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

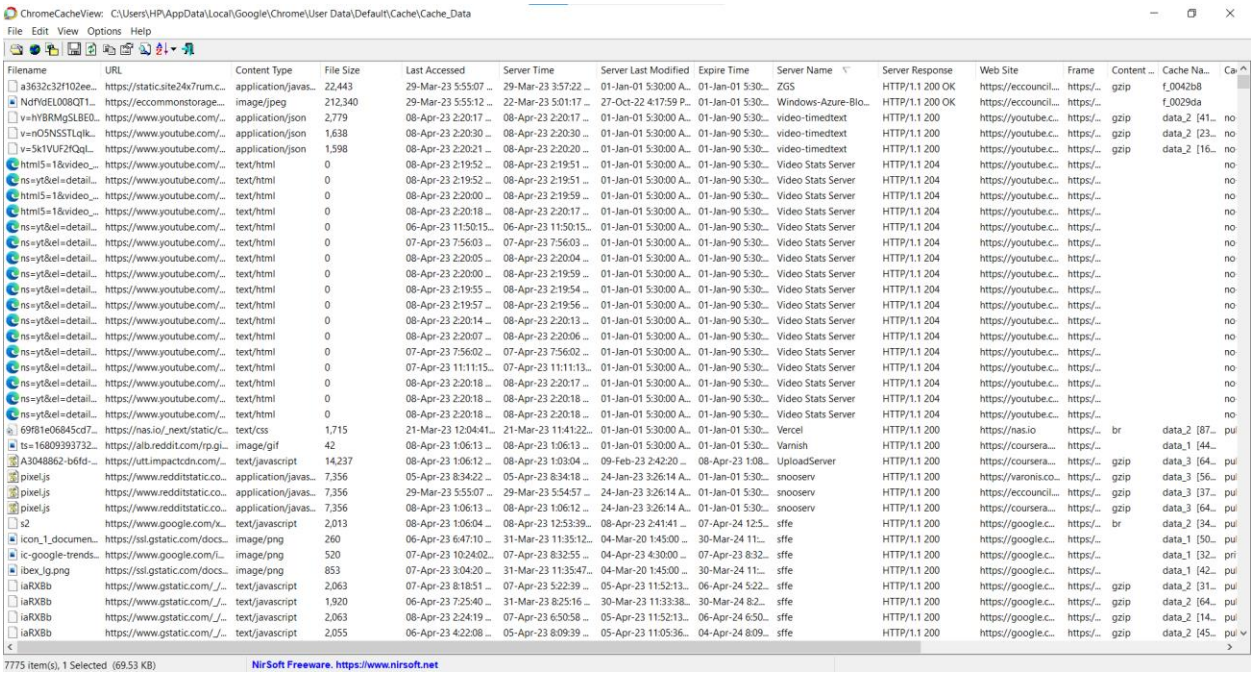
Download chrome-cache-view from –

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

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

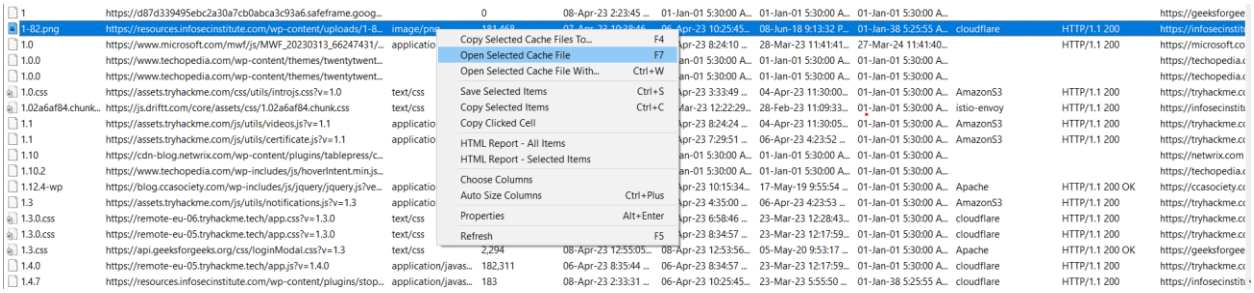
```
Microsoft Windows [Version 10.0.19045.2728]
(c) Microsoft Corporation. All rights reserved.

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.



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”-

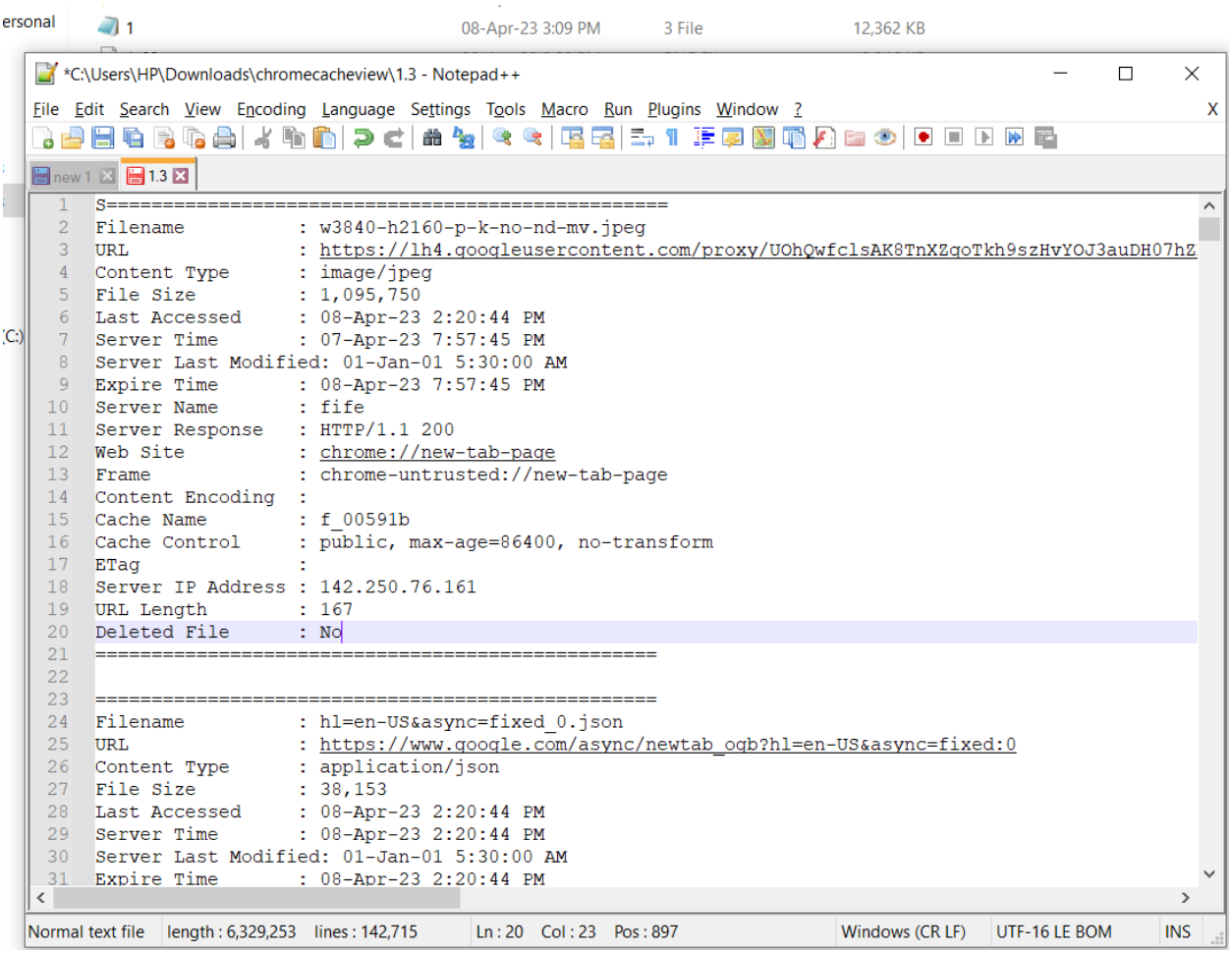


Commands –

“/stext <Filename>”-

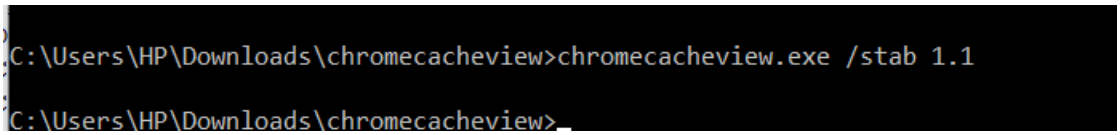
To save the list of all cache files and with their details into a regular text file.

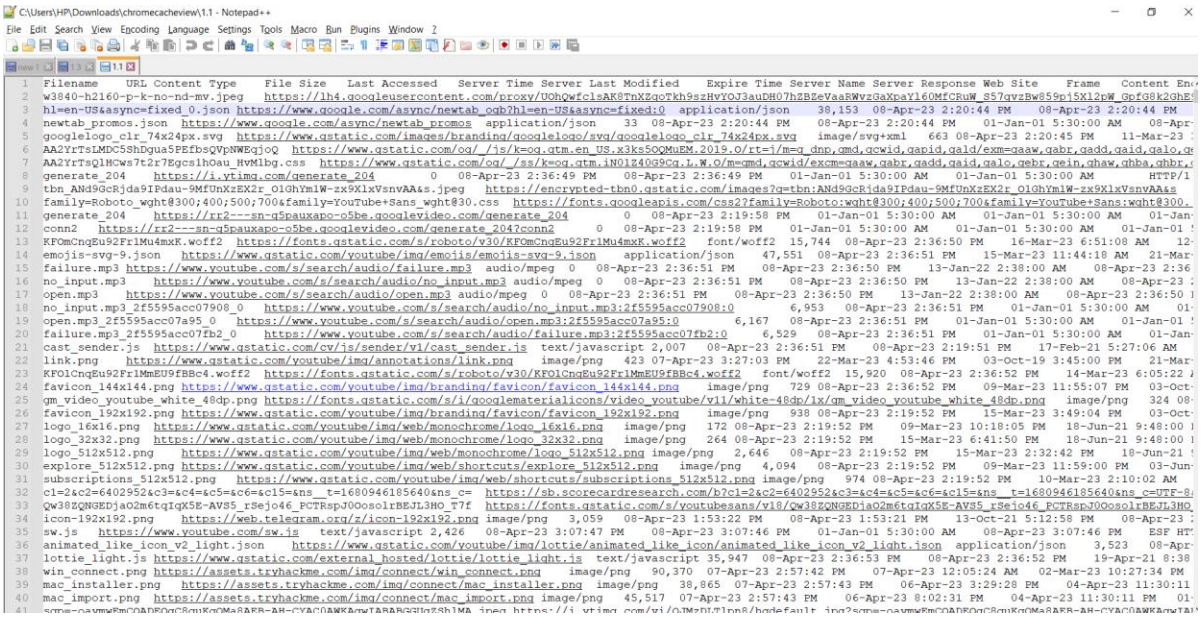
```
C:\Users\HP\Downloads\chromecacheview>chromecacheview.exe /stext 1.3

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



/stab <Filename> -

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





/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).

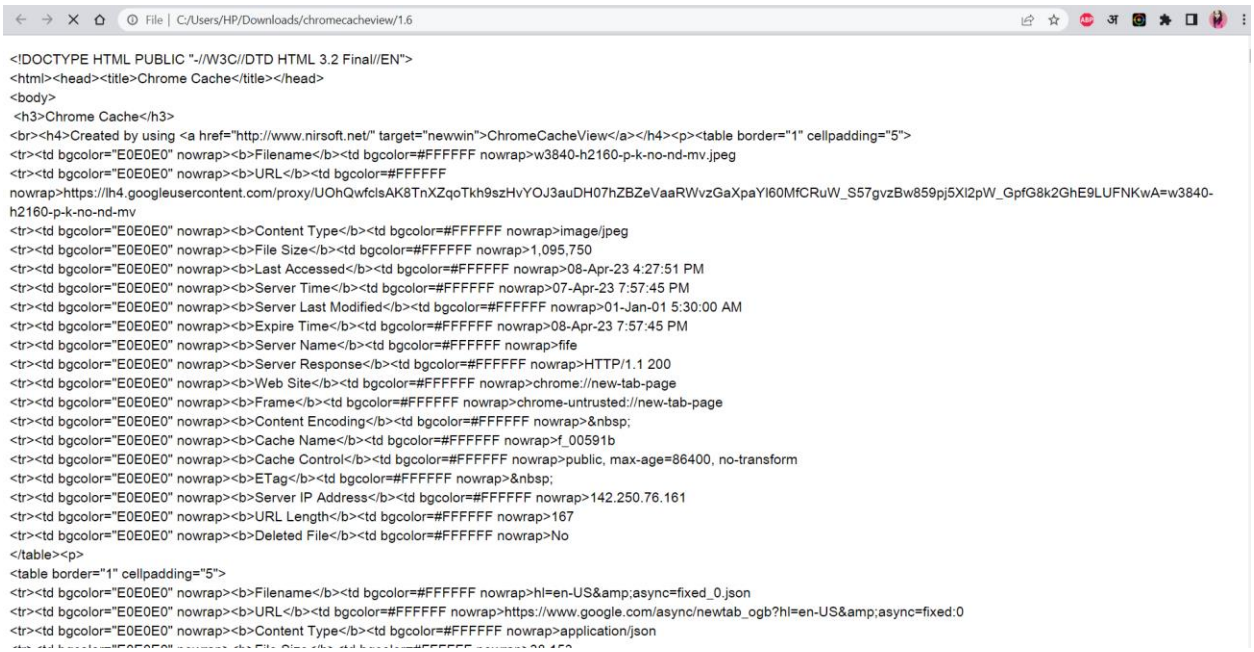
/sverhtml <Filename> -

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
```



File | C:/Users/HP/Downloads/chromecacheview/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 bgcolor="E0E0E0" nowrap><b>Filename</b><td bgcolor=#FFFFFF nowrap>w3840-h2160-p-k-no-nd-mv.jpeg
<tr><td bgcolor="E0E0E0" nowrap><b>URL</b><td bgcolor=#FFFFFF
nowrap>https://lh4.googleusercontent.com/proxy/UOhQwfclsAK8TnXZqoTkh9szHvYOJ3auDH07hZBZeVaaRWvzGaXpaYl60MfCRuW_S57gvzBw859pj5Xl2pW_GpfG8k2GhE9LUFNKwA=w3840-
h2160-p-k-no-nd-mv
<tr><td bgcolor="E0E0E0" nowrap><b>Content Type</b><td bgcolor=#FFFFFF nowrap>image/jpeg
<tr><td bgcolor="E0E0E0" nowrap><b>File Size</b><td bgcolor=#FFFFFF nowrap>1,095,750
<tr><td bgcolor="E0E0E0" nowrap><b>Last Accessed</b><td bgcolor=#FFFFFF nowrap>08-Apr-23 4:27:51 PM
<tr><td bgcolor="E0E0E0" nowrap><b>Server Time</b><td bgcolor=#FFFFFF nowrap>07-Apr-23 7:57:45 PM
<tr><td bgcolor="E0E0E0" nowrap><b>Server Last Modified</b><td bgcolor=#FFFFFF nowrap>01-Jan-01 5:30:00 AM
<tr><td bgcolor="E0E0E0" nowrap><b>Expire Time</b><td bgcolor=#FFFFFF nowrap>08-Apr-23 7:57:45 PM
<tr><td bgcolor="E0E0E0" nowrap><b>Server Name</b><td bgcolor=#FFFFFF nowrap>fife
<tr><td bgcolor="E0E0E0" nowrap><b>Server Response</b><td bgcolor=#FFFFFF nowrap>HTTP/1.1 200
<tr><td bgcolor="E0E0E0" nowrap><b>Web Site</b><td bgcolor=#FFFFFF nowrap>chrome://new-tab-page
<tr><td bgcolor="E0E0E0" nowrap><b>Frame</b><td bgcolor=#FFFFFF nowrap>chrome-untrusted://new-tab-page
<tr><td bgcolor="E0E0E0" nowrap><b>Content Encoding</b><td bgcolor=#FFFFFF nowrap> 
<tr><td bgcolor="E0E0E0" nowrap><b>Cache Name</b><td bgcolor=#FFFFFF nowrap>f_00591b
<tr><td bgcolor="E0E0E0" nowrap><b>Cache Control</b><td bgcolor=#FFFFFF nowrap>public, max-age=86400, no-transform
<tr><td bgcolor="E0E0E0" nowrap><b>ETag</b><td bgcolor=#FFFFFF nowrap> 
<tr><td bgcolor="E0E0E0" nowrap><b>Server IP Address</b><td bgcolor=#FFFFFF nowrap>142.250.76.161
<tr><td bgcolor="E0E0E0" nowrap><b>URL Length</b><td bgcolor=#FFFFFF nowrap>167
<tr><td bgcolor="E0E0E0" nowrap><b>Deleted File</b><td bgcolor=#FFFFFF nowrap>No
</table><p>
<table border="1" cellpadding="5">
<tr><td bgcolor="E0E0E0" nowrap><b>Filename</b><td bgcolor=#FFFFFF nowrap>hl=en-US&amp;async=fixed_0.json
<tr><td bgcolor="E0E0E0" nowrap><b>URL</b><td bgcolor=#FFFFFF nowrap>https://www.google.com/async/newtab_ogb?hl=en-US&amp;async=fixed:0
<tr><td bgcolor="E0E0E0" nowrap><b>Content Type</b><td bgcolor=#FFFFFF nowrap>application/json
```

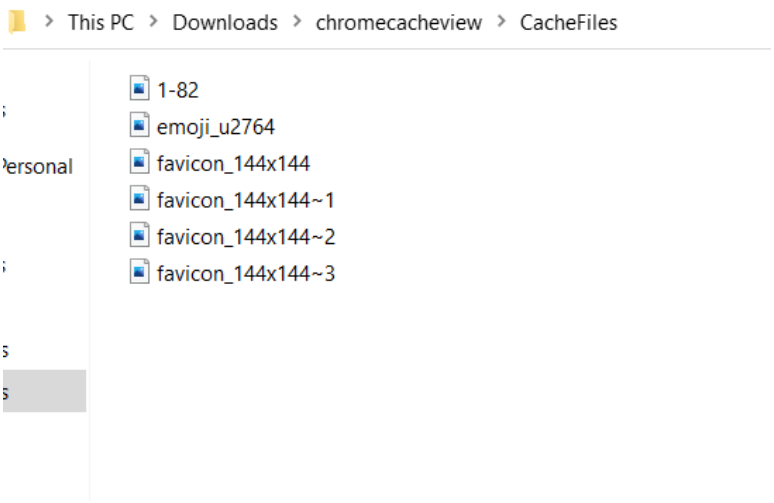
/copycache <URL> <Content Type> -

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

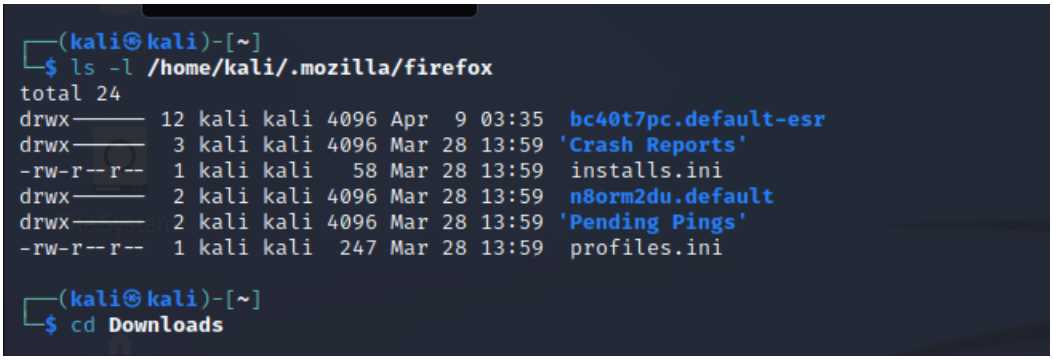
In Firefox, browser's saved data in profiles, to extract the data for forensic we use dumpzilla. Here we need to know the path of default profile. Different operating system have different path, here we are using kali-

Linux or UNIX profile path

/home/$USER/.mozilla/firefox/xxxx.deafult

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

Firstly we will check the profile-



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
```

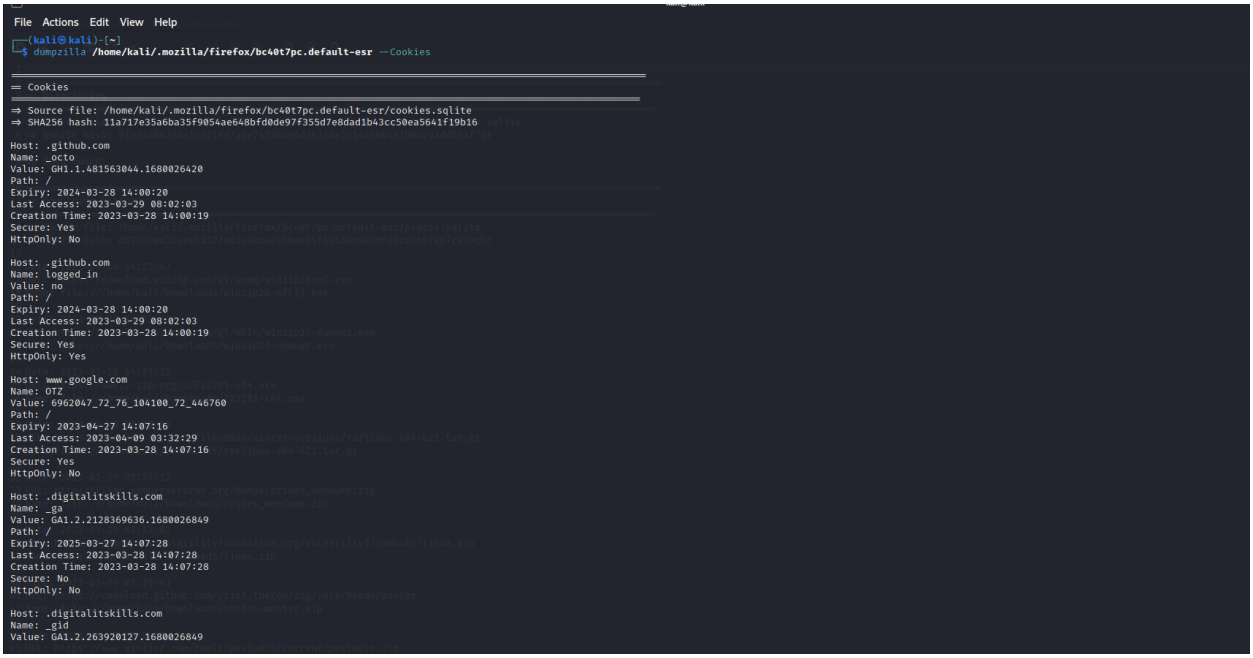
If we want we can save the information in a text file-

```
URL: https://www.7-zip.org/a/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
URL: https://www.winmd5.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/b65e167b864675b261847bf5bebbc011/64242978/100004102/software/programming/PEiD-0.95-20081103.zip
Name: file:///home/kali/Downloads/PEiD-0.95-20081103.zip

═══════════════════════════════════════════════════════════════════════════════
== Total Information
═══════════════════════════════════════════════════════════════════════════════

Total Directories          : 0
Total Downloads history    : 11


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

┌──(kali㉿kali)-[~]
└─$
```

To get the passwords-

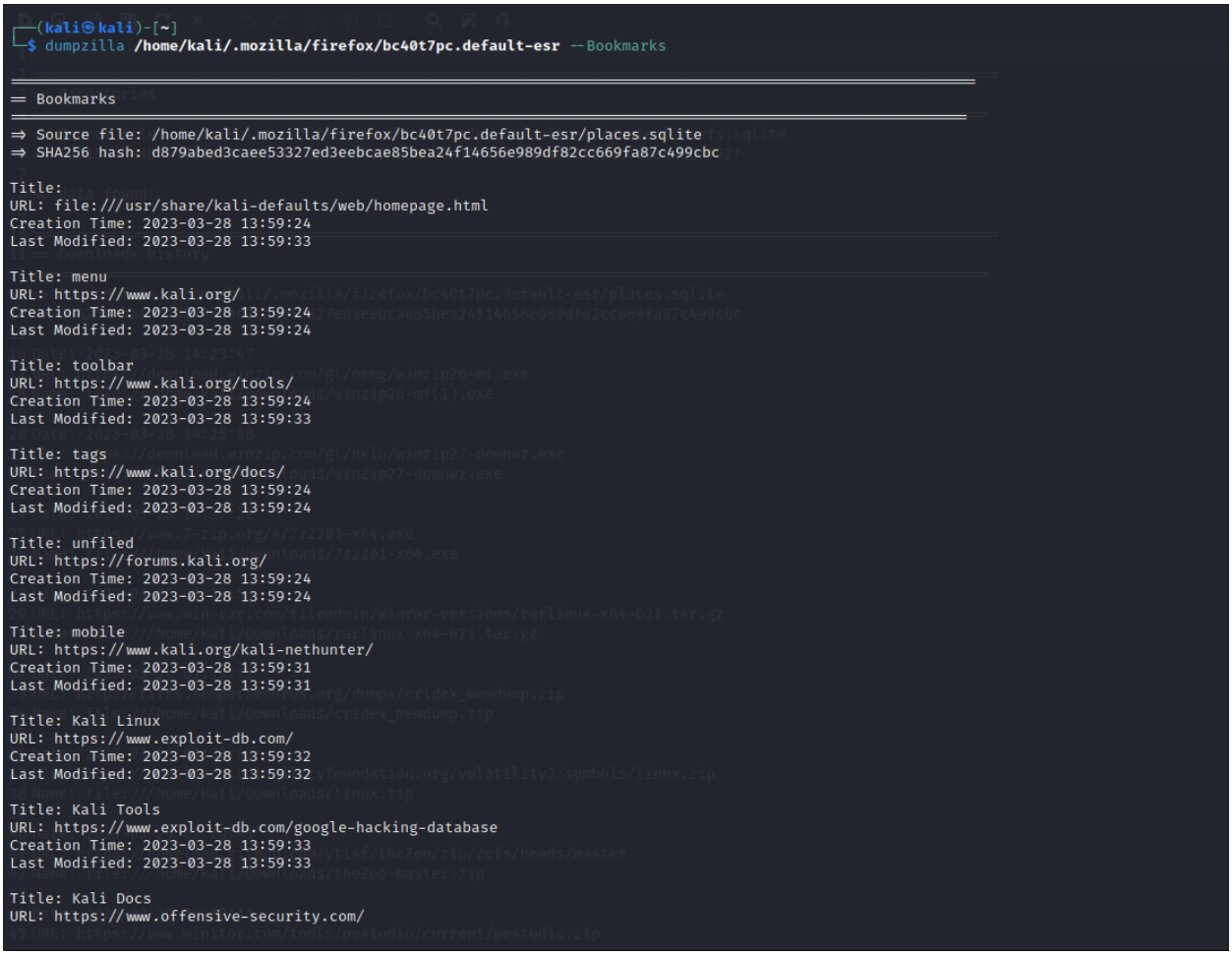
```
┌──(kali㉿kali)-[~]
└─$ dumpzilla /home/kali/.mozilla/firefox/bc40t7pc.default-esr --Passwords
[ERROR] Error decoding passwords: libnss not found (libnss3.so)

═══════════════════════════════════════════════════════════════════════════════
== Decode Passwords
═══════════════════════════════════════════════════════════════════════════════
⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/logins.json
⇒ SHA256 hash: 645534fe025ac2742418e2b28817cb4b3cde545e52af08d3070b9fda1d1babe3

Web: chrome://FirefoxAccounts
Username:
Password:

═══════════════════════════════════════════════════════════════════════════════
== Passwords
═══════════════════════════════════════════════════════════════════════════════
⇒ Source file: /home/kali/.mozilla/firefox/bc40t7pc.default-esr/logins.json
⇒ SHA256 hash: 645534fe025ac2742418e2b28817cb4b3cde545e52af08d3070b9fda1d1babe3

Web: chrome://FirefoxAccounts
User field:
Password field:
User login (crypted): MFIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECHelttstdudwBCgWd5zhRxGETO6/V6vaVst0b1bukBtT29Q9apmvdiI68p1CgjQpIoM9
Password login (crypted): MIIDdAQQ+AAAAAAAAAAAAAAAAAAAATAUBggqhkiG9w0DBwQIrwvcjydO/zUEggNIht2aAKuweaVPPQlvGircQ9zHbO92/rs+R/+3AtFC8oQQJ3blg/XAoOja9ddHNzFeti9n+Z8vmNNrtR0n4L9nz1ARendBXy1Ggk+pBopnZ+YP8+A8oHJ0MY45lWDaQ/esrSZaf6YEynTmyWfdPyWwFU+LXoI97cQH3GUOxxHbCdr/dshg3yfN7vDus/B9LKdbliwtlymDuzQoA+PcuBvVD4EmHQwRYLiUnP9g8NDCn12xYQaboDveC9NjlFNWeLhl26Z2fmdC+lN//M+O41hCGpwKM6ZvP5AGprYg9SdxJL4MPt60chGk1ZOUnd+1C9/NShR1FHPBm5qXfVWV7FjWm7QlG1F2qg26ViYRENdlrSqfPdEybwk2EIkkgF98W6BTQva82YnsI1Eo3PV2ZcMdryEwGqahf6LL6bcIvTzVOcKosxEOcBdLQzIPpThghpFBEJg2ajNV6qiQoCIbMveUcSBjh0osdRImheUNu7HoX/2CAUyAzFSZ7PzE6tQ2SSl+fkjd9lhp3RxgfP8olFeezjeiUqbB9JarZrAPiNOdHYtjBajAT8S/u2HPF1SWO/X6penzziNfZnsTrCUcsBEL0RYhuyp12a27p/ZOS8A3w1B0bJ5pVqJGF2LyBxy6uD/b0D72lvqp7wjO65Vp/PQhQtxsMENW6y8J2JNfbN3koGgxv6QUd2amFJekvOCI4ouE7axgysPU8tz0Cz5RvpksihHH58PrDsoRTo8B3EY+ivflqAE6kmkdpdAibswduqTZ2ruMAMP5Fo9IxbtZA7JMQEDmtUhGpbXuZs9kaknojnekb/Vkf15aEuMEkbpe+Ul36q4oM7tqyI4/19RJycbVdXKk4mC2bz/TxymHnmFjiyEnlcf/Qo2c2SVF2btVZScl/GqTakUSGlmE83t0JhwcE+TcGvo9yARtaM/yDvwTU7BHTSZ+fdUzoDLO/+N+0f4FhAwdcRgwh/5z/nmMX1dA0iC+RCxCar6uJOX3bXH5ja4S+fx6R/gCOTDTkkf+3JeIP6Zmfe1Y6EDh3h0gmri8xK/dMuWhJUCtwVyJy4pZmgXu1zeao/QyL6eWN5A9ocgmYWweBGJSpccrxDufNB7MFzpe2Fklcd
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,



Search engines-

All the pages that has been bookmarked-



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.

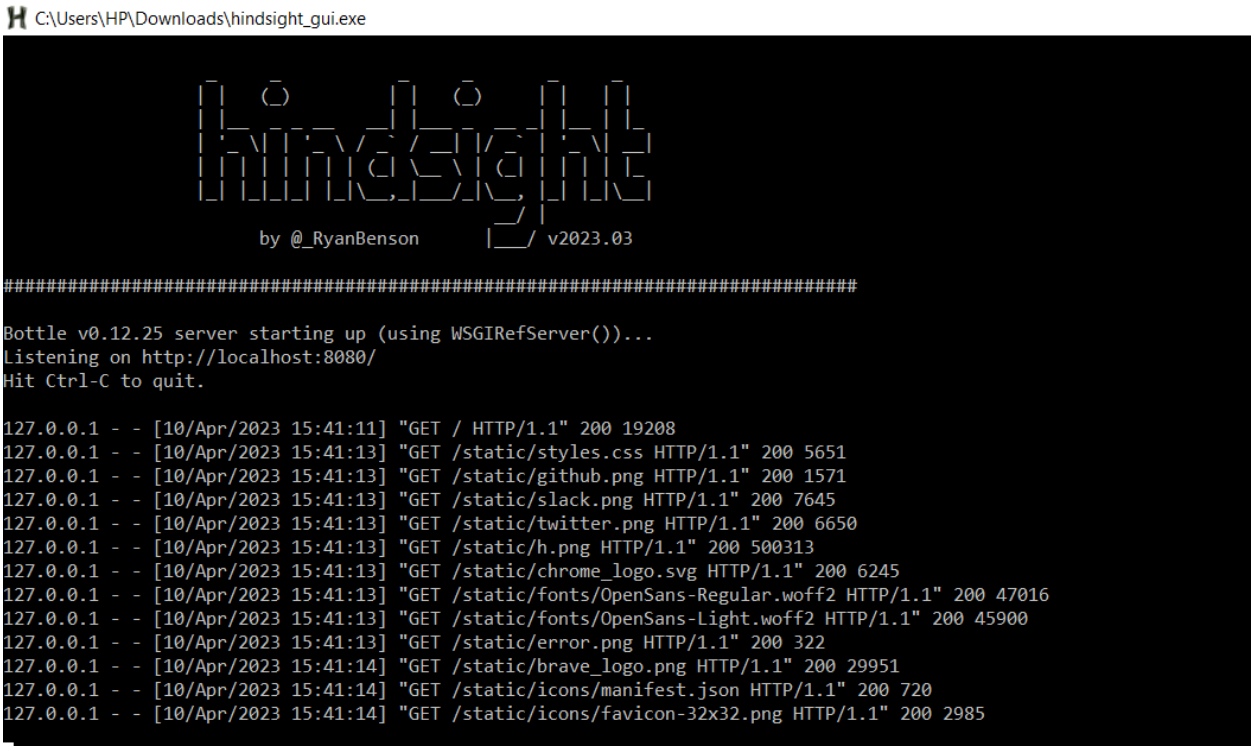
Features-

- 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-

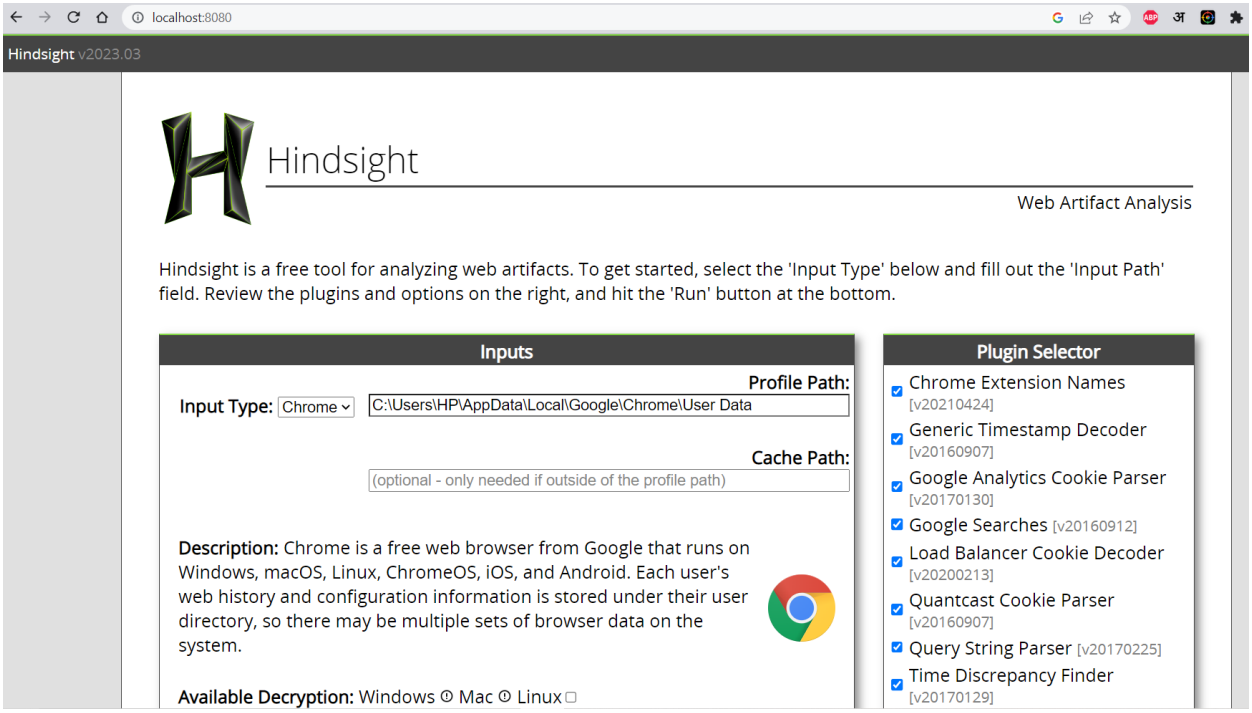


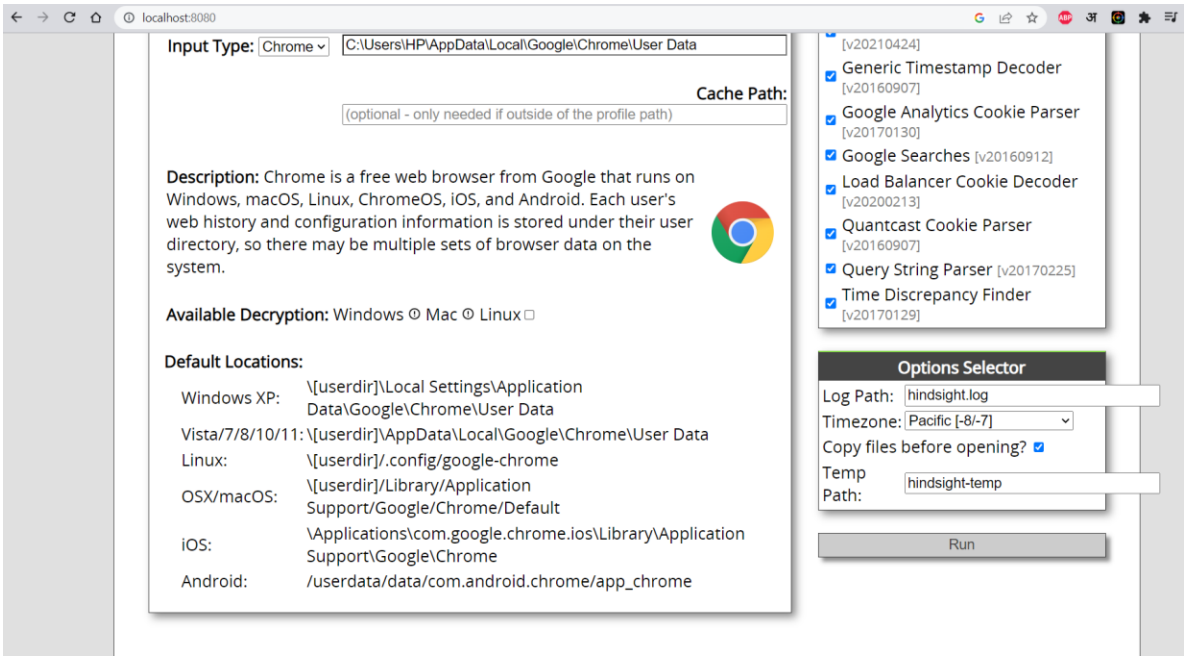
Now to start using the tool open the local host mentioned in the interface i.e - http://localhost:8080/

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

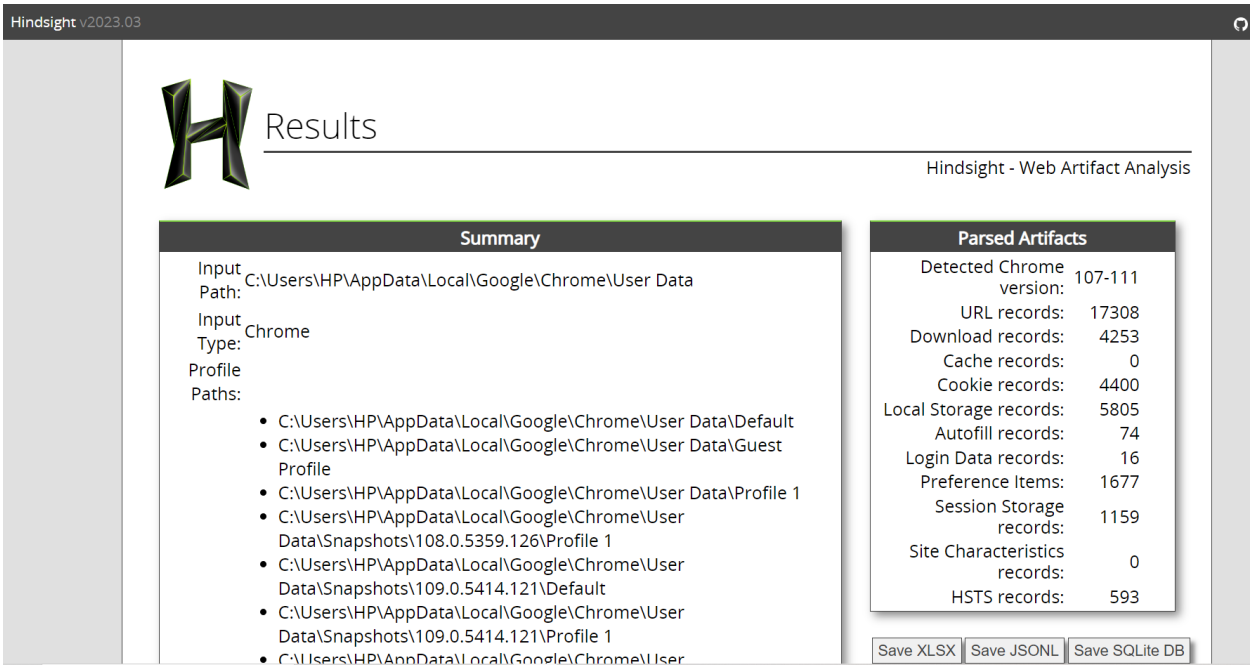
C:\Users\HP\AppData\Local\Google\Chrome\User Data

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

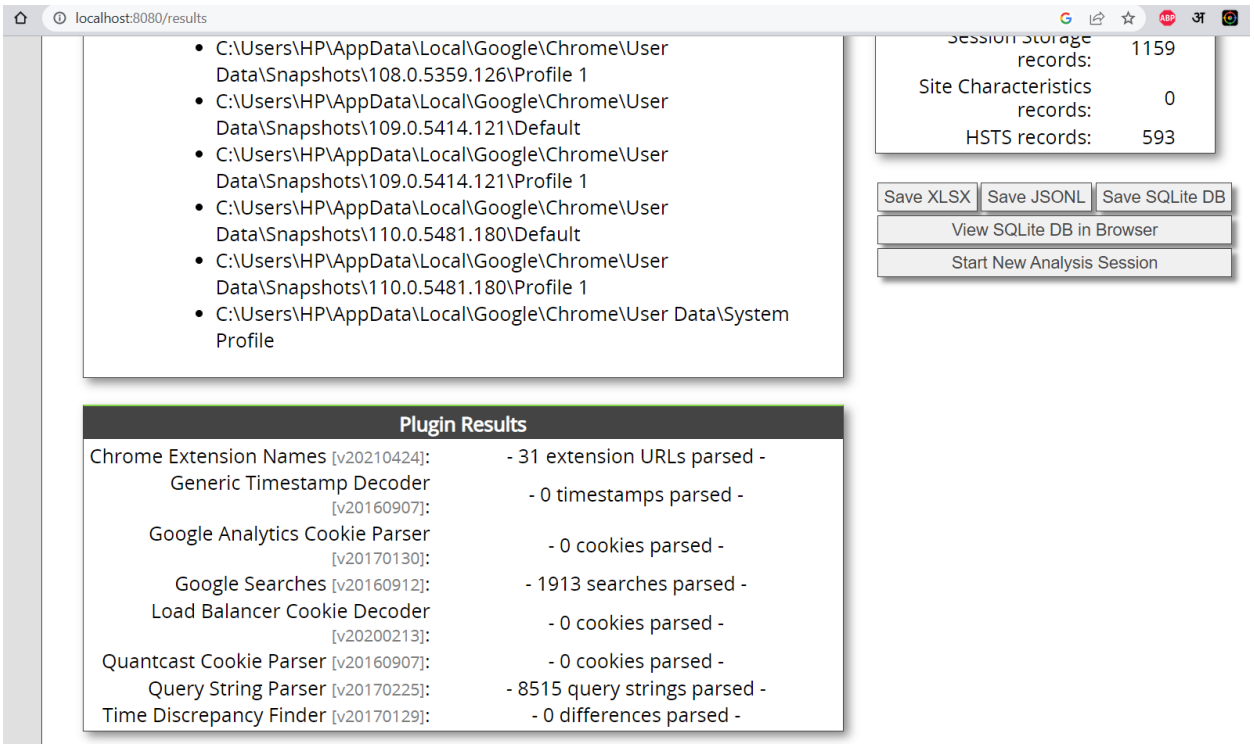




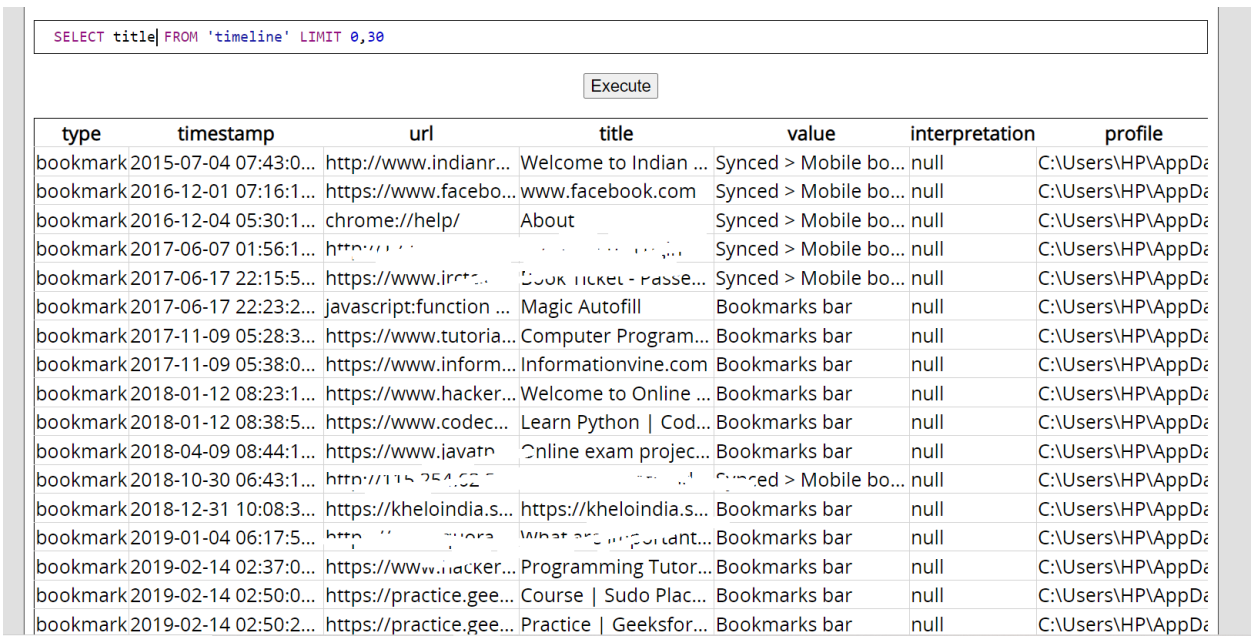
In the result summary we can see the parsed artifacts, profile paths



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



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
```

Execute

title
Welcome to Indian Railway Passenger reservation Enquiry
www.facebook.com
About
[illegible]
Book Ticket - Passengers Information
Magic Autofill
Computer Programming
Informationvine.com
Welcome to Online Programming
Learn Python | Codecademy
Online exam project in java swing without database - javatpoint
[illegible]
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

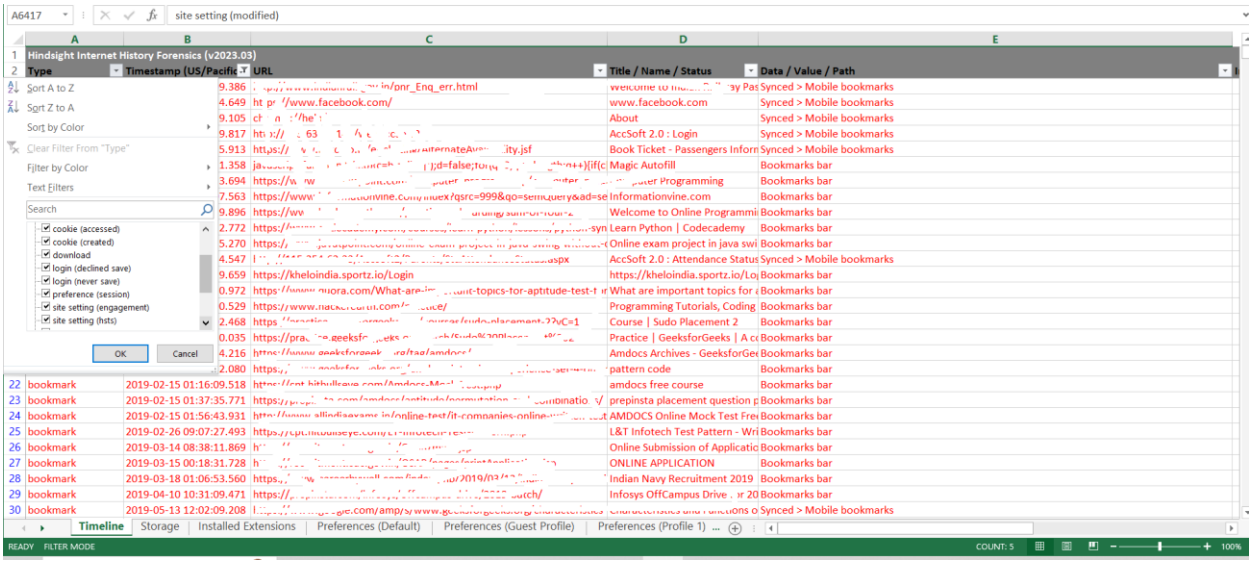
timeline (28921 rows)

```
SELECT URL FROM 'timeline' WHERE URL = 'https://www.facebook.com/'
```

Execute

url
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
https://www.facebook.com/
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.



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	[illegible]	Default
4	GHunt Companion	Load all needed cookies to use GHunt peacefully.	2.0.0	[illegible]	Default
5	Adobe Acrobat: PDF edit, conver	Do more in Google Chrome with Adobe Acrobat PDF tools. View, fill, comm	15.1.3.43	[illegible]	Default
6	Google Docs Offline	Edit, create, and view your documents, spreadsheets, and presentations —	1.60.0	[illegible]	Default
7	Google Input Tools	Input Tools lets you type in the language of your choice.	10.2.0.2	[illegible]	Default
8	Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	[illegible]	Default
9	Google Docs Offline	Edit, create, and view your documents, spreadsheets, and presentations —	1.50.1	[illegible]	Profile 1
10	Chrome Web Store Payments	Chrome Web Store Payments	1.0.0.6	[illegible]	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-

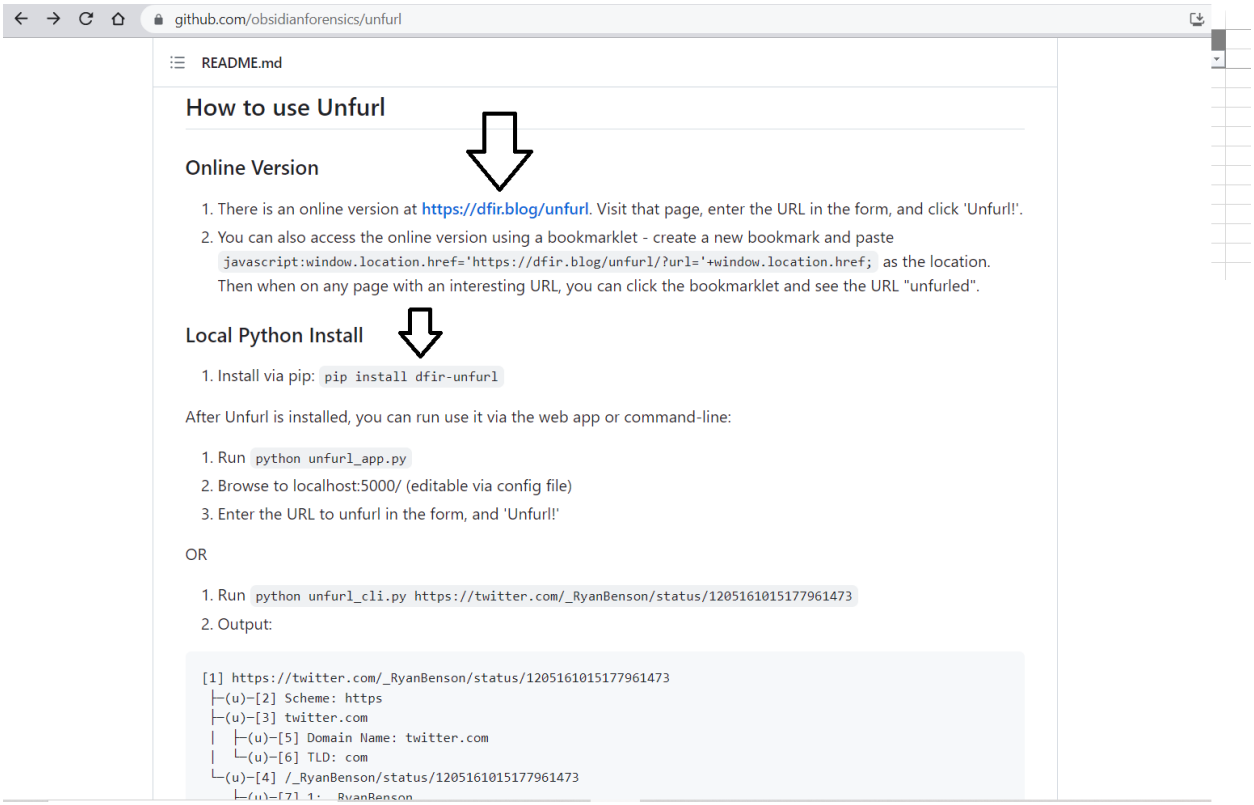
- Unfurl has parsers for URLs, search engines, chat applications, social media sites, and more.

- 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.

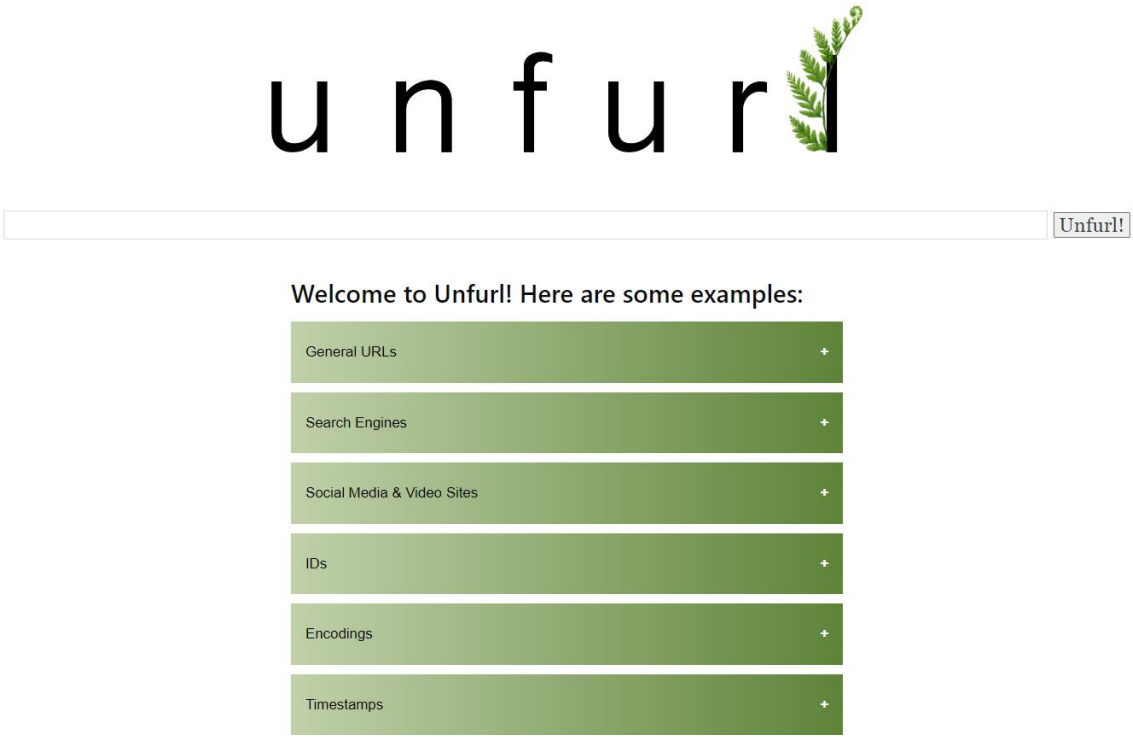
We can get the tool from the github page-

https://github.com/obsidianforensics/unfurl

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

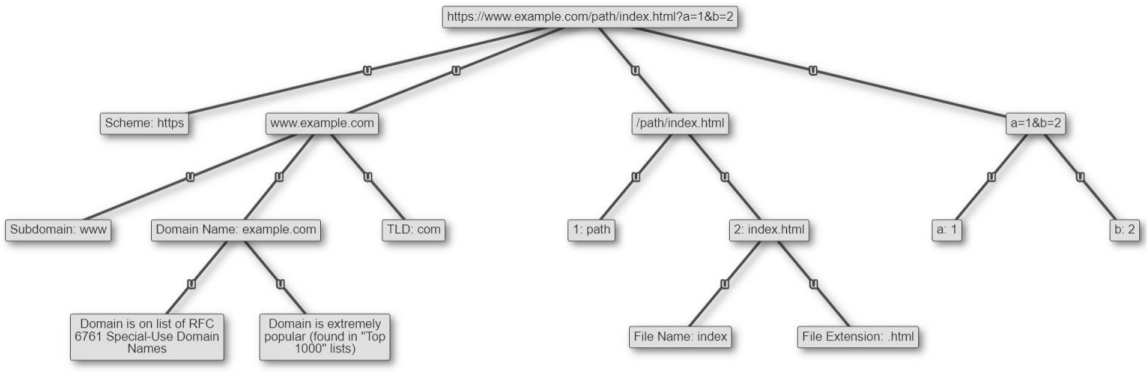


All the modules here we can see, it can parse data from any type of source – general URL, search engines, from social media or any videos, IDs(UUID, tiktok ID), timestamps etx.

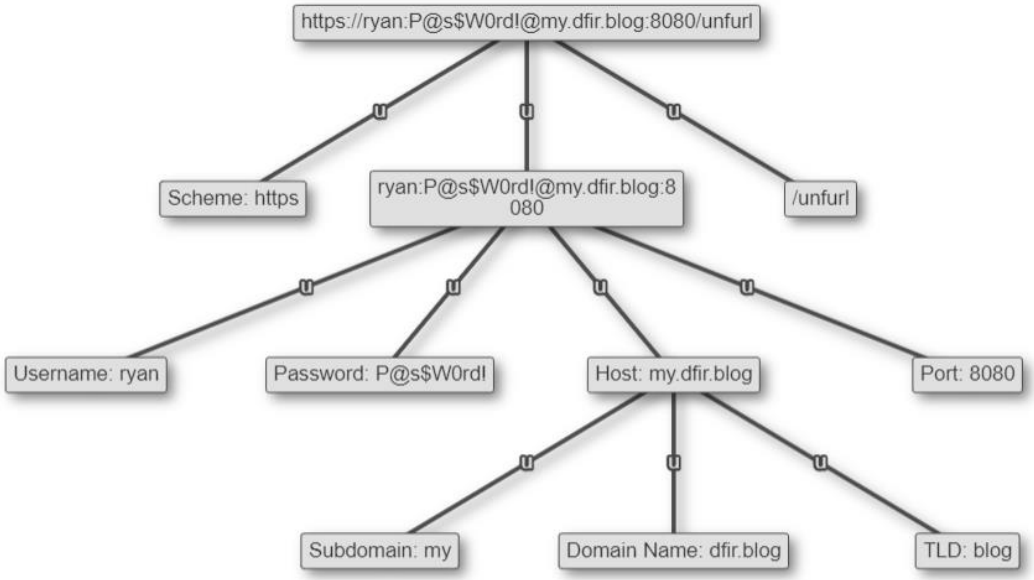


General URL- (simple link, complicated link, short link etc.)

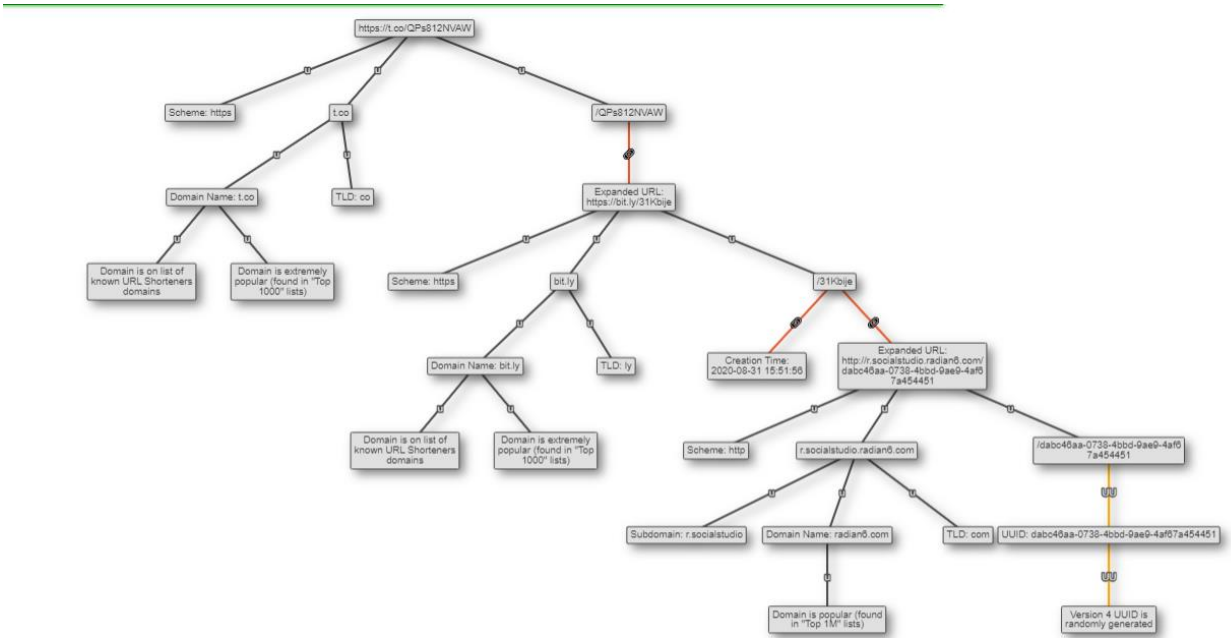
Simple URL- scheme, domain information, subdomain, TLD, URL path segment, parsing function, URL query.



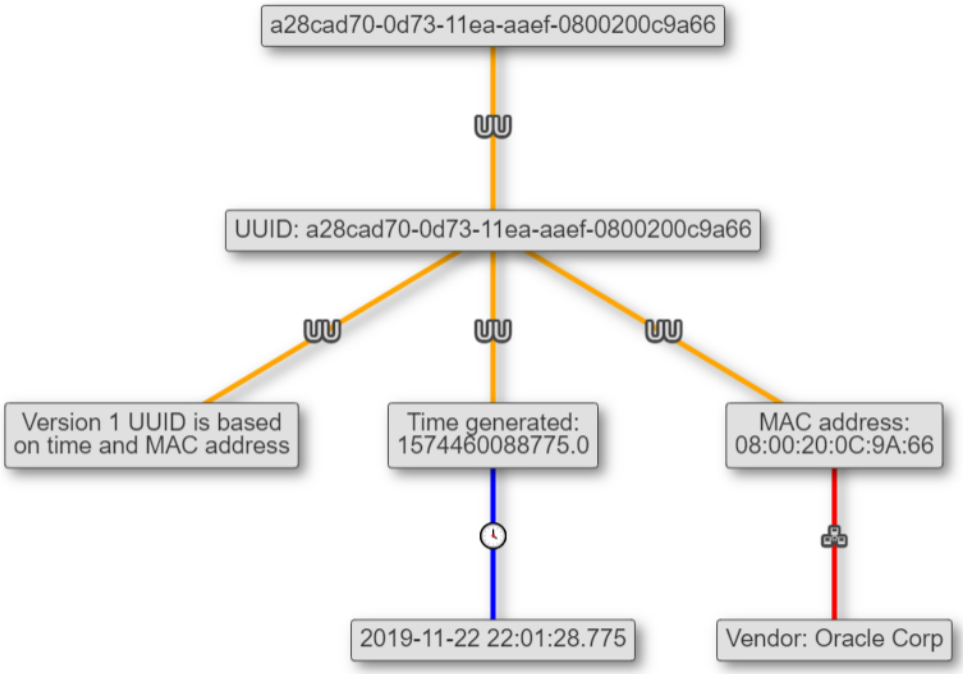
Complicated URL - getting host details



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

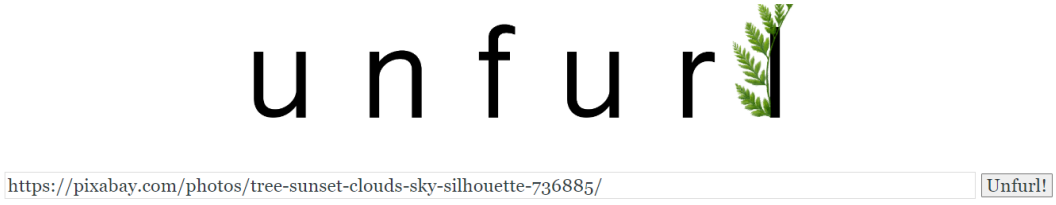


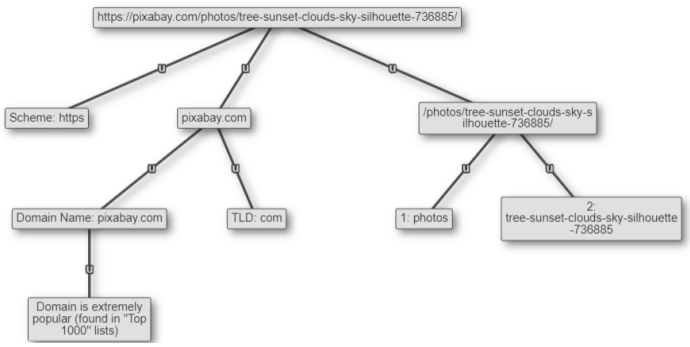
UUID- Mac address, timestamp, vendor



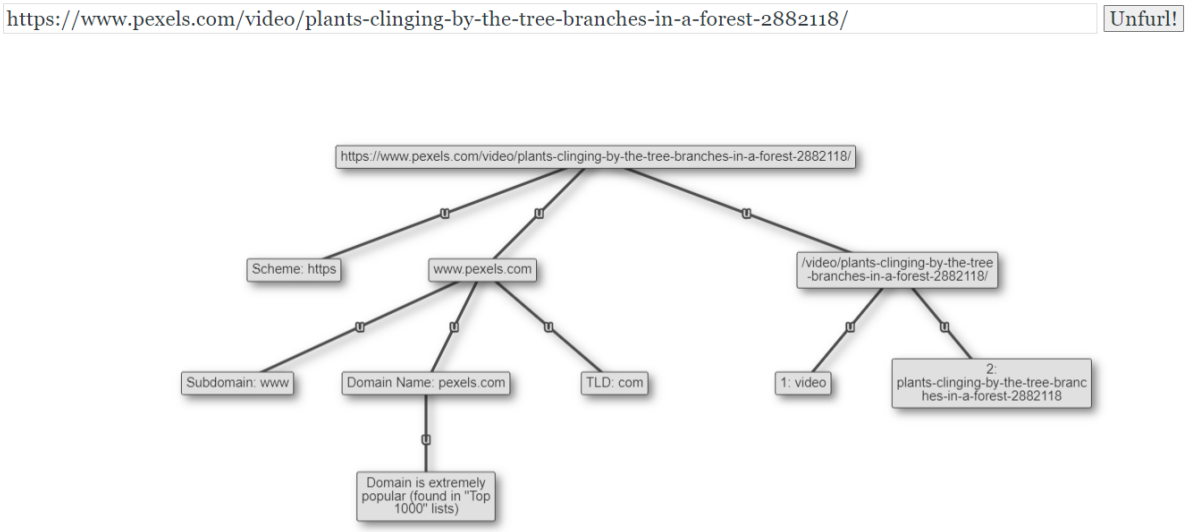
Searching for some URL to see what this tool will provide information –

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

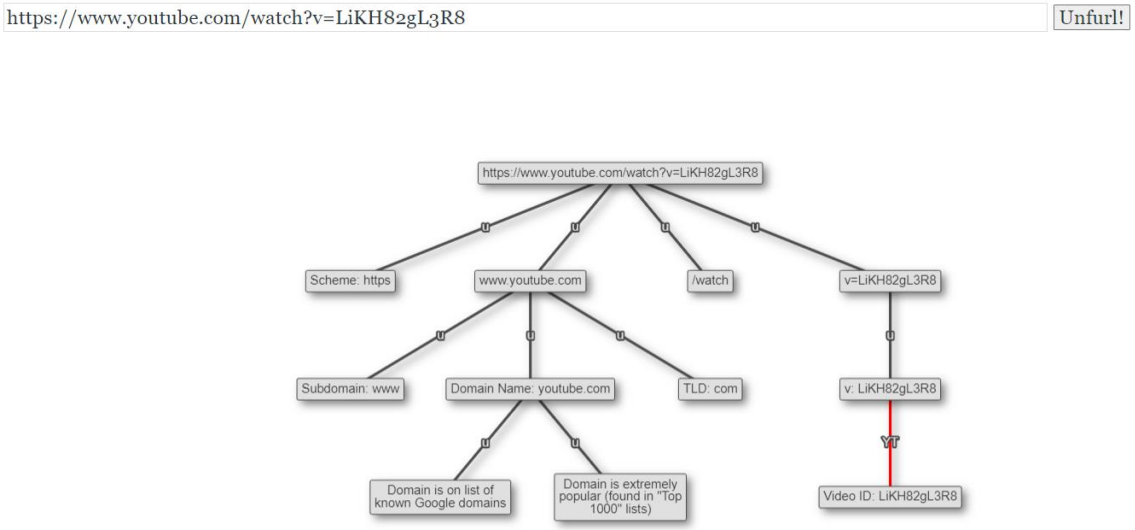




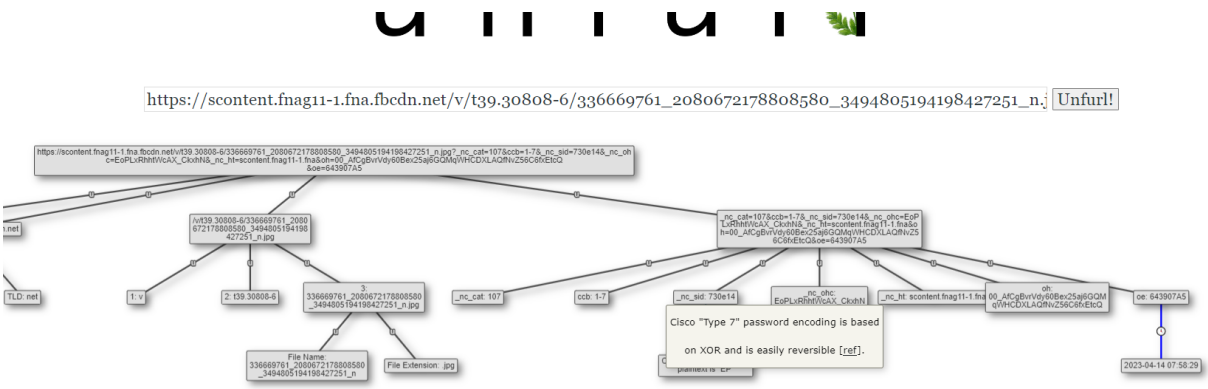
2. https://www.pexels.com/video/plants-clinging-by-the-tree-branches-in-a-forest-2882118/



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



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.

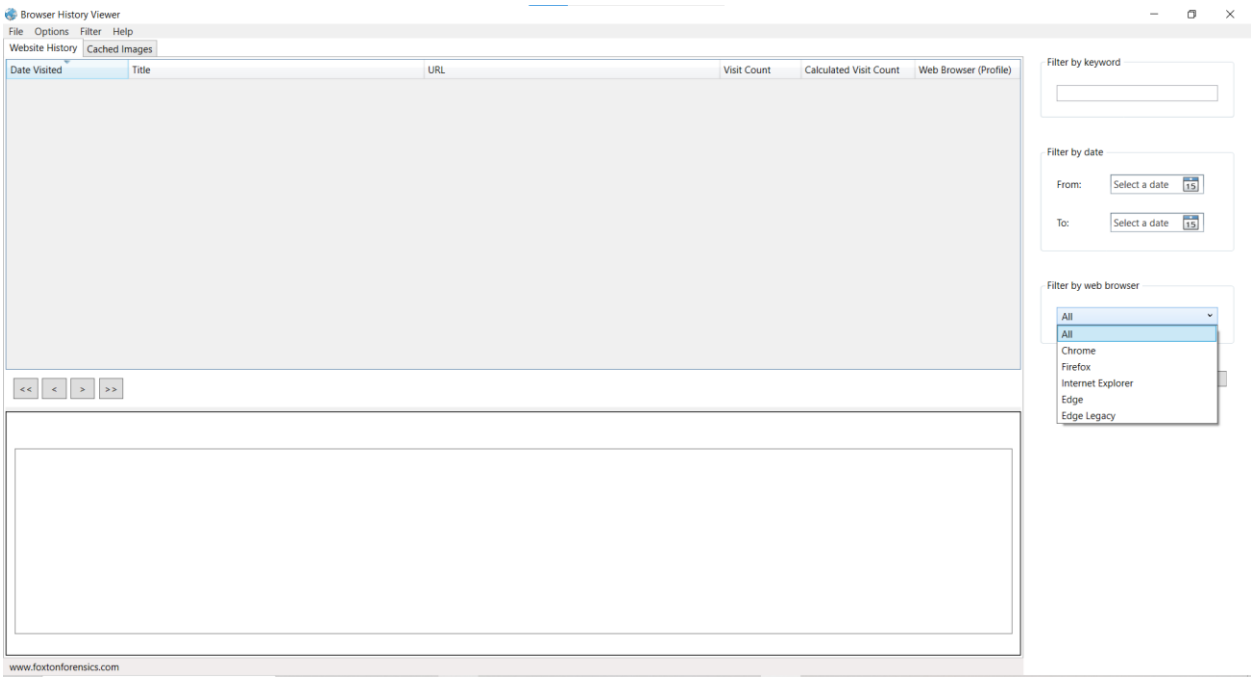
The examiner premium version has some additional features-

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

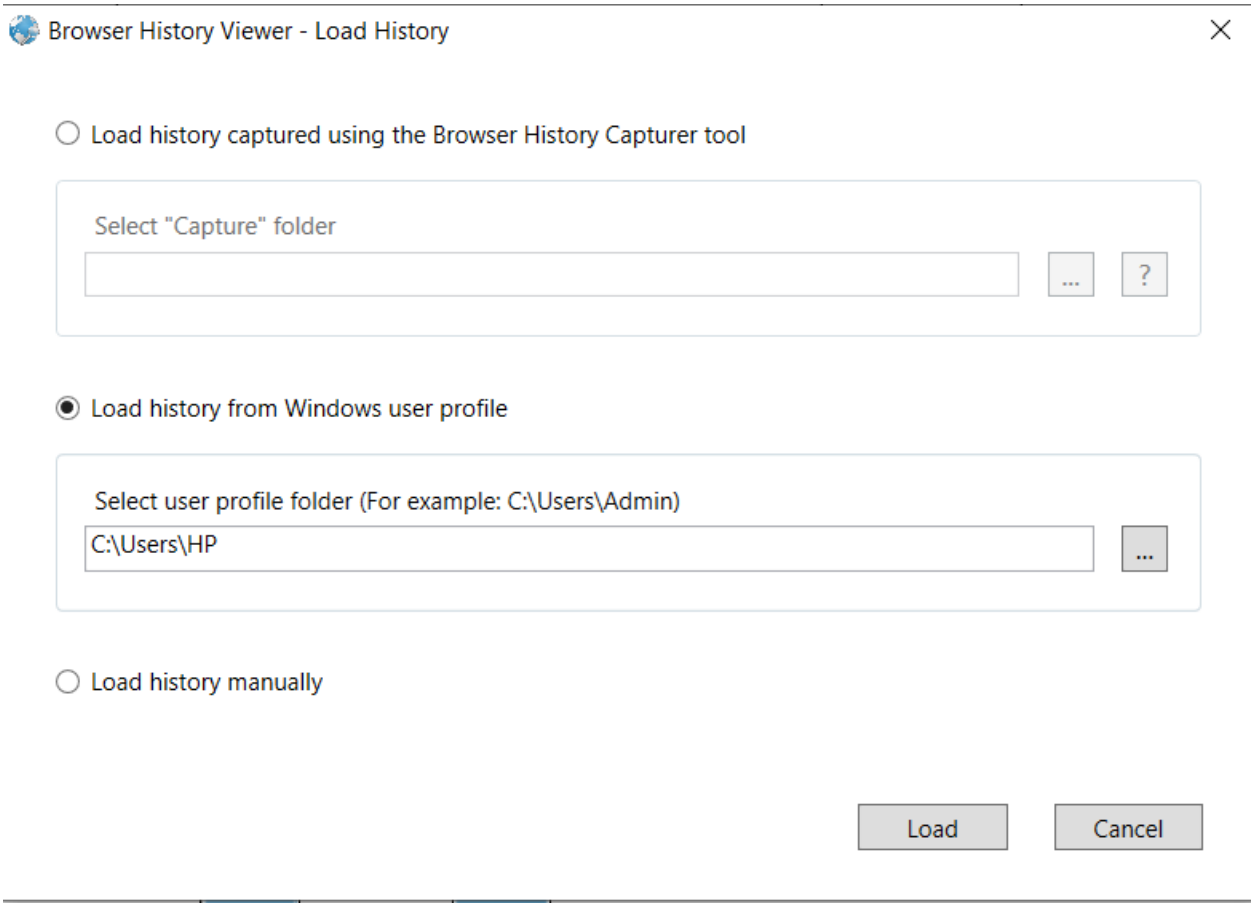
Can download the tool from –

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

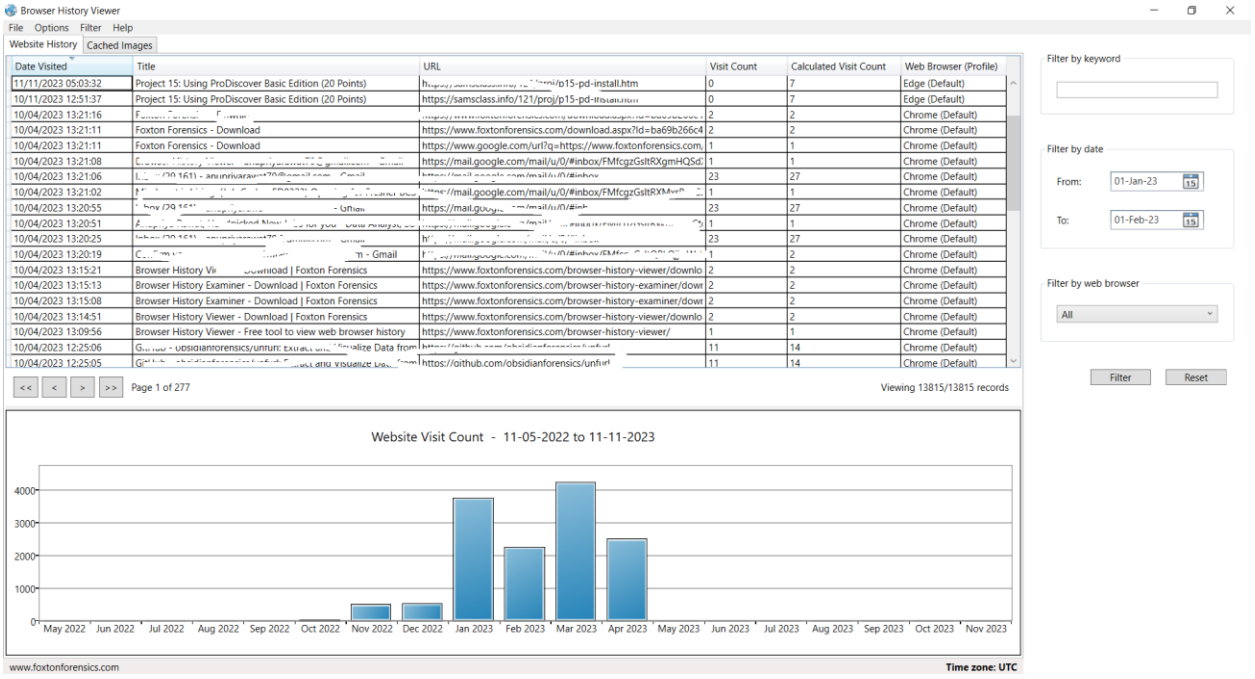
Here we can filter by keyword, timestamp, by browser –



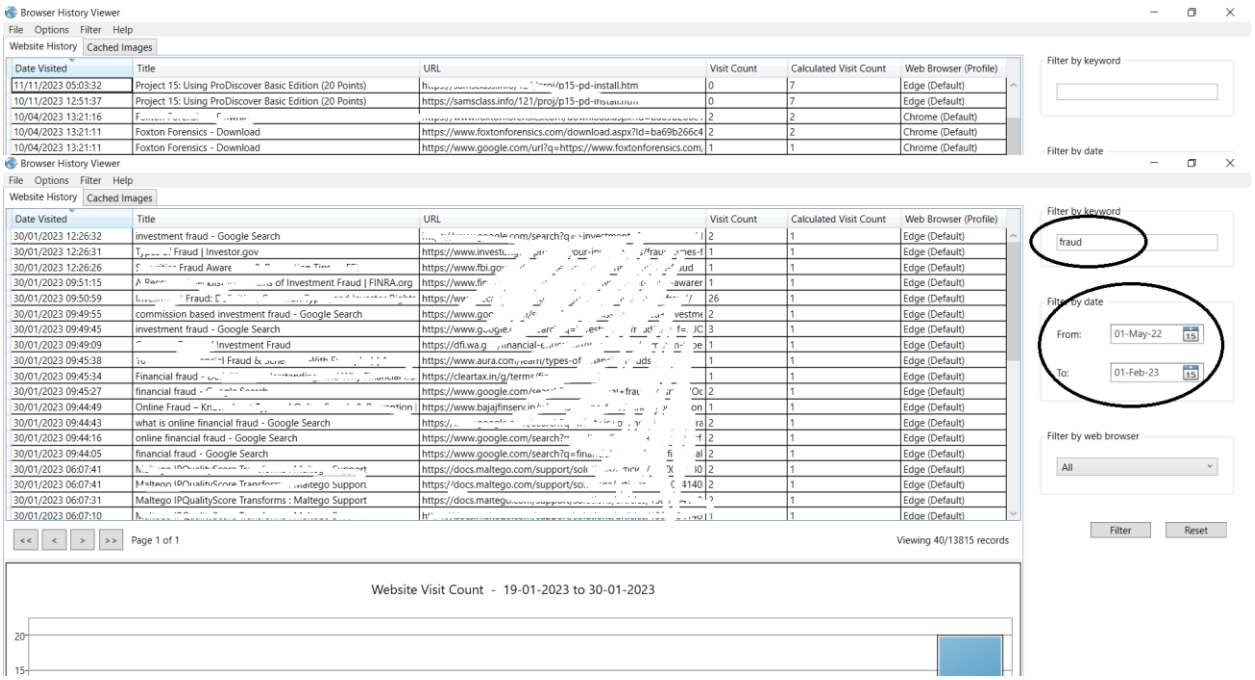
From file select – load history – choose the appropriate option.



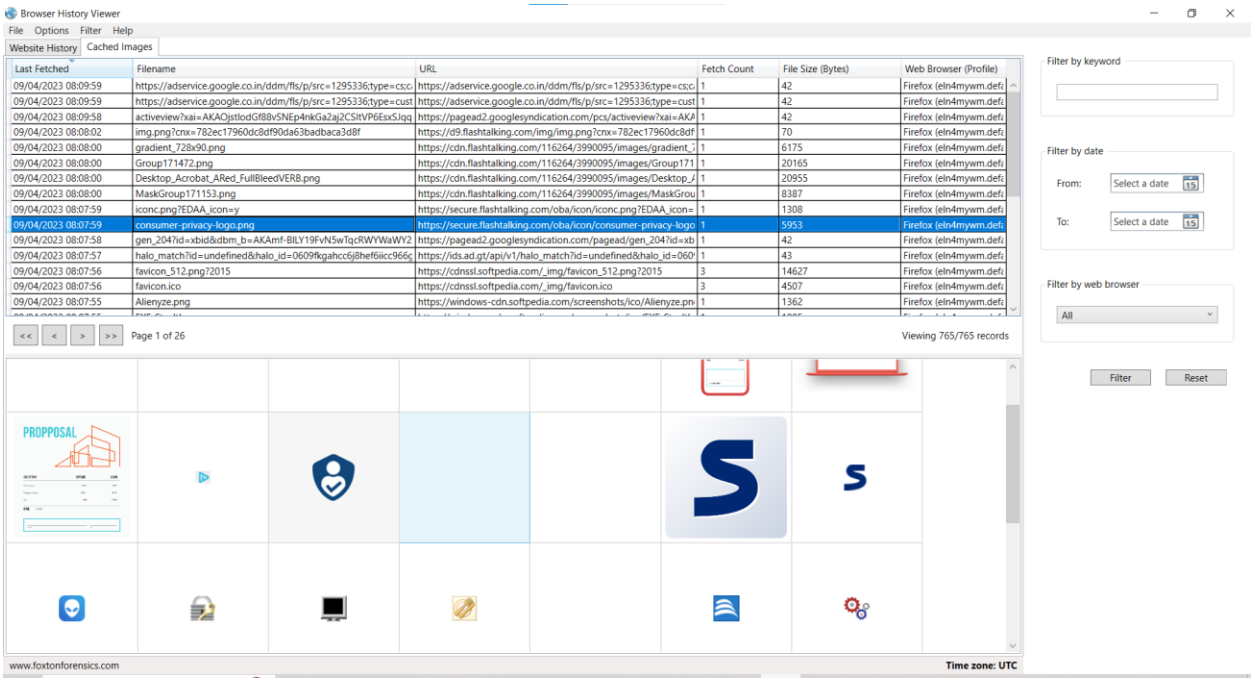
This tool retrieves all the history data with the time stamp and provides the no of counts, the graph of website visit count with times stamp.



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-



All the cached images with details-



References-

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