Digital Forensic Analyses of TOR And Web Browser Records

A Dissertation Report Submitted in partial fulfilment of the requirements for the online internship offered by Centre of Excellence in Cyber Security, JNTUH

12 WEEK ONLINE INTERNSHIP

in

CYBER SECURITY and FORENSICS

Submitted by

Tejaswi Sunarkar (20011DA817)
Ambati Bhargav (18QM1A0406)
Dasari Gokul Pavan (18BK1A0511)

Under the mentoring of

Mr.Jaya Prasad Botsa
(Senior Forensic Examiner)

Vasavi.B
(Ph.D scholar, JNTUH)

CENTRE OF EXCELLENCE CYBER SECURITY

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

Kukatpally, Hyderabad - 500 085, Telangana, India ACCREDITED BY NAAC WITH 'A' GRADE

CENTRE OF EXCELLENCE CYBERSECURITY

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

DECLARATION

We declare that the internship project work entitled "**Digital Forensic Analyses of TOR And Web Browser Records**" submitted in Center Of Excellence CyberSecurity, Jawaharlal Nehru Technological University Hyderabad, in partial fulfillment of the requirement for the award of the 12-week Online Internship in Center of Excellence Cybersecurity is a bona fide record of our own work carried out under the mentoring of **Vasavi.B,Ph.D scholar, JNTUH.**

Tejaswi Sunarkar (20011DA817)	**Ambati Bhargav** (18QM1A0406)	**Dasari Gokul Pavan** (18BK1A0511)

ACKNOWLEDGEMENT

Firstly, we would like to express our immense gratitude towards our institution Jawaharlal Nehru Technological University Hyderabad, which created a great platform to attain profound technical skills in the field of Cybersecurity, thereby fulfilling our most cherished goal.

We are very much thankful to our Professor in CSE Coordinator CoE in cybersecurity, Dr.R.Sridevi And our Mentor Mr.JayaPrasad, for extending their cooperation in doing this project in stipulated time.

We extend our heartfelt thanks to the project coordinator Vasavi Ph.D Scholar for their enthusiastic guidance throughout the course of our project.

Last but not least, our appreciable obligation also goes to all the staff members of CoE CyberSecurity department and to our fellow classmates who directly or indirectly helped us.

Sunarkar Tejaswi(20011DA817)
Ambati Bhargav(18QM1A0406)
Gokul Pavan(18BK1A0511)

ABSTRACT

Internet browsers are the most frequently used applications by the majority of personal computers. Users engage in a wide range of activities, such as browsing the internet, downloading files, utilizing social media applications, as well as accessing email accounts through a web browser. Many of the crimes committed on digital resources must be investigated through the use of web browser logs.

Such information must be included in the reports of the examiners to create one of the data obtained, particularly in crimes involving entered the URL, access times, browser type, time, downloaded files, and search words[1]. User records are stored in a variety of ways by web browsers. So, browser vendors provide a very useful feature on the browser called "Private Mode" and TOR Browser to protect end users' privacy.

The onion router (Tor) browser is one such application which not only ensures the privacy preservation goals but also provides promising anonymity. This Private Browser data can be recovered using some recovery tools. During the memory dump using FTK, based on analysis of the browsers in private mode, it was found that browser data was recoverable for all the browsers.

Keywords: Internet browsers, The onion router (Tor), memory dump, FTK imager

TABLE OF CONTENTS

1.INTRODUCTION

Web browsers are the tools that users use to perform various tasks on the Internet. Browsers are used for a variety of tasks, including information search, access to email accounts, e-commerce, banking, instant messaging, online blogs, and social networking. A web browser saves a lot of information about a user's activity. Users' visited URLs, search terms, cookies, cache files, access time, and use time are all stored in the system's memory[2]. The suspects can use web browsers for activities such as to collect information, to hide the crime, to get in touch with crime partners The evidence obtained from use of the Web browser is a key component of the forensic expert. Suspicious leaves a mark on his computer about every movement, as long as the use of a web browser [3].

Malicious users over the internet are constantly trying to steal as much data as they can for personal benefit from other users. The kind of information that can be valuable to the malicious user include but not limited to Social Security numbers, credit card numbers, online banking passwords, user email addresses, user address book, user browsing history, user download history, user search history, autocomplete information stored in browsers, user temporary internet files and user browser cookies, etc. Therefore, it is very important to ensure privacy over the internet[4].

To handle information stored at end users' systems, the different browser vendors have introduced a new feature in their browser called In Private Browsing (Internet Explorer), Private Browsing (Firefox), Incognito Window (Chrome) and Private Browsing (Safari). These vendors claim that when the feature is used, the following data is usually discarded after the browser is closed: Cookies, Temporary Internet Files, Webpage history, Form data and passwords, Anti-phishing cache, Address bar and search AutoComplete, Automatic Crash Restore (ACR) and Document Object Model (DOM) storage[5].

The internet is used by almost everyone, including suspects under investigation. A suspect may use a web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by web browsing activity is typically a crucial component of digital forensic investigations. Almost every movement of a suspect performed by using a web browser thus would leave a trace on a computer.

Thus, when an investigator analyzes the suspect's computer, this evidence can provide useful information. After retrieving data such as cookies, cache, history and download list from a suspect's computer, it is possible to analyze this evidence for websites visited, time and frequency of access, and search engine keywords used by the suspect.

In the analysis, the process should first identify the web browsers. Users can use different processes related to offenses in different web browsers.There are many web browsers it can use on the internet today. Utilization ratio of used web browsers is shown in Fig.. For doing analysis correctly, it is necessary to examine the registry of web browsers on image. The analysis of only a web browser is not enough to obtain the evidence.

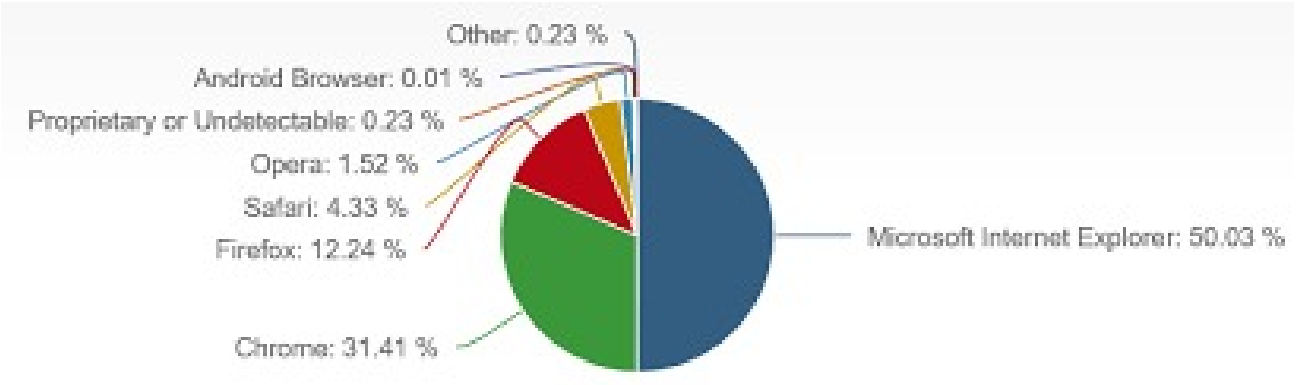


fig1.1Utilization and Analysis of Web Browser[6]

Every forensic investigation should follow a proper set of processes and procedures for the evidence to be admissible in the court of law. The process used to retrieve the evidence till getting the final results should be repeatable using the process and procedure.

Types of Evidence

During an investigation, the below are the different kinds of evidences that an investigator would be looking for [29]:

a. Surfing history:

Surfing history of a user would mainly contain typed URLs, redirects and also the number of visits to a particular site.

b. Bookmarks:

This would mainly contain shortcuts or bookmarks created to specific websites by the user.

c. Downloads:

An investigator would mainly need to check for downloaded file in the default locations, also in the user defined locations or sometimes files are downloaded to default locations and then are moved or copied to user defined locations.

d. Cookies:

These are files that contain a wealth of information about the user. It would contain information like usernames, passwords and web session information.

e. Cache:

It is a temporary area on the disk which is used to store the most recently visited website.

2. OBJECTIVE

The aim is to identify and collect evidence and essential information related to a crime from recovered traces of browsing sessions to be used for forensic investigation purposes. Browsers store a notable proportion of user data and their browsing activities that range from cached files and visited URLs to usernames and passwords used during browsing sessions. This has led to the development of private browsing modes and consequently private browsers that claim to erase all data related to a browsing session and prevent it from persisting on the device as a way to honor the privacy of its users.

The study in 2014 defined a threat model and then conducted experiments by applying common local and remote attacks to assess the security of private browsing in the four most popular browsers: Chrome, Safari, Firefox and Brave. Analysis of the results obtained brought to light a range of vulnerabilities applicable to private browsing implementations due to a couple of reasons, such as lack of control of extensions running in private mode and negligence of edge case testing. Furthermore, bookmarks and program crashes were proved to cause privacy leaks.

Objective of this research is to collect all the Tor artifacts from the registry, memory and storage of the host machine. For detailed analysis, different scenarios were also considered. In registry analysis, artifacts added or removed during installation and uninstallation were collected. While for memory and storage analysis, scenarios of browser open and closed were considered[7].

3. LITERATURE SURVEY

Browser Forensics

The Internet is used by almost everyone, including suspects under investigation. A suspect may use a Web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by Web browsing activity is typically a crucial component of digital forensic investigations. Almost every movement a suspect performs while using a Web browser leaves a trace on the computer, even searching for information using a Web browser.

Therefore, when an investigator analyzes the suspect's computer, this evidence can provide useful information. After retrieving data such as cache, history, cookies, and download list from a suspect's computer, it is possible to analyze this evidence for Websites visited, time and frequency of access, and search engine keywords used by the suspect.

Research studies and tools related to analysis of Web browser log files exist, and a number of them share common characteristics. First, these studies and tools are targeted to a specific Web browser or a specific log file from a certain Web browser. Many kinds of Web browsers provide Internet services today, so that a single user can use and compare different kinds of Web browser at the same time.

For this reason, performing a different analysis for each Web browser is not an appropriate way to detect evidence of a user's criminal activity using the Internet. Moreover, it is not sufficient to investigate a single file from a single browser because the evidence may be spread over several files[8].

PROPOSED WORK

Analyses of Web Browser Records

Web browsers are one of the most commonly used applications in digital devices. Users perform their internet activities with web browsers in different operating systems. Web browsers are used for many purposes like, searching information, e-mail, e-commerce, news, e-banking, social media and blog writing. For this reason, it is one of the most important parts of evidence analysis. Information like which URLs were visited by the user, which words were searched, when these actions were made, are used by digital forensics experts to determine the crime. Also, usage of different web browsers in the same period must be analyzed. A lot of open sources and licensed tools exist for performing analysis. Users often perform activities specified in web browsers.

Forensics is mainly performed to collect evidence based on the subject of the case. The evidence can be collected from different parts of a communication channel. Those different parts can be: Server side which stores access logs, error logs, application logs, system logs etc. Intermediate site logs which can be from firewall logs, router logs, antivirus logs, web filter logs, switch logs, network access control logs etc. Client side which stores temporary internet files, index.dat files, history.dat, cookies, favorites, HTML stored in unallocated space, registry etc.

Our main aim of the project is to analyze web browser activity Digital Forensic Analyses of TOR And Web Browser Records using FTK Imager, SQLite and HDX tools.

FTK Imager

FTK Imager is an open-source software by Access Data that is used for creating accurate copies of the original evidence without actually making any changes to it. The Image of the original evidence is remaining the same and allows us to copy data at a much faster rate, which can be soon be preserved and can be analyzed further.
Using FTK Imager in our project, we can perform

- Creating a Forensic Image
- Capturing Memory

Creating a Forensic Image

Forensic Imaging is one of the most crucial steps involved in digital forensic investigation. It is the process of making an archival or backup copy of the entire hard drive. It is a storage file that contains all the necessary information to boot to the operating system.

Capturing Memory

It is the method of capturing and dumping the contents of a volatile content into a non-volatile storage device to preserve it for further investigation. A ram analysis can only be successfully conducted when the acquisition has been performed accurately without corrupting the image of the volatile memory. In this phase, the investigator has to be careful about his decisions to collect the volatile data as it won't exist after the system undergoes a reboot

HxD

HxD is a tool that can be used to edit or modify hexadecimal values, disk content, main memory and so on. It can also export modified files and save them to the Visual Basic or C++ language form. It is freeware and available in multiple languages. The user-friendly interface of this tool can help extract data readily.

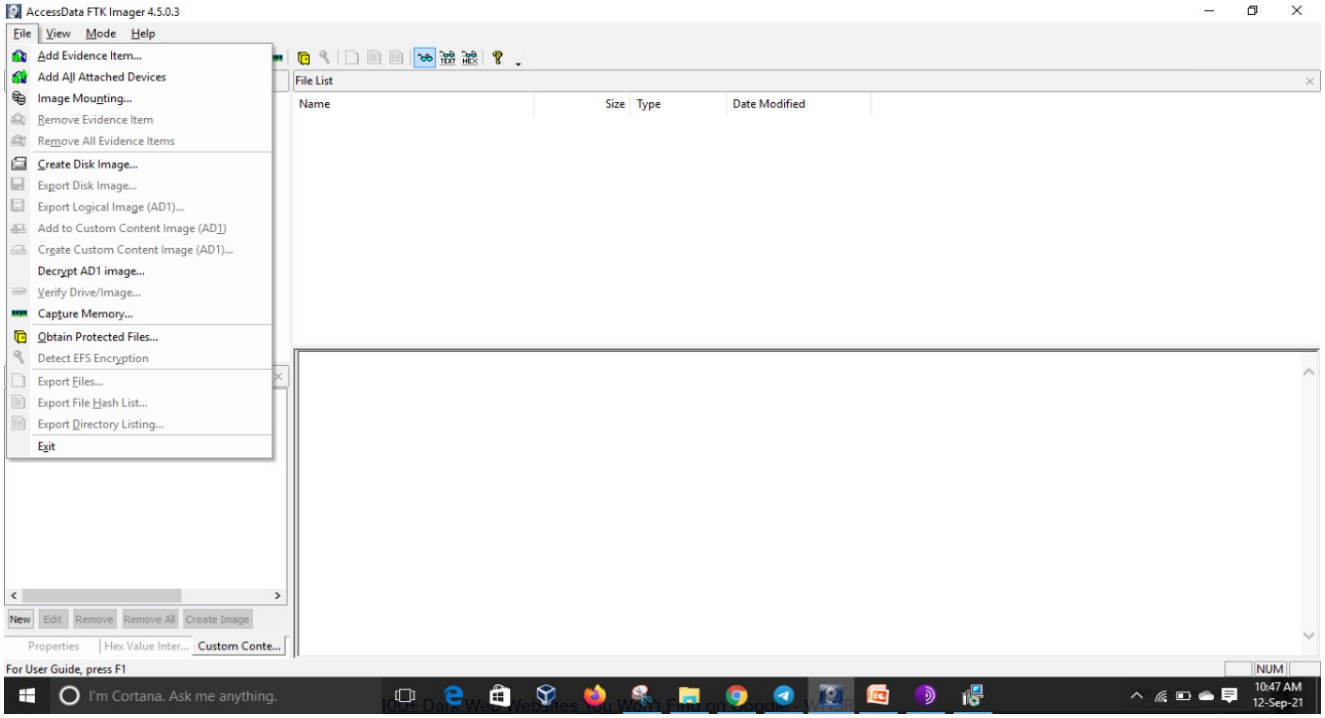
SQLite

SQLite is a forensic tool with a number of functions. It can recover complete SQLite databases, quickly scan SQLite data files, allow SQLite data type mapping, and so on. SQLite Forensic Explorer is an investigative tool designed to show every single byte of an SQLite database, journal or WAL file along with its decoded data.

IMPLEMENTATION

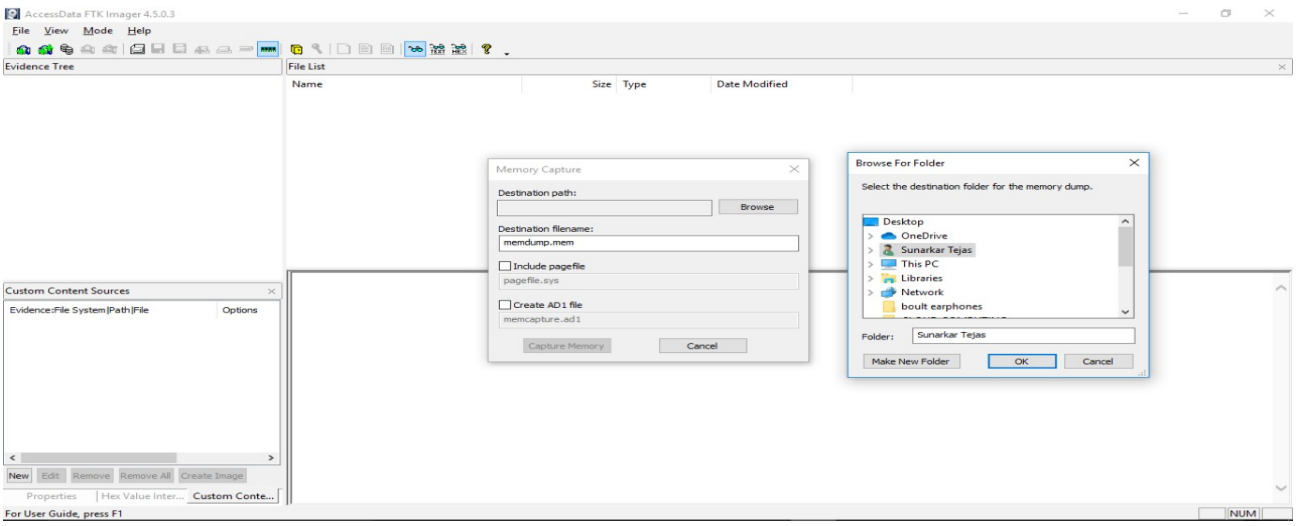
Extracting Browser Artifacts if Tor Browser using FTK tool and HXD

Analysis of TOR Browser History Data

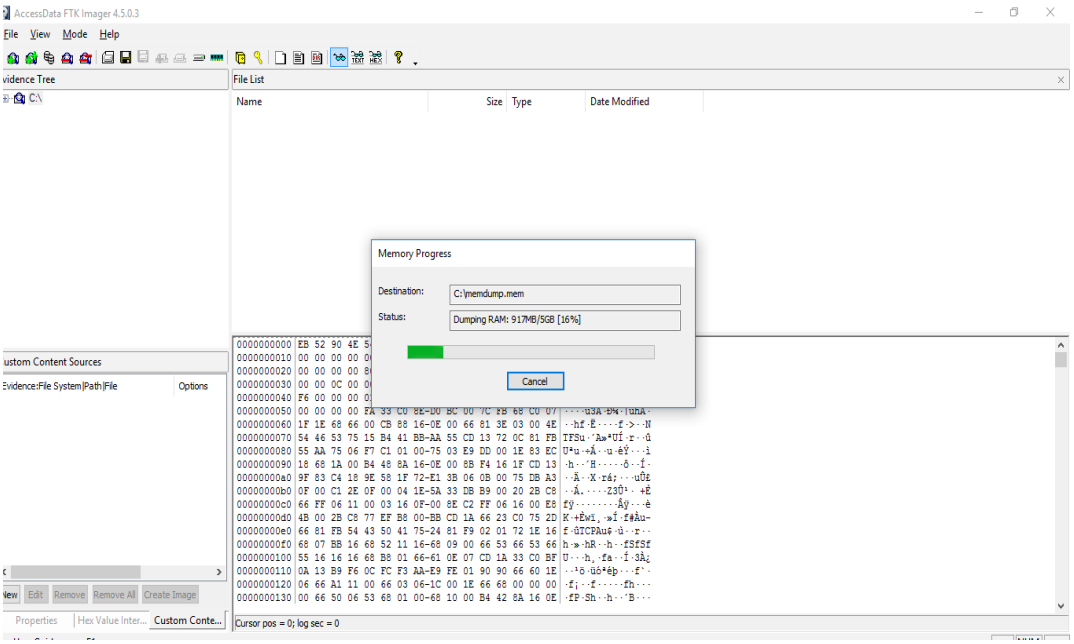


- Open FTK Imager → Click on File option and Start capturing the memory.

Capturing the memory dump

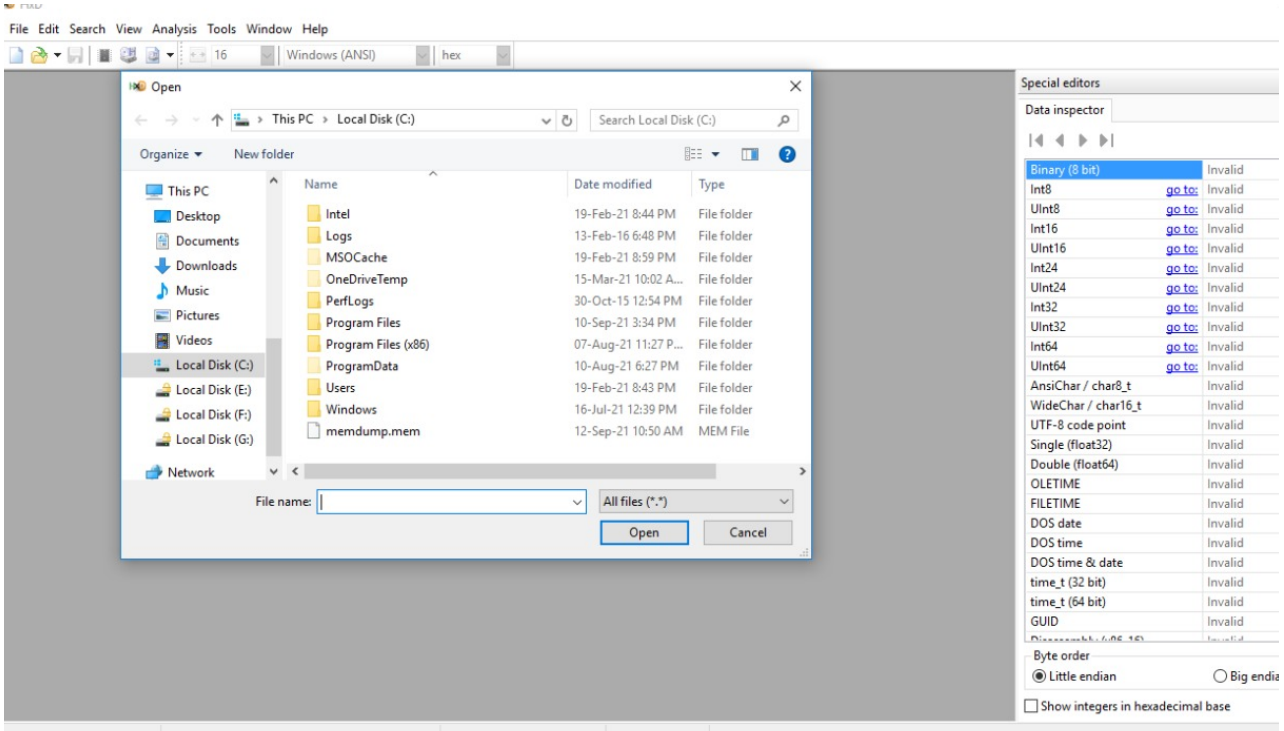


- Click one browse and save your path location
- Memory capturing starts with a running ticker memory dumping



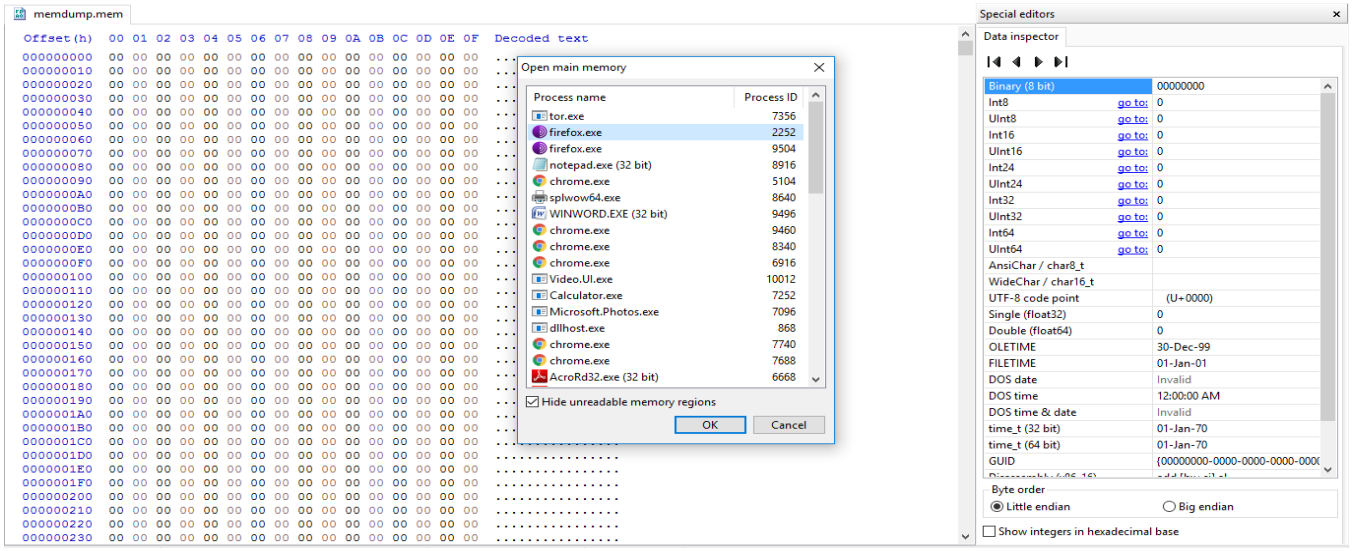
- After a successful dump I.e; extension file “memdump.mem” , proceed to next tool

HDX

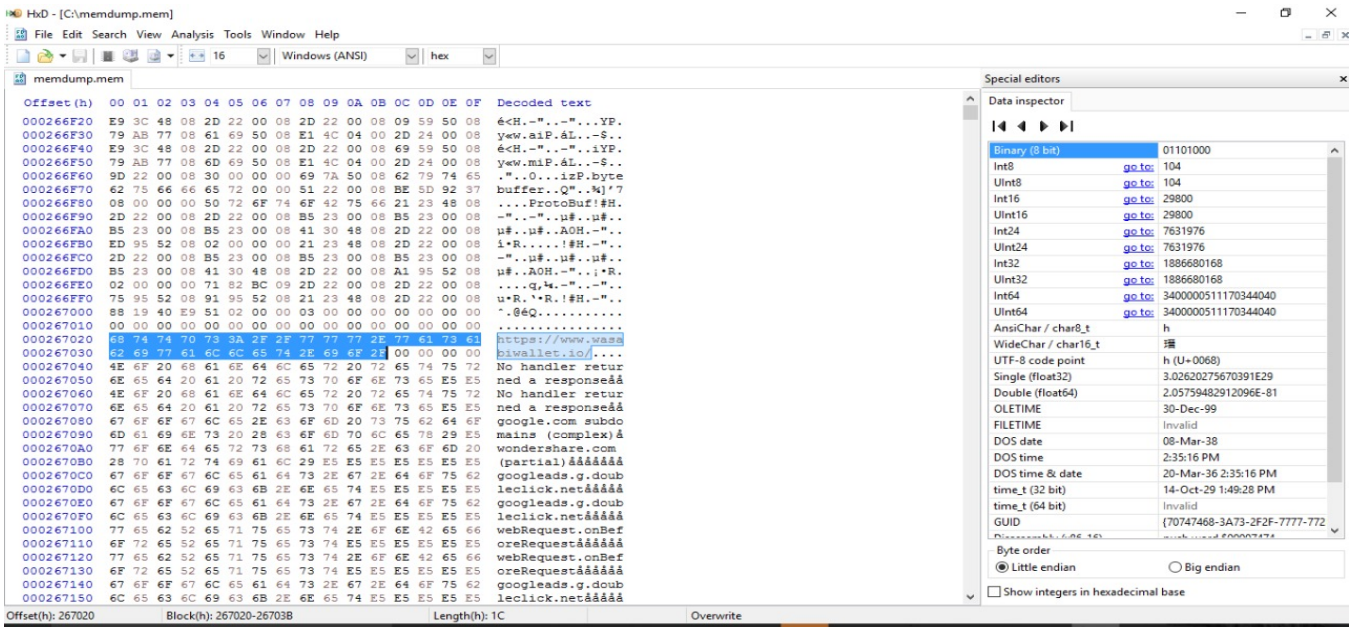


- Open HDX Tool and Click on file.
- Go to open → Select your previously saved path location.
- Open the extension file i.e; “memdump.mem”.

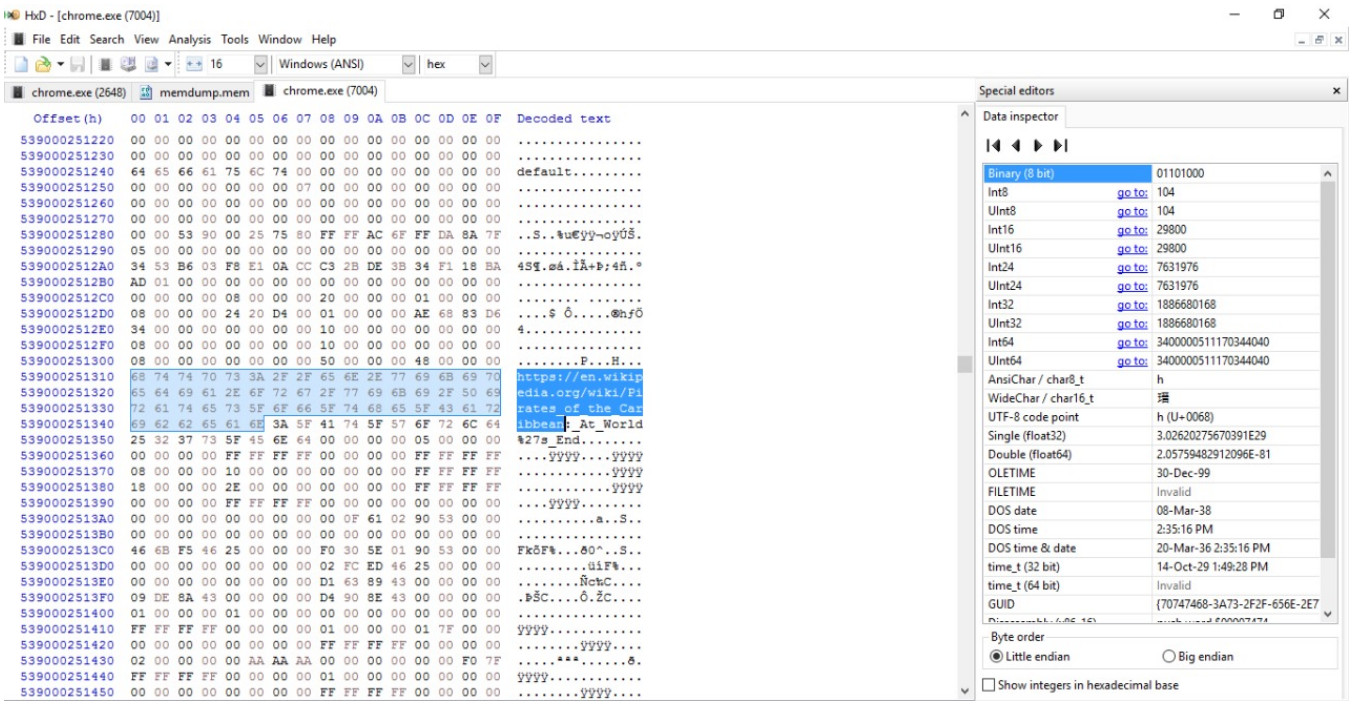
TOR BROWSER History



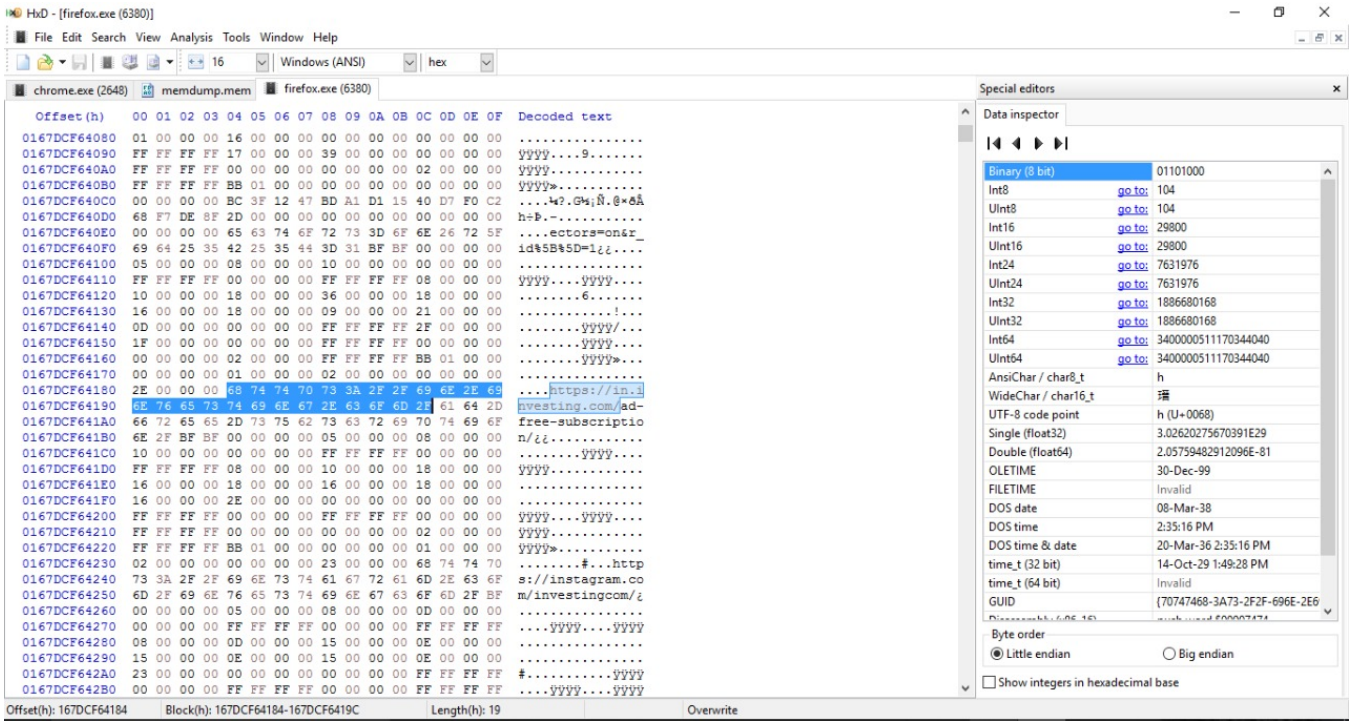
- Click on tools then main memory select your used browser then OK.
- Click on search to find and enter your domain(.com, .in, .org, .onion, .edu, etc).
- Therefore we get our domain highlighted.



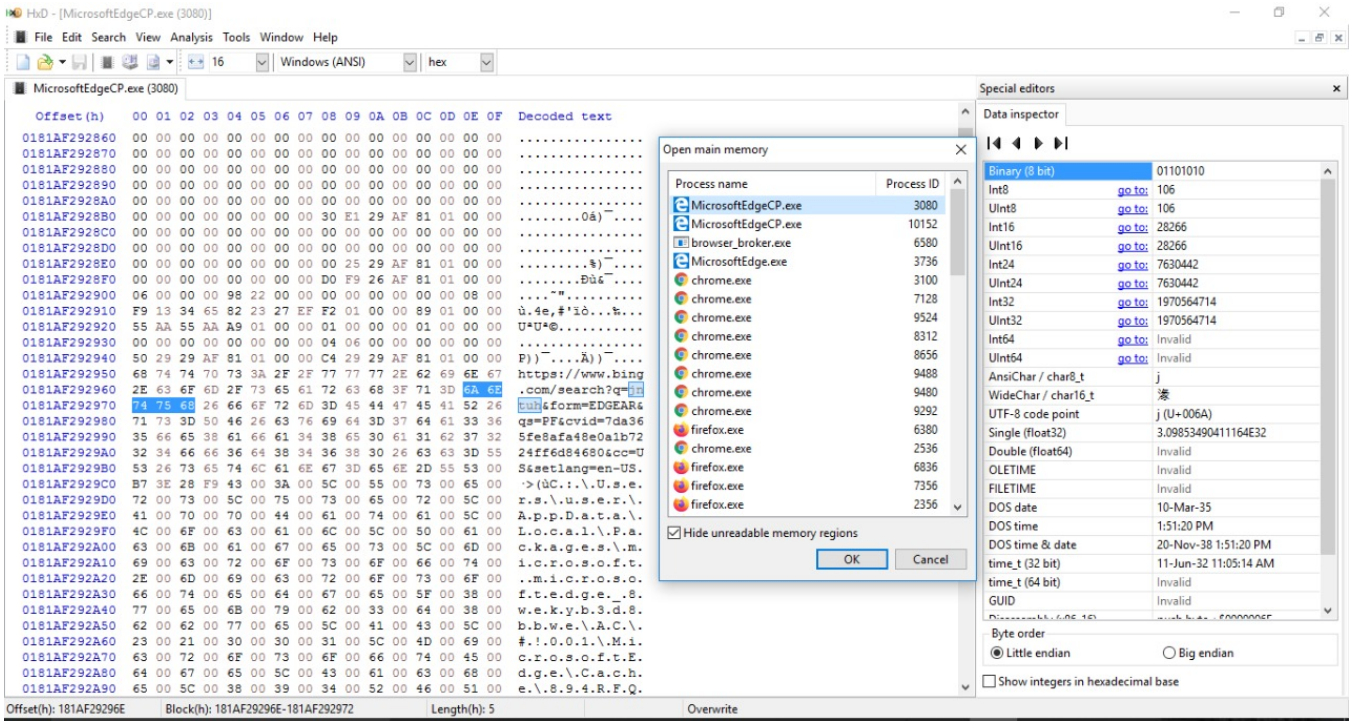
Analysis of Private Browser History of Chrome(Incognito)



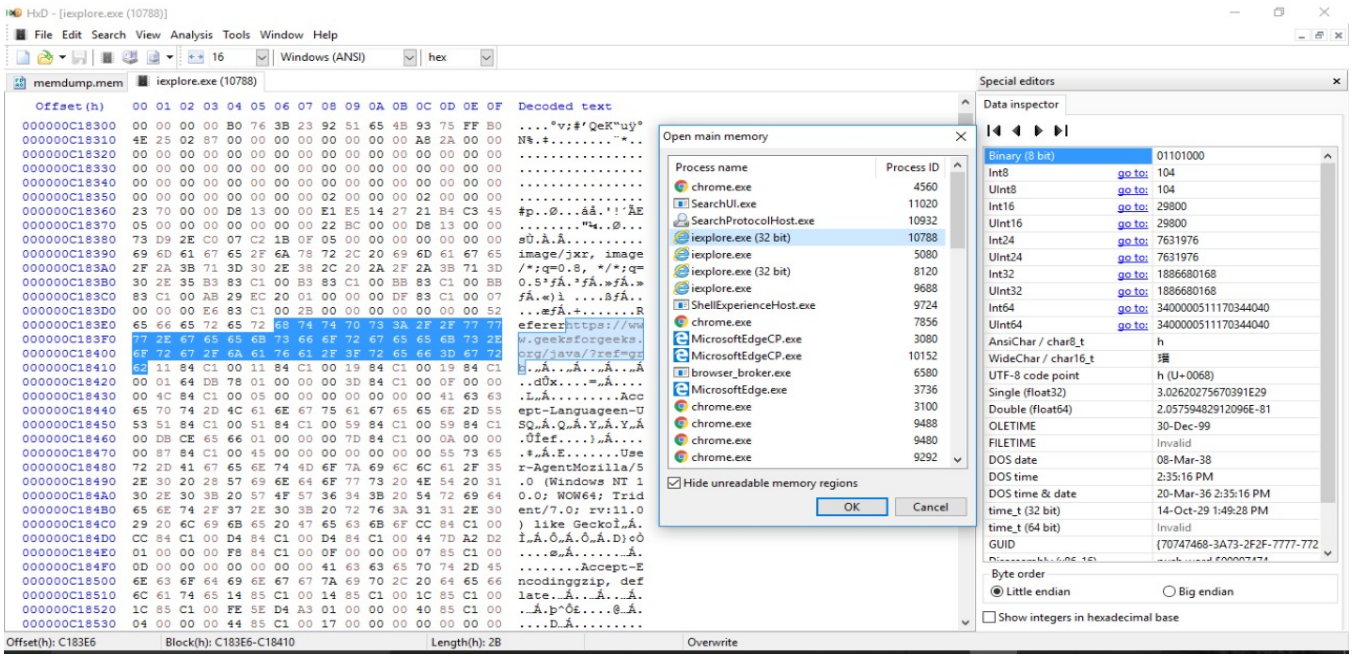
Analysis of Private Browser History of Mozilla(Private Browser)



Analysis of Private Browser History of Microsoft Edge (New PrivateWindow)



Analysis of Private Browser History of Internet Explorer (In private Browsing)



Keeping Records on Computers

Web browsers are stored in different parts of the operating system user activity. To access the user information, analysis is required in various fields. Furthermore, data varies according to web browsers type. Web browsers keep user records on 4 different sections. These are Cache Records, History Records, Cookies Registry, and Downloaded Files. The locations which are web browsers stores data on operating systems is shown on Table:-

File Location in the Web Browser Operating System

Web Browser	Operating System	File Path
Google Chrome	Windows 10	C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Preferences
	Windows 7	C:\Users\%username%\AppData\Local\Google\Chrome\User Data\Default\Preferences
	Windows XP	C:\Documents and Settings\%username%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
	Linux	/home/$USER/.config/google-chrome/Default/Preferences
	Mac OS	/Users/$USER/Library/Application Support/Google/Chrome/Default/Preferences

Table 1: File location of Google Chrome Data

Web Browser	Operating System	File Path
Firefox	Windows 10	C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Windows 7	C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Windows XP	C:\Documents and Settings\%username%\Application

		Data\Mozilla\Firefox\Profiles\%PROFILE%.default\places.sqlite
	Linux	/home/$USER/.mozilla/firefox/$PROFILE.default/places.sqlite
	Mac OS	/Users/$USER/Library/Application Support/Firefox/Profiles/$PROFILE.default/places.sqlite

Table 2: File location of Firefox Data

Web Browser	**Operating System**	**File Path**
Safari	Windows 10	\ C:\Users\%username%\AppData\Local\Apple Computer\Safari\
	Windows 7	\ C:\Users\%username%\AppData\Local\Apple Computer\Safari\
	Windows XP	C:\Documents and Settings\%username%\Local Settings\Application Data\Apple Computer\Safari\
	Mac OS	/Users/$USER/Library/Caches/com.apple.Safari/

Table 3: File location of Safari Data

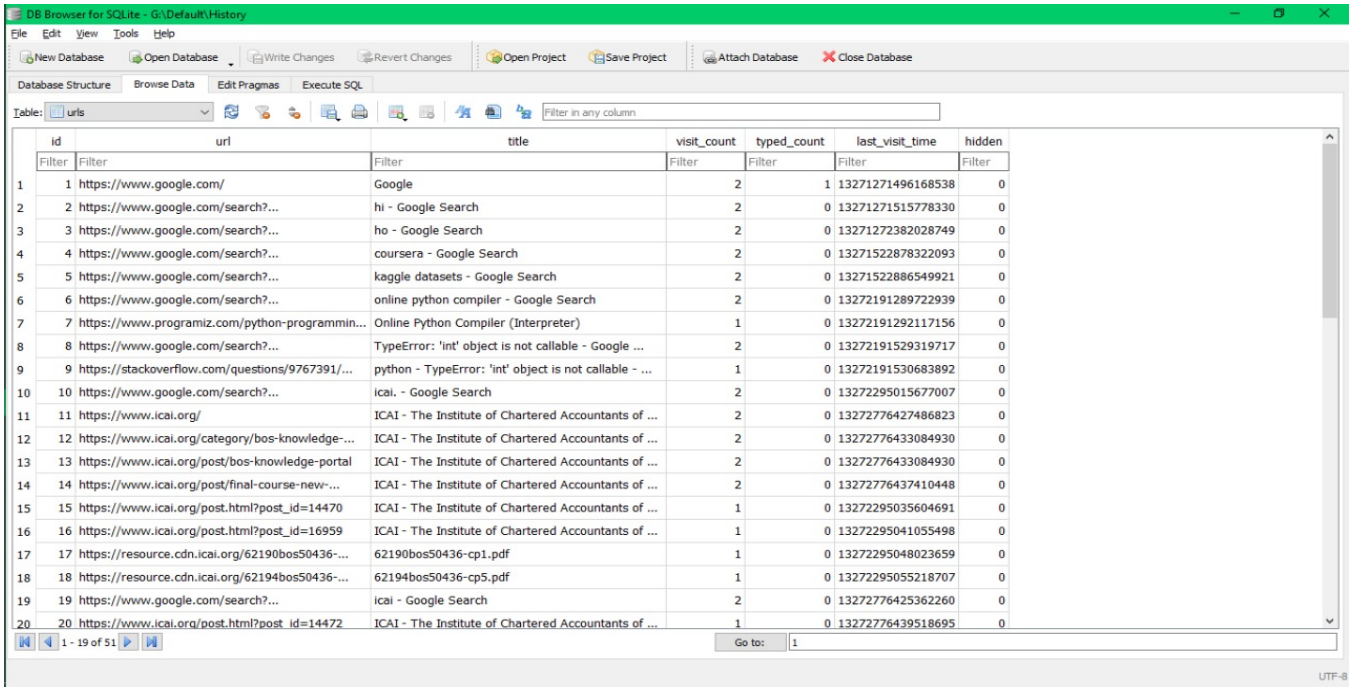
Web Browser	**Operating System**	**File Path**
Opera	Windows 10	C:\Users\%username%\AppData\Roaming\Opera\Opera\
	Windows 7	C:\Users\%username%\AppData\Roaming\Opera\Opera\
	Windows XP	C:\Documents and Settings\%username%\Application Data\Opera\Opera\
	Linux	/home/$USER/.opera/
	Mac OS	/Users/$USER/Library/Opera/

Table 4: File location of Opera Data

According to web browsers, the system stores data in different folders and locations. In the analysis process, it is necessary to examine data in different folders. Folders should be searched for in 4 different record types mentioned above. Types of storing web browsers are listed below.

Internet Explorer is a web browser which computer users use commonly. Internet activity records are stored for each user separately under the user profile folder. Data stores in Cookies, Cache, Download History and history folders separately under the locations which are shown in Table. Data stores under folders in index.dat or container.dat database files. Data is stored in binary format in this file. Safari stores web browser data in a file which is named History.plist in binary format under the web browser data locations. It stores the information of URL addresses, date of visit, time, and the number of visits for each website Firefox stores web browsers data in a file which is named places.SQLite.

The file uses the SQLite database format. Opera keeps data in different files with the extension .dat. These files are cookies4.dat, download.dat, global_history.dat, search_field_history.dat. Google Chrome stores data in the preferences file. There is a separate file for each user. There is information about user policies, master preferences, and local locations' data.


DB Browser for SQLite - G:\Default\History

File Edit View Tools Help

New Database | Open Database | Write Changes | Revert Changes | Open Project | Save Project | Attach Database | Close Database

Database Structure | Browse Data | Edit Pragmas | Execute SQL

Table: urls | Filter in any column

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.google.com/	Google	2	1	13271271496168538	0
2	2	https://www.google.com/search?...	hi - Google Search	2	0	13271271515778330	0
3	3	https://www.google.com/search?...	ho - Google Search	2	0	13271272382028749	0
4	4	https://www.google.com/search?...	coursera - Google Search	2	0	13271522878322093	0
5	5	https://www.google.com/search?...	kaggle datasets - Google Search	2	0	13271522886549921	0
6	6	https://www.google.com/search?...	online python compiler - Google Search	2	0	13272191289722939	0
7	7	https://www.programiz.com/python-programmin...	Online Python Compiler (Interpreter)	1	0	13272191292117156	0
8	8	https://www.google.com/search?...	TypeError: 'int' object is not callable - Google ...	2	0	13272191529319717	0
9	9	https://stackoverflow.com/questions/9767391/...	python - TypeError: 'int' object is not callable - ...	1	0	13272191530683892	0
10	10	https://www.google.com/search?...	icai. - Google Search	2	0	13272295015677007	0
11	11	https://www.icai.org/	ICAI - The Institute of Chartered Accountants of ...	2	0	13272776427486823	0
12	12	https://www.icai.org/category/bos-knowledge-...	ICAI - The Institute of Chartered Accountants of ...	2	0	13272776433084930	0
13	13	https://www.icai.org/post/bos-knowledge-portal	ICAI - The Institute of Chartered Accountants of ...	2	0	13272776433084930	0
14	14	https://www.icai.org/post/final-course-new-...	ICAI - The Institute of Chartered Accountants of ...	2	0	13272776437410448	0
15	15	https://www.icai.org/post.html?post_id=14470	ICAI - The Institute of Chartered Accountants of ...	1	0	13272295035604691	0
16	16	https://www.icai.org/post.html?post_id=16959	ICAI - The Institute of Chartered Accountants of ...	1	0	13272295041055498	0
17	17	https://resource.cdn.icai.org/62190bos50436-...	62190bos50436-cp1.pdf	1	0	13272295048023659	0
18	18	https://resource.cdn.icai.org/62194bos50436-...	62194bos50436-cp5.pdf	1	0	13272295055218707	0
19	19	https://www.google.com/search?...	icai - Google Search	2	0	13272776425362260	0
20	20	https://www.icai.org/post.html?post_id=14472	ICAI - The Institute of Chartered Accountants of ...	1	0	13272776439518695	0

1 - 19 of 51 | Go to: 1

UTF-8

Fig 1: Analysis of Chrome History Data

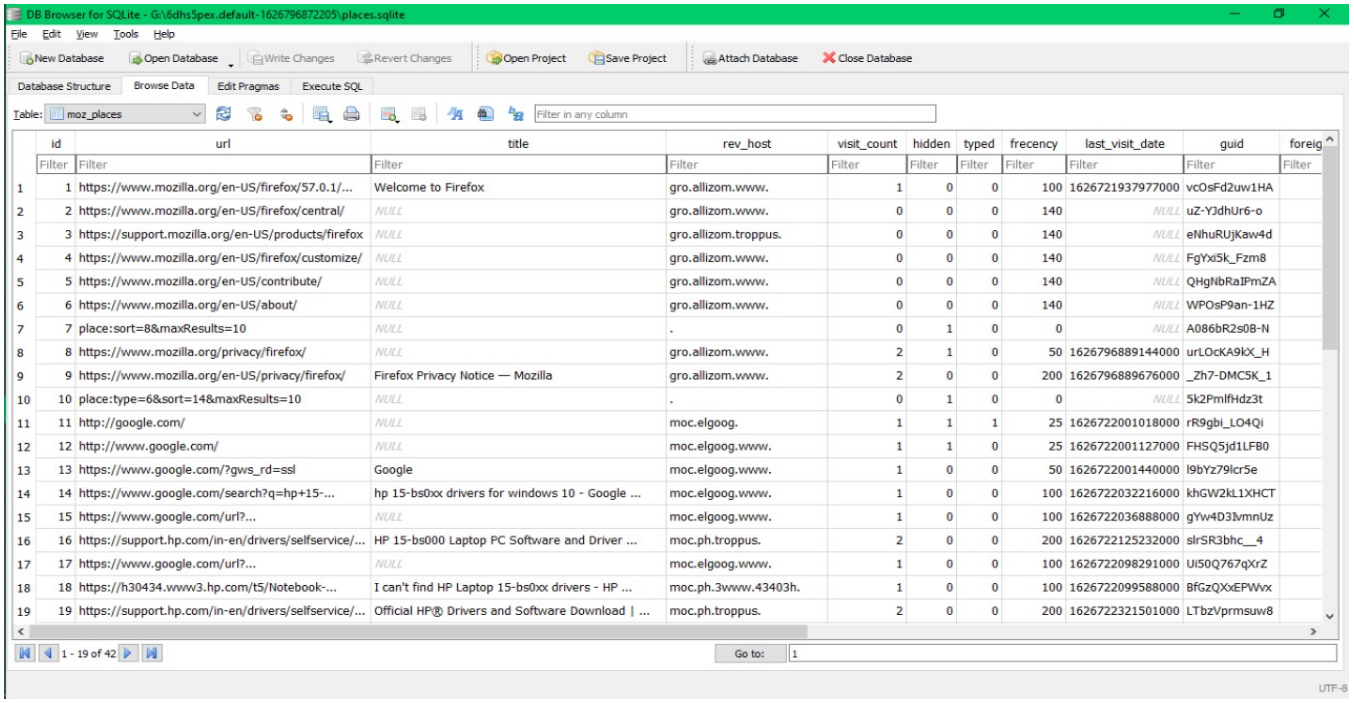


Fig 2: Analysis of FireFox History Data

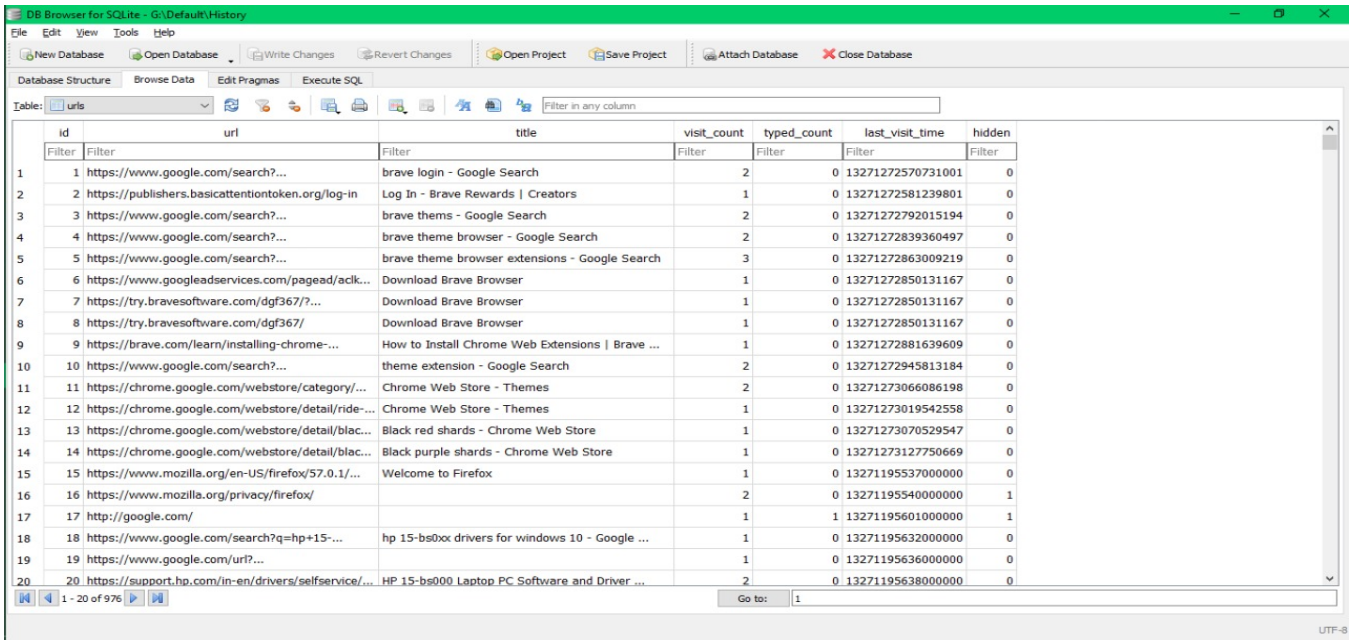


Fig 3:Analysis of Brave History Data

Download Analysis

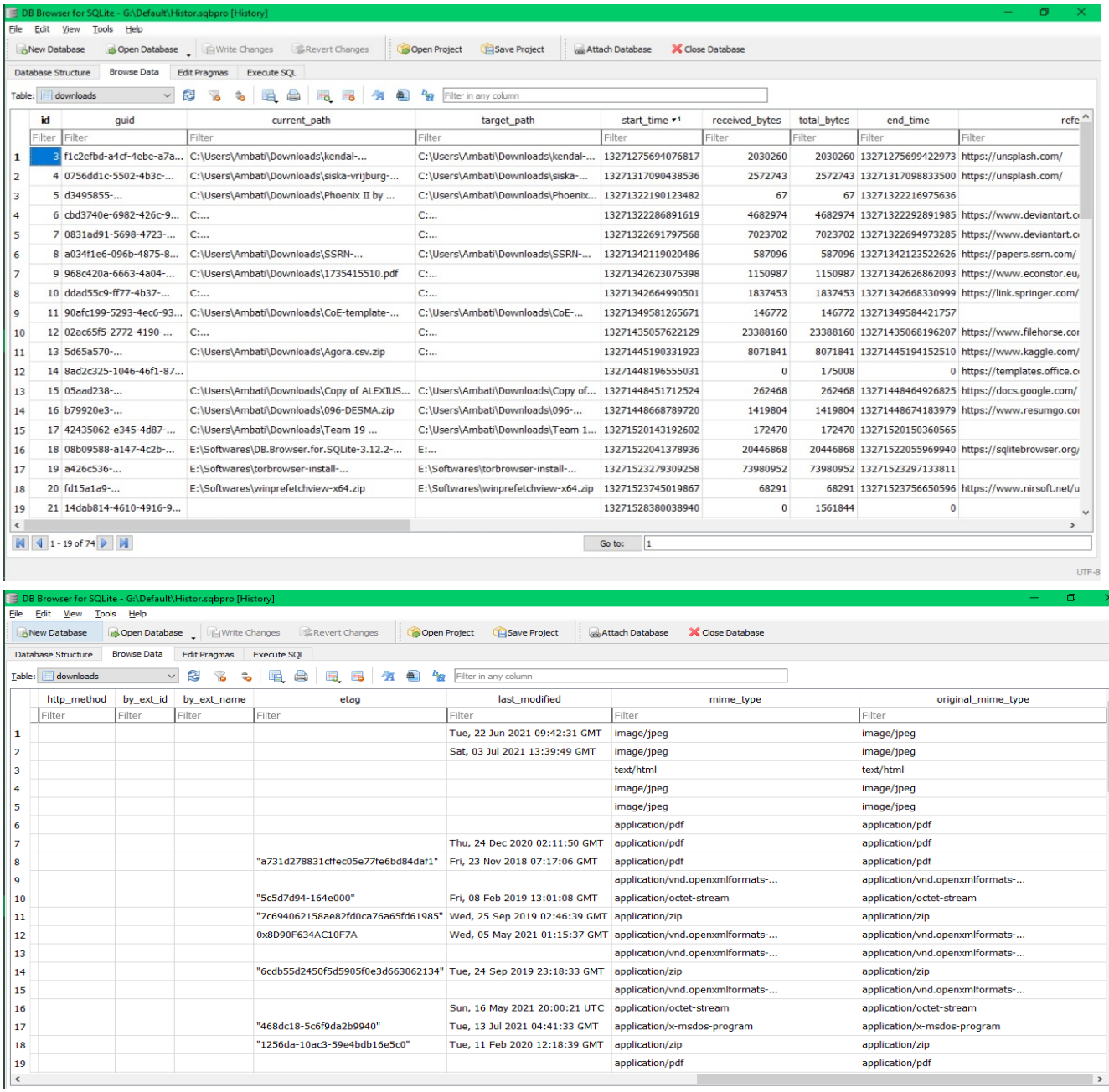
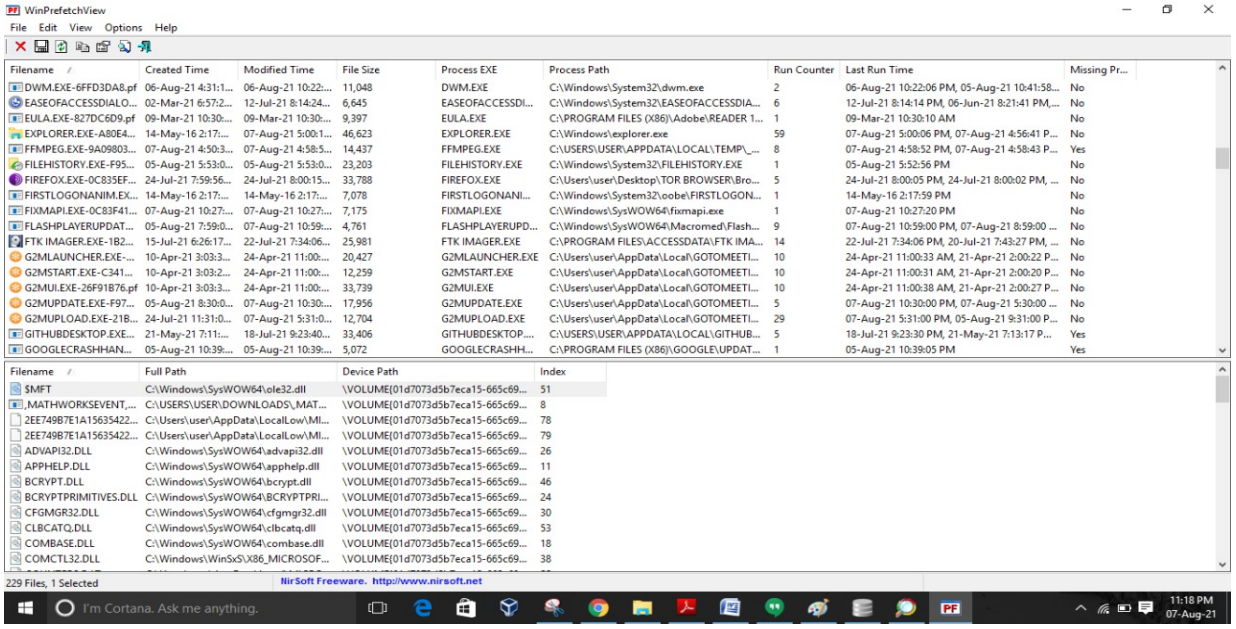


Fig 4 : Download Analysis

WinPrefetchView

WinPrefetchView is a small **process management** utility for reading the prefetch files stored in your **system** and displaying the information stored in them.
Each time that you run an application in your system, a Prefetch file that contains information about the files loaded by the app is created by the Windows operatin system.

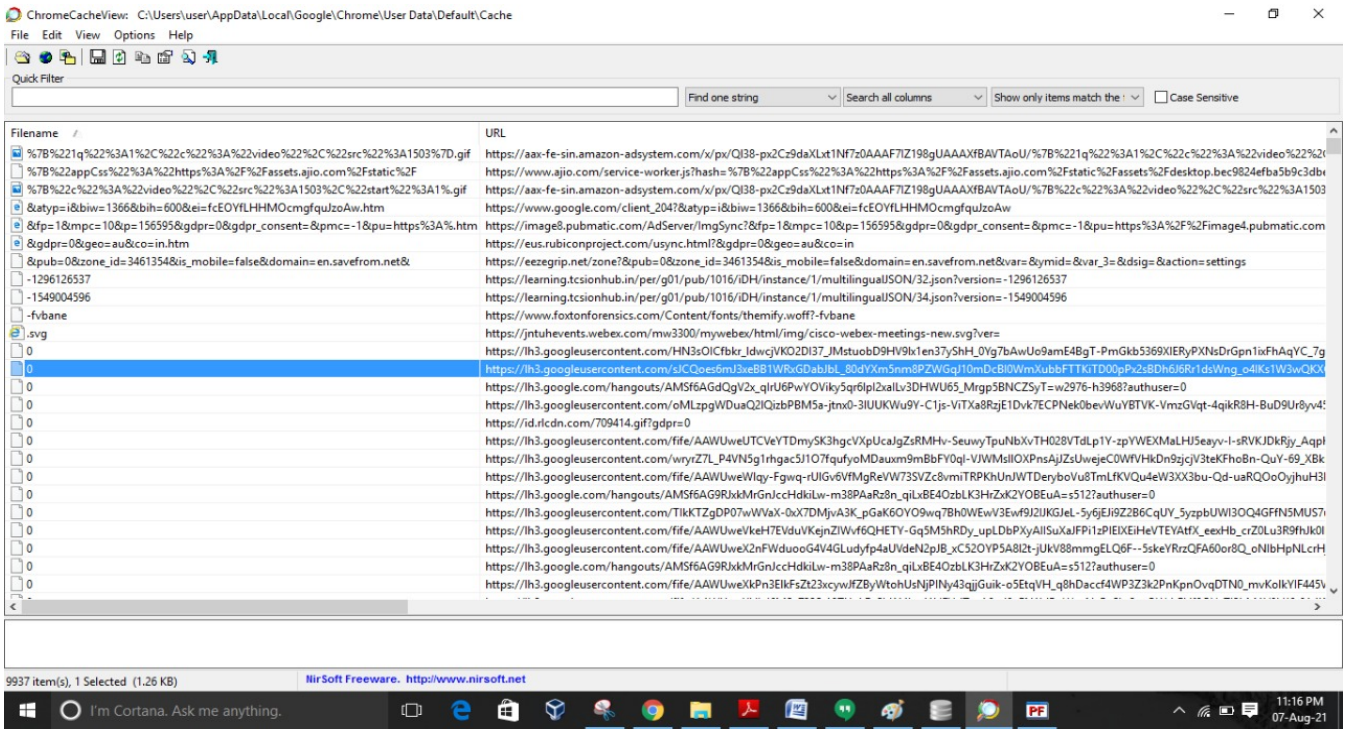
By looking in these files, you can learn which files every application is using, and which files are loaded on Windows boot. The information in the prefetch file is used for optimizing the loading time of the application the next time that you run it.

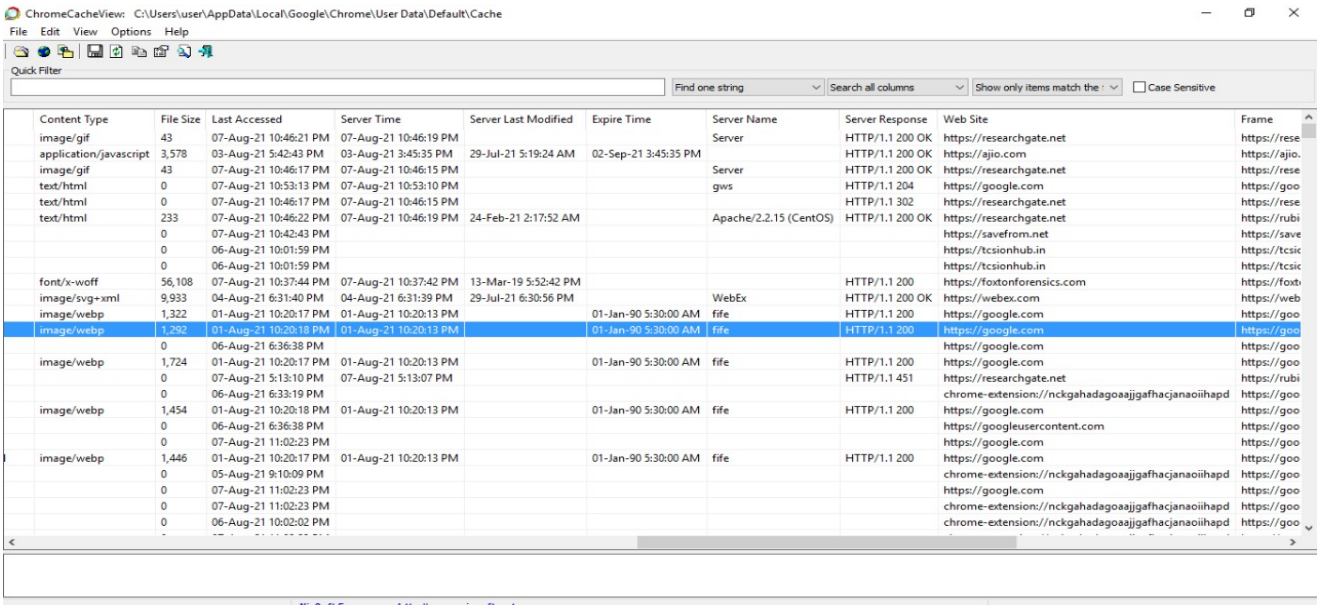


ChromeCacheView

ChromeCacheView 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. For each cache file, the following information is displayed: URL, content type, file size, last accessed time, Expiration time, Server name, Server response, and more.

You can easily select one or more items from the cache list, and then extract the files to another folder, or copy the URLs list to the clipboard.





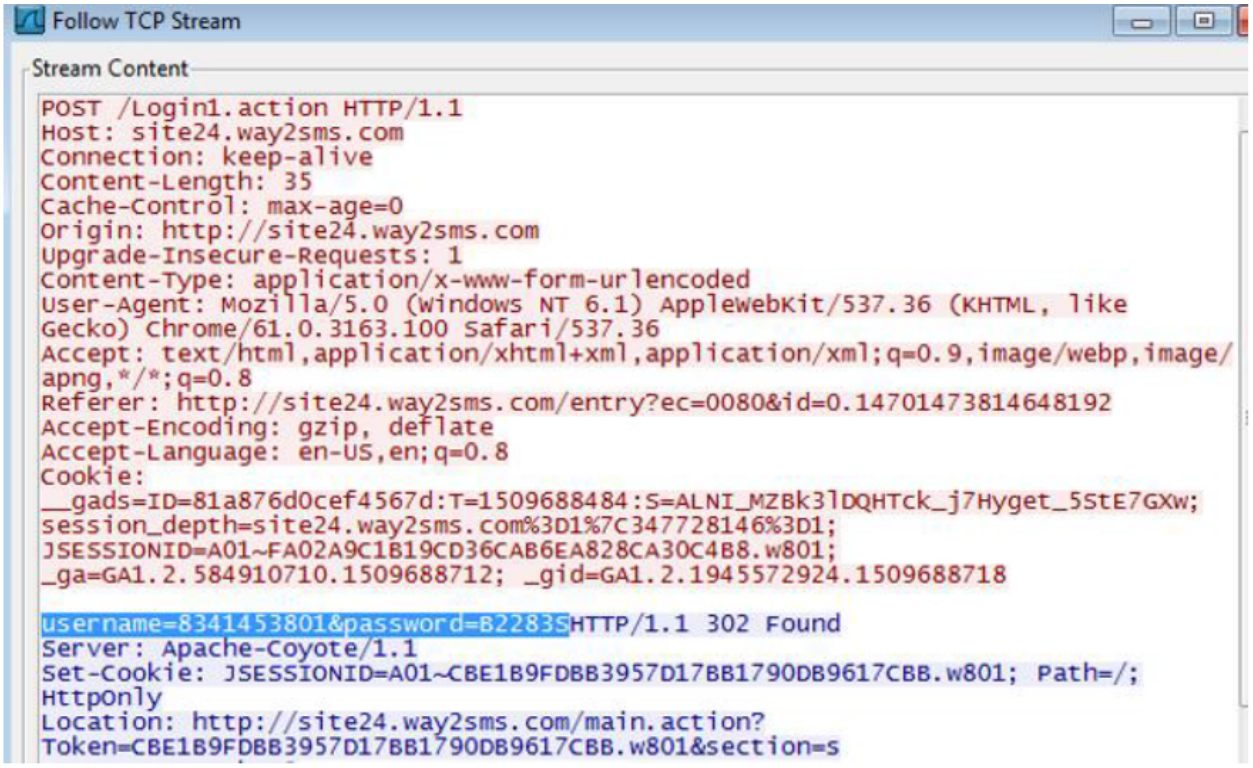
Working with sniffers for monitoring network communication (Ethereal)

Wireshark is a free and open source network protocol analyzer that enables users to interactively browse the data traffic on a computer network. The development project was started under the name Ethereal, but was renamed Wireshark in 2006.

Many networking developers from all around the world have contributed to this project with network analysis, troubleshooting, software development and communication protocols. Wireshark is used in many educational institutions and other industrial sectors.

Open Wireshark –Network Protocol Analysis

- Simultaneously open a less secure website for login
- Click on capture options and start sniffing packets
- Enter login credentials for logging into the website after starting the sniffer
- After logging in, stop the running live capture
- Observe the packets using filter
- Enter HTTP in the filter which shows HTTP packets as a result
- Search for login application packet
- When found, right click on it and click on "follow TCP Stream"
- A new window will be opened which shows the login credentials we have entered, since the website is not secure.



RESULTS

Web browser analysis is one of the most important processes in digital forensics. Most of the crimes committed through computer systems are performed via web browsers and a lot of crimes are revealed by this analysis. Digital forensics experts must know how web browsers save data in different operating systems to be able to collect evidence from web browsers. Obtaining search history of the suspect, search words, visited URLs, download history and cache data is very important for gathering evidence. Information obtained from user files reveals whether the offense occurred or not. Therefore, experts must analyze browser data correctly.

CONCLUSION

In this paper it is shown how most commonly used web browsers store data, what information can be recovered or analyzed and how different operating systems store records. Besides, applications which can be used by experts who perform analysis in this field, are introduced. Thus, it is put forward which data will be obtained and analyzed by expert in this field

FUTURE SCOPE

Future work could be to assess the effectiveness of the popular privacy eraser software to check if they would actually get rid of all the browsing history related information. Additionally, further assessment can be performed for the remaining browsers in the market. With a shift in users heavily adopting mobile devices, there have been browsers developed specifically for mobile devices. Performing analysis of these browsers in normal mode and private mode would be a good area for future analysis.

References

[1] http://www.jsoftware.us/vol11/170-CS019.pdf

[2] https://www.researchgate.net/publication/330926008_Firefox_Browser_Forensic_Analysis_via_Recovery_of_SQLite_Artefacts_from_Unallocated_Space

[3] https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=9474&context=theses#:~:text=The%20main%20aim%20of%20Chrome,itself%20running%20with%20limited%20privileges.

[4] https://support.microsoft.com/en-us/microsoft-edge/browse-inprivate-in-microsoft-edge-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2

[5] https://www.google.com/search?q=Utilization+ratio+of+web+browsers&rlz=1C1CHBD_enIN941IN941&sxsrf=AOaemvJAOVSL7h1a6xRNzGy9RiBEfmk1Zw:1631802674126&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiQzebV2oPzAhXI8HMBHW26Bc4Q_AUoAXoECAEQAw&biw=1366&bih=657&dpr=1

[6] https://www.researchgate.net/publication/332004753_Forensic_Analysis_of_Tor_Browser_A_Case_Study_for_Privacy_and_Anonymity_on_the_Web

[7] https://www.usenix.org/legacy/event/sec10/tech/full_papers/Aggarwal.pdf

[7] https://www.researchgate.net/publication/330926008_Firefox_Browser_Forensic_Analysis_via_Recovery_of_SQLite_Artefacts_from_Unallocated_Space