

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	1
2) OBJECTIVE.....	4
3) LITERATURE SURVEY.....	5
4) PROPOSED WORK.....	6
5) IMPLEMENTATION.....	8
6) RESULTS.....	21
7) CONCLUSION.....	22
8) FUTURE SCOPE.....	23
9) REFERENCES.....	24

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.

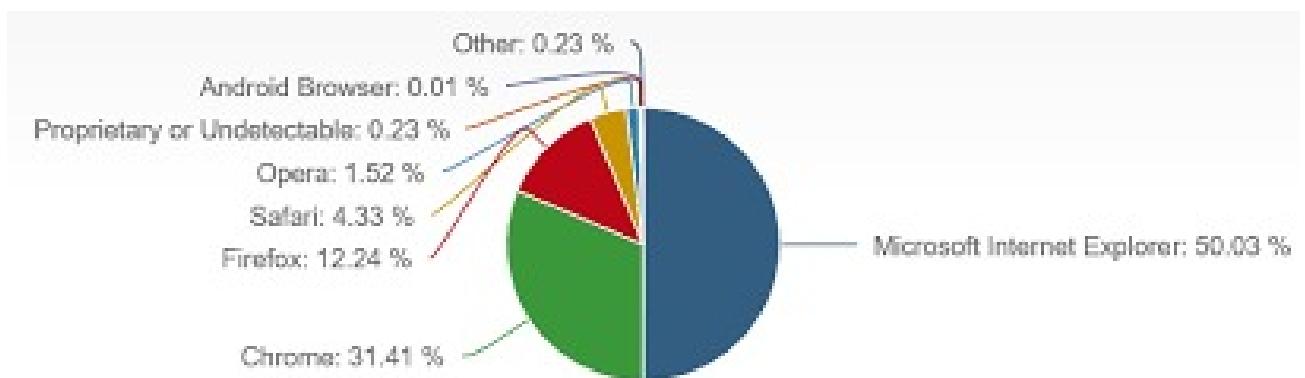


fig1.1Utilization and Analysis of Web Browser[[6](#)]

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.

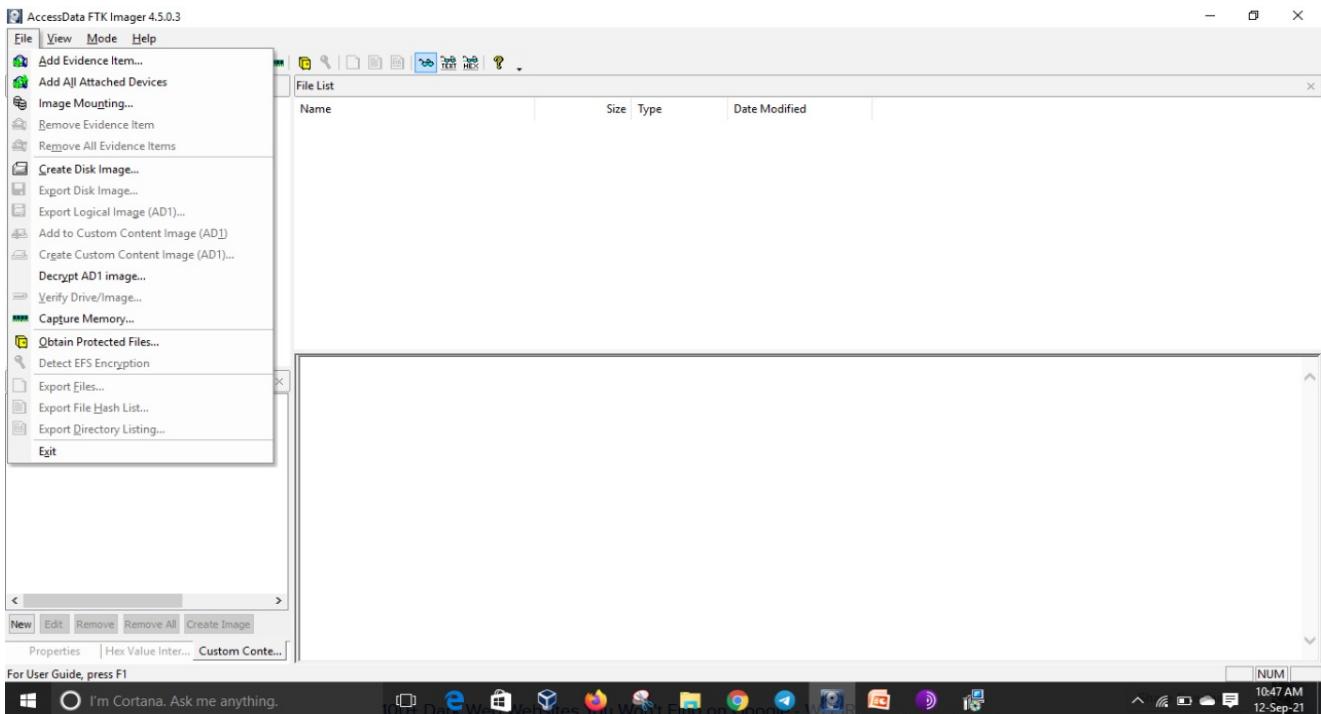
SQLite

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

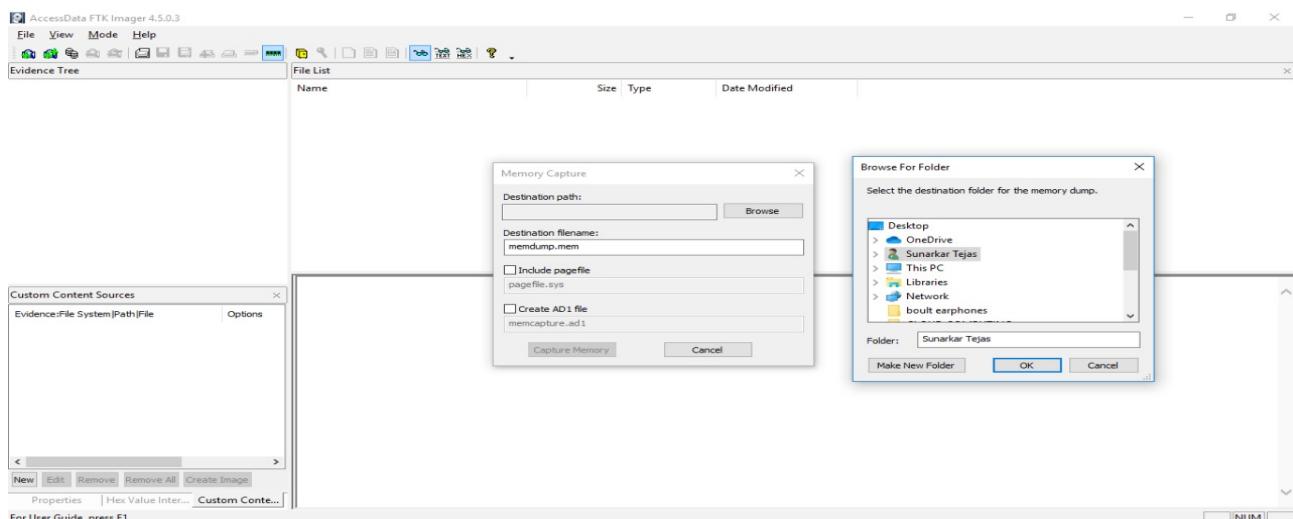
Extracting Browser Artifacts if Tor Browser using FTK tool and HXD

Analysis of TOR Browser History Data

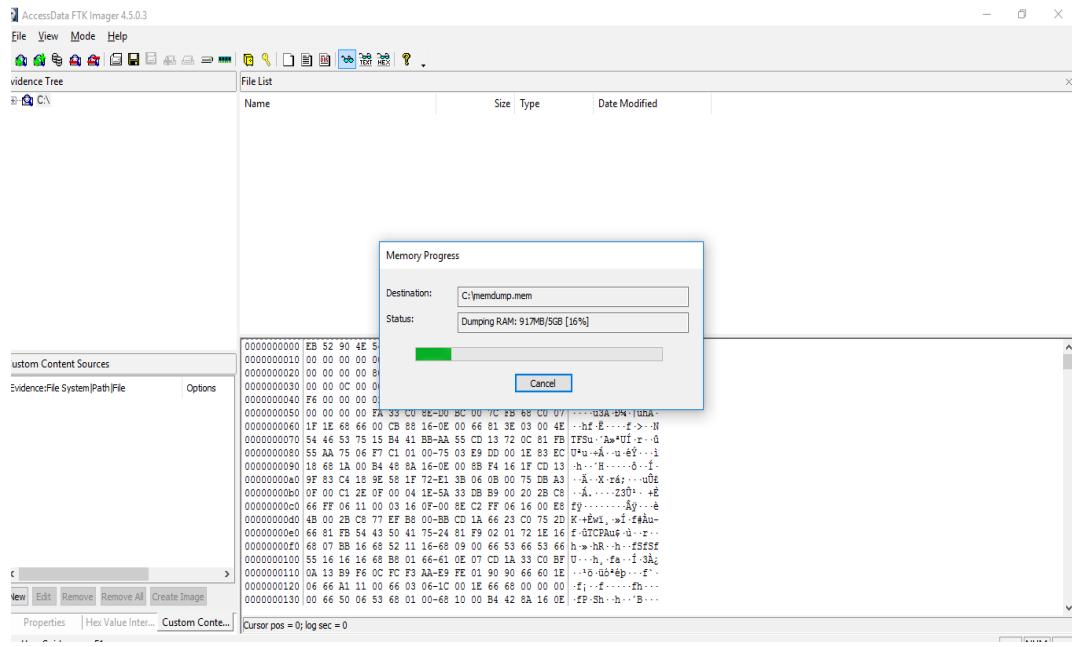


- Open FTK Imager → Click on File option and Start capturing the memory.

Capturing the memory dump

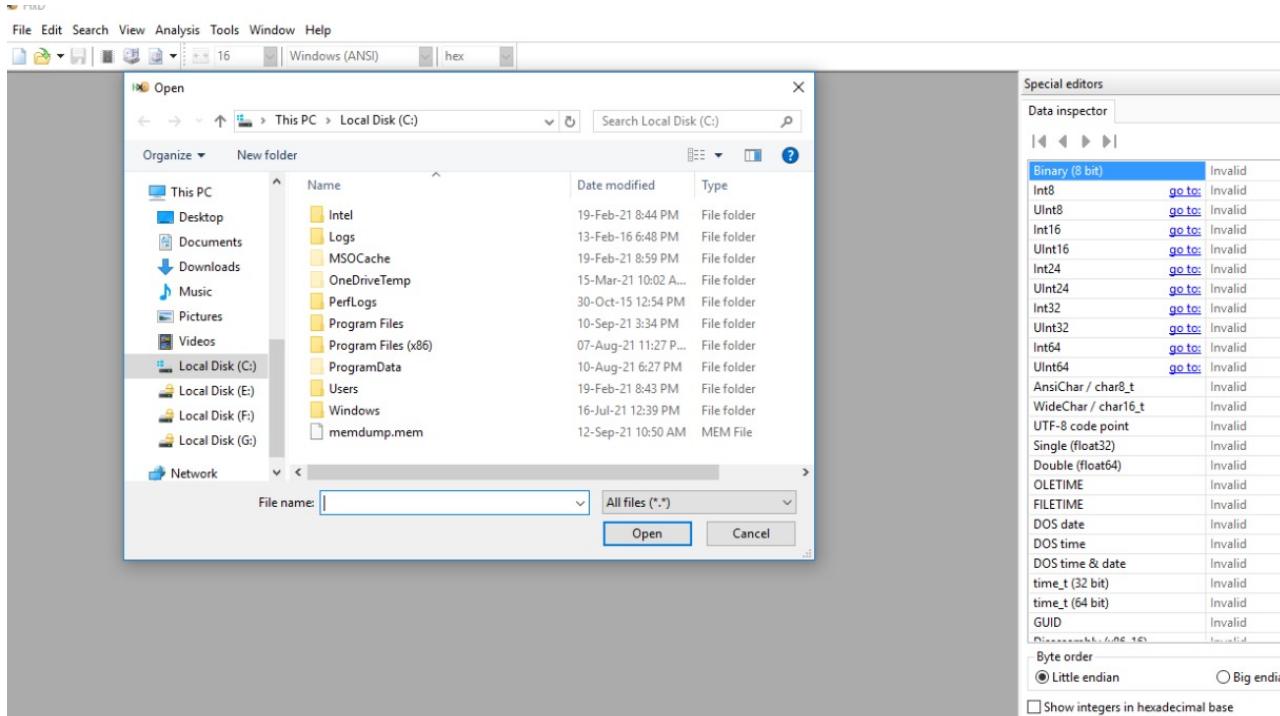


- Click one browse and save your path location
- Memory capturing starts with a running ticker memory dumping



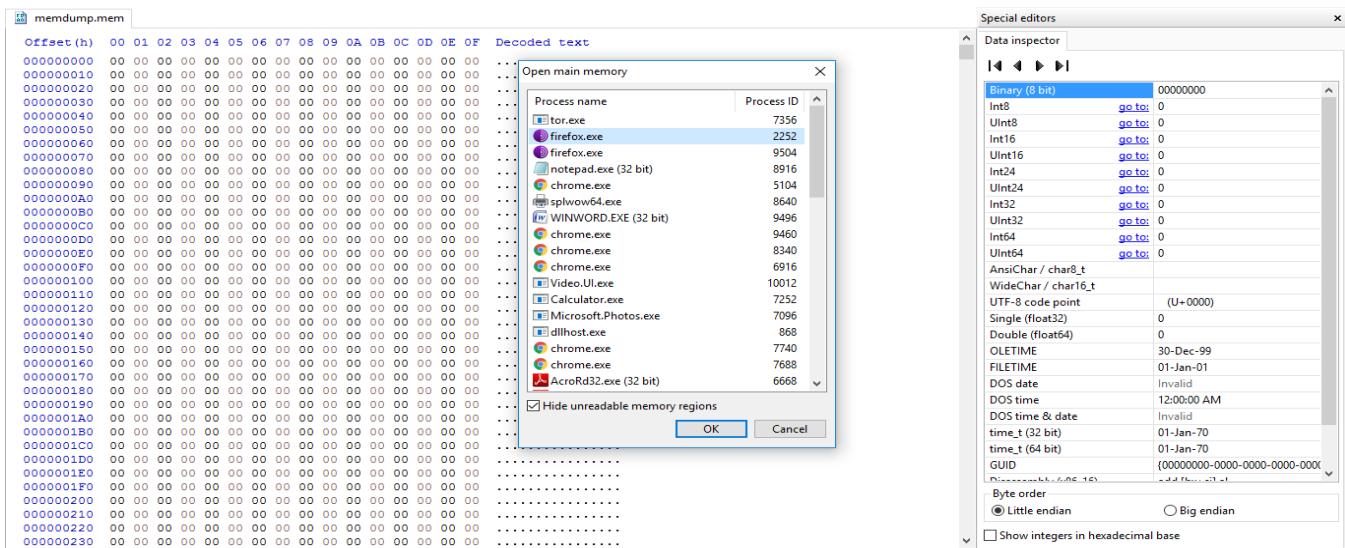
- After a successful dump I.e; extension file “memdump.mem” , proceed to next tool

HDX

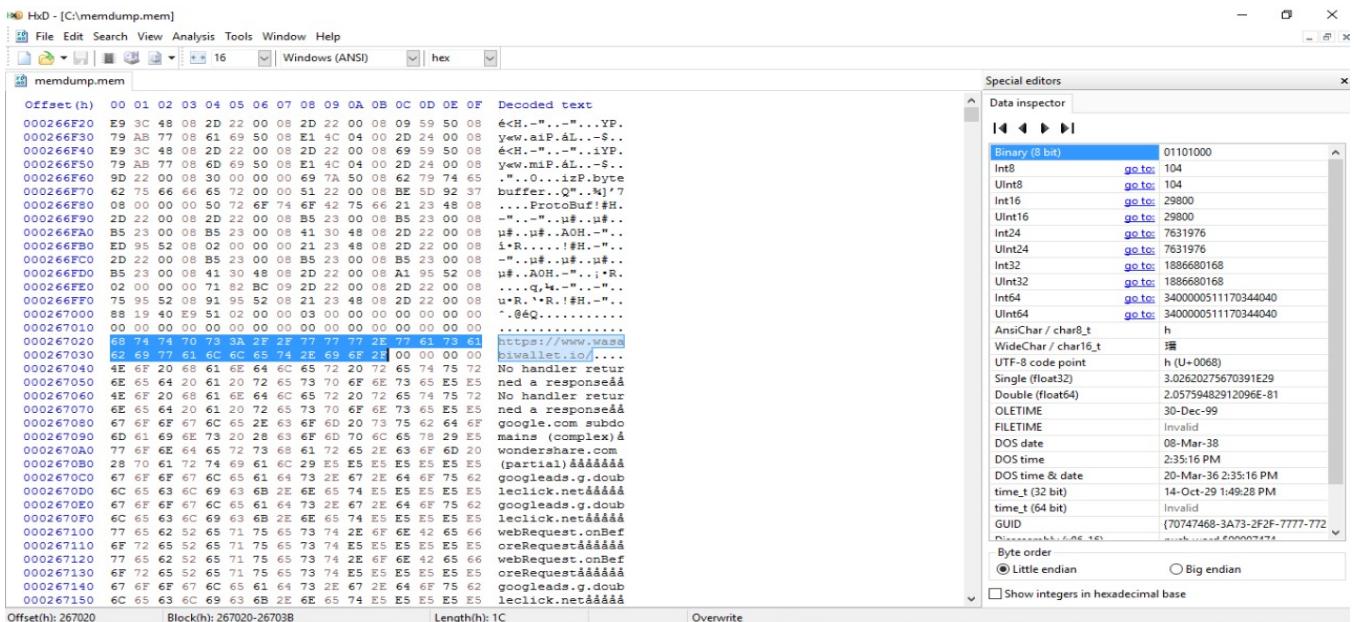


- Open HDX Tool and Click on file.
- Go to open → Select your previously saved path location.
- Open the extension file i.e; “memdump.mem”.

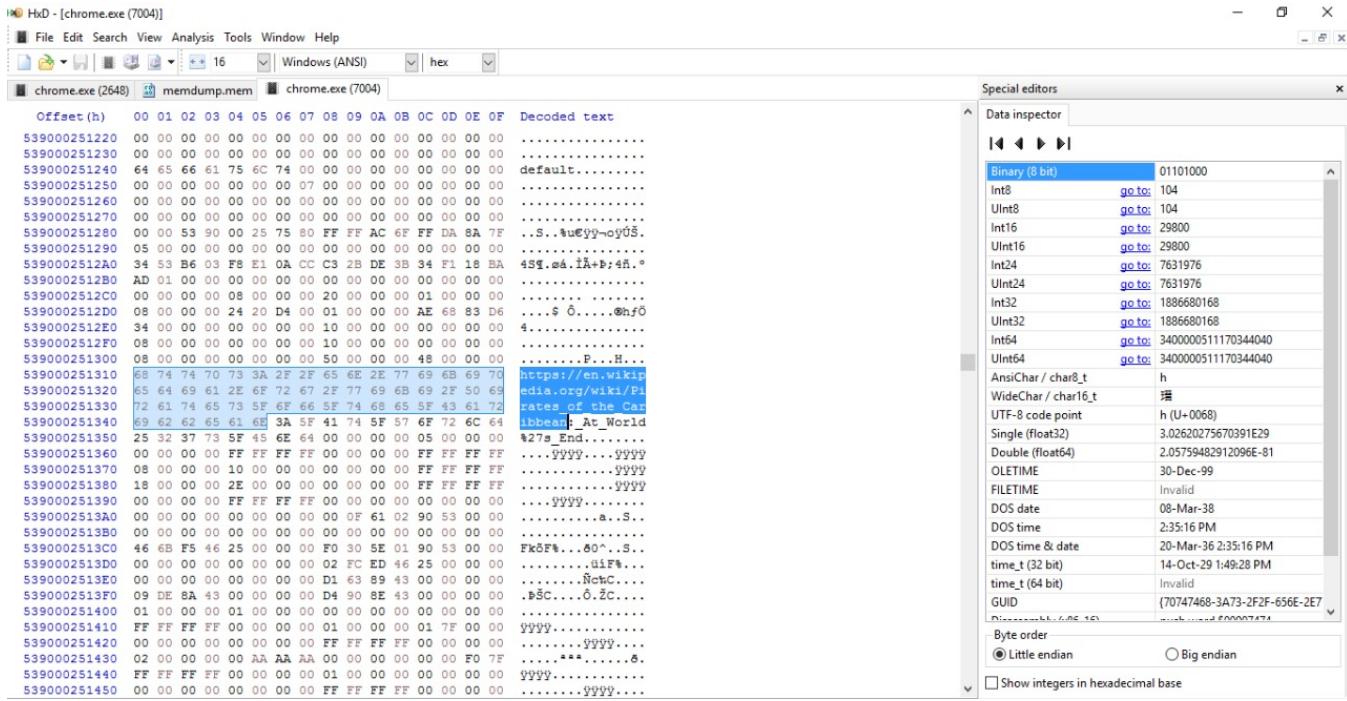
TOR BROWSER History



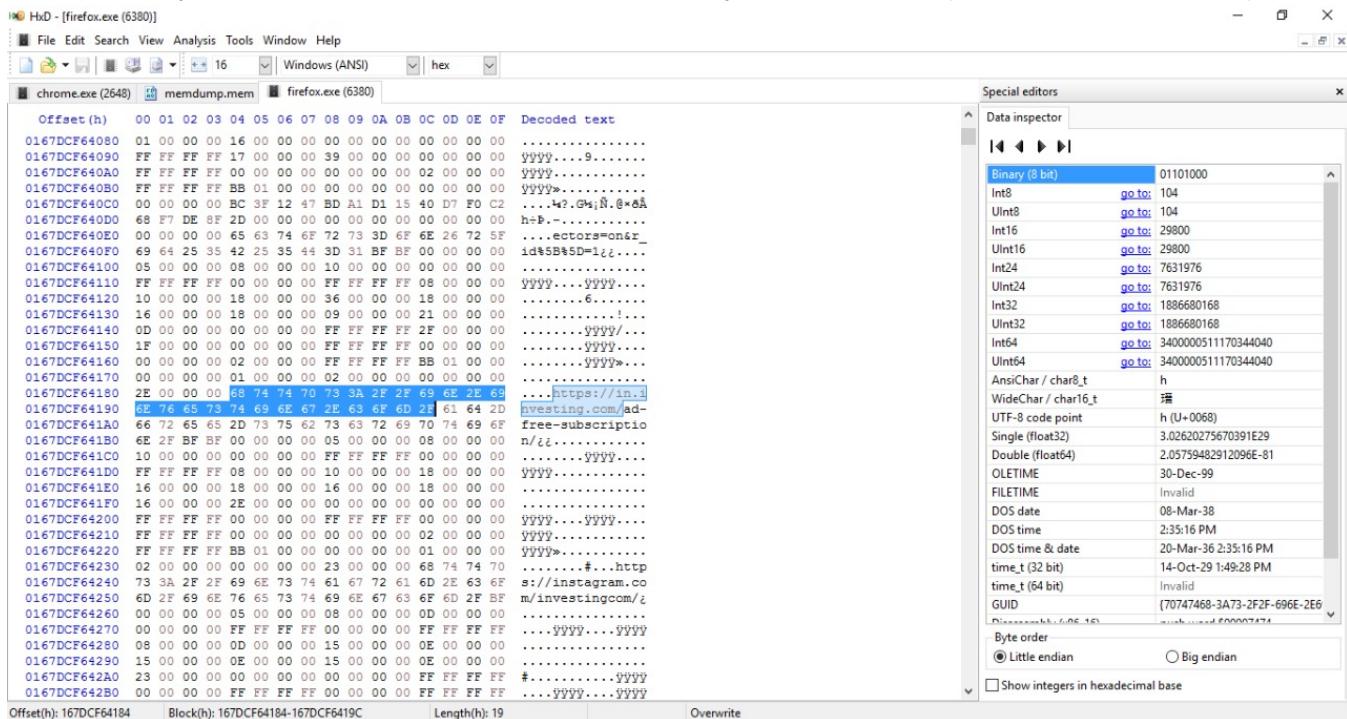
- Click on tools then main memory select your used browser then OK.
- Click on search to find and enter your domain(.com, .in, .org, .onion, .edu, etc).
- Therefore we get our domain highlighted.



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)

HxD - [MicrosoftEdgeCP.exe (3080)]

File Edit Search View Analysis Tools Window Help

MicrosoftEdgeCP.exe (3080)

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
0181AF292860	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF292870	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF292880	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF292890	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF2928A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF2928B0	00 00 00 00 00 00 00 00 30 E1 29 AF 81 01 00 00 000A.....
0181AF2928C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF2928D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0181AF2928E0	00 00 00 00 00 00 00 00 00 25 29 AF 81 01 00 00 00
0181AF2928F0	00 00 00 00 00 00 00 00 D0 F9 26 AF 81 01 00 00 00B&.....
0181AF292900	06 00 00 00 98 22 00 00 00 00 00 00 00 00 00 00?.....
0181AF292910	F9 13 34 65 82 23 27 EF F2 01 00 00 89 01 00 00 00	ù.e;#id...k...
0181AF292920	55 AA 55 AA A9 01 00 00 01 00 00 00 01 00 00 00 00	U*U@.....
0181AF292930	00 00 00 00 00 00 00 00 04 00 00 06 00 00 00 00 00
0181AF292940	50 29 29 A9 81 01 00 C4 29 29 AF 81 01 00 00 00	F).....A).....
0181AF292950	68 74 74 70 3A 2F 77 77 72 E6 69 0E 7A 00 00 00	https://www.bing
0181AF292960	2E 63 6F 6D 2F 73 63 61 72 63 68 3F 71 3D 6A EB	.com/search?=.....
0181AF292970	74 75 26 66 6F 72 6D 3D 45 44 47 45 41 52 26form=EDGE&
0181AF292980	71 73 3D 50 46 26 63 76 69 64 3D 37 64 61 33 36	q=PFcvrid=7da36
0181AF292990	35 66 65 38 61 66 61 34 38 65 30 61 31 62 37 32	5fe8afa48e0a1b72
0181AF2929A0	32 34 66 66 36 64 38 34 36 38 30 26 63 63 55	24ff6d846804cc+o=
0181AF2929B0	53 26 73 65 74 6C 61 6E 67 3D 65 6E 2D 55 53 00	S@setlang=en-US.
0181AF2929C0	B7 3E 28 F9 43 00 30 0C 5C 00 55 00 73 00 65 00	>(U.C.:.\.U.s.e.
0181AF2929D0	72 00 73 00 5C 00 75 00 73 00 65 00 72 00 5C 00	r.s.\.u.s.e.r.\.
0181AF2929E0	41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00	A.p.p.D.a.t.a.\.
0181AF2929F0	4C 00 6F 00 63 00 61 00 6C 00 5C 00 50 00 61 00	L.o.c.a.l.\.P.a.
0181AF292A00	63 00 6B 00 61 00 67 00 65 00 73 00 5C 00 6D 00	c.k.a.g.e.s.\.m.
0181AF292A10	69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00	i.c.r.o.s.o.f.
0181AF292A20	2E 00 6D 00 69 00 63 00 72 00 6F 00 73 00 6F 00	..m.i.c.r.o.s.o.
0181AF292A30	66 00 74 00 65 00 64 00 67 00 65 00 5F 00 38 00	f.t.e.d.g.e._s.
0181AF292A40	77 00 65 00 6B 00 79 00 62 00 33 00 64 00 38 00	w.e.k.y.b.3.d.8.
0181AF292A50	62 00 62 00 77 00 65 00 5C 00 41 00 43 00 5C 00	b.b.w.e.\.A.C.\.
0181AF292A60	23 00 21 00 30 00 30 00 31 00 5C 00 4D 00 69 00	#!.0.0.1.\.M.i.
0181AF292A70	63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 45 00	c.r.o.s.o.f.t.E.
0181AF292A80	64 00 67 00 65 00 5C 00 43 00 61 00 63 00 68 00	d.g.e.\.C.a.c.h.
0181AF292A90	65 00 5C 00 38 00 39 00 34 00 52 00 46 00 51 00	e.\.8.9.4.R.F.Q.

Offset(h): 181AF2929E6 Block(h): 181AF2929E6-181AF292972 Length(h): 5 Overwrite

Special editors Data inspector

Open main memory

Process name	Process ID
MicrosoftEdgeCP.exe	3080
MicrosoftEdgeCP.exe	10152
browser_broker.exe	6580
MicrosoftEdge.exe	3736
chrome.exe	3100
chrome.exe	7128
chrome.exe	9524
chrome.exe	8656
chrome.exe	9488
chrome.exe	9480
chrome.exe	9292
chrome.exe	6380
firefox.exe	2536
firefox.exe	6836
firefox.exe	7356
firefox.exe	2356

Binary (8 bit) 01101010

Int8 go to: 106

UInt8 go to: 106

Int16 go to: 28266

UInt16 go to: 28266

Int24 go to: 7630442

UInt24 go to: 7630442

Int32 go to: 1970564714

UInt32 go to: 1970564714

Int64 go to: Invalid

UInt64 go to: Invalid

AnsiChar / char8_t j

WideChar / char16_t 瑪

UTF-8 code point j (U+006A)

Single (float32) 3.09853490411164E32

Double (float64) Invalid

OLETIME Invalid

FILETIME Invalid

DOS date 10-Mar-35

DOS time 1:51:20 PM

DOS time & date 20-Nov-38 1:51:20 PM

time_t (32 bit) 11-Jun-32 11:05:14 AM

time_t (64 bit) Invalid

GUID Invalid

Byte order Little endian Big endian

Show integers in hexadecimal base

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

HxD - [iexplore.exe (10788)]

File Edit Search View Analysis Tools Window Help

iexplore.exe (10788)

memdump.mem

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
000000C18300	00 00 00 00 B0 76 3B 23 92 51 65 4B 93 75 FF B0v;#'QeK"uy"
000000C18310	4E 25 02 87 00 00 00 00 00 00 A8 2A 00 00	N%.#.....*
000000C18320	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C18330	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C18340	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000C18350	00 00 00 00 00 00 00 00 00 02 00 00 00 02 00 00
000000C18360	23 70 00 00 D8 13 00 E1 E5 14 27 21 B4 C3 45	#p..0...å..!..Ä
000000C18370	05 00 00 00 00 00 00 00 22 BC 00 00 D8 13 00 00w..!..O...
000000C18380	73 09 2E C0 07 C2 1B 07 05 00 00 00 00 00 00	å..Å..Å..
000000C18390	69 6D 61 67 65 2F 6A 78 72 69 6D 61 67 65	image/jxr, image
000000C183A0	2F 2A 3B 71 3D 30 2F 3B 2C 20 2A 2F 2A 3B 71 3D	/+q=0.8, /*:*=
000000C183B0	30 2E 35 B3 83 C1 00 B8 83 C1 00 BB 6C 62 65	0.5!fA..!Å..w..w..
000000C183C0	83 C1 00 A9 29 EC 20 01 00 00 DF 83 C1 00 07	f..w..!..Å..
000000C183D0	00 00 E6 83 C1 00 28 00 00 00 00 00 00 00 00	..w..!..R
000000C183E0	65 66 62 72 65 72 68 74 74 70 73 7A 2F 77 77	eferer=https://w..
000000C183F0	77 2F 67 65 69 6B 73 66 6F 72 67 65 65 69 73	w..geekforgeeks..
000000C18400	7E 67 2F 62 65 6B 61 76 61 76 61 7F 72 65 66 3D	z..java//?ze=q-q
000000C18410	61 11 84 C1 00 11 84 C1 00 19 84 C1 00 19 C1	h..Å..Å..Å..Å..
000000C18420	00 00 64 DB 78 01 00 00 3D 84 C1 00 0F 00	..dx..!..Å..Å..
000000C18430	00 4C 84 C1 00 05 00 00 00 00 00 41 63 63	L..Å..!..Acc
000000C18440	65 70 74 2D 4C 61 6E 75 61 67 65 65 6E 2D 55	ept-Langugage-U
000000C18450	53 51 84 C1 00 S1 84 C1 00 59 84 C1 00 59 84 C1	SQ..Q..Q..A..Å..Å..Å..
000000C18460	00 DB C6 66 01 00 00 7D 84 C1 00 0A 00 00	0.Üfer..!..Å..
000000C18470	00 87 84 C1 00 05 00 00 00 00 00 00 55 73 65	..Å..E..!..Use
000000C18480	72 2D 41 67 65 6E 44 4F 6F 7A 69 73 6C 61 2F 35	-AgentMozilla/5
000000C18490	2E 30 20 18 57 69 6E 6F 77 73 20 4E 54 20 31	..Windows NT 1
000000C184A0	50 2E 30 20 57 4F 57 36 34 3B 20 54 72 69 64	0..; NCG64; Trid
000000C184B0	65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 32 2E 30	ent/7.0; rv:1.0
000000C184C0	29 20 6C 69 6B 65 20 47 65 63 6B 6F CC 84 00 00	j like Gecko,Å..
000000C184D0	CC 84 C1 00 D4 84 C1 00 44 7D 2B D0 1..A..Å..Å..D..Ö	..Å..Å..Å..
000000C184E0	01 00 00 00 F8 84 C1 00 0F 00 00 07 85 C1 00w..!..Å..
000000C184F0	00 00 00 00 00 00 41 63 65 65 70 74 2D 45Accept-E
000000C18500	6E 63 6F 64 69 6E 67 7A 69 70 2C 20 64 65 66	ncodinggzip, def
000000C18510	6C 61 74 65 14 85 C1 00 14 85 C1 00 1C 85 C1 00	late..Å..Å..Å..
000000C18520	1C 85 C1 00 FE SE D4 A3 01 00 00 40 85 C1 00	..A..p..Ö..!..Å..
000000C18530	04 00 00 44 85 C1 00 17 00 00 00 00 00D..Å..

Offset(h): C183E6 Block(h): C183E6-C18410 Length(h): 2B Overwrite

Special editors Data inspector

Open main memory

Process name	Process ID
chrome.exe	4560
SearchProtocolHost.exe	11020
iexplore.exe (32 bit)	10788
iexplore.exe	5080
iexplore.exe (32 bit)	8120
ShellExperienceHost.exe	9688
chrome.exe	7924
MicrosoftEdgeCP.exe	3080
MicrosoftEdgeCP.exe	10152
browser_broker.exe	6580
MicrosoftEdge.exe	3736
chrome.exe	3100
chrome.exe	9488
chrome.exe	9480
chrome.exe	9292

Binary (8 bit) 01101000

Int8 go to: 104

UInt8 go to: 104

Int16 go to: 29800

UInt16 go to: 29800

Int24 go to: 7631976

UInt24 go to: 7631976

Int32 go to: 1886690168

UInt32 go to: 1886690168

Int64 go to: 340000511170344040

UInt64 go to: 340000511170344040

AnsiChar / char8_t h

WideChar / char16_t 瑪

UTF-8 code point h (U+0068)

Single (float32) 3.02620275670391E29

Double (float64) 2.05759482912096E-81

OLETIME 30-Dec-99

FILETIME Invalid

DOS date 08-Mar-38

DOS time 2:35:16 PM

DOS time & date 20-Mar-36 2:35:16 PM

time_t (32 bit) 14-Oct-29 1:49:28 PM

time_t (64 bit) Invalid

GUID {70747468-3A73-2F2F-7777-772

Byte order Little endian Big endian

Show integers in hexadecimal base

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.

urls							
	id	url	title	visit_count	typed_count	last_visit_time	hidden
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

Fig 1: Analysis of Chrome History Data

DB Browser for SQLite - G:\dhds\pex.default-162679687235\places.sqlite

The screenshot shows the DB Browser for SQLite interface with the 'moz_places' table selected. The table has columns: id, url, title, rev_host, visit_count, hidden, typed, frequency, last_visit_date, guid, and foreign. The data includes various Mozilla-related pages like 'Welcome to Firefox' and 'Firefox Privacy Notice — Mozilla'. The visit count column shows values like 1, 0, 1, 0, etc., and the last_visit_date column shows dates like 1626721937977000.

	id	url	title	rev_host	visit_count	hidden	typed	frequency	last_visit_date	guid	foreign
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.mozilla.org/en-US/firefox/57.0.1/...	Welcome to Firefox	gro.allizom.www...	1	0	0	100	1626721937977000	vcOsFd2uv1HA	
2	2	https://www.mozilla.org/en-US/firefox/central/...	NULL	gro.allizom.www...	0	0	0	140	NULL	uZ-YJdhUr6-o	
3	3	https://support.mozilla.org/en-US/products/firefox	NULL	gro.allizom.troppus.	0	0	0	140	NULL	eNhuRJkQw4d	
4	4	https://www.mozilla.org/en-US/firefox/customize/...	NULL	gro.allizom.www...	0	0	0	140	NULL	Fg'xdSk_Fzm8	
5	5	https://www.mozilla.org/en-US/contribute/...	NULL	gro.allizom.www...	0	0	0	140	NULL	QHgNbRaIPmZA	
6	6	https://www.mozilla.org/en-US/about/...	NULL	gro.allizom.www...	0	0	0	140	NULL	WPOsP9an-1HZ	
7	7	place:sort=8&maxResults=10	NULL	.	0	1	0	0	NULL	A06bR2s0B-N	
8	8	https://www.mozilla.org/privacy/firefox/...	NULL	gro.allizom.www...	2	1	0	50	1626796889144000	urOckA9KX_H	
9	9	https://www.mozilla.org/en-US/privacy/firefox/...	Firefox Privacy Notice — Mozilla	gro.allizom.www...	2	0	0	200	1626796889676000	_Zh7-DMC5K_1	
10	10	place:type=6&sort=14&maxResults=10	NULL	.	0	1	0	0	NULL	5k2PmIfHdZt	
11	11	http://google.com/...	NULL	moc.elgoog...	1	1	1	25	1626722001018000	rR9gbL_L04Qi	
12	12	http://www.google.com/...	NULL	moc.elgoog.www...	1	1	0	25	1626722001127000	FHSQ5jd1LFB0	
13	13	https://www.google.com/?gws_rd=ssl	Google	moc.elgoog.www...	1	0	0	50	1626722001440000	l9bYz79lcr5e	
14	14	https://www.google.com/search?q=hp+15-...	hp 15-bs0xx drivers for windows 10 - Google ...	moc.elgoog.www...	1	0	0	100	1626722032216000	khGW2kL1XHCT	
15	15	https://www.google.com/url?...	NULL	moc.elgoog.www...	1	0	0	100	1626722036888000	gYw4D3lvmnUz	
16	16	https://support.hp.com/in-en/drivers/selfservice/...	HP 15-bs000 Laptop PC Software and Driver ...	moc.ph.troppus.	2	0	0	200	1626722125232000	sI5R3bhC_4	
17	17	https://www.google.com/url?...	NULL	moc.elgoog.www...	1	0	0	100	1626722098291000	UI50Q767qxrZ	
18	18	https://h30434.www3.hp.com/t5/Notebook-...	I can't find HP Laptop 15-bs0xx drivers - HP ...	moc.ph.3www.43403h...	1	0	0	100	1626722099588000	BfGzQXxEFWvx	
19	19	https://support.hp.com/in-en/drivers/selfservice/...	Official HP® Drivers and Software Download ...	moc.ph.troppus.	2	0	0	200	1626722321501000	LTbzVprmsuw8	

Fig 2: Analysis of FireFox History Data

DB Browser for SQLite - G:\Default\History

The screenshot shows the DB Browser for SQLite interface with the 'urls' table selected. The table has columns: id, url, title, visit_count, typed_count, last_visit_time, and hidden. The data includes various Brave-related search results and extension pages like 'brave login - Google Search' and 'How to Install Chrome Web Extensions | Brave ...'. The visit count column shows values like 2, 0, 1, 0, etc., and the last_visit_time column shows dates like 13271272850131167.

	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.google.com/search?...	brave login - Google Search	2	0	13271272570731001	0
2	2	https://publishers.basicattentiontoken.org/login	Log In - Brave Rewards Creators	1	0	13271272581239801	0
3	3	https://www.google.com/search?...	brave themes - Google Search	2	0	13271272792015194	0
4	4	https://www.google.com/search?...	brave theme browser - Google Search	2	0	13271272839360497	0
5	5	https://www.google.com/search?...	brave theme browser extensions - Google Search	3	0	13271272863009219	0
6	6	https://www.googleadservices.com/pagead/adclk...	Download Brave Browser	1	0	13271272850131167	0
7	7	https://try.bravesoftware.com/dgF367/...	Download Brave Browser	1	0	13271272850131167	0
8	8	https://try.bravesoftware.com/dgF367/...	Download Brave Browser	1	0	13271272881639609	0
9	9	https://brave.com/learn/installing-chrome-...	How to Install Chrome Web Extensions Brave ...	1	0	13271272881639609	0
10	10	https://www.google.com/search?...	theme extension - Google Search	2	0	13271272945813184	0
11	11	https://chrome.google.com/webstore/category/...	Chrome Web Store - Themes	2	0	1327127306608198	0
12	12	https://chrome.google.com/webstore/detail/r1de/...	Chrome Web Store - Themes	1	0	13271273019542558	0
13	13	https://chrome.google.com/webstore/detail/blac...	Black red shards - Chrome Web Store	1	0	13271273070529547	0
14	14	https://chrome.google.com/webstore/detail/blac...	Black purple shards - Chrome Web Store	1	0	13271273127750669	0
15	15	https://www.mozilla.org/en-US/firefox/57.0.1/...	Welcome to Firefox	1	0	13271195537000000	0
16	16	https://www.mozilla.org/privacy/firefox/...	...	2	0	13271195540000000	1
17	17	http://google.com/...	...	1	1	13271195601000000	1
18	18	https://www.google.com/search?q=hp+15-...	hp 15-bs0xx drivers for windows 10 - Google ...	1	0	13271195632000000	0
19	19	https://www.google.com/url?...	...	1	0	13271195636000000	0
20	20	https://support.hp.com/in-en/drivers/selfservice/...	HP 15-bs000 Laptop PC Software and Driver ...	2	0	13271195638000000	0

Fig 3:Analysis of Brave History Data

Download Analysis

The screenshot shows two windows of DB Browser for SQLite displaying download history from a SQLite database.

Table 1: downloads

	id	guid	current_path	target_path	start_time	received_bytes	total_bytes	end_time	ref
1	3	f1c2efbd-a4cf-4ebe-a7a...	C:\Users\Ambati\Downloads\kendal...	C:\Users\Ambati\Downloads\kendal...	13271275694076817	2030260	2030260	13271275699422973	https://unsplash.com/
2	4	0756dd1c-5502-4b3c...	C:\Users\Ambati\Downloads\siska-vrijburg...	C:\Users\Ambati\Downloads\siska-vrijburg...	13271317090438536	2572743	2572743	13271317098833500	https://unsplash.com/
3	5	d3495855-...	C:\Users\Ambati\Downloads\Phoenix II by ...	C:\Users\Ambati\Downloads\Phoenix...	13271322190123482	67	67	1327132216975636	
4	6	cbd3740e-6982-426c-9...	C:...	C:...	13271322286891619	4682974	4682974	13271322292891985	https://www.deviantart.c
5	7	0831ad91-5698-4723...	C:...	C:...	13271322691797568	7023702	7023702	13271322694973285	https://www.deviantart.o
6	8	a034f1e6-096b-4875-8...	C:\Users\Ambati\Downloads\SSRN...	C:\Users\Ambati\Downloads\SSRN...	13271342119020486	587096	587096	13271342123522626	https://papers.ssrn.com/
7	9	968c420a-6663-4a04...	C:\Users\Ambati\Downloads\1735415510.pdf	C:...	13271342623075398	1150987	1150987	13271342626862093	https://www.econstor.eu
8	10	ddad55c9-ff77-4b37-...	C:...	C:...	13271342664990501	1837453	1837453	13271342668330999	https://link.springer.com/
9	11	90afac199-5293-4ec6-93...	C:\Users\Ambati\Downloads\CoE-template-...	C:\Users\Ambati\Downloads\CoE-templa...	13271349581265671	146772	146772	13271349584421757	
10	12	02ac65f5-2772-4190-...	C:...	C:...	13271435057622129	23388160	23388160	13271435068196207	https://www.filehorse.co
11	13	5d65a570-...	C:\Users\Ambati\Downloads\Agora.csv.zip	C:...	13271445190331923	8071841	8071841	13271445194152510	https://www.kaggle.com/
12	14	8ad2c325-1046-46f1-87...				0	175008	0	https://templates.office.co
13	15	05aad238-...	C:\Users\Ambati\Downloads\Copy of ALEXIUS...	C:\Users\Ambati\Downloads\Copy of...	13271448451712524	262468	262468	13271448464926825	https://docs.google.com/
14	16	b79920a3-...	C:\Users\Ambati\Downloads\096-DESPA.zip	C:\Users\Ambati\Downloads\096-...	13271448668789720	1419804	1419804	13271448674183979	https://www.resumgo.co
15	17	42420506-e345-4d87-...	C:\Users\Ambati\Downloads\Team 19 ...	C:\Users\Ambati\Downloads\Team 19 ...	13271520143192602	172470	172470	13271520150360565	
16	18	08b09588-a147-4c2b-...	E:\Softwares\DB.Browser.for.SQLite-3.12.2-...	E:...	13271522041378936	20446868	20446868	13271522055969940	https://sqlitebrowser.org/
17	19	a426c536-...	E:\Softwares\torbrowser-install-...	E:\Softwares\torbrowser-install-...	13271523279309258	73980952	73980952	13271523297133811	
18	20	fd15a1a9-...	E:\Softwares\winprefetchview-x64.zip	E:\Softwares\winprefetchview-x64.zip	13271523745019867	68291	68291	13271523756650596	https://www.nirsoft.net/u
19	21	14dab814-4610-4916-9...				0	1561844	0	

Table 2: file_metadata

	http_method	by_ext_id	by_ext_name	etag	last_modified	mime_type	original_mime_type
1					Tue, 22 Jun 2021 09:42:31 GMT	image/jpeg	image/jpeg
2					Sat, 03 Jul 2021 13:39:49 GMT	image/jpeg	image/jpeg
3						text/html	text/html
4						image/jpeg	image/jpeg
5						image/jpeg	image/jpeg
6						application/pdf	application/pdf
7					Thu, 24 Dec 2020 02:11:50 GMT	application/pdf	application/pdf
8			"a731d278831cffec05e77fe6bd84daf1"		Fri, 23 Nov 2018 07:17:06 GMT	application/pdf	application/pdf
9						application/vnd.openxmlformats-...	application/vnd.openxmlformats-...
10			"5c5d7d94-164e000"		Fri, 08 Feb 2019 13:01:08 GMT	application/octet-stream	application/octet-stream
11			"7c694062158ae82fd0ca76a65fd61985"		Wed, 25 Sep 2019 02:46:39 GMT	application/zip	application/zip
12			0x8D90F634AC10F7A		Wed, 05 May 2021 01:15:37 GMT	application/vnd.openxmlformats-...	application/vnd.openxmlformats-...
13			"6cdb55d2450f5d5905f0e3d663062134"		Tue, 24 Sep 2019 23:18:33 GMT	application/zip	application/zip
14						application/vnd.openxmlformats-...	application/vnd.openxmlformats-...
15					Sun, 16 May 2021 20:00:21 UTC	application/octet-stream	application/octet-stream
16			"468dc18-5c6f9da2b9940"		Tue, 13 Jul 2021 04:41:33 GMT	application/x-msdos-program	application/x-msdos-program
17			"1256da-10ac3-59e4bdb16e5c0"		Tue, 11 Feb 2020 12:18:39 GMT	application/zip	application/zip
18						application/pdf	application/pdf
19							

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 operating 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.

The screenshot shows the WinPrefetchView application window. It displays a table of prefetch files with columns for Filename, Created Time, Modified Time, File Size, Process EXE, Process Path, Run Counter, Last Run Time, and Missing Pr... . The table lists numerous files from various applications like DWM, EASEOFACCESSDIALO..., EXPLORER, FFMPEG, FILEHISTORY, FIREFOX, FIRSTLOGONANIM, FIXMAPLEXE, FLASHPLAYERUPDAT..., FTK IMAGER, G2MLAUNCHER, G2MSTART, G2MULEXE, G2MUPDATE, G2MUPLOAD, GITHUBDESKTOP, and GOOGLECRASHHAN... . The last two rows show system files like \$MFT, MATHWORKSEVENT..., and others.

Filename	/	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr...
DWM.EXE-6FFD3DA&.pf	06-Aug-21 4:31:1...	06-Aug-21 10:22:...	11,048	DWM.EXE	C:\Windows\System32\dwm.exe	2	06-Aug-21 10:22:06 PM, 05-Aug-21 10:41:58...	No	
EASEOFACCESSDIALO...	02-Mar-21 6:57:2...	12-Jul-21 8:14:24...	6,645	EASEOFACCESSDIALO...	C:\Windows\System32\EASEOFACCESSDIALO...	6	12-Jul-21 8:14:14 PM, 06-Jun-21 8:21:41 PM, ...	No	
EULA.EXE-827DC6D9.pf	09-Mar-21 10:30:...	09-Mar-21 10:30:...	9,397	EULA.EXE	C:\PROGRAM FILES (X86)\Adobe\READER 1...	1	09-Mar-21 10:30:10 AM	No	
EXPLORER.EXE-A0B4E...	14-May-16 2:17:...	07-Aug-21 5:00:1...	46,623	EXPLORER.EXE	C:\Windows\explorer.exe	59	07-Aug-21 5:00:06 PM, 07-Aug-21 4:56:41 P...	No	
FFMPEG.EXE-9A09803...	07-Aug-21 4:50:3...	07-Aug-21 4:58:5...	14,437	FFMPEG.EXE	C:\USERS\USER\APPDATA\LOCAL\TEMP\...	8	07-Aug-21 4:58:52 PM, 07-Aug-21 4:58:43 P...	Yes	
FILEHISTORY.EXE-P95...	05-Aug-21 5:33:0...	05-Aug-21 5:53:0...	23,203	FILEHISTORY.EXE	C:\Windows\System32\FILEHISTORY.EXE	1	05-Aug-21 5:52:56 PM	No	
FIREFOX.EXE-0C835EF...	24-Jul-21 7:59:56...	24-Jul-21 8:00:15...	33,788	FIREFOX.EXE	C:\Users\user\Desktop\TOR BROWSER\Bro...	5	24-Jul-21 8:00:05 PM, 24-Jul-21 8:00:02 PM, ...	No	
FIRSTLOGONANIM.EX...	14-May-16 2:17:...	14-May-16 2:17:...	7,078	FIRSTLOGONANIM...	C:\Windows\System32\oobe\FIRSTLOGON...	1	14-May-16 2:17:59 PM	No	
FIXMAPLEXE-0CB3F41...	07-Aug-21 10:27:...	07-Aug-21 10:27:...	7,175	FIXMAPLEXE	C:\Windows\SysWOW64\fixmaplexe	1	07-Aug-21 10:27:20 PM	No	
FLASHPLAYERUPDAT...	05-Aug-21 7:59:0...	07-Aug-21 10:59:...	4,761	FLASHPLAYERUPD...	C:\Windows\SysWOW64\Macromed\Flash...	9	07-Aug-21 10:59:00 PM, 07-Aug-21 8:59:00 ...	No	
FTK IMAGER.EXE-1B2...	15-Jul-21 6:26:17...	22-Jul-21 7:34:06...	25,981	FTK IMAGER.EXE	C:\PROGRAM FILES\ACCESSDATA\FTK IMA...	14	22-Jul-21 7:34:06 PM, 20-Jul-21 7:43:27 PM, ...	No	
G2MLAUNCHER.EXE-...	10-Apr-21 3:03:3...	24-Apr-21 11:00:...	20,427	G2MLAUNCHER.EXE	C:\Users\user\AppData\Local\GOTOMEET...	10	24-Apr-21 11:00:33 AM, 21-Apr-21 2:00:22 P...	No	
G2MSTART.EXE-C341...	10-Apr-21 3:03:2...	24-Apr-21 11:00:...	12,259	G2MSTART.EXE	C:\Users\user\AppData\Local\GOTOMEET...	10	24-Apr-21 11:00:31 AM, 21-Apr-21 2:00:20 P...	No	
G2MULEXE-26F91B76.pf	10-Apr-21 3:03:3...	24-Apr-21 11:00:...	33,739	G2MULEXE	C:\Users\user\AppData\Local\GOTOMEET...	10	24-Apr-21 11:00:30 AM, 21-Apr-21 2:00:27 P...	No	
G2MUPDATE.EXE-F97...	05-Aug-21 8:30:0...	07-Aug-21 10:30:...	17,956	G2MUPDATE.EXE	C:\Users\user\AppData\Local\GOTOMEET...	5	07-Aug-21 10:30:00 PM, 07-Aug-21 9:30:00 ...	No	
G2MUPLOAD.EXE-21B...	24-Jul-21 11:31:0...	07-Aug-21 5:10:1...	12,704	G2MUPLOAD.EXE	C:\Users\user\AppData\Local\GOTOMEET...	29	07-Aug-21 5:10:00 PM, 05-Aug-21 9:31:00 P...	No	
GITHUBDESKTOP.EXE...	21-May-21 7:11:1...	18-Jul-21 9:23:40...	33,406	GITHUBDESKTOP...	C:\USERS\USER\APPDATA\LOCAL\GITHUB...	5	18-Jul-21 9:23:30 PM, 21-May-21 7:13:17 P...	Yes	
GOOGLECRASHHAN...	05-Aug-21 10:39:...	05-Aug-21 10:39:...	5,072	GOOGLECRASHHAN...	C:\PROGRAM FILES (X86)\GOOGLE\UPDAT...	1	05-Aug-21 10:39:05 PM	Yes	
\$MFT				C:\Windows\SysWOW64\ole32.dll	\VOLUME\b10d703db7eca15-665c69...	51			
MATHWORKSEVENT...				C:\USERS\USER\DOWNLOADS\MAT...	\VOLUME\b10d703db7eca15-665c69...	8			
2E74987E1A1563542...				C:\Users\user\AppData\Local\Low\ML...	\VOLUME\b10d703db7eca15-665c69...	78			
2E74987E1A1563542...				C:\Users\user\AppData\Local\Low\ML...	\VOLUME\b10d703db7eca15-665c69...	79			
ADVAPI32.DLL				C:\Windows\SysWOW64\advapi32.dll	\VOLUME\b10d703db7eca15-665c69...	26			
APPHELP.DLL				C:\Windows\SysWOW64\apphelp.dll	\VOLUME\b10d703db7eca15-665c69...	11			
BCRYPT.DLL				C:\Windows\SysWOW64\bcrypt.dll	\VOLUME\b10d703db7eca15-665c69...	46			
BCRYPTPRIMITIVES.DLL				C:\Windows\SysWOW64\BCRYPTPRIMI...	\VOLUME\b10d703db7eca15-665c69...	24			
CFGMGR32.DLL				C:\Windows\SysWOW64\cfgmgr32.dll	\VOLUME\b10d703db7eca15-665c69...	30			
CLBCATQ.DLL				C:\Windows\SysWOW64\clbcatq.dll	\VOLUME\b10d703db7eca15-665c69...	53			
COMBASE.DLL				C:\Windows\SysWOW64\combase.dll	\VOLUME\b10d703db7eca15-665c69...	18			
COMCTL32.DLL				C:\Windows\WinSxS\x86_MICROSO...	\VOLUME\b10d703db7eca15-665c69...	38			



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.

Filename	URL
%7B%221q%22%3A1%2C%22c%22%3A%22video%22%2C%22src%22%3A1503%7D.gif	https://aax-fe-sin.amazon-adsystem.com/x/pv/Qj38-px2Cz9dLxt1NF7z0AAAF7z198gUAAXFBVTAoU/%7B%221q%22%3A1%2C%22c%22%3A%22video%22%2C%22src%22%3A1503%7D.gif
%7B%22appCss%22%3A%22https%3A%2F%2Fassets.ajio.com%2Fstatic%2F	https://www.ajio.com/service-worker.js?hash=%7B%22appCss%22%3A%22https%3A%2F%2Fassets.ajio.com%2Fstatic%2Fassets%2Fdesktop.bec9824eba5b9c3db
%7B%22c%22%3A%22video%22%2C%22src%22%3A%22start%22%3A1%1.gif	https://aax-fe-sin.amazon-adsystem.com/x/pv/Qj38-px2Cz9dLxt1NF7z0AAAF7z198gUAAXFBVTAoU/%7B%22c%22%3A%22video%22%2C%22src%22%3A1503%7D.gif
&typ=1&bwi=1366&bih=600&ei=fEOYLLHMOcmgfqluzoAw.htm	https://www.google.com/client_204?&atyp=1&bwi=1366&bih=600&ei=fEOYLLHMOcmgfqluzoAw
&fp=1&mpc=10&p=156595&gdp=0&gdp_consent=&pmc=1&p=https%3A%1.htm	https://image3.pubmatic.com/AdServer/img?nc=8fp=1&mpc=10&p=156595&gdp=0&gdp_consent=&pmc=1&p=https%3A%2F%2Fimage4.pubmatic.com
&gdp=0&geo=au&co=in.htm	https://eus.rubiconproject.com/usync.htm?&gdp=0&geo=au&co=in
&pub=0&zzone_id=3461354&is_mobile=false&domain=en.savefrom.net&	https://ezegrin.net/?zpub=0&zzone_id=3461354&is_mobile=false&domain=en.savefrom.net&var=bymid=&var_3=&dsig=&action=settings
-1296126537	https://learning.tsconihub.in/per/g01/pub/1016/DH/instance/1/multilingualJSON/32.json?version=-1296126537
-1549004596	https://learning.tsconihub.in/per/g01/pub/1016/DH/instance/1/multilingualJSON/34.json?version=-1549004596
&fbane	https://www.foxtonforensics.com/Content/fonts/themify/woff?&fbane
.svg	https://intuhvents.webex.com/mw3300/mw/webex/html/img/cisco-webex-meetings-new.svg?ver=
0	https://lh3.googleusercontent.com/HN3oULCfbkrJdwciVK02D137_MJstuobD9HV9lx1en37ySH_0y7baUo9amE4BgT-PmGbs369XIErPxNdGpn1xhAqYC_7g
0	https://lh3.googleusercontent.com/s/Qoe6m93xeBB1WrxGtAbJb_80dYxmSmnpZrWZQqj10nDbC0V0VmubbFT1kTD00pZs2BDh6j0rdsWng_041ks1W3wQfX
0	https://lh3.google.com/hangouts/AM5f6AGdgv2x_qJr1UpWvOIVky5q6j2lxaIv3DHWU65_Mrp5BNCSzT=w297-h396#authuser=0
0	https://lh3.googleusercontent.com/oMLzpgWDuaQ1QzbBM5a-jtxm0-3IUUKwU9y-C1js_ViTxaR8jzE1Dvk7ECPNKe0bewVuYbTVK-VmzGvt-4qikR8H-BuD9Ruyv4:
0	https://id.ridcm.com/70414.gif?gdr=0
0	https://lh3.googleusercontent.com/fife/AAUWuUETCVeYTdmKy3hgcVxpUcaJzSrRMhv-SeuwyTpuNbVxTh028VtDlp1y-zpYWEVXMaLHJ5eavy1-s1RvJKdRjy_Aqpl
0	https://lh3.googleusercontent.com/wyzTzL1P4N591rhga5J1l07qfu0MDauxm9mBqFV0q1-JWMsN0lXpnsAjuZsUwejeC0WVHkDn9j2l3teKfhObn-QvY-69_XbK
0	https://lh3.googleusercontent.com/fife/AAUWuUewLfg-Wqy-UlGv6fMvRgW73SvZ8mviTRPKhUnWtDerybo/u8TmLkVQu4eW3X3bu-Qd-uRQOoOyjhH3l
0	https://lh3.google.com/hangouts/AM5f6AG9RkxMrgJnChdklwl-m38PAaRz0n_qJ6e40zLk3HrzXk2Y0EbeA=s512#authuser=0
0	https://lh3.googleusercontent.com/tIkTzDp0TwvAx-x0XTDmjya3K_cGkG6VOY9wq7h0BwWv3Ew9f2UkGle_5y6jEJZzB6CqUY_5zpbUW13Q4GFJN5MUS7
0	https://lh3.googleusercontent.com/fife/AAUWuUek17EdvKjZInWfQHETy_g5M5hRdy_upLbDyvAIIuSuJaFPI21PIEXLevTEVAYfj_eedB_hcr20l3uR9hjkl0
0	https://lh3.googleusercontent.com/fife/AAUWuEx2NfWduoG4V4Ludyfp4uUdeNp2jB_zX2OY5P8A8l2t-jUK8vmmgELQF8--5skeYRzQfA60o8Q_oNlbHpnLcR
0	https://lh3.google.com/hangouts/AM5f6AG9RjxkMrGnjChdklwl-m38PAaRz0n_qJ6e40zLk3HrzXk2Y0EbeA=s512#authuser=0
0	https://lh3.googleusercontent.com/fife/AAUWuXkPn3ElFkzLz23cycwlfZBwYbthohUsJNjP43qjGuik-5EtqVhL-q8hDacc4WP3zKpKnPnQvqDtnO_mvKolkYf445v

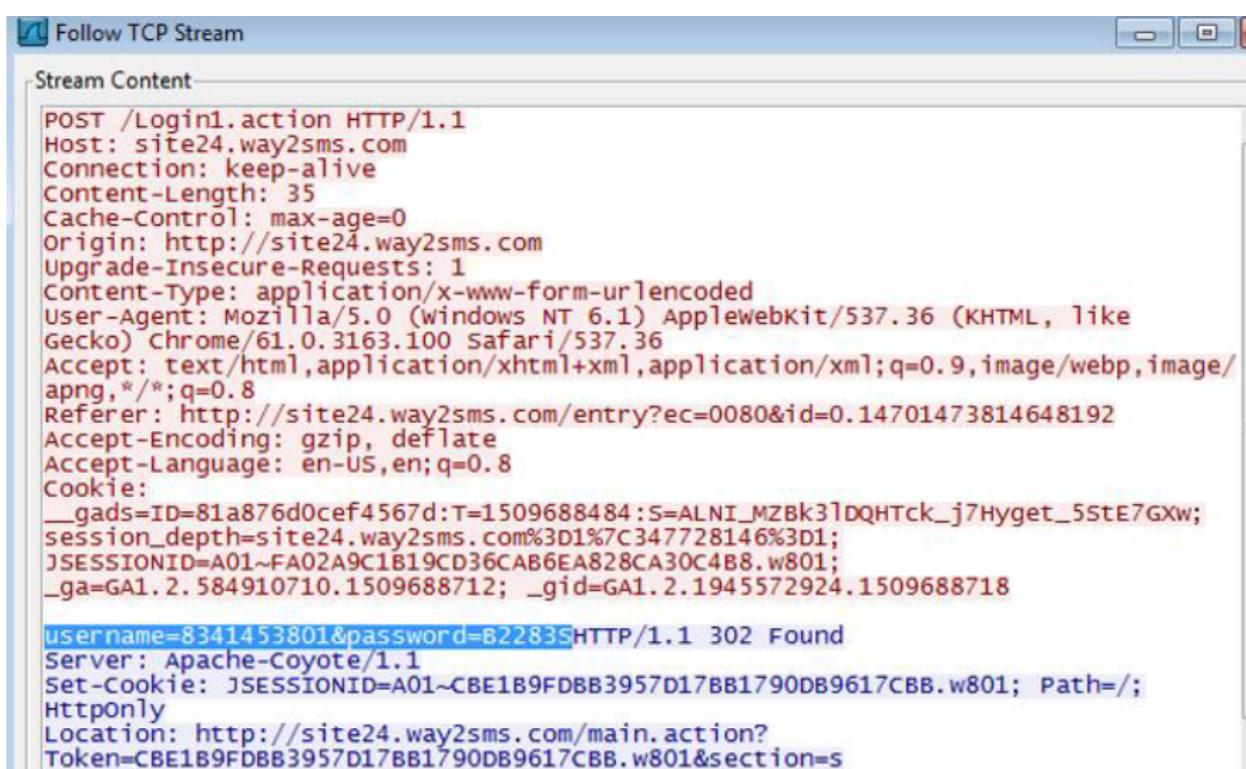
ChromeCacheView: C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cache								
Content Type	File Size	Last Accessed	Server Time	Server Last Modified	Expire Time	Server Name	Server Response	Web Site
image/gif	43	07-Aug-21 10:46:21 PM	07-Aug-21 10:46:19 PM			Server	HTTP/1.1 200 OK	https://researchgate.net
application/javascript	3,578	03-Aug-21 5:42:43 PM	03-Aug-21 3:45:35 PM	29-Jul-21 5:19:24 AM	02-Sep-21 3:45:35 PM	Server	HTTP/1.1 200 OK	https://ajio.com
image/gif	43	07-Aug-21 10:46:17 PM	07-Aug-21 10:46:15 PM			Server	HTTP/1.1 200 OK	https://researchgate.net
text/html	0	07-Aug-21 10:53:13 PM	07-Aug-21 10:53:10 PM			gws	HTTP/1.1 204	https://google.com
text/html	0	07-Aug-21 10:46:17 PM	07-Aug-21 10:46:15 PM				HTTP/1.1 302	https://researchgate.net
text/html	233	07-Aug-21 10:46:22 PM	07-Aug-21 10:46:19 PM	24-Feb-21 2:17:52 AM		Apache/2.2.15 (CentOS)	HTTP/1.1 200 OK	https://researchgate.net
	0	07-Aug-21 10:42:43 PM					HTTP/1.1 200 OK	https://savefrom.net
	0	06-Aug-21 10:01:59 PM					HTTP/1.1 200 OK	https://tcsionhub.in
	0	06-Aug-21 10:01:59 PM					HTTP/1.1 200 OK	https://tcsionhub.in
font/x-woff	56,108	07-Aug-21 10:37:44 PM	07-Aug-21 10:37:42 PM	13-Mar-19 5:52:42 PM			HTTP/1.1 200	https://fontforensics.com
image/svg+xml	9,933	04-Aug-21 6:31:40 PM	04-Aug-21 6:31:39 PM	29-Jul-21 6:30:56 PM		WebEx	HTTP/1.1 200 OK	https://webex.com
image/webp	1,322	01-Aug-21 10:20:17 PM	01-Aug-21 10:20:13 PM		01-Jan-90 5:30:00 AM	fife	HTTP/1.1 200	https://google.com
image/webp	1,292	01-Aug-21 10:20:18 PM	01-Aug-21 10:20:13 PM		01-Jan-90 5:30:00 AM	fife	HTTP/1.1 200	https://google.com
	0	06-Aug-21 6:36:38 PM					HTTP/1.1 200	https://google.com
image/webp	1,724	01-Aug-21 10:20:17 PM	01-Aug-21 10:20:13 PM		01-Jan-90 5:30:00 AM	fife	HTTP/1.1 200	https://google.com
	0	07-Aug-21 5:13:10 PM	07-Aug-21 5:13:07 PM				HTTP/1.1 451	https://rubi
image/webp	0	06-Aug-21 6:33:19 PM					HTTP/1.1 200	https://researchgate.net
image/webp	1,454	01-Aug-21 10:20:18 PM	01-Aug-21 10:20:13 PM		01-Jan-90 5:30:00 AM	fife	HTTP/1.1 200	chrome-extension://nckghadagoajigfahcjanaoihapd
	0	06-Aug-21 6:36:38 PM					HTTP/1.1 200	https://google.com
	0	07-Aug-21 11:02:23 PM					HTTP/1.1 200	https://googleusercontent.com
image/webp	1,446	01-Aug-21 10:20:17 PM	01-Aug-21 10:20:13 PM		01-Jan-90 5:30:00 AM	fife	HTTP/1.1 200	https://google.com
	0	05-Aug-21 9:10:09 PM					HTTP/1.1 200	chrome-extension://nckghadagoajigfahcjanaoihapd
	0	07-Aug-21 11:02:23 PM					HTTP/1.1 200	https://google.com
	0	07-Aug-21 11:02:23 PM					HTTP/1.1 200	chrome-extension://nckghadagoajigfahcjanaoihapd
	0	06-Aug-21 10:02:02 PM					HTTP/1.1 200	chrome-extension://nckghadagoajigfahcjanaoihapd

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.



The screenshot shows the 'Follow TCP Stream' dialog box in Wireshark. The title bar says 'Follow TCP Stream'. The main area is labeled 'Stream Content' and displays the following text:

```
POST /Login1.action HTTP/1.1
Host: site24.way2sms.com
Connection: keep-alive
Content-Length: 35
Cache-Control: max-age=0
Origin: http://site24.way2sms.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://site24.way2sms.com/entry?ec=0080&id=0.14701473814648192
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie:
__gads=ID=81a876d0cef4567d:T=1509688484:S=ALNI_MZBk3lDQHTck_j7Hyget_5stE7GXw;
session_depth=site24.way2sms.com%3D1%7C347728146%3D1;
JSESSIONID=A01~FA02A9C1B19CD36CAB6EA828CA30C4B8.w801;
_ga=GA1.2.584910710.1509688712; _gid=GA1.2.1945572924.1509688718

username=8341453801&password=B2283S HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=A01~CBE1B9FDBB3957D17BB1790DB9617CBB.w801; Path=/;
HttpOnly
Location: http://site24.way2sms.com/main.action?
Token=CBE1B9FDBB3957D17BB1790DB9617CBB.w801&section=s
```

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_for_forensic_analysis_via_Recovery_of_SQLite_Artifacts_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&tbo=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_for_forensic_analysis_via_Recovery_of_SQLite_Artifacts_from_Unallocated_Space

