mar-23 5:55:07...	29-Mar-23 3:57:22...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	ZGS	HTTP/1.1 200 OK	https://econci...	https://.../gzip	f_0042b8		
NdfYgELO08GT1...	https://eccommonstorage...	image/jpeg	212,340	29-Mar-23 5:55:12...	22-Mar-23 5:01:17...	27-Oct-22 4:17:59 P...	01-Jan-01 5:30:00...	Windows-Azure-Blo...	HTTP/1.1 200 OK	https://eccom...	https://.../gzip	f_0029da		
v=vhBYRMqS1BED...	https://www.youtube.com/...	application/json	2,779	08-Apr-23 2:20:17...	08-Apr-23 2:20:17...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	video-timedtext	HTTP/1.1 200	https://youtu...	https://.../gzip	data_2 (41...	no	
Vn+0SN5STLqlk...	https://www.youtube.com/...	application/json	1,638	08-Apr-23 2:20:30...	08-Apr-23 2:20:30...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	video-timedtext	HTTP/1.1 200	https://youtu...	https://.../gzip	data_2 (23...	no	
v=sKtVUF2QkLq...	https://www.youtube.com/...	application/json	1,598	08-Apr-23 2:20:21...	08-Apr-23 2:20:20...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	video-timedtext	HTTP/1.1 200	https://youtu...	https://.../gzip	data_2 (16...	no	
html5=1&video=...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:19:52...	08-Apr-23 2:19:51...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:19:52...	08-Apr-23 2:19:51...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
html5=1&video=...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:00...	08-Apr-23 2:19:59...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
html5=1&video=...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:18...	08-Apr-23 2:20:17...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	06-Apr-23 11:05:15...	06-Apr-23 11:05:15...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	07-Apr-23 15:03:03...	07-Apr-23 15:03:03...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:05...	08-Apr-23 2:20:04...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:00...	08-Apr-23 2:19:59...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:19:55...	08-Apr-23 2:19:54...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:19:57...	08-Apr-23 2:19:56...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:14...	08-Apr-23 2:20:13...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:07...	08-Apr-23 2:20:06...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	07-Apr-23 15:06:02...	07-Apr-23 15:06:02...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	07-Apr-23 11:11:13...	07-Apr-23 11:11:13...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:18...	08-Apr-23 2:20:17...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:18...	08-Apr-23 2:20:18...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
ns=y8el=detail...	https://www.youtube.com/...	text/html	0	08-Apr-23 2:20:18...	08-Apr-23 2:20:18...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Video Stats Server	HTTP/1.1 204	https://youtu...	https://.../no			
69f1e06645c07...	https://nas.io/_next/static/c...	text/css	1,715	21-Mar-23 12:04:41...	21-Mar-23 11:41:22...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Vercel	HTTP/1.1 200	https://nas.io...	https://.../br	data_2 [87...	pu	
ts=1609393732...	https://alt.reddit.com/p/g...	image/gif	42	08-Apr-23 10:06:13...	08-Apr-23 10:06:13...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:...	Vanish	HTTP/1.1 200	https://courser...	https://.../no	data_1 [44...		
A304862-b6fd...	https://utimpactcdn.com/c...	text/javascript	14,237	08-Apr-23 10:16:12...	08-Apr-23 10:03:04...	09-Feb-23 2:42:20...	08-Apr-23 1:08:...	UploadServer	HTTP/1.1 200	https://courser...	https://.../gzip	data_3 [64...	pu	
pix.js	https://www.redditstatic.co...	application/avas...	7,356	05-Apr-23 8:34:22...	05-Apr-23 8:34:18...	24-Jan-23 3:26:14 A...	01-Jan-01 5:30:...	snooserv	HTTP/1.1 200	https://varonis...	https://.../no	data_3 [56...	pu	
pix.js	https://www.redditstatic.co...	application/avas...	7,356	29-Mar-23 5:55:07...	29-Mar-23 5:54:57...	24-Jan-23 3:26:14 A...	01-Jan-01 5:30:...	snooserv	HTTP/1.1 200	https://econci...	https://.../gzip	data_3 [57...	pu	
pix.js	https://www.redditstatic.co...	application/avas...	7,356	08-Apr-23 10:16:13...	08-Apr-23 10:06:12...	24-Jan-23 3:26:14 A...	01-Jan-01 5:30:...	snooserv	HTTP/1.1 200	https://courser...	https://.../gzip	data_3 [64...	pu	
s2	https://www.google.com/...	text/javascript	2,013	08-Apr-23 10:06:04...	08-Apr-23 2:25:39...	08-Apr-23 2:41:41...	07-Apr-24 12:5...	sffe	HTTP/1.1 200	https://google.c...	https://.../br	data_2 [34...	pu	
icon_1_document...	https://ssl.gstatic.com/d...	image/png	260	06-Apr-23 10:06:13...	31-Mar-23 11:51:12...	04-Mar-20 1:45:00...	30-Mar-24 11:1...	sffe	HTTP/1.1 200	https://google.c...	https://.../no	data_1 [50...		
ic-google-trends...	https://www.google.com/...	image/png	520	07-Apr-23 10:24:02...	07-Apr-23 8:32:55...	04-Mar-23 4:30:00...	07-Apr-23 8:32:...	sffe	HTTP/1.1 200	https://google.c...	https://.../no	data_1 [32...	pri	
iberi_lg.png	https://ssl.gstatic.com/docs/...	image/png	853	07-Apr-23 3:04:20...	31-Mar-23 11:35:47...	04-Mar-20 1:45:00...	30-Mar-24 11:...	sffe	HTTP/1.1 200	https://google.c...	https://.../no	data_1 [42...	pri	
aRxBb	https://ssl.gstatic.com/...	text/javascript	2,063	07-Apr-23 18:51...	07-Apr-23 5:22:39...	05-Apr-23 11:52:13...	06-Apr-24 5:22:...	sffe	HTTP/1.1 200	https://google.c...	https://.../gzip	data_2 [31...	pu	
aRxBb	https://ssl.gstatic.com/...	text/javascript	1,920	06-Apr-23 2:27:40...	31-Mar-23 8:25:16...	30-Mar-23 11:33:38...	30-Mar-24 8:2...	sffe	HTTP/1.1 200	https://google.c...	https://.../gzip	data_2 [64...	pu	
aRxBb	https://ssl.gstatic.com/...	text/javascript	2,063	08-Apr-23 2:24:19...	07-Apr-23 6:50:58...	05-Apr-23 11:52:13...	06-Apr-24 6:50:...	sffe	HTTP/1.1 200	https://google.c...	https://.../gzip	data_2 [14...	pu	
aRxBb	https://www.gstatic.com/...	text/javascript	2,055	06-Apr-23 4:22:08...	05-Apr-23 8:09:39...	05-Apr-23 11:05:36...	04-Apr-24 8:09:...	sffe	HTTP/1.1 200	https://google.c...	https://.../gzip	data_2 [45...	pu	

Information gathered – file name, URL, timestamp, website, server time, IP address etc.

To extract files from cache simply click f4 or right click and choose “open selected cache file”-

□ 1	https://d87d339495eb2a30a7cb0abca3c93a6safeframe.goog...	0	08-Apr-23 2:23:45 ...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	https://geeksforgee...			
▀ 1-82.png	https://resources.infosecinstitute.com/wp-content/uploads/1-8...	image/png	F4	Apr-23 10:25:45 ...	08-Jun-18 9:13:32 P...	01-Jan-38 5:25:55 A...	cloudflare			
□ 1.0	https://www.microsoft.com/mwf/js/MWF_20230313_662474311...	application	Copy Selected Cache File To...	F4	Apr-23 8:24:10 ...	28-Mar-23 11:41:40...	HTTP/1.1 200	https://microsoft.co...		
□ 1.0.0	https://www.techopedia.com/wp-content/themes/twentytwent...	text/css	Open Selected Cache File	F7	Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	HTTP/1.1 200	https://techopedia.c...		
□ 1.0.0	https://www.techopedia.com/wp-content/themes/twentytwent...	text/css	Open Selected Cache File With...	Ctrl+W	Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	HTTP/1.1 200	https://infosecinsti...		
▀ 1.0.css	https://assets.tryhackme.com/css/utils/introjs.css?v=1.0	text/css	Save Selected Items	Ctrl+S	Apr-23 3:33:49 ...	04-Apr-23 11:30:00...	01-Jan-01 5:30:00 A...	AmazonS3		
▀ 1.02a6af04.chunk.	https://js.drift.com/core/assets/css/1.02a6af04.chunk.css	text/css	Copy Selected Items	Ctrl+C	Apr-23 12:22:24 ...	28-Feb-23 11:09:33...	01-Jan-01 5:30:00 A...	istio-envoy		
□ 1.1	https://assets.tryhackme.com/js/util/videos.js?v=1.1	application	Copy Clicked Cell	Ctrl+V	Apr-23 8:24:24 ...	04-Apr-23 11:00:05...	01-Jan-01 5:30:00 A...	AmazonS3		
▀ 1.1	https://assets.tryhackme.com/js/util/certificate.js?v=1.1	application	HTML Report - All Items	Ctrl+Shift+P	Apr-23 7:29:51 ...	06-Apr-23 4:23:52 ...	01-Jan-01 5:30:00 A...	AmazonS3		
□ 1.10	https://cdn-blog.netwrix.com/wp-content/plugins/tablepress/...	application	HTML Report - Selected Items	Ctrl+Shift+L	Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	AmazonS3		
□ 1.10.2	https://www.techopedia.com/wp-includes/js/hoverIntent/min.js	application	Choose Columns	Ctrl+Shift+M	Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	01-Jan-01 5:30:00 A...	Apache		
▀ 1.12.4-wp	https://blog.ccsociety.org/wp-includes/js/jquery/jquery.j...e...	application	Auto Size Columns	Ctrl+Plus	Apr-23 4:35:00 ...	06-Apr-23 4:23:53 ...	01-Jan-01 5:30:00 A...	AmazonS3		
□ 1.3	https://assets.tryhackme.com/js/util/notifications.js?v=1.3	text/css	Properties	Alt+Enter	Apr-23 6:58:46 ...	23-Mar-23 12:28:43...	01-Jan-01 5:30:00 A...	cloudflare		
▀ 1.3.0.css	https://remote-eu-05.tryhackme.tech/app.css?v=1.3.0	text/css	Refresh	F5	Apr-23 6:34:57 ...	23-Mar-23 12:17:59...	01-Jan-01 5:30:00 A...	cloudflare		
▀ 1.3.css	https://api.geeksforgeeks.org/css/loginModal.css?v=1.3	text/css			2:294	08-Apr-23 12:55:05...	08-Apr-23 12:53:56...	05-May-20 9:51:17 ...	01-Jan-01 5:30:00 A...	Apache
□ 1.4.0	https://remote-eu-05.tryhackme.tech/app.js?v=1.4.0	application/javascript			182,311	06-Apr-23 8:35:44 ...	06-Apr-23 8:34:57 ...	23-Mar-23 12:17:59...	01-Jan-01 5:30:00 A...	cloudflare
▀ 1.4.7	https://resources.infosecinstitute.com/wp-content/plugins/stop...	application/javascript			183	08-Apr-23 2:33:31 ...	06-Apr-23 10:25:45...	23-Mar-23 5:55:50 ...	01-Jan-38 5:25:55 A...	cloudflare

Commands –

"/stext <Filename>" -

To save the list of all cache files and with their details into a regular text file.

```
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /stext 1.3

C:\Users\HP\Downloads\chromecacheview>
```

ersonal 1 08-Apr-23 3:09 PM 3 File 12,362 KB

*C:\Users\HP\Downloads\chromecacheview\1.3 - Notepad++

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

new 1 1.3

```
1 S=====
2 Filename      : w3840-h2160-p-k-no-nd-mv.jpeg
3 URL          : https://lh4.googleusercontent.com/proxy/UOhQwfclsAK8TnXZgoTk9szHvYOJ3auDH07hz
4 Content Type   : image/jpeg
5 File Size     : 1,095,750
6 Last Accessed  : 08-Apr-23 2:20:44 PM
7 Server Time    : 07-Apr-23 7:57:45 PM
8 Server Last Modified: 01-Jan-01 5:30:00 AM
9 Expire Time    : 08-Apr-23 7:57:45 PM
10 Server Name   : fife
11 Server Response : HTTP/1.1 200
12 Web Site      : chrome://new-tab-page
13 Frame          : chrome-untrusted://new-tab-page
14 Content Encoding :
15 Cache Name     : f_00591b
16 Cache Control   : public, max-age=86400, no-transform
17 ETag           :
18 Server IP Address : 142.250.76.161
19 URL Length    : 167
20 Deleted File   : No
21 =====
22
23 =====
24 Filename      : hl=en-US&async=fixed_0.json
25 URL          : https://www.google.com/async/newtab_oqb?hl=en-US&async=fixed:0
26 Content Type   : application/json
27 File Size     : 38,153
28 Last Accessed  : 08-Apr-23 2:20:44 PM
29 Server Time    : 08-Apr-23 2:20:44 PM
30 Server Last Modified: 01-Jan-01 5:30:00 AM
31 Expire Time    : 08-Apr-23 2:20:44 PM
```

Normal text file length : 6,329,253 lines : 142,715 Ln:20 Col:23 Pos:897 Windows (CR LF) UTF-16 LE BOM INS ...

/stab <Filename> -

To save the list of all cache files into a tab-delimited text file (details shown line-by-line).

```
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /stab 1.1
C:\Users\HP\Downloads\chromecacheview>
```

```

C:\Users\HP\Downloads\chromecacheview\1.1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window 2
new new cd .. E 11:14
1 Filenames Last Accessed Server Time Server Last Modified Expire Time Server Name Web Site Frame Content Enc.
2 13840... URL Content Type File Size Last Accessed Server Time Server Last Modified Expire Time Server Name Web Site Frame Content Enc.
3 h1-en-US&sync=fixed_0.json https://www.googleapis.com/async/newtab_onb3hleen-US&sync=fixed_0 application/json 38,153 08-Apr-23 2:20:44 PM 08-Apr-23 2:20:44 PM
4 newtab_promos.json https://www.googleapis.com/async/newtab_promos application/json 33 08-Apr-23 2:20:44 PM 08-Apr-23 2:20:44 PM 01-Jan-01 5:30:00 AM 08-Apr-
5 googleLogo_clr_74x24px.svg https://www.gstatic.com/images/branding/nogoleLogo/svga/nogoleLogo_clr_74x24px.svga image/svg+xml 663 08-Apr-23 2:20:45 PM 11-Mar-23
6 AA2Yrt5tMDc5S5hgu5PEfbepqNWEgiqoq https://www.gstatic.com/col/_/is/kcq_en_EM.x3ks5QOuEM.2019.0/rti/m=q_dnn.cmd.ccwid.anpid.gald/exm=qaw_gahr_gadd_oaid_galo_oa
7 tbn_ANd9cRjdja9Tfdau_9tHmXxEK2r_019hYmlW-zx9XlyVsnvAAas.js https://encrypted-tbn.gstatic.com/images?q=tbn:ANd9cRjdja9Tfdau_9tHmXxEK2r_019hYmlW-zx9XlyVsnvAAas
8 generate_204 https://i.ytimg.com/generate_204 0 08-Apr-23 2:36:48 PM 08-Apr-23 2:36:49 PM 01-Jan-01 5:30:00 AM 01-Jan-01 5:30:00 AM HTTP/1
9 tbn_ANd9cRjdja9Tfdau_72r78gc1hoau_HMkbj.css https://www.gstatic.com/qod/_/ss/kcq_en_EM.iN0124009Cg_L.W.o/mem_md_ccwid/exm=qaw_gahr_gadd_oaid_galo_gein_qhba_qhbk_j
10 familyRoboto_wght@300:400:500:700?family=Sans wght@30..css https://fonts.googleapis.com/css2?family=Roboto:wght@300;400;500;700&family=YouTube+Sans:wght@300..
11 generate_204 https://rx2---sn-q5pauxapc-c5be.googlevideo.com/generate_204 0 08-Apr-23 2:19:58 PM 01-Jan-01 5:30:00 AM 01-Jan-01 5:30:00 AM 01-Jan-
12 com2 https://rx2---sn-q5pauxapc-c5be.googlevideo.com/generate_204?com2 0 08-Apr-23 2:19:58 PM 01-Jan-01 5:30:00 AM 01-Jan-01 5:30:00 AM 01-Jan-01 !
13 KF0McngEu92Fr1m4mnxF.woff2 https://fonts.gstatic.com/s/roboto/v30/KF0McngEu92Fr1m4mnxF.woff2 font/woff2 15,748 08-Apr-23 2:36:50 PM 16-Mar-23 6:51:08 AM 12-
14 emojis-svg-9.json https://www.gstatic.com/youtube/img/emojis/emojis-svga-9.json application/json 47,551 08-Apr-23 2:36:51 PM 15-Mar-23 11:44:18 AM 21-Mar-
15 failure.mp3 https://www.youtube.com/s/search/audio/failure.mp3 audio/mpeg 0 08-Apr-23 2:36:51 PM 08-Apr-23 2:36:50 PM 08-Apr-23 2:38:00 AM 08-Apr-23 2:36
16 no_input.mp3 https://www.youtube.com/s/search/audio/no_input.mp3 audio/mpeg 0 08-Apr-23 2:36:51 PM 08-Apr-23 2:36:51 PM 13-Jan-22 2:38:00 AM 08-Apr-23 :
17 open.mpg https://www.youtube.com/s/search/audio/open.mpg audio/mpeg 0 08-Apr-23 2:36:51 PM 08-Apr-23 2:36:51 PM 13-Jan-22 2:38:00 AM 08-Apr-23 2:36:50
18 no_output.mpg https://www.youtube.com/s/search/audio/no_output.mpg audio/mpeg 0 08-Apr-23 2:36:51 PM 08-Apr-23 2:36:51 PM 01-Jan-01 5:30:00 AM 01-Jan-
19 open.mp3 2f5595acc07a95_0 https://www.youtube.com/s/search/audio/open.mp3?2f5595acc07a95_0 6,167 08-Apr-23 2:36:51 PM 01-Jan-01 5:30:00 AM 01-Jan-01 !
20 failure.mp3 2f5595acc07fb2_0 https://www.youtube.com/s/search/audio/failure.mp3?2f5595acc07fb2_0 6,529 08-Apr-23 2:36:51 PM 01-Jan-01 5:30:00 AM 01-Jan-01 !
21 cast_sender.js https://www.gstatic.com/cv/s/sender/v1/cast_sender.js text/javascript 2,007 08-Apr-23 2:36:51 PM 08-Apr-23 2:19:51 PM 17-Feb-21 5:27:06 AM
22 link.png https://www.gstatic.com/youtube/img/annotations/link.png image/png 423 07-Apr-23 3:27:03 PM 22-Mar-23 4:53:50 PM 03-Oct-19 3:45:00 PM 21-Mar-
23 KFOlcnqEu92Fr1mEu9FB8c4.woff2 https://fonts.gstatic.com/s/roboto/v30/KFOlcnqEu92Fr1mEu9FB8c4.woff2 font/woff2 15,920 08-Apr-23 2:36:52 PM 14-Mar-23 6:05:22 J
24 favicon_144x144.png https://www.gstatic.com/youtube/img/branding/favicon_144x144.png image/png 729 08-Apr-23 2:36:52 PM 09-Mar-23 11:55:07 PM 03-Oct-
25 gm_video_youtube_white_48dp.png https://fonts.gstatic.com/s/googlematerial/icon/video_youtube/v1/white_48dp/1x/gm_video_youtube_white_48dp.png image/png 324 08-
26 favicon_192x192.png https://www.gstatic.com/youtube/img/branding/favicon_192x192.png image/png 938 08-Apr-23 2:19:52 PM 15-Mar-23 3:49:04 PM 03-Oct-
27 logo_16x16.png https://www.gstatic.com/youtube/img/web/monochrome/logo_16x16.png image/png 172 08-Apr-23 2:19:52 PM 09-Mar-23 10:18:05 PM 18-Jun-21 9:48:00 I
28 logo_32x32.png https://www.gstatic.com/youtube/img/web/monochrome/logo_32x32.png image/png 264 08-Apr-23 2:19:52 PM 15-Mar-23 6:41:50 PM 18-Jun-21 9:48:00 I
29 logo_512x512.png https://www.gstatic.com/youtube/img/web/monochrome/logo_512x512.png image/png 2,646 08-Apr-23 2:19:52 PM 15-Mar-23 2:32:42 PM 18-Jun-21
30 explore_512x512.png https://www.gstatic.com/youtube/img/web/shortcuts/explore_512x512.png image/png 4,094 08-Apr-23 2:19:52 PM 09-Mar-23 11:59:00 PM 03-Jun-
31 subscriptions_512x512.png https://www.gstatic.com/youtube/img/web/shortcuts/subscriptions_512x512.png image/png 974 08-Apr-23 2:19:52 PM 10-Mar-23 2:10:02 AM
32 cl=zcc2-64029524cd=ac4=ac5=ac6=ac7=ac8=ac9=t=1680946185640sns_c=TFP-8 https://sb.scorecardresearch.com/b/cl=zcc2-64029524cd=ac4=ac6=ac7=ac8=ac9=t=1680946185640sns_c=TFP-8
33 QwJ02QNBG9B9Dy94j6_PCTRSw0rLJMO_7f https://www.firebaseio.com/.json?sv=cache&v=1/t/01BZQNG9B9Dy94j6_PCTRSw0rLJMO_7f
34 logo_192x192.png https://www.gstatic.com/youtube/img/web/monochrome/logo_192x192.png image/png 3,059 08-Apr-23 2:19:52 PM 09-Mar-23 10:18:05 PM 18-Jun-21 9:48:00 I
35 sw.js https://www.youtube.com/v_is_text/javascript 2,426 08-Apr-23 3:07:47 PM 09-Apr-23 5:30:00 AM 01-Jan-01 5:30:00 AM 08-Apr-23 5:12:58 PM 08-Apr-23 5:
36 animated_like_icon_v2_light.json https://www.gstatic.com/youtube/img/lottie/animated_like_icon_v2_light.json application/json 3,523 08-Apr-
37 lottie_light.js https://www.gstatic.com/external_hosted/lottie/lottie_light.js text/javascript 35,947 08-Apr-23 2:36:53 PM 08-Apr-23 2:36:52 PM 19-Apr-21 8:38
38 win_connect.png https://assets.tryhackme.com/img/connect/win_connect.png image/png 90,370 07-Apr-23 2:57:42 PM 07-Apr-23 12:05:24 AM 02-Mar-23 10:27:34 PM
39 mac_installer.png https://assets.tryhackme.com/img/connect/mac_installer.png image/png 38,861 07-Apr-23 2:57:43 PM 06-Apr-23 3:29:28 PM 04-Apr-23 11:30:11
40 mac_import.png https://assets.tryhackme.com/img/connect/mac_import.png image/png 45,517 07-Apr-23 2:57:43 PM 06-Apr-23 8:02:31 PM 04-Apr-23 11:30:11 PM 01-
41 scomma-n-aumwPm7nDfDrnRm1KmOmaARR-AH-CVaOmkAmuTARAk2mzSh1Ma inet https://vtimer.com/vi/0TMzH71nn8/handle/default inr?com=scomma-n-aumwPm7nDfDrnRm1KmOmaARR-AH-CVaOmkAmuTARAk2mzSh1Ma
```

/scomma <Filename> -

To save the list of all cache files into a comma-delimited text file.

/stabular <Filename> -

To save the list of all cache files into a tabular text file.

/shtml <Filename> -

To save the list of all cache files into HTML file (Horizontal).

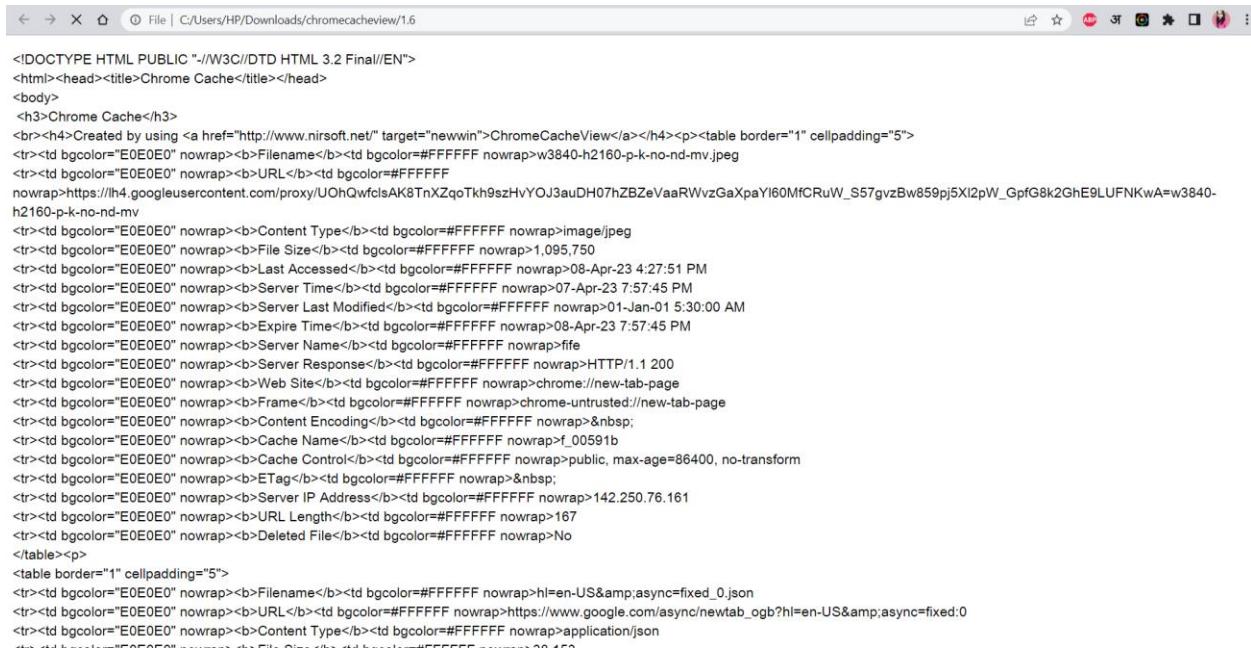
/sverhtml <Filename> -

To save the list of all cache files into HTML file (Vertical).

/sxml <Filename> -

To save the list of all cache files to XML file.

```
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /stab 1.1
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /stabular 1.4
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /shtml 1.5
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /sverhtml 1.6
```



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html><head><title>Chrome Cache</title></head>
<body>
<h3>Chrome Cache</h3>
<br><h4>Created by using <a href="http://www.nirsoft.net/" target="newwin">ChromeCacheView</a></h4><p><table border="1" cellpadding="5">
<tr><td bcolor="#E0E0E0" nowrap><b>Content Type</b></td bcolor="#FFFFFF" nowrap>image/jpeg
<tr><td bcolor="#E0E0E0" nowrap><b>File Size</b></td bcolor="#FFFFFF" nowrap>1,095,750
<tr><td bcolor="#E0E0E0" nowrap><b>Last Accessed</b></td bcolor="#FFFFFF" nowrap>08-Apr-23 4:27:51 PM
<tr><td bcolor="#E0E0E0" nowrap><b>Server Time</b></td bcolor="#FFFFFF" nowrap>07-Apr-23 7:57:45 PM
<tr><td bcolor="#E0E0E0" nowrap><b>Server Last Modified</b></td bcolor="#FFFFFF" nowrap>01-Jan-01 5:30:00 AM
<tr><td bcolor="#E0E0E0" nowrap><b>Expire Time</b></td bcolor="#FFFFFF" nowrap>08-Apr-23 7:57:45 PM
<tr><td bcolor="#E0E0E0" nowrap><b>Server Name</b></td bcolor="#FFFFFF" nowrap>fife
<tr><td bcolor="#E0E0E0" nowrap><b>Server Response</b></td bcolor="#FFFFFF" nowrap>HTTP/1.1 200
<tr><td bcolor="#E0E0E0" nowrap><b>Web Site</b></td bcolor="#FFFFFF" nowrap>chrome://new-tab-page
<tr><td bcolor="#E0E0E0" nowrap><b>Frame</b></td bcolor="#FFFFFF" nowrap>chrome-untrusted://new-tab-page
<tr><td bcolor="#E0E0E0" nowrap><b>Content Encoding</b></td bcolor="#FFFFFF" nowrap>&nbsp;
<tr><td bcolor="#E0E0E0" nowrap><b>Cache Name</b></td bcolor="#FFFFFF" nowrap>f_00591b
<tr><td bcolor="#E0E0E0" nowrap><b>Cache Control</b></td bcolor="#FFFFFF" nowrap>public, max-age=86400, no-transform
<tr><td bcolor="#E0E0E0" nowrap><b>ETag</b></td bcolor="#FFFFFF" nowrap>&nbsp;
<tr><td bcolor="#E0E0E0" nowrap><b>Server IP Address</b></td bcolor="#FFFFFF" nowrap>142.250.76.161
<tr><td bcolor="#E0E0E0" nowrap><b>URL Length</b></td bcolor="#FFFFFF" nowrap>167
<tr><td bcolor="#E0E0E0" nowrap><b>Deleted File</b></td bcolor="#FFFFFF" nowrap>No
</table><p>
<table border="1" cellpadding="5">
<tr><td bcolor="#E0E0E0" nowrap><b>Filename</b></td bcolor="#FFFFFF" nowrap>hi=en-US&amp;async=fixed_0.json
<tr><td bcolor="#E0E0E0" nowrap><b>URL</b></td bcolor="#FFFFFF" nowrap>https://www.google.com/async/newtab_ogb?hi=en-US&amp;async=fixed:0
<tr><td bcolor="#E0E0E0" nowrap><b>Content Type</b></td bcolor="#FFFFFF" nowrap>application/json
<tr><td bcolor="#E0E0E0" nowrap><b>Content Encoding</b></td bcolor="#FFFFFF" nowrap>&nbsp;
```

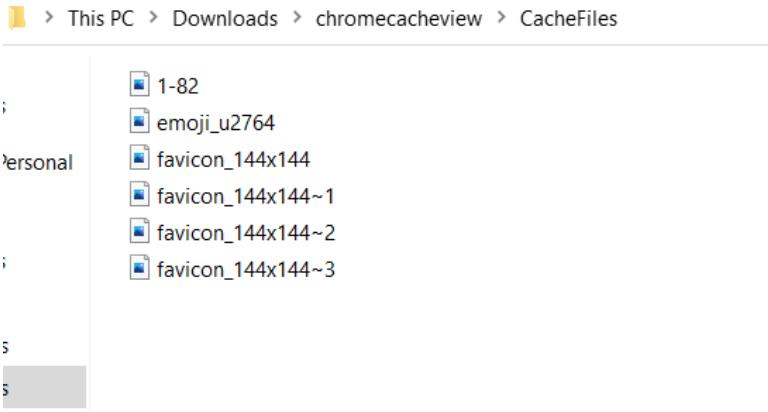
/copycache <URL> <Content Type> -

Copy files from the cache.

In the <URL> parameter, you can specify the URL of the Web site (for example: <http://www.nirsoft.net>) or empty string ("") if you want to copy files from all Web sites.

In the <Content Type> parameter, you can specify full content type (like image/png), partial content type (like 'image') or empty string ("") if you want to copy all types of files.

```
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /copycache https://www.youtube.com png
```



Here I specified the URL of YouTube and the file type is image, the command copied all the images associated with the URL.

2. Dumpzilla

Dumpzilla is a browser forensic command line tool it works on Windows, Mac and Linux. It comes pre-installed in our Kali Linux machine. We can get browser's passwords, history, bookmarks, cookies, extensions, sessions, permissions, downloads etc.

Dumpzilla is written in Python3 and it can extract all forensic interesting information of browser like firefox.

Features and uses-

Dumpzilla can collect information of following:

- Cookies + DOM storage (HTML5)
- Downloads
- Web forms
- History
- Offline Cache
- Thumbnail Extraction
- Addons / Extensions and used path or URLs.
- Browser saved passwords
- SSL certificates added as a exception
- Session data
- Visualize live user surfing, URL used in each tab

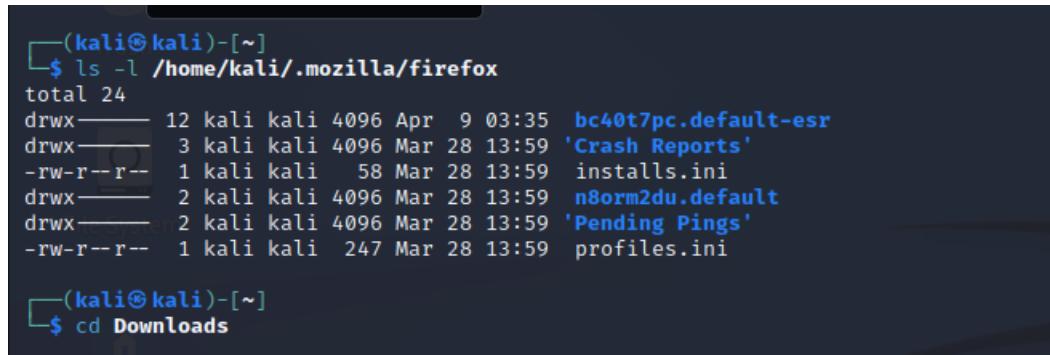
In Firefox, browser's saved data in profiles, to extract the data for forensic we use dumpzilla. Here we need to know the path of default profile. Different operating system have different path, here we are using kali-

Linux or UNIX profile path

/home/\$USER/.mozilla/firefox/xxxx.default

Download the tool from the official website or from github page.

Firstly we will check the profile-



```
(kali㉿kali)-[~]
└─$ ls -l /home/kali/.mozilla/firefox
total 24
drwx----- 12 kali kali 4096 Apr  9  03:35 bc40t7pc.default-esr
drwx-----  3 kali kali 4096 Mar 28 13:59 'Crash Reports'
-rw-r--r--  1 kali kali   58 Mar 28 13:59 installs.ini
drwx-----  2 kali kali 4096 Mar 28 13:59 n8orm2du.default
drwx-----  2 kali kali 4096 Mar 28 13:59 'Pending Pings'
-rw-r--r--  1 kali kali  247 Mar 28 13:59 profiles.ini

(kali㉿kali)-[~]
└─$ cd Downloads
```

Now we will run the commands to get information from the browser,

Here we are checking all the downloads-

```
(kali㉿kali)-[~]
└─$ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Downloads

=====
= Directories
=====

⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/content-prefs.sqlite
⇒ SHA256 hash: 9f82ad8620da1e921fd7a9e742806e0d343fae2b14a968482b06e9add83af72f

No data found!

=====
= Downloads history
=====

⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/places.sqlite
⇒ SHA256 hash: d879abed3caee53327ed3eebcae85bea24f14656e989df82cc669fa87c499cbc

Date: 2023-03-28 14:23:47
URL: https://download.winzip.com/gl/oemg/winzip26-mf.exe
Name: file:///home/kali/Downloads/winzip26-mf(1).exe

Date: 2023-03-28 14:25:08
URL: https://download.winzip.com/gl/nkln/winzip27-downwz.exe
Name: file:///home/kali/Downloads/winzip27-downwz.exe

Date: 2023-03-28 14:27:22
URL: https://www.7-zip.org/a/7z2201-x64.exe
Name: file:///home/kali/Downloads/7z2201-x64.exe

Date: 2023-03-29 01:19:53
URL: https://www.win-rar.com/fileadmin/winrar-versions/rarlinux-x64-621.tar.gz
Name: file:///home/kali/Downloads/rarlinux-x64-621.tar.gz

Date: 2023-03-29 01:27:12
URL: http://files.sempersecurus.org/dumps/cridex_memdump.zip
Name: file:///home/kali/Downloads/cridex_memdump.zip

Date: 2023-03-29 01:33:02
URL: https://downloads.volatilityfoundation.org/volatility3/symbols/linux.zip
Name: file:///home/kali/Downloads/linux.zip

Date: 2023-03-29 07:29:41
URL: https://codeload.github.com/ytisf/theZoo/zip/refs/heads/master
Name: file:///home/kali/Downloads/theZoo-master.zip

Date: 2023-03-29 08:02:13
URL: https://www.winitor.com/tools/pestudio/current/pestudio.zip
Name: file:///home/kali/Downloads/pestudio.zip

Date: 2023-03-29 08:03:24
```

If we want we can save the information in a text file-

```

URL: https://www.7-zip.org/a/z2201-x64.exe
Name: file:///home/kali/Downloads/z2201-x64.exe

Date: 2023-03-29 01:19:53
URL: https://www.wln-rar.com/fileadmin/winrar-versions/rarlinux-x64-621.tar.gz
Name: file:///home/kali/Downloads/rarlinux-x64-621.tar.gz

Date: 2023-03-29 01:27:29
URL: http://files.sempersecurus.org/dumps/crindex_memdump.zip
Name: file:///home/kali/Downloads/crindex_memdump.zip

Date: 2023-03-29 01:33:02
URL: https://downloads.volatilityfoundation.org/volatility3/symbols/linux.zip
Name: file:///home/kali/Downloads/linux.zip

Date: 2023-03-29 07:29:41
URL: https://codeload.github.com/tysis/theZoo/zip/refs/heads/master
Name: file:///home/kali/Downloads/theZoo-master.zip

Date: 2023-03-29 08:02:13
URL: https://www.wimitor.com/tools/pestudio/current/pestudio.zip
Name: file:///home/kali/Downloads/pestudio.zip

Date: 2023-03-29 08:03:24
URL: https://www.wimds5.com/download/winmd5free.zip
Name: file:///home/kali/Downloads/winmd5free.zip

Date: 2023-03-29 08:04:02
URL: https://www.dependencywalker.com/depends22_x86.zip
Name: file:///home/kali/Downloads/depends22_x86.zip

Date: 2023-03-29 08:05:26
URL: https://softpedia-secure-download.com/dl/b65e167b864675b261847bf5bebcb011/64242978/100004102/software/programming/PEid-0.95-20081103.zip
Name: file:///home/kali/Downloads/PEid-0.95-20081103.zip

Date: 2023-03-29 08:27:12
URL: https://www.sempersecurus.org/downloads/crindex_mandump.zip
== Total Information
Total Directories inloads: : 0 lityfoundation.org/volatility3/symbols/linux.zip
Total Downloads history: : 11 loads/Linux.zip
2023-03-29 07:29:41
└─(kali㉿kali)-[~]
  $ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Downloads >> output.txt
 2023-03-29 08:02:13
└─(kali㉿kali)-[~]
  $ ┌── https://www.wimitor.com/tools/pestudio/current/pestudio.zip

```

To get the passwords-

```

└─(kali㉿kali)-[~]
  $ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Passwords
  [dump] Error decoding passwords: libnss not found (libnss3.so)
  == Decode Passwords
  => Source File: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/logins.json
  => SHA256 hash: 645534fe025ac272418eb2b28837cb4b3cd5e552af8bd3b78b9fd1d1bab3

  Web: chrome://FirefoxAccounts
  Username: https://accounts.firefox.com/accountSettings
  Password: https://accounts.firefox.com/accountSettings

  == Decode Passwords
  => Source File: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/logins.json
  => SHA256 hash: 645534fe025ac272418eb2b28837cb4b3cd5e552af8bd3b78b9fd1d1bab3

  Web: chrome://FirefoxAccounts
  User Field:
  Password Field:
  User Login (encrypted): MfIEEPgAAAAAAAAAAAAAAwFAyIKoZihvCNAwcEHeHttstdudwBcgW5zhRxGEt06/V6vaVst0bbukBttZ9Q24pmvdI168plcsjQploM9
  Passphrase (encrypted): E53C90D6538E441A2494A905E981645E05940488972Eggm
  Passphrase (salt): 0X07e0C969394d83a97b4f7b1y1ynduzlPeku+V0AeW0m0Jy1lPl9qL0z1xyaahobvcCmJ1fWNelh1h672fwm+1W/+Ma041hCpoxM7uPsAqrq95dxLAMPI66-hNg1720hd+1C9/NShelFm1F41FVW7fJm8701GfJng3avIVBENd1prqJ0j5i7Y51EtMkgF9
  SHA256 hash: 645534fe025ac272418eb2b28837cb4b3cd5e552af8bd3b78b9fd1d1bab3

  AlwIBB0SpVqJOFzLybqy6u0/bb072loop/wj065Vp/P0NQtssxEWwyB32JNFBN3kdsgvxDQd2amF3xxOC1kuoEaxgysPUt#BzCzRvpks1MHHSBpOsRt083EY+L+f1qL6kmkdpaAbwsuqTzzruuMMP9f91xbtZATJMQEgmtUhgbxu29aknjheko/Vkf1SaUfEBpe-U3sq4ow7tq14/l9Ryc
  cOvdkdQmQc3S00u3rxDfuF0cKb0fRkla
  Created: 2023-04-09 03:26:28
  Last used: 2023-04-09 03:26:28
  Change: 2023-04-09 03:27:03
  Frequency: 1

  == Total Information
  Total Decode Passwords : 1
  Total Passwords : 1

└─(kali㉿kali)-[~]

```

We can get information about all the cookies stored,

```
(kali㉿kali)-[~]
$ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Cookies

== Cookies

⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/cookies.sqlite
⇒ SHA256 hash: 11a71e75a6ba35f905ae646bfdd0de97f355d7e8dad1b43c5c0ea5641f19b16

Host: github.com
Name: octo
Value: GH1.1.481563044.1680026420
Path: /
Expires: 2024-03-28 14:00:20
Last Access: 2023-03-29 08:02:03
Creation Time: 2023-03-28 14:00:19
Secure: Yes
HttpOnly: No
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: github.com
Name: _logged_in
Value: no
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
Expires: 2024-03-29 14:00:20
Last Access: 2023-03-29 08:02:03
Creation Time: 2023-03-28 14:00:19
Secure: Yes
HttpOnly: Yes
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: www.google.com
Name: OTZ
Value: 6962047_72_76_104100_72_446760
Path: /
Expires: 2023-04-27 14:07:16
Last Access: 2023-04-09 03:32:29
Creation Time: 2023-03-28 14:07:16
Secure: Yes
HttpOnly: No
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: digitalskills.com
Name: _ga
Value: GA1.2.2128369636.1680026849
Path: /
Expires: 2025-03-27 14:07:28
Last Access: 2023-03-28 14:07:28
Creation Time: 2023-03-28 14:07:28
Secure: No
HttpOnly: No
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: .digitalskills.com
Name: _gid
Value: GA1.2.263920127.1680026849
Path: /
Expires: 2023-03-29 01:27:12
Last Access: 2023-03-28 14:07:28
Creation Time: 2023-03-28 14:07:28
Secure: No
HttpOnly: No
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: www.sempersecurus.org/dumps/cridex_memdump.zip
Name: _crd
Value: d879abed3caeef53327ed3eebcae85bea24f14656e989df82cc669fa87ca99cb
Path: /
Expires: 2023-03-28 14:25:08
Last Access: 2023-03-28 14:25:08
Creation Time: 2023-03-28 14:25:08
Secure: No
HttpOnly: No
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb

Host: https://download.winzip.com/g1/nkln/winzip27-downwz.exe
Name: Wikipedia (en)
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://download.winzip.com/g1/nkln/winzip27-downwz.exe

Host: https://www.7-zip.org/a/7z2201-x64.exe
Name: Bing
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.7-zip.org/a/7z2201-x64.exe

Host: https://www.duckduckgo.com/fileadmin/winrar-versions/rarlinux-x64-621.tar.gz
Name: DuckDuckGo
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.duckduckgo.com/fileadmin/winrar-versions/rarlinux-x64-621.tar.gz

Host: https://www.amazon.com/.sempresecurus.org/dumps/cridex_memdump.zip
Name: Amazon.com
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.amazon.com/.sempresecurus.org/dumps/cridex_memdump.zip

Total Date: 2023-03-29 01:29:41
Total Search Engines : 5
```

Search engines-

```
(kali㉿kali)-[~]
$ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Search

== Search Engines d879abed3caeef53327ed3eebcae85bea24f14656e989df82cc669fa87ca99cb

⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/search.json.mozlz4
⇒ SHA256 hash: 3a99c56a249f169ad327d0347194c8ed5206e99d2a6fd7646e40b2bbba40e4d6

Name: Google
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.google.com/search?rlz=1C1GCEU_enUS911US911&q=winzip+27+downwz+exe

Name: Wikipedia (en)
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://en.wikipedia.org/wiki/WinZip

Name: Bing
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.bing.com/search?q=winzip+27+downwz+exe

Name: DuckDuckGo
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://duckduckgo.com/?q=winzip+27+downwz+exe

Name: Amazon.com
Description:
Path: /_matrix/client/rust/src/lib.rs?ts=1679882122&file=b6a25f1656e890f82cc669fa07ca99cb
URL: https://www.amazon.com/.sempresecurus.org/dumps/cridex_memdump.zip

Total Date: 2023-03-29 01:29:41
Total Search Engines : 5
```

All the pages that has been bookmarked-

```
(kali㉿kali)-[~] ~ % dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr -- Bookmarks
=====
= Bookmarks
=====
⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/places.sqlite
⇒ SHA256 hash: d879abed3cae53327ed3eebcae85bea24f14656e989df82cc669fa87c499cbc
=====
Title: Data found
URL: file:///usr/share/kali-defaults/web/homepage.html
Creation Time: 2023-03-28 13:59:24
Last Modified: 2023-03-28 13:59:33
=====
Title: menu
URL: https://www.kali.org/1/mozilla/firefox/bc40t7pc.default-esr/places.sqlite
Creation Time: 2023-03-28 13:59:24
Last Modified: 2023-03-28 13:59:24
=====
Title: toolbar
URL: https://www.kali.org/tools/Downloads/winzip26-mf(1).exe
Creation Time: 2023-03-28 13:59:24
Last Modified: 2023-03-28 13:59:33
=====
Title: tags
URL: https://download.winzip.com/gl/nkln/winzip27-downwz.exe
Creation Time: 2023-03-28 13:59:24
Last Modified: 2023-03-28 13:59:24
=====
Title: unfiled
URL: https://forums.kali.org/Downloads/7zz201-x64.exe
Creation Time: 2023-03-28 13:59:24
Last Modified: 2023-03-28 13:59:24
=====
Title: rar
URL: https://www.rar.com/raradmin/winrar-versions/rarlinux-x64-621.tar.gz
Creation Time: 2023-03-28 13:59:31
Last Modified: 2023-03-28 13:59:31
=====
Title: mobile
URL: https://home/kali/Downloads/rarlinux-x64-621.tar.gz
Creation Time: 2023-03-28 13:59:31
Last Modified: 2023-03-28 13:59:31
=====
Title: Kali Linux
URL: https://www.exploit-db.com/
Creation Time: 2023-03-28 13:59:32
Last Modified: 2023-03-28 13:59:32
=====
Title: Kali Tools
URL: https://www.exploit-db.com/google-hacking-database
Creation Time: 2023-03-28 13:59:33
Last Modified: 2023-03-28 13:59:33
=====
Title: Kali Docs
URL: https://www.offensive-security.com/
=====
Title: PEStudio
URL: https://www.willt01.com/tools/pestudio/current/pestudio.zip
```

3. Hindsight-

Hindsight is an internet history forensics for Google Chrome browser.

Hindsight is a free tool for analyzing web artifacts.

Uses –

Hindsight is an open-source tool that has been used to analyze or investigate web artifacts and used to correlate the root cause or origination of intrusion.

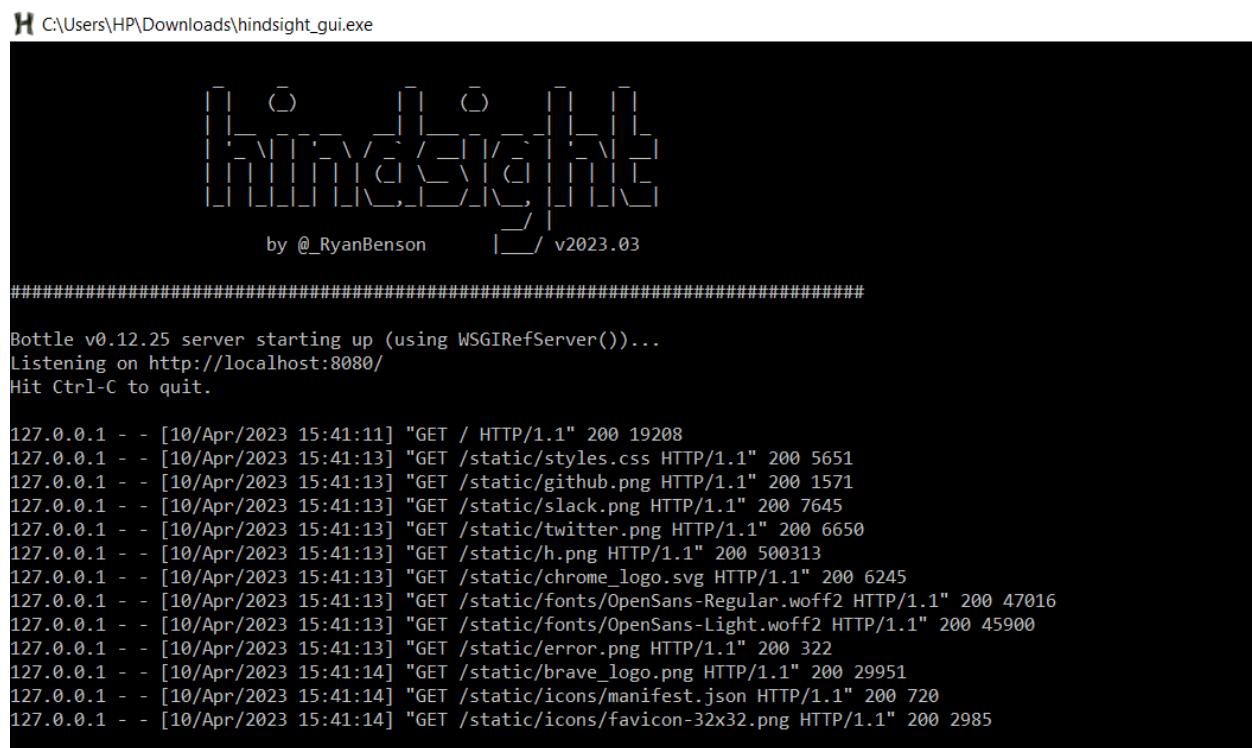
Features-

- It starts with the browsing history of the Google Chrome web browser and has expanded to support other chrome-based applications.
- Hindsight can parse a number of different types of web artifacts, including URLs, download history, cache records, bookmarks, auto fill records, saved passwords, preferences, browser extensions, HTTP cookies, and Local Storage records (HTML5 cookies).
- Once the data is extracted from each file, it is correlated with data from other history files and placed in a timeline.

The tool can be downloaded from the github page, we can download the executable files from the release page-

<https://github.com/obsidianforensics/hindsight/releases/tag/v2023.03>

Run the executable file and this interface will appear-



The screenshot shows a terminal window with the following content:

```
H C:\Users\HP\Downloads\hindsight_gui.exe
#####
#           _   _ _ _ _ 
#      _ _ | | | | | | |
#     | | | | | | | | | |
#     | | | | | | | | | |
#     | | | | | | | | | |
#     | | | | | | | | | |
#     | | | | | | | | | |
# by @_RyanBenson    |_ v2023.03
#####
Bottle v0.12.25 server starting up (using WSGIRefServer())...
Listening on http://localhost:8080/
Hit Ctrl-C to quit.

127.0.0.1 - - [10/Apr/2023 15:41:11] "GET / HTTP/1.1" 200 19208
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/styles.css HTTP/1.1" 200 5651
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/github.png HTTP/1.1" 200 1571
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/slack.png HTTP/1.1" 200 7645
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/twitter.png HTTP/1.1" 200 6650
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/h.png HTTP/1.1" 200 500313
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/chrome_logo.svg HTTP/1.1" 200 6245
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/fonts/OpenSans-Regular.woff2 HTTP/1.1" 200 47016
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/fonts/OpenSans-Light.woff2 HTTP/1.1" 200 45900
127.0.0.1 - - [10/Apr/2023 15:41:13] "GET /static/error.png HTTP/1.1" 200 322
127.0.0.1 - - [10/Apr/2023 15:41:14] "GET /static/brave_logo.png HTTP/1.1" 200 29951
127.0.0.1 - - [10/Apr/2023 15:41:14] "GET /static/icons/manifest.json HTTP/1.1" 200 720
127.0.0.1 - - [10/Apr/2023 15:41:14] "GET /static/icons/favicon-32x32.png HTTP/1.1" 200 2985
```

Now to start using the tool open the local host mentioned in the interface i.e -
<http://localhost:8080/>

Depending on the operating system provide the path in the input here,

C:\Users\HP\AppData\Local\Google\Chrome\User Data

In the plugins selector we can select the results we want according to our requirements, and click on RUN to start gathering information.

The screenshot shows the Hindsight v2023.0 web interface. At the top, there's a navigation bar with back, forward, and search icons, followed by the URL localhost:8080 and the title Hindsight v2023.0. Below the title is a large stylized 'H' logo and the word 'Hindsight'. To the right of the logo is the text 'Web Artifact Analysis'. The main content area is divided into two main sections: 'Inputs' on the left and 'Plugin Selector' on the right.

Inputs Section:

- Profile Path:** C:\Users\HP\AppData\Local\Google\Chrome\User Data
- Cache Path:** (optional - only needed if outside of the profile path)
- Description:** Chrome is a free web browser from Google that runs on Windows, macOS, Linux, ChromeOS, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system. (A small Chrome icon is shown next to the text).
- Available Decryption:** Windows ☐ Mac ☐ Linux ☐

Plugin Selector Section:

- Chrome Extension Names [v20210424] (checked)
- Generic Timestamp Decoder [v20160907] (checked)
- Google Analytics Cookie Parser [v20170130] (checked)
- Google Searches [v20160912] (checked)
- Load Balancer Cookie Decoder [v20200213] (checked)
- Quantcast Cookie Parser [v20160907] (checked)
- Query String Parser [v20170225] (checked)
- Time Discrepancy Finder [v20170129] (checked)

This screenshot shows the Hindsight v2023.0 web interface with three main sections: Inputs, Plugin Selector, and Options Selector.

Inputs Section:

- Input Type:** Chrome
- Profile Path:** C:\Users\HP\AppData\Local\Google\Chrome\User Data
- Cache Path:** (optional - only needed if outside of the profile path)
- Description:** Chrome is a free web browser from Google that runs on Windows, macOS, Linux, ChromeOS, iOS, and Android. Each user's web history and configuration information is stored under their user directory, so there may be multiple sets of browser data on the system. (A small Chrome icon is shown next to the text).
- Available Decryption:** Windows ☐ Mac ☐ Linux ☐

Plugin Selector Section: This section is identical to the one in the first screenshot, listing the same set of checked plugins.

Options Selector Section:

- Log Path:** hindsight.log
- Timezone:** Pacific [-8/-7]
- Copy files before opening?**
- Temp Path:** hindsight-temp
- Run** button

In the result summary we can see the parsed artifacts, profile paths

The screenshot shows the Hindsight v2023.03 application window. At the top left is the logo and text "Hindsight v2023.03". The main title "Results" is centered above a horizontal line. To the right of the line is the text "Hindsight - Web Artifact Analysis". Below the title, there are two main sections: "Summary" on the left and "Parsed Artifacts" on the right.

Summary

- Input Path: C:\Users\HP\AppData\Local\Google\Chrome\User Data
- Input Type: Chrome
- Profile Paths:
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Default
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Guest Profile
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Profile 1
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Snapshots\108.0.5359.126\Profile 1
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Snapshots\109.0.5414.121\Default
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Snapshots\109.0.5414.121\Profile 1
 - C:\Users\HP\AppData\Local\Google\Chrome\User Data\Snapshots\109.0.5414.121\Profile 2

Parsed Artifacts

Category	Count
Detected Chrome version:	107-111
URL records:	17308
Download records:	4253
Cache records:	0
Cookie records:	4400
Local Storage records:	5805
Autofill records:	74
Login Data records:	16
Preference Items:	1677
Session Storage records:	1159
Site Characteristics records:	0
HSTS records:	593

At the bottom right of the interface are three buttons: "Save XLSX", "Save JSONL", and "Save SQLite DB".

All the result is shown on the interface, result can be save as excel sheet,json file or sql DB file.

The screenshot shows the NetworkMiner interface with the following details:

- Session Statistics:** records: 1159, Site Characteristics records: 0, HSTS records: 593.
- User Data:** A list of user data profiles found in the User Data\Local\Google\Chrome\User Data\Snapshots directory, including profiles for versions 108.0.5359.126, 109.0.5414.121, 109.0.5414.121, 110.0.5481.180, and 110.0.5481.180.
- Plugin Results:** A table showing the number of items parsed by various plugins:

Plugin	Count
Chrome Extension Names [v20210424]	- 31 extension URLs parsed -
Generic Timestamp Decoder [v20160907]	- 0 timestamps parsed -
Google Analytics Cookie Parser [v20170130]	- 0 cookies parsed -
Google Searches [v20160912]	- 1913 searches parsed -
Load Balancer Cookie Decoder [v20200213]	- 0 cookies parsed -
Quantcast Cookie Parser [v20160907]	- 0 cookies parsed -
Query String Parser [v20170225]	- 8515 query strings parsed -
Time Discrepancy Finder [v20170129]	- 0 differences parsed -

We can also see the database in the browser and can run queries to extract desirable data from the database-

SELECT title FROM 'timeline' LIMIT 0,30							
<input type="button" value="Execute"/>							
type	timestamp	url	title	value	interpretation	profile	
bookmark	2015-07-04 07:43:0...	http://www.indianr...	Welcome to Indian ...	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2016-12-01 07:16:1...	https://www.facebook.com	www.facebook.com	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2016-12-04 05:30:1...	chrome://help/	About	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2017-06-07 01:56:1...	http://www...	...	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2017-06-17 22:15:5...	https://www.irctc...	Book Ticket - Passen...	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2017-06-17 22:23:2...	javascript:function ...	Magic Autofill	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2017-11-09 05:28:3...	https://www.tutoria...	Computer Program...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2017-11-09 05:38:0...	https://www.inform...	Informationvine.com	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2018-01-12 08:23:1...	https://www.hacker...	Welcome to Online ...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2018-01-12 08:38:5...	https://www.codec...	Learn Python Cod...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2018-04-09 08:44:1...	https://www.javatn...	Online exam projec...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2018-10-30 06:43:1...	http://175.251.22...	...	Synced > Mobile bo...	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2018-12-31 10:08:3...	https://kheloindia.s...	https://kheloindia.s...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2019-01-04 06:17:5...	http://www...	What are important...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2019-02-14 02:37:0...	https://www.hacker...	Programming Tutor...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2019-02-14 02:50:0...	https://practice.gee...	Course Sudo Plat...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	
bookmark	2019-02-14 02:50:2...	https://practice.gee...	Practice Geeksfor...	Bookmarks bar	null	C:\Users\HP\AppData\Roaming\NetworkMiner\Profiles\Default	

SELECT title FROM 'timeline' LIMIT 0,30	<input type="button" value="Execute"/>
title	
Welcome to Indian Railway Passenger reservation Enquiry	
www.facebook.com	
About	
https://www.facebook.com/Login	
Book Ticket - Passengers Information	
Magic Autocomplete	
Computer Programming	
Informationvine.com	
Welcome to Online Programming	
Learn Python Codecademy	
Online exam project in java swing without database - javatpoint	
.....	
https://kheloindia.sportz.io/Login	
What are important topics for aptitude test for campus? - Quora	
Programming Tutorials, Coding Problems and Practice Questions HackerEarth	
Course Sudo Placement 2	
Practice GeeksforGeeks A computer science portal for geeks	

timeline (28921 rows)	<input type="button" value=""/>
SELECT URL FROM 'timeline' WHERE URL = 'https://www.facebook.com/'	<input type="button" value="Execute"/>
url	
https://www.facebook.com/	

In the excel result file we can see we got a lot of information related to all the bookmarks, URL, cache accessed and created, login information, downloads, site settings, session with time stamps. Other information like preferences-all profile/account information.

A6417 site setting (modified)					
A	B	C	D	E	F
1 Hindsight Internet History Forensics (v2023.03)					
2 Type	Timestamp (US/Pacific-T URL		Title / Name / Status	Data / Value / Path	
Sort A to Z	9.386 https://www.google.com/in/pnr_Eng_err.html		welcome to hindsight	Synced > Mobile bookmarks	
Sort Z to A	4.649 https://www.facebook.com/		www.facebook.com	Synced > Mobile bookmarks	
Sort by Color	9.105 chrome://newtab/		About	Synced > Mobile bookmarks	
Clear Filter From "Type"	9.817 https://t.me/		AccSoft 2.0 : Login	Synced > Mobile bookmarks	
Filter by Color	5.913 https://yoursite.com/alternatealternatecity.jsf		Book Ticket - Passengers Inform	Synced > Mobile bookmarks	
Text Filters	1.358 javascript:((function(){if(!document.cookie){document.cookie="MagicAutofill=true";}})());		Welcome to Online Programming	Bookmarks bar	
Search	3.694 https://www.informationvine.com/muex?src=999&qo=sem:query&ad=se		Informationvine.com	Bookmarks bar	
<input checked="" type="checkbox"/> cookie (accessed)	7.563 https://www.informationvine.com/muex?src=999&qo=sem:query&ad=se		Welcome to Online Programming	Bookmarks bar	
<input checked="" type="checkbox"/> cookie (created)	2.772 https://www.informationvine.com/muex?src=999&qo=sem:query&ad=se		Learn Python Codecademy	Bookmarks bar	
<input checked="" type="checkbox"/> download	5.270 https://www.informationvine.com/muex?src=999&qo=sem:query&ad=se		Online exam project in java swi	Bookmarks bar	
<input checked="" type="checkbox"/> login (declined save)	4.547 https://www.informationvine.com/muex?src=999&qo=sem:query&ad=se		AccSoft 2.0 : Attendance Status	Synced > Mobile bookmarks	
<input checked="" type="checkbox"/> login (never save)	9.659 https://kheloindia.sportz.io/Login		https://kheloindia.sportz.io/Login	Bookmarks bar	
<input checked="" type="checkbox"/> preference (session)	0.972 https://www.naukri.com/what-are-the-best-topics-for-aptitude-test-in-india		What are important topics for	Bookmarks bar	
<input checked="" type="checkbox"/> site setting (engagement)	0.529 https://www.naukri.com/what-are-the-best-topics-for-aptitude-test-in-india		Programming Tutorials, Coding	Bookmarks bar	
<input checked="" type="checkbox"/> site setting (hits)	2.468 https://www.naukri.com/what-are-the-best-topics-for-aptitude-test-in-india		Course Sudo Placement 2	Bookmarks bar	
	0.035 https://practicalgeeksforsaamikarlaamduke!		Practice GeeksforGeeks	Bookmarks bar	
	4.216 https://www.geeksforgeeks.org/algorithm-patterns/		Amdocs Archives - GeeksforGeeks	Bookmarks bar	
	2.080 https://www.geeksforgeeks.org/algorithm-patterns/		pattern code	Bookmarks bar	
22 bookmark	2019-02-15 01:16:09.518 https://test.bihubllc.com/Andrea.Mart/compagni		amdocs free course	Bookmarks bar	
23 bookmark	2019-02-15 01:37:35.771 https://preplounge.com/online-test/combination/		prepinsta placement question	Bookmarks bar	
24 bookmark	2019-02-15 01:56:43.931 https://thomashollidaysavvy.inlining-test.it/communities-online-test/		L&T Infotech Test Pattern - WRI	Bookmarks bar	
25 bookmark	2019-02-26 09:07:27.493 https://spineuseye.com/online-test/		Online Submission of Application	Bookmarks bar	
26 bookmark	2019-03-14 08:38:11.869 https://www.indianarmy.nic.in/online-test/		ONLINE APPLICATION	Bookmarks bar	
27 bookmark	2019-03-15 00:18:31.728 https://www.indiannavy.gov.in/2019/nts/online-test/		Indian Navy Recruitment 2019	Bookmarks bar	
28 bookmark	2019-03-18 01:06:53.560 https://www.infojobs.in/online-test/		Infosys OffCampus Drive - v20 Bookmarks bar		
29 bookmark	2019-04-10 10:31:09.471 https://www.infojobs.in/online-test/				
30 bookmark	2019-05-13 12:02:09.208 https://www.infojobs.in/online-test/				

Extensions installed-

A	B	C	D	E
1 Installed Extensions				
2 Extension Name	Description	Version	App ID	Profile Folder
3 Adblock Plus - free ad blocker	Block YouTube™ ads, pop-ups & fight malware!	3.16.2	com.adblockplus.adblockplus	Default
4 GHunt Companion	Load all needed cookies to use GHunt peacefully.	2.0.0	com.johnnysteel.ghunt.companion	Default
5 Adobe Acrobat: PDF edit, convert	Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comment.	15.1.3.43	com.adobe.acrobat.pdfedit	Default
6 Google Docs Offline	Edit, create, and view your documents, spreadsheets, and presentations —	1.6.0	com.google.docs.offline	Default
7 Google Input Tools	Input Tools lets you type in the language of your choice.	10.2.0.2	com.google.inputtools	Default
8 Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	com.google.chrome.webstorepayments	Default
9 Google Docs Offline	Edit, create, and view your documents, spreadsheets, and presentations —	1.50.1	com.google.docs.offline	Profile 1
10 Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	com.google.chrome.webstorepayments	Profile 1
11				
12				
13				

4. Unfurl –

Unfurl is used to extract and visualize all possible data from URLs.

Unfurl takes a URL and expands it into a directed graph, extracting every bit of information from the URL and exposing the hidden.

Unfurl breaks up an URL into components and extracts as much information as it can from each piece, and presents it visually.

Features-

- Unfurl has parsers for URLs, search engines, chat applications, social media sites, and more.

- It also has more generic parsers (timestamps, UUIDs, etc) helpful for exploring new URLs or reverse engineering.
- Even if the URL is extracted from a memory image or carve from slack space, or pull out from a browser's history file, this tool can provide every bit of information it can.

We can get the tool from the github page-

<https://github.com/obsidianforensics/unfurl>

Either we can use it online or we can install it locally on our console

How to use Unfurl

Online Version

1. There is an online version at <https://dfir.blog/unfurl>. Visit that page, enter the URL in the form, and click 'Unfurl!'.
2. You can also access the online version using a bookmarklet - create a new bookmark and paste
`javascript:window.location.href='https://dfir.blog/unfurl?url='+window.location.href;` as the location.
Then when on any page with an interesting URL, you can click the bookmarklet and see the URL "unfurled".

Local Python Install

1. Install via pip: `pip install dfir-unfurl`

After Unfurl is installed, you can run use it via the web app or command-line:

1. Run `python unfurl_app.py`
2. Browse to `localhost:5000/` (editable via config file)
3. Enter the URL to unfurl in the form, and 'Unfurl!'

OR

1. Run `python unfurl_cli.py https://twitter.com/_RyanBenson/status/1205161015177961473`
2. Output:

```
[1] https://twitter.com/_RyanBenson/status/1205161015177961473
[1] [2] Scheme: https
[1] [3] twitter.com
[1] [4] Domain Name: twitter.com
[1] [5] TLD: com
[1] [6] /_RyanBenson/status/1205161015177961473
[1] [7] 1. _RyanBenson
```

All the modules here we can see, it can parse data from any type of source – general URL, search engines, from social media or any videos, IDs(UUID, tiktok ID), timestamps etc.



The Unfurl! logo consists of the word "unfurl" in a lowercase sans-serif font. The letter "l" is replaced by a stylized green leafy sprig. The entire logo is set against a white background with a thin gray border.

Unfurl!

Welcome to Unfurl! Here are some examples:

- General URLs
- Search Engines
- Social Media & Video Sites
- IDs
- Encodings
- Timestamps

Unfurl!

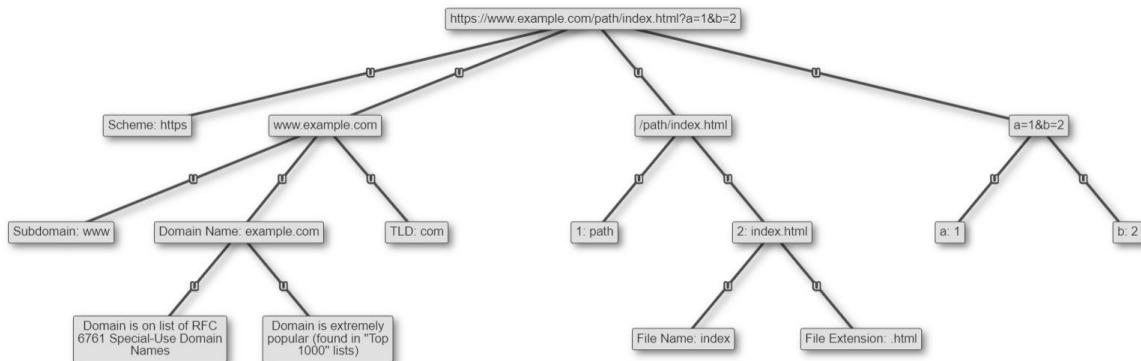
General URL- (simple link, complicated link, short link etc.)

Welcome to Unfurl! Here are some examples:

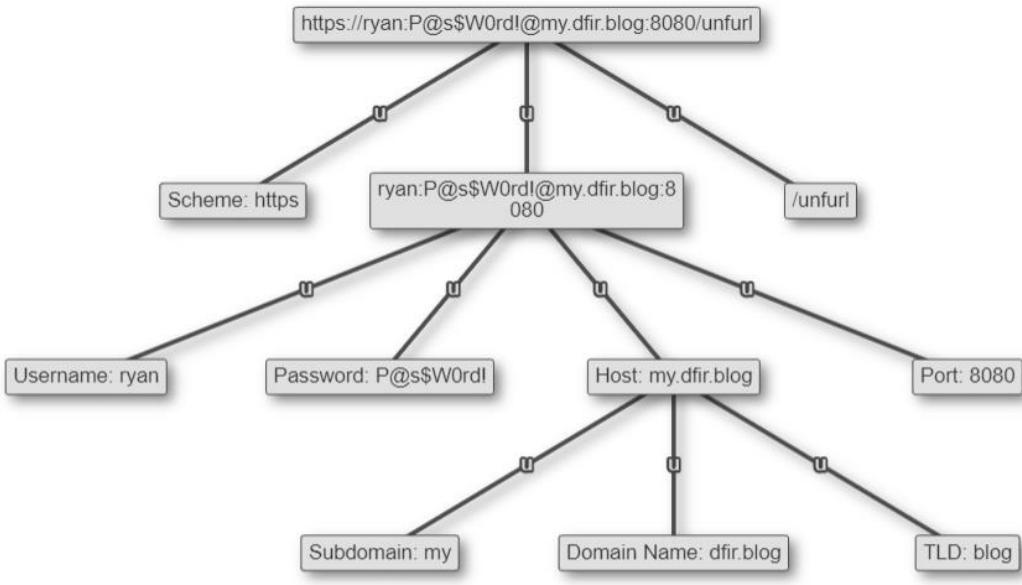
General URLs

- Simple URL ([https://www.example.com/path/index.html?
a=1&b=2](https://www.example.com/path/index.html?a=1&b=2))
- Complicated Domain
([https://ryan:P@s\\$W0rdl@my.dfir.blog:8080/unfurl](https://ryan:P@s$W0rdl@my.dfir.blog:8080/unfurl))
- Magnet Link (magnet:?xt=urn:btih:c9e15763f722f23e98a29decdfae34...)
- Mailto: Link ([mailto:to@example.com?
cc=cc@second.example&bcc=bcc...](mailto:to@example.com?cc=cc@second.example&bcc=bcc...))
- Punycode Domain (<https://www.xn--85x722f.com.cn>)
- Shortlinks (<https://t.co/QPs812NVAW>)

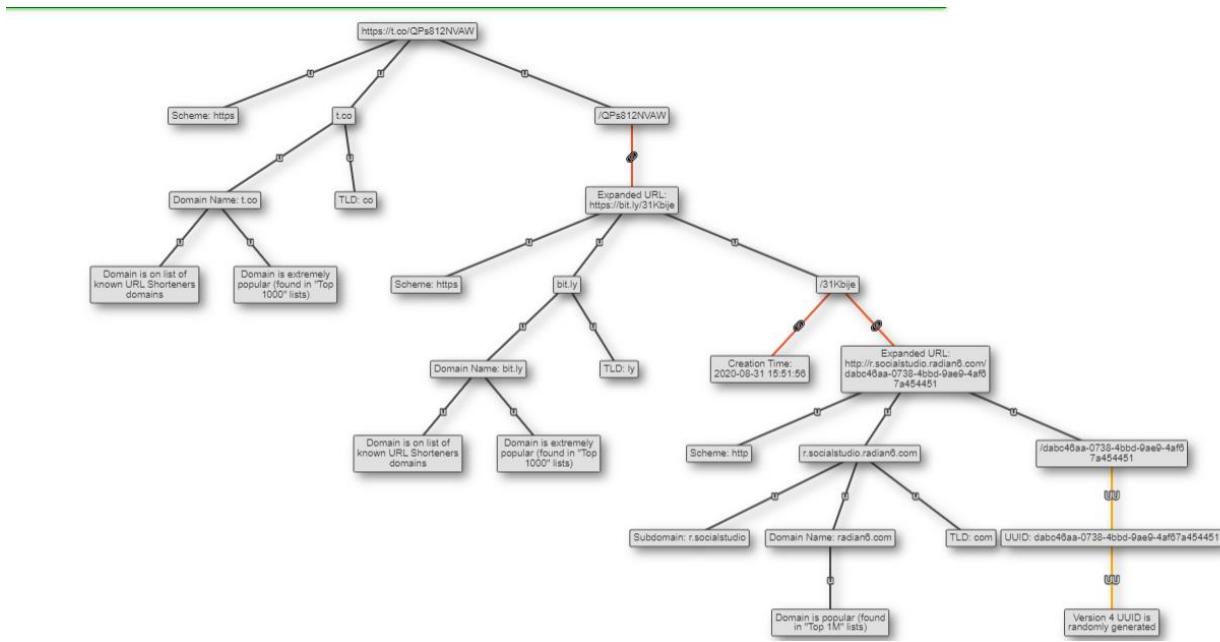
Simple URL- scheme, domain information, subdomain, TLD, URL path segment, parsing function, URL query.



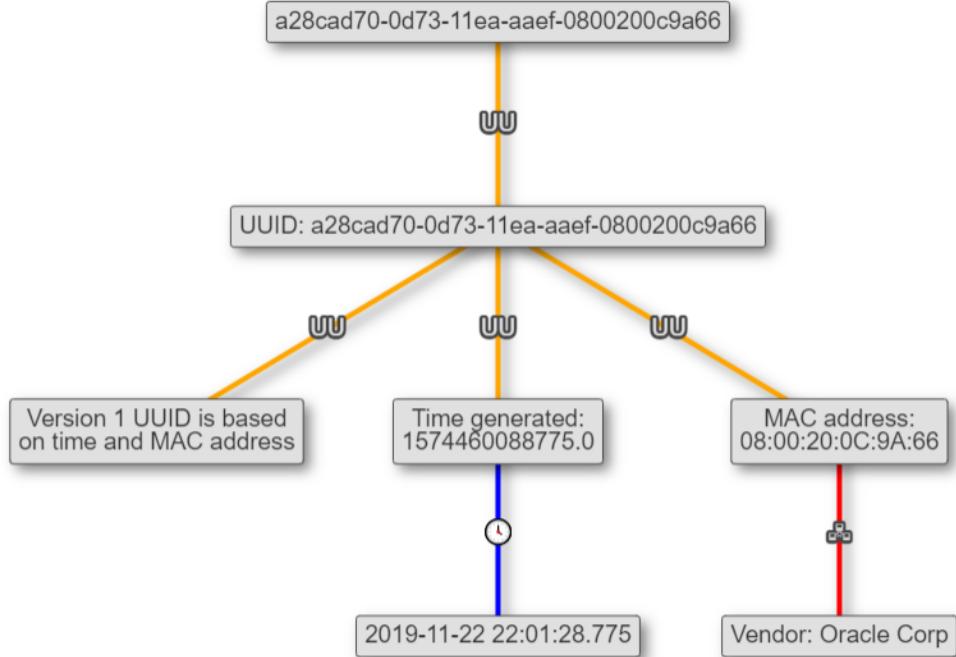
Complicated URL - getting host details



Short links- details about domain, host details, expanded URL and the website used, creation time, UUID generated, URL path etc.

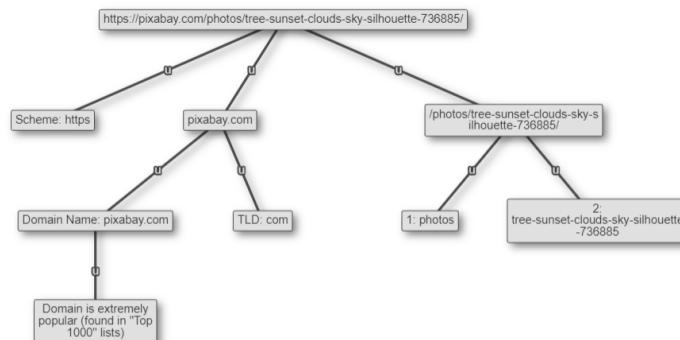


UUID- Mac address, timestamp, vendor



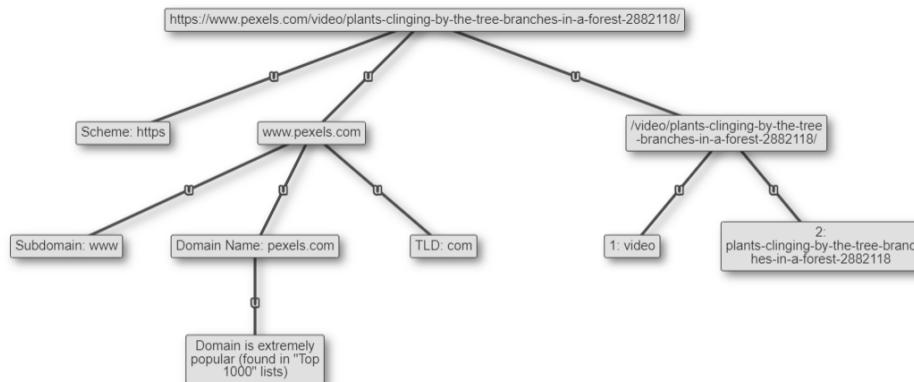
Searching for some URL to see what this tool will provide information –

1. <https://pixabay.com/photos/tree-sunset-clouds-sky-silhouette-736885/>



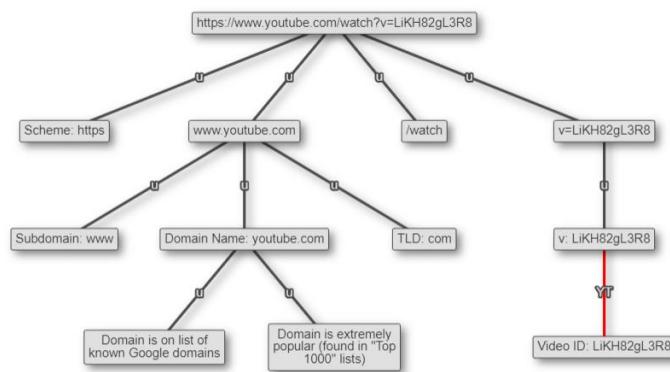
2. <https://www.pexels.com/video/plants-clinging-by-the-tree-branches-in-a-forest-2882118/>

<https://www.pexels.com/video/plants-clinging-by-the-tree-branches-in-a-forest-2882118/> Unfurl!

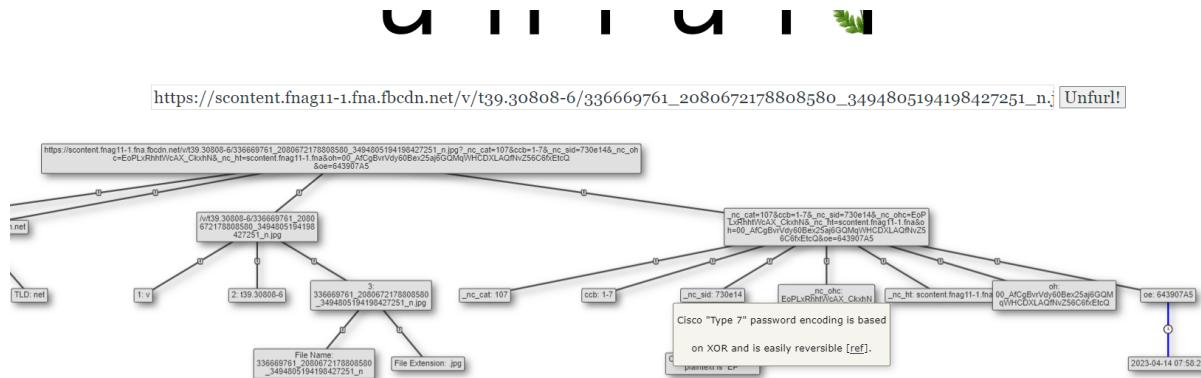


3. <https://www.youtube.com/watch?v=LiKH82gL3R8>

<https://www.youtube.com/watch?v=LiKH82gL3R8> Unfurl!



4. https://scontent.fnag11-1.fna.fbcdn.net/v/t39.30808-6/336669761_2080672178808580_3494805194198427251_n.jpg?_nc_cat=107&ccb=1-7&_nc_sid=730e14&_nc_ohc=EoPLxRhhtWcAX_CkxhN&_nc_ht=scontent.fnag11-1.fna&oh=00_AfCgBvrVdy60Bex25aj6GQMqWHCDXLAQfNvZ56C6fxEtcQ&oe=643907A5



5. Browser History Viewer-

Browser History Viewer is a forensic software tool by Foxton Forensics for extracting and viewing internet history from web browsers like fire fox, chrome, edge, internet explorer etc.

Features-

- Website Activity Timeline- Identify peaks in internet activity using the interactive timeline.
- Filtering- Find relevant data faster with filtering by keywords and date/time range.
- Cached Image Gallery- Browse the images a user has viewed online using the built-in image gallery.

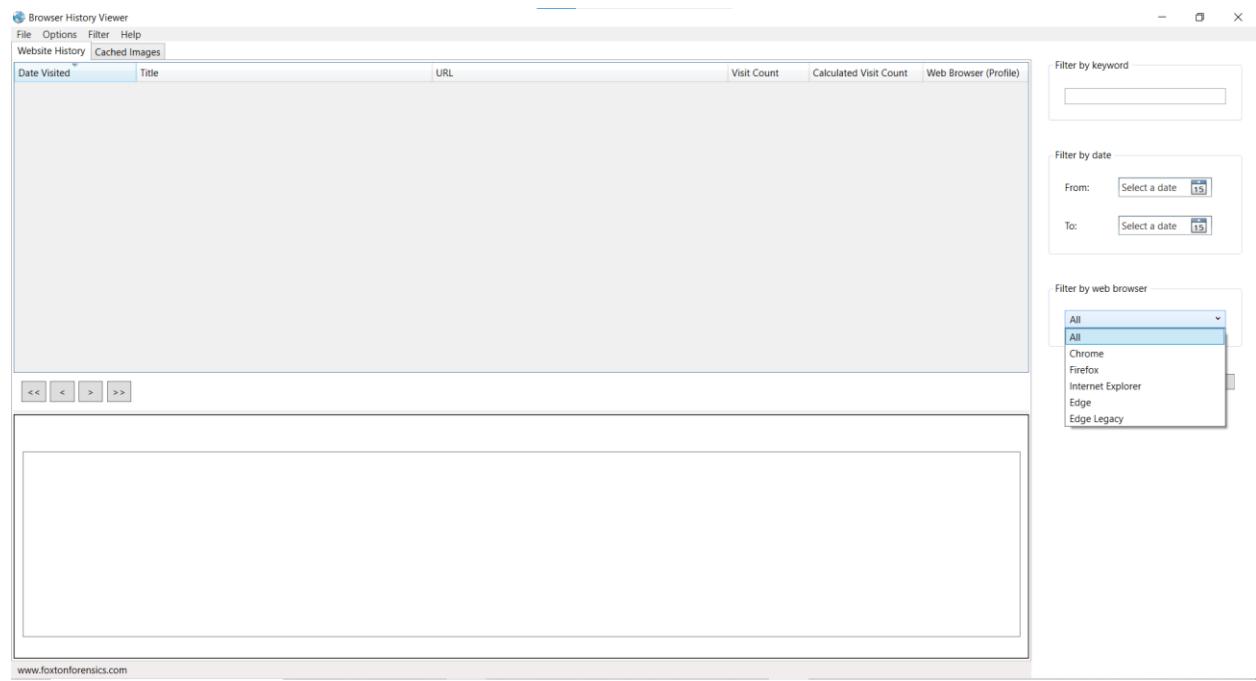
The examiner premium version has some additional features-

- Remote data capture
- Recover deleted history
- Cached web page viewer
- Advanced filtering & searching

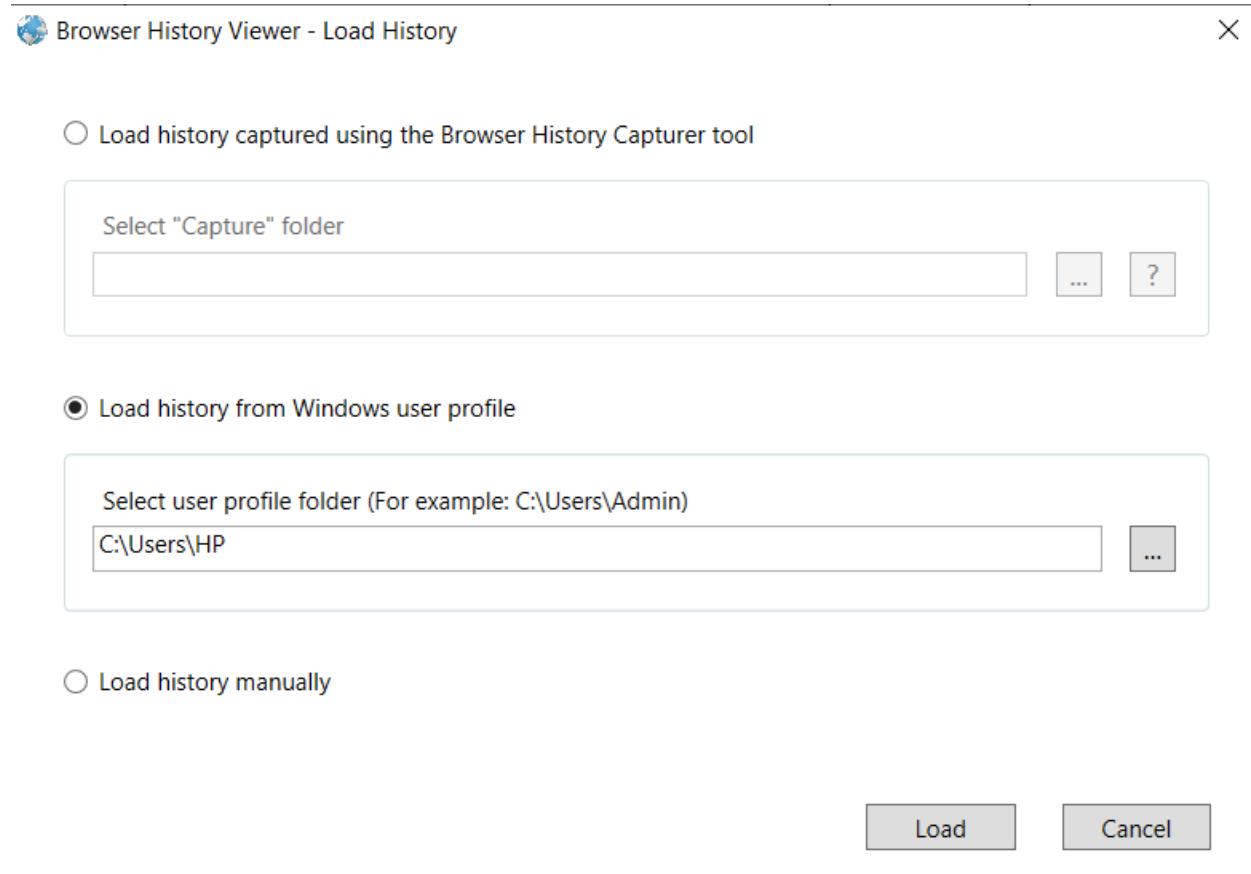
Can download the tool from –

<https://www.foxtonforensics.com/browser-history-viewer/download>

Here we can filter by keyword, timestamp, by browser –



From file select – load history – choose the appropriate option.



This tool retrieves all the history data with the time stamp and provides the no of counts, the graph of website visit count with times stamp.

The screenshot shows the 'Browser History Viewer' application interface. On the left, a table lists browser history entries with columns for Date Visited, Title, URL, Visit Count, Calculated Visit Count, and Web Browser (Profile). On the right, there are three filter panels: 'Filter by keyword' (with a search input), 'Filter by date' (with 'From: 01-Jan-23' and 'To: 01-Feb-23'), and 'Filter by web browser' (with a dropdown set to 'All'). Below the table is a bar chart titled 'Website Visit Count - 11-05-2022 to 11-11-2023'. The x-axis represents months from May 2022 to November 2023, and the y-axis represents visit counts from 0 to 4000. The chart shows a significant peak in March 2023. At the bottom, a message says 'www.foxtonforensics.com Time zone: UTC'.

If we want to look for particular thing in a particular timeline then we can search in the keyword box by providing the desired timeline-

The screenshot shows the 'Browser History Viewer' application interface with a filtered dataset. The 'Filter by keyword' panel has 'fraud' entered. The 'Filter by date' panel shows 'From: 01-May-22' and 'To: 01-Feb-23'. The table on the left lists browser history entries for this filtered period. On the right, the same three filter panels are present. Below the table is a bar chart titled 'Website Visit Count - 19-01-2023 to 30-01-2023', showing visit counts for January 2023. A message at the bottom says 'www.foxtonforensics.com Time zone: UTC'.

All the cached images with details-

Browser History Viewer

File Options Filter Help

Website History Cached Images

Last Fetched	Filename	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
09/04/2023 08:09:59		https://adservice.google.co.in/ddm/fls/p/src=1295336&type=csc_1	42	Firefox (eln4mywm.def)	
09/04/2023 08:09:59		https://adservice.google.co.in/ddm/fls/p/src=1295336&type=cust_1	42	Firefox (eln4mywm.def)	
09/04/2023 08:09:58	actview/xai=AKAOjstodG98vSNEp4nkGa2ajzCSIVP0esx5jq	https://pagead2.googleyindication.com/pc/actview/xai=AKA_1	42	Firefox (eln4mywm.def)	
09/04/2023 08:08:02	img.png?cnw=782ec17960dc0df90da63badbaca3d8f	https://99.flashtalking.com/img/img.png?cnw=782ec17960dc0df_1	70	Firefox (eln4mywm.def)	
09/04/2023 08:08:00	gradient_728x90.png	https://cdn.flashtalking.com/116264/390095/images/gradient_1	6175	Firefox (eln4mywm.def)	
09/04/2023 08:08:00	Group171472.png	https://cdn.flashtalking.com/116264/390095/images/Group171_1	20165	Firefox (eln4mywm.def)	
09/04/2023 08:08:00	Desktop_Acrobat_ARed_FullBleedVERB.png	https://cdn.flashtalking.com/116264/390095/images/Desktop_1	20955	Firefox (eln4mywm.def)	
09/04/2023 08:08:00	MaskGroup171153.png	https://cdn.flashtalking.com/116264/390095/images/MaskGroup171153_1	8387	Firefox (eln4mywm.def)	
09/04/2023 08:07:59	iconc.png?EDAA.icon=y	https://secure.flashtalking.com/oba/icon/iconc.png?EDAA.icon=y_1	1308	Firefox (eln4mywm.def)	
09/04/2023 08:07:59	consumer-privacy-logs.png	https://secure.flashtalking.com/oba/icon/consumer-privacy-logo_1	5953	Firefox (eln4mywm.def)	
09/04/2023 08:07:58	gen_204id=xbid&dbm_b=AKAmf-BILY19FvN5wTqCRWtWaWY2	https://pagead2.googleyindication.com/pagead/gen_204id=xb_1	42	Firefox (eln4mywm.def)	
09/04/2023 08:07:57	halo_match?id=undefined&halo_id=0609kgahcc6jhheflicc966c	https://ids.ad.gt/api/v1/halo/match?id=undefined&halo_id=0609kgahcc6jhheflicc966c_1	43	Firefox (eln4mywm.def)	
09/04/2023 08:07:56	favicon_512.png?2015	https://cdns1.softpedia.com/_img/favicon_512.png?2015_3	14627	Firefox (eln4mywm.def)	
09/04/2023 08:07:56	favicon.ico	https://cdns1.softpedia.com/_img/favicon.ico_3	4507	Firefox (eln4mywm.def)	
09/04/2023 08:07:55	Alienzyne.png	https://windows-cdn.softpedia.com/screenshots/ico/Alienzyne.pn_1	1362	Firefox (eln4mywm.def)	

<< < > >> Page 1 of 26 Viewing 765/765 records

Filter by keyword

Filter by date From: To:

Filter by web browser All

References-

<https://www.kalilinux.in/2019/10/dumpzilla-kali-linux.html>