

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/332093270>

WEB BROWSER FORENSICS: Evidence collection And Analysis for Most Popular Web Browsers usage in Windows 10

Thesis in International Journal of Cyber Criminology · September 2018

DOI: 10.13140/RG.2.2.25857.51049

CITATIONS

0

READS

610

1 author:



David Mugisha

Gujarat Forensic Sciences University

10 PUBLICATIONS **0** CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Android Application Malware Analysis [View project](#)

Gujarat Forensic Sciences University

Institute of Forensic Science

M.Sc. Digital Forensics and Information Security



FSMSDFIS SII : Minor Project 1



WEB BROWSER FORENSICS:



Evidence collection And Analysis for Most Popular Web Browsers usage in Windows

10

By

David MUGISHA

Guided by

Dr. Parag Rughani (Associate Professor)

Institute of Forensic Science

Gujarat Forensic Sciences University

ABSTRACT:

A web browser is an essential application program for accessing and performing various activities on the internet such as browsing internet, email, financial transaction, download files and videos, accessing social media application, etc.

As web browser is the only way to access the internet and cybercrime criminals use the web browser to commit the internet crimes.

It is essential for the digital forensic examiners and particularly for computer forensic investigators, to collect and analyze artifacts related to web browser usage from suspect's device machine.

There are various browsers used such as Google Chrome, Firefox Mozilla, Internet Explorer, Safari, opera, etc, among which Google chrome is very popular among the internet user community.

In this Research paper, we collected and analyzed different artifacts such as history, cookies, cache, Session Restore, flash & super cookies, etc on Windows 10 operating System installed Google chrome, Firefox Mozilla and internet explorer browser.

As result, reveals that web browsers leave traces of browsing activity on the host computer's hard disk.

The outcome of this project will serve to be significant source for digital forensic research community, law enforcement practitioners especially for computer forensic investigators.

ACKNOWLEDGEMENT

This Research would have been hardly possible without the help and support of others.

It is my pleasure to take this opportunity to thank all those who helped me directly or indirectly in my research work.

A sincere gratitude to my guide **Dr.Parag Rughani** (Associate Professor), Gujarat Forensic Sciences University for always encouraging me and providing me with his valuable support and guideline though out the completion of the project.

I would also like to express my sincere thanks toward **Dr. Digvijaysinh Rathod** (Assistant Professor) and **Mr.Dharmesh Dave** (Assistant Professor) and all the faculties of Institute of Forensic Science, Gujarat Forensic Sciences University who helped me in creation and completion of this project.

Last but not the least, my heartfelt thanks to my parents and friends for their constant support and providing me with the opportunity and encouragement to pursue my goals.

TABLE OF CONTENTS

Abstract

Acknowledgement

1.Introduction.....	6
2. literature Review.....	5
3.Overview of Web Browser	8
3.2. Types of Evidence	8
3.3. How Browser works.....	9
3.4. Most Popular Web Browsers	11
3.4.1. Google Chrome.....	11
3.4.2. Mozilla Firefox	11
3.4.3. Internet Explorer (IE).....	12
4. Methodology.....	13
4.1. Preparation and Procedure	13
4.2. Tools and Technology used	13
4.3. Integrated Analysis.....	14
4.4. Timeline Analysis.....	15
4.5. Analysis of search history.....	15
4.6. Analysis on URL encoding	16
4.7. Web Browser Mode Analysed.....	16
5. Result of Evidence collection and Analysis	17
5. 1. Regular Mode Analysis	17
5.1.1. Google Chrome	17
5.1.2. Mozilla Firefox.....	24
5.1.3. Internet Explorer	29
5.2. Private Mode Analysis	33
5.2.1. Live Memory Capture	33
5.2.2. Private Web Browser.....	34
5.2.3. Detecting private mode:.....	35
5.3. Summary of Analysis in Private mode.....	39
6. Summary of Regular and Private Mode	40
7. Future Trends	41
8. Conclusion.	41
9. References.....	42

1. Introduction

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 Web sites 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 browser 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. It is very important for the digital forensic examiner to know various ways to perform forensics of web browser and these forensically collected artifacts from the suspect's browser can be useful in examination of case related to cybercrime. The aim and objective of the research paper is to identify source of information along with sound forensic techniques to collect evidences which shows internet usage.

It focuses on the most frequently used Web browsers, namely IE (Internet Explorer), Firefox, Chrome.

2. LITERATURE REVIEW

General research related to Web browser forensics has been targeted to specific Web browsers or to structural analysis of particular log files.

Jones (2003) explained the structure of the index.dat file and how to extract deleted activity records from Internet Explorer. He also introduced the Pasco tool to analyze the index.dat file. After simulating an actual crime, he described the IE and Firefox 2 Web browser forensics in two different publications (Jones and Rohyt, 2002a,b). In Section 1, he introduced the Pasco and Web Historian tools for IE forensics, which are available to the public, and the IE History and FTK tools, which are not. In Section 2, he described forensics in Firefox 2 using a cache file. The cache file in Firefox 2 is not saved in the same way as in IE, so he suggested an analysis method using the cache file structure.

Pereira (2009) explained in detail the changes in the history system that occurred when Firefox 2 was updated to Firefox 3 and proposed a new method of searching deleted history information using unallocated fields. During execution of Firefox 3, a rollback journal file is generated using a small section or the entire contents of Places.sqlite. If processing is stopped, this rollback journal file is erased (Pereira, 2009). For this reason, it is possible to extract history information of Firefox 3 in unallocated field. The author suggests a method of extracting history information from Firefox 3 by examining the SQLite database structure.

Their major focus is to see that artifacts related to private browsing, browsing history, usernames / email accounts, images, and videos is discovered or not. Andrew Marrington, Ibrahim Baggili and Talal Al Ismail has discussed the forensics of Google Chrome in normal and private mode and extracted evidences related to internet activity from hard disk.

Research paper wrote by JunghoonOha, SeungbongLeeb and SangjinLee has considered browser's log file as source of information to extracted potential artifacts. Huwida Said, Noora Al Mutawa and Ibtesam Al Awadhi extracted evidences using RAM analysis. Literature survey we used in in this research project,shows that most of the researcher used browser log, local files or RAM analysis as source of information to extract artifacts related of internet usage.

In our research paper, we used broader range of information source such as default artifacts location, history, cookies, login data, topsides, shortcuts, user profile, prefetch file and RAM analysis which gives an opportunity to extract more, related and various types of artifacts related to cybercrime.

3. Overview of Web Browser

A web browser is a software program that allows a user to locate, access, and display web pages. It is also only way used to access the internet for purpose such as accessing email, accessing social networking, uploading and downloading files-videos, and other information typically located on a web page at a website on World Wide Web (www) or a local network.

There are a variety of web browsers available with different features, and are designed to run on different operating systems. Common browsers include Google Chrome, Mozilla Firefox and Internet Explorer etc. These are also web browsers will be discussed deeply in this project.

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, session restore from a suspect's computer, and it is possible to analyze this evidence for Web sites visited, time and frequency of access, and search engine keywords used by suspect.

3.1. Types of Evidence

During investigation of web browser usage, there are various types of evidence found, as listed below:

- **History:** Records websites visited by date and time, details stored for each local user account, records number of times visited (frequency) and also tracks access of local system files.
- **Cookies:** They gave insight into what websites have been visited and what activities may have taken place there.

- **Cache :**
 - It is where web page components can be stored locally to speed up subsequent visits;
 - Gives the investigator a “snapshot in time” of what a user was looking at online;
 - Identifies websites which were visited;
 - Provides the actual files the user viewed on a given websites;
 - Cached files are tied to a specific local user account;
 - Timestamps shows when the site was first saved and last viewed.
- **Session Restore:** Automatic crash Recovery features built into the Browser.
- **Downloads:** All the downloaded files are stored in downloads folder so investigator would also check that default download folder.

3.2. How Browser works

The main function of Browser is to locate, retrieve and display content on the World Wide Web, including Web pages, images, video and other files.

As a client/Server model, the browser is the client run on a computer that contacts the web server and requests information. The Web server sends the information back to the Web browser which displays the results on the computer.

Architecture of Browser functionality

The below image shows the main components of a web browser:

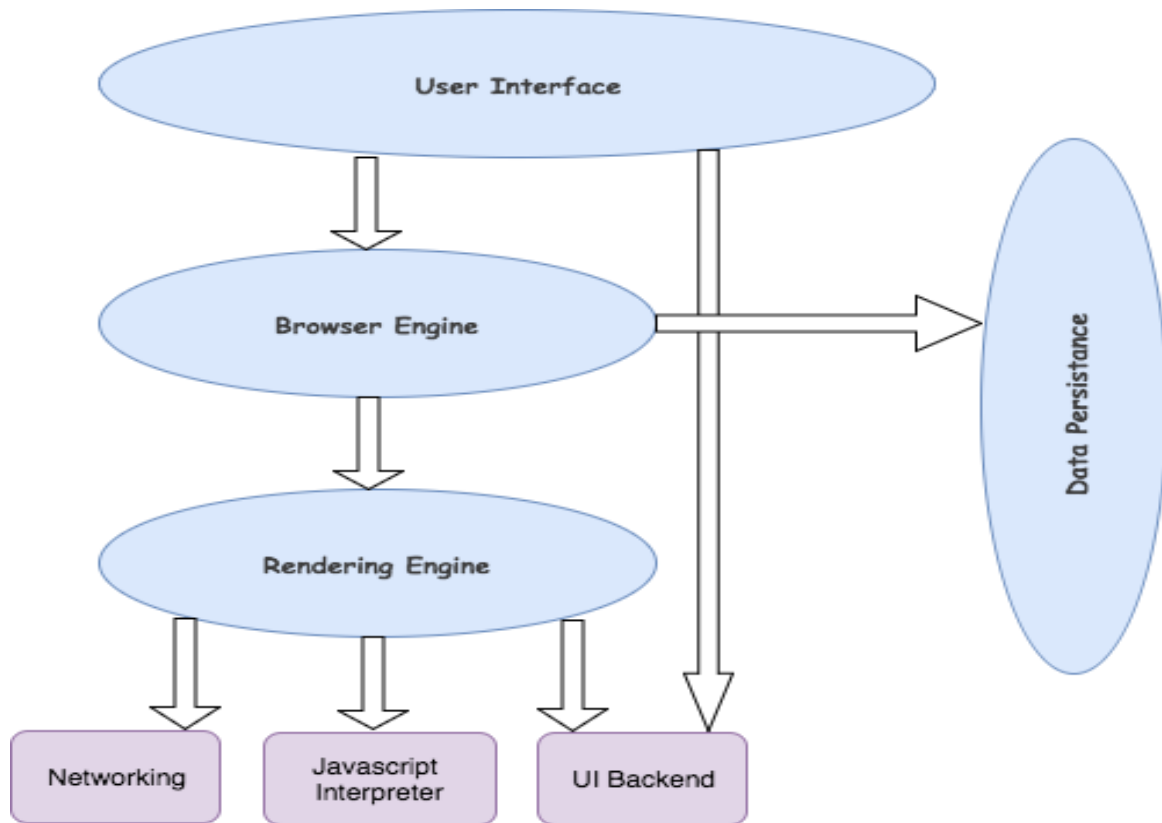


Fig.1.The main components of a web browser

Main Components of the browser:

1. **The User Interface:** The user interface is the space where user interface interacts with the browser. it includes the address bar, back and next buttons, home button, refresh and stop, bookmark option, etc. Every other part, except the window where requested web page is displayed, comes under it.
2. **The Browser Engine:** The browser engine works as a bridge between the User interface and the rendering engine. According to the inputs from various user interfaces, it queries and manipulates the rendering engine.
3. **The Rendering Engine:** The rendering engine, as the name suggests is responsible for rendering the requested web page on the browser screen. The rendering engine interprets the HTML,XML documents and images that are formatted using CSS and generates the layout that is displayed in the User interface. However, using plugins or

extensions, it can display other types data also. Different browsers use different rendering engines :

- Chrome & Opera15+:Blink
- Firefox & other Mozilla browsers :Gecko
- Internet Explorer : Trident

4. **Networking:** Components of the browser which retrieves the URLs using the common internet protocols of HTTP or FTP. The networking component hands all aspects of internet communication and security. The network component may implement a cache of retrieved documents in order to reduce network traffic.
5. **JavaScript Interpreter:** It is the component of the browser which interprets and executes the JavaScript code embedded in a website. The interpreted results are sent to the rendering engine for display. if the scripts is external then first the resource is fetched from the network. Parser keeps on hold until the scripts is executed.
6. **UI Backend:** UI backend is used for drawing basic widgets like combo boxes and windows. This backend exposes a generic interface that is not platform specific. It underneath uses operating system user interface methods.
7. **Data Persistence / Storage:** This is a persistence layer. Browser support storage mechanisms such as localStorage, IndexedDB, WebSQL and FileSystem.It are a small database created on the local drive of the computer where the browser is installed. It manages user data such as cache, cookies, bookmarks and preferences.

3.3. Most Popular Web Browsers

3.3.1. Google Chrome

It is the fastest and most used web browser in the world today. The folder contains files of our interest such as Bookmarks, Cookies, Current tabs, Top sites and web data. These web browsing artifacts are stored in SQLite Databases. The structure of the DB (Database) file is quite different from that of other renowned browsers such as Mozilla Firefox.

3.3.2. Mozilla Firefox

With Mozilla Firefox and its many variations, most of the information is stored in SQLite databases. We can find those databases at different locations upon the operating system.

3.3.3. Internet Explorer (IE)

It is installed on every single Windows systems as the default browser (except on newer versions of Windows 10 where Edge is Default, though IE is still installed), so it widely use. Internet explorer places its records in different places depending upon the version of windows.

TABLE1. File Location of popular Web Browser in Windows 10

Web Browser	File Path
Google Chrome	C:\Users\[USERNAME]\AppData\Local\Google\Chrome\ User Data\Default
Mozilla Firefox	C:\Users\[USERNAME]\AppData\Roaming\Mozilla\Firefox\Profiles\< profile folder >\
Internet Explorer	C:\Users\[USERNAME]\AppData\Loacal\Microsoft\Windows\Temporary Internet Files\. C:\Users\[USERNAME]\AppData\Loacal\Microsoft\Windows\Temporary Internet Files\Low.

4. Methodology

4.1. Preparation and Procedure

Forensic research in this paper is carried out on Oracle VM Virtual Box Version 5.1.32 running Windows 10 Pro. Chrome 68 (64bit), Firefox Quantum 61.0.2 (32 bit), and Internet Explorer 11 were installed on the virtual machine for experimenting with regular and private mode of operation. It was made sure that those browsers are in use for more than one week, so that abundant amount of information is present to carry out its forensic analysis.

In general, the investigation methodology depends largely on the OS installed on suspected PC, the web browsers under investigation, the type of evidence etc. One way to analyze the browser forensically is to take the image of the hard drive, select some user's search words from the history file, and use different browser forensic tools to search those keywords in the imaged drive.

The second approach for Browser usage analysis is to open each file present in the Default Chrome folder and analyze it separately for internet evidences using various forensic tools and techniques.

Table2. Where to find Browser Contents

Content	Found in (File/Folder)
Website visited	History, Cache, Cookies, Recovery Folders ,Suggested Sites
Visit count	History
Search Words	Auto Complete ,Cache
Sites Saved	Bookmarks

4.2. Tools and Technology used

Users perform various activities with a Web browser, such as information retrieval, e-mail, shopping, news, online banking, blogging, etc. Therefore, the forensic investigator should be able to analyze the user's activities when performing the investigation. Table 2 below enlists the software that will be used for Browser analysis of popular browsers discussed in this research paper.

Table 3.Representative forensic tools for Web browsers

Tool	Targeted Web Browser	Information to be Analyzes
DiskInternals Linux Leader (x64) 3.0.	Chrome,Firefox	Cookies,Urls,Downloads, Cache,search keywords
IECacheView 1.5.5.0	Internet Explorer	Webcache
Index.Dat Viewer 4	Internet Explorer	Index.dat
FoxAnalysis 1.6.0.	Firefox	Cookies, History, Download list, Bookmarks
ChromeAnalysis 1.7.2.	Chrome	History, Cookies, Bookmarks, Download list, Search words
Hetman Internet Spy	Internet Explorer, Firefox, Chrome	History,Downloads,Sessions, Topsites
WinHex 19.3.0.0	Internet Explorer, Firefox, Chrome	Cache, History, Cookies
DB Browser for SQLite 3.10.1.	Firefox	Cookies.sqlite (Cookies)
Magnet Ram Capture 1.1.0.2.	Windows 10 (Internet Explorer, Firefox, Chrome)	Acquire Live Ram image

4.3. Integrated Analysis

Web browser is diverse, with each one having its own characteristics. This enables users to choose their own Favorites or to try various Web browsers at the same time. In this situation, it is hard to trace the Web sites that a user has visited if the forensic investigator can analyze only log files from a specific Web browser.

Therefore, the investigator must be able to examine all existing Web browsers in one system and to perform integrated analysis of multiple Web browsers. For integrated analysis, the critical information, more than all other information, is time information. Every Web browser's log file contains time information, and therefore it is possible to construct a timeline array using this time information. However, the three popular Web browsers have different time format.

4.4. Timeline Analysis

In a forensic investigation, it is critical to detect the movement of suspect along a timeline. By performing a timeline analysis, the investigator can trace the criminal activities of the suspect in their entirety. The analysis provides the path of motion from one Web site to another and what the suspect did on each specific Web site. More than to that, time zone information must be considered.

TABLE 4. Time formats used by three popular browsers

Web browsers	Time Format
Google Chrome	WEBKIT Time :microsecond(10^{-6}) Since January 1,1601 00:00:00 (UTC)
Mozilla Firefox	PRTIME: microsecond (10^{-6}) Since January 1,1970 00:00:00 (UTC)
Internet Explore	FILETIME:100-ns (10^{-9}) Since January 1,1601 00:00:00 (UTC)

4.5. Analysis of search history

Beyond the investigation of which Web sites the suspect has visited, it is important to investigate the search words he used in the search engine. These search words may provide keywords for his crime, whether a single word or sometimes a sentence. In this case, search words are evidence of the suspect's efforts to gather information for his crime and may specify the purpose, target, and methods of the crime. After using a search engine, search words are saved as HTTP URL information. Figure Bellow shows the general HTTP URL Structure:

Https://	Host	Port	/	Path	?	Search Part
----------	------	------	---	------	---	-------------

It is important for examiner to find the keyword which stored in the URL, for example, in Google search engine, if the word forensic is entered, the following URL is generated:

<https://www.google.co.in/search?q=forensic&oq=forensic&aqs=chrome..69i57j69i60l3j69i59l2.3747863j0j8&sourceid=chrome&ie=UTF-8>

From this above HTTP URL, more information can be extracted, for example the host is google.com and the path is/search.

This provides relevant HTTP URL information related to search activity. The search words that the suspect wants to find are clearly noticeable after the variable q, For instance, forensic. In other words, the value of the variable q is the search words.

4.6. Analysis on URL encoding

In an HTTP URL, characters other than ASCII are encoded for storage. In other words, when encoded characters appear, the Words are not English. In a digital forensic investigation, encoded characters create confusion for the investigator.

Therefore, decoding encoded characters is important for investigators in non-English-speaking countries. In most cases, non-English search words are encoded. If you search for the word forensic in Korean, the resulting HTTP URL address is as follows:

`http://www.google.com/search?hl%4den&source%4hp&q%4%ED%8F%AC%EB%A0%8C%EC%8B%9D&aq%4f&oq%4&aqi%4g10.`

Encoded characters in an HTTP URL are expressed by means of a hexadecimal code and the character %, which is added before every one-byte character.

4.7. Web Browser Mode Analysed.

- I. Regular Mode: it is the default mode that is most commonly used. it stores entire user's activity on disk.
- II. Private Mode: This mode is designed to give user privacy while surfing. It does not keep a track of all of the user's activity.

5. Result of Evidence collection and Analysis

5.1. Regular Mode Analysis

5.1.1. Google Chrome

Google Chrome browser is an open source program for accessing the World Wide Web and running Web-based applications .It is also the fastest and most used web browser in the world today.

This section will discuss the analysis of the artifacts stored on disk in the Regular Browsing mode from the forensic point of view. Chrome version 68 was installed on the laptop running Windows 10. This section covers the forensic analysis of Google Chrome by opening the files present in the Default Chrome folder i.e. History, Cookies, Bookmarks, Top Sites, Web Data, Shortcuts etc., separately in various forensic tools and analyzing them for required internet evidences.

5.1.1. A. History

The History file found in the path bellow:

C:\user\win10\AppData\Local\Google\Chrome\UserData\Default\History folder is basically a database file that contains record of user's all web history. It contains tables for downloads, visits, urls, segment_usage, keyword_search_terms, meta, presentation, and segments, that provide useful information to the forensic experts about the victim's web activity. The forensic investigator can simply use History Viewer tool to open the History file present in the Chrome Default folder. The software makes search easy for the investigator as seen in the Figure 1 below.

ChromeAnalysis - Chrome Internet History Analysis

File Filter Sort Cache Help

Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache Session Tabs

☐ Filter web visit type Link Show Timeline

ID	Date Visited (UTC, DST Enabled)	URL	Visit Type	Visited From	Total Visit Count	Calculated Visit Count	Duration (seconds)	Title
144	9/5/2018 3:10:07 AM	file:///C:/Program%20Files%20(x86...	Auto Toplevel		1	1	0	ChromeAnalysis - Help
143	9/5/2018 3:06:10 AM	https://www.foxtonforensics.com/...	Link	https://ww...	2	2	0	Browser History Viewer - Download Foxton Forensics
142	9/5/2018 3:05:55 AM	https://www.foxtonforensics.com/...	Link	https://ww...	3	3	15.56	Download Digital Forensic Software Foxton Forensi...
141	9/5/2018 3:05:22 AM	https://www.foxtonforensics.com/f...	Form Submit	https://ww...	2	2	33.03	FoxAnalysis - Download Foxton Forensics
140	9/5/2018 3:05:17 AM	https://www.foxtonforensics.com/f...	Link	https://ww...	2	2	4.60	FoxAnalysis - Download Foxton Forensics
139	9/5/2018 3:04:49 AM	https://www.foxtonforensics.com/...	Link	https://ww...	3	3	28.30	Download Digital Forensic Software Foxton Forensi...
138	9/5/2018 3:04:47 AM	https://www.foxtonforensics.com/...	Form Submit	https://ww...	6	6	1.71	ChromeAnalysis - Download Foxton Forensics
137	9/5/2018 3:04:42 AM	https://www.foxtonforensics.com/...	Link	https://ww...	6	6	4.99	ChromeAnalysis - Download Foxton Forensics
136	9/5/2018 3:04:40 AM	https://www.foxtonforensics.com/...	Form Submit	https://ww...	6	6	0	ChromeAnalysis - Download Foxton Forensics
135	9/5/2018 3:04:36 AM	https://www.foxtonforensics.com/...	Link	https://ww...	6	6	4.58	ChromeAnalysis - Download Foxton Forensics
134	9/5/2018 3:03:49 AM	https://www.foxtonforensics.com/...	Form Submit	https://ww...	6	6	0	ChromeAnalysis - Download Foxton Forensics
133	9/5/2018 3:03:46 AM	https://www.foxtonforensics.com/...	Link	https://ww...	6	6	2.93	ChromeAnalysis - Download Foxton Forensics
132	9/5/2018 3:03:06 AM	https://www.foxtonforensics.com/...	Link	https://ww...	3	3	96.01	Download Digital Forensic Software Foxton Forensi...
131	9/5/2018 3:02:54 AM	https://www.foxtonforensics.com/...	Link	https://ww...	2	2	12.33	Browser History Viewer - Free tool to analyse web br...
130	9/5/2018 3:02:45 AM	https://www.google.com/search?e...	Form Submit	https://ww...	1	1	0	browser history viewer - Google Search
129	9/5/2018 2:59:33 AM	https://hetmanrecovery.com/web...	Link		1	1	0	Software For Viewing The History of Visited Sites in ...
128	9/5/2018 2:58:50 AM	https://www.techworld.com/downl...	Link		1	1	23.22	BrowsingHistoryView 2.17 Software Downloads T...
127	9/5/2018 2:58:42 AM	https://www.techworld.com/downl...	Link		1	1	34.17	
126	9/5/2018 2:58:37 AM	https://www.techworld.com/downl...	Link		1	1	0	BrowsingHistoryView 2.17 Software Downloads T...

Fig. 2: History file opened in ChromeAnalysis

Hetman Internet Spy 1.0 (Unregistered version)

Browser information
Select the required section on the left

Find Info panel Export gfsudf Google Chrome

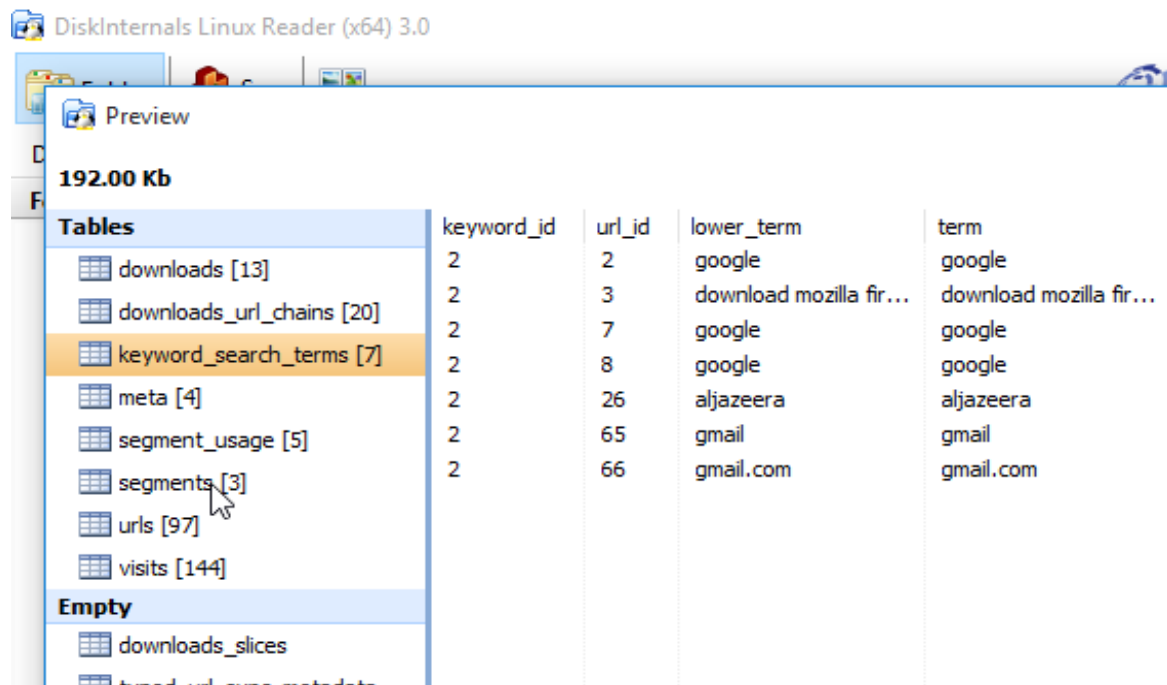
Visits	Search	Total items: 152
History	Set filter here...	
Passwords	Set filter here...	
Sessions	Set filter here...	
Top Sites		
Downloads		
Files		
Images		

Website	Title	Visit time
file	ChromeAnalysis - Help	9/4/2018 7:10 PM
www.foxtonforensics.com	Browser History Viewer - Download Foxton Forensics	9/4/2018 7:06 PM
www.foxtonforensics.com	Download Digital Forensic Software Foxton Forensics	9/4/2018 7:05 PM
www.foxtonforensics.com	FoxAnalysis - Download Foxton Forensics	9/4/2018 7:05 PM
www.foxtonforensics.com	FoxAnalysis - Download Foxton Forensics	9/4/2018 7:05 PM
www.foxtonforensics.com	Download Digital Forensic Software Foxton Forensics	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis - Download Foxton Forensics	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis - Download Foxton Forensics	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis - Download Foxton Forensics	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis - Download Foxton Forensics	9/4/2018 7:04 PM
www.foxtonforensics.com	Only in Registered version!	9/4/2018 7:03 PM
www.foxtonforensics.com	Only in Registered version!	9/4/2018 7:03 PM
www.foxtonforensics.com	Only in Registered version!	9/4/2018 7:03 PM
www.foxtonforensics.com	Only in Registered version!	9/4/2018 7:02 PM

Fig. 3: History file opened in Hetman Internet spy.

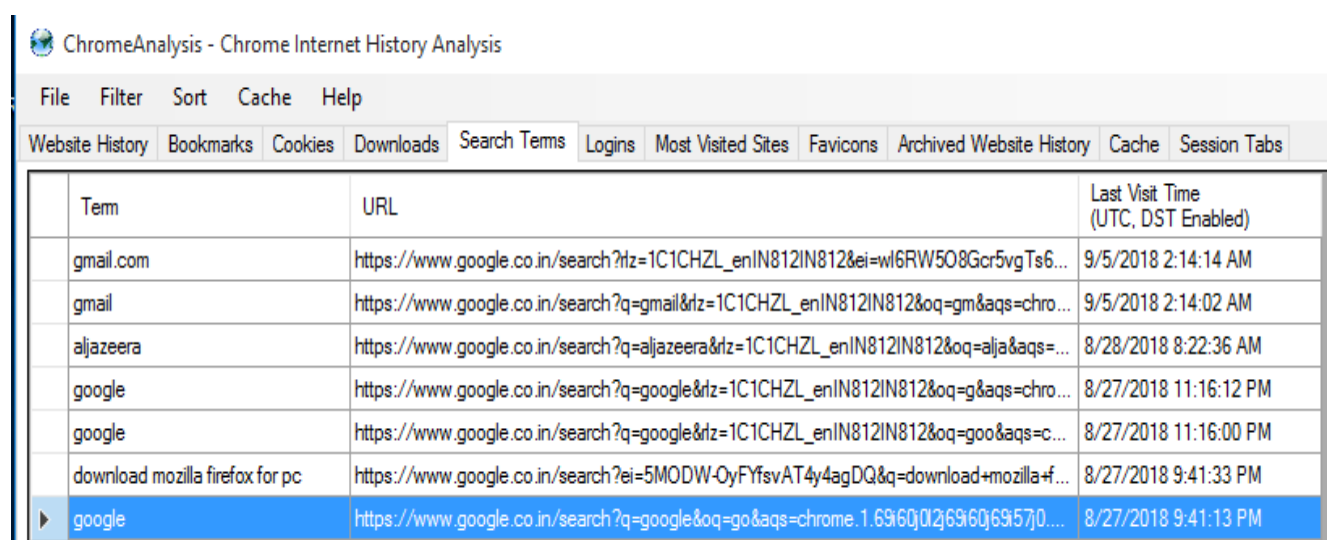
5.1.1. B. Search Keywords

It is important for the forensic examiner to understand that the words searched by the user, on the web browser, simply get stored in the URL. The recent search words of the suspect can be viewed by opening the Default Chrome folder in tool like DiskInternals Linux Reader, ChromeAnalysis, etc.



keyword_id	url_id	lower_term	term
2	2	google	google
2	3	download mozilla fir...	download mozilla fir...
2	7	google	google
2	8	google	google
2	26	aljazeera	aljazeera
2	65	gmail	gmail
2	66	gmail.com	gmail.com

Fig. 4: keyword searched terms opened in DiskInternals Linux Reader.



Term	URL	Last Visit Time (UTC, DST Enabled)
gmail.com	https://www.google.co.in/search?rlz=1C1CHZL_enIN812IN812&ei=wI6RW5O8Gcr5vgTs6...	9/5/2018 2:14:14 AM
gmail	https://www.google.co.in/search?q=gmail&rlz=1C1CHZL_enIN812IN812&oq=gm&aqs=chro...	9/5/2018 2:14:02 AM
aljazeera	https://www.google.co.in/search?q=aljazeera&rlz=1C1CHZL_enIN812IN812&oq=alja&aqs=...	8/28/2018 8:22:36 AM
google	https://www.google.co.in/search?q=google&rlz=1C1CHZL_enIN812IN812&oq=g&aqs=chro...	8/27/2018 11:16:12 PM
google	https://www.google.co.in/search?q=google&rlz=1C1CHZL_enIN812IN812&oq=goo&aqs=c...	8/27/2018 11:16:00 PM
download mozilla firefox for pc	https://www.google.co.in/search?ei=5MODW-OyFYfsvAT4y4agDQ&q=download+mozilla+f...	8/27/2018 9:41:33 PM
google	https://www.google.co.in/search?q=google&oq=go&aqs=chrome.1.69i6QjQ2j69i6Qj69i57j0....	8/27/2018 9:41:13 PM

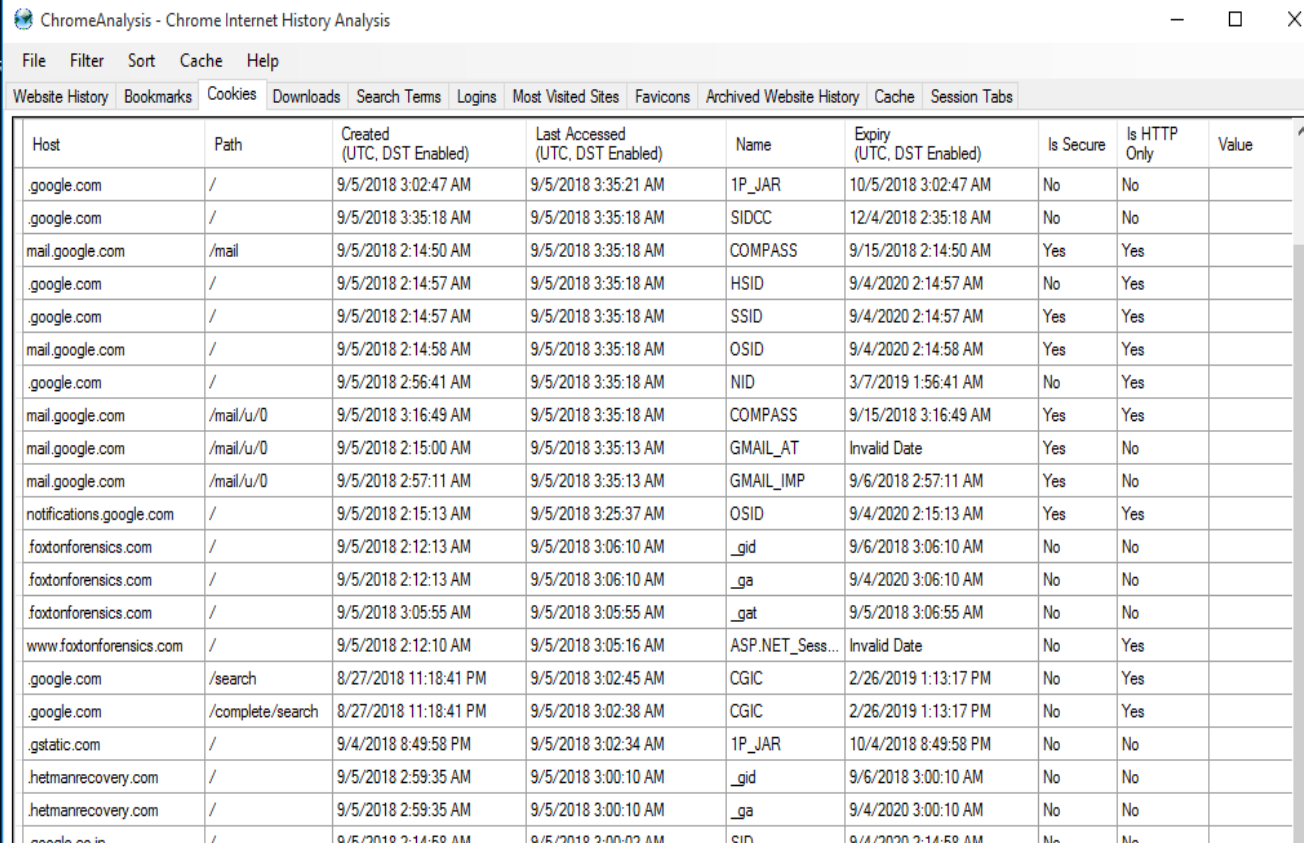
Fig. 5: keyword searched terms opened in ChromeAnalysis.

5.1.1. C. Cookies

Cookies are basically the SQL files, that websites create to store the users' browsing information such as his/her site preferences, location or personal profile information etc. Cookies also help analyze web traffic and are often necessary for website's functionality.

The cookies are of two types; first party (set by site domain) and third party cookies (comes from sources that display items or adds on that particular page.)

To view the cookies from Google Chrome, go to Chrome Menu > Settings > Show advance settings > Privacy section > All cookies and site data. Following figures shows list of the cookies which are stored in database.



Host	Path	Created (UTC, DST Enabled)	Last Accessed (UTC, DST Enabled)	Name	Expiry (UTC, DST Enabled)	Is Secure	Is HTTP Only	Value
google.com	/	9/5/2018 3:02:47 AM	9/5/2018 3:35:21 AM	1P_JAR	10/5/2018 3:02:47 AM	No	No	
google.com	/	9/5/2018 3:35:18 AM	9/5/2018 3:35:18 AM	SIDCC	12/4/2018 2:35:18 AM	No	No	
mail.google.com	/mail	9/5/2018 2:14:50 AM	9/5/2018 3:35:18 AM	COMPASS	9/15/2018 2:14:50 AM	Yes	Yes	
google.com	/	9/5/2018 2:14:57 AM	9/5/2018 3:35:18 AM	HSID	9/4/2020 2:14:57 AM	No	Yes	
google.com	/	9/5/2018 2:14:57 AM	9/5/2018 3:35:18 AM	SSID	9/4/2020 2:14:57 AM	Yes	Yes	
mail.google.com	/	9/5/2018 2:14:58 AM	9/5/2018 3:35:18 AM	OSID	9/4/2020 2:14:58 AM	Yes	Yes	
google.com	/	9/5/2018 2:56:41 AM	9/5/2018 3:35:18 AM	NID	3/7/2019 1:56:41 AM	No	Yes	
mail.google.com	/mail/u/0	9/5/2018 3:16:49 AM	9/5/2018 3:35:18 AM	COMPASS	9/15/2018 3:16:49 AM	Yes	Yes	
mail.google.com	/mail/u/0	9/5/2018 2:15:00 AM	9/5/2018 3:35:13 AM	GMAIL_AT	Invalid Date	Yes	No	
mail.google.com	/mail/u/0	9/5/2018 2:57:11 AM	9/5/2018 3:35:13 AM	GMAIL_IMP	9/6/2018 2:57:11 AM	Yes	No	
notifications.google.com	/	9/5/2018 2:15:13 AM	9/5/2018 3:25:37 AM	OSID	9/4/2020 2:15:13 AM	Yes	Yes	
foxtonforensics.com	/	9/5/2018 2:12:13 AM	9/5/2018 3:06:10 AM	_gid	9/6/2018 3:06:10 AM	No	No	
foxtonforensics.com	/	9/5/2018 2:12:13 AM	9/5/2018 3:06:10 AM	_ga	9/4/2020 3:06:10 AM	No	No	
foxtonforensics.com	/	9/5/2018 3:05:55 AM	9/5/2018 3:05:55 AM	_gat	9/5/2018 3:06:55 AM	No	No	
www.foxtonforensics.com	/	9/5/2018 2:12:10 AM	9/5/2018 3:05:16 AM	ASP.NET_Sess...	Invalid Date	No	Yes	
google.com	/search	8/27/2018 11:18:41 PM	9/5/2018 3:02:45 AM	CGIC	2/26/2019 1:13:17 PM	No	Yes	
google.com	/complete/search	8/27/2018 11:18:41 PM	9/5/2018 3:02:38 AM	CGIC	2/26/2019 1:13:17 PM	No	Yes	
gstatic.com	/	9/4/2018 8:49:58 PM	9/5/2018 3:02:34 AM	1P_JAR	10/4/2018 8:49:58 PM	No	No	
hetmanrecovery.com	/	9/5/2018 2:59:35 AM	9/5/2018 3:00:10 AM	_gid	9/6/2018 3:00:10 AM	No	No	
hetmanrecovery.com	/	9/5/2018 2:59:35 AM	9/5/2018 3:00:10 AM	_ga	9/4/2020 3:00:10 AM	No	No	
google.co.in	/	9/5/2018 2:14:58 AM	9/5/2018 3:00:02 AM	SID	9/4/2020 2:14:58 AM	No	No	

Fig. 6: Cookie file opened in ChromeAnalysis.

DiskInternals Linux Reader (x64) 3.0

Folders Save

DiskInternals Data Recovery Software Search C:

Preview

384.00 Kb

Tables	creation_utc	host_key	name	value	path	expires_utc
cookies [598]	13179876115350918	www.mozilla.org	moz-stub-attributio...		/	13179962...
	13179876115351325	www.mozilla.org	moz-stub-attributio...		/	13179962...
meta [3]	13179876145992919	www.mozilla.org	experiment-downlo...		/en-US/firefox...	13179962...
Empty	13179876116724918	.mozilla.org	_ga		/	13242948...
System	13179876116725740	.mozilla.org	_gid		/	13179962...
sqlite_master	13179881760815542	.google.co.in	CGIC		/complete/search	13195660...
	13179881760815578	.google.co.in	CGIC		/search	13195660...
	13179881921561372	.google.com	CGIC		/complete/search	13195660...
	13179881921561403	.google.com	CGIC		/search	13195660...
	13179881945962360	.fsdn.com	__cfduid		/	13211417...
	13179881947302743	.advertising.com	Cfp		/	0
	13179881951220692	.sourceforge.net	_scp		/	13242953...
	13179881951429488	.scorecardresearch...	UID		/	13242089...
	13179881951429536	.scorecardresearch...	UIDR		/	13242089...
	13179881951948534	.mathtag.com	uuid		/	13213837...
	13179881951993076	.eyeota.net	mako_uid		/	13211417...
	13179881952045591	.bluekai.com	bkdc		/	13195433...
	13179881952108735	.crwdcntrl.net	_cc_dc		/	13203209...
	13179881953146653	.sourceforge.net	_gads		/	13242913...
	13179881953170671	.exposebox.com	_etn		/	13210985...
	13179881954021993	.mfadsrvr.com	huuid		/	13242953...

Fig. 7: Cookie file opened in DiskInternal Linux Leader

5.1.1. D. Top Sites

Top sites, or the sites most visited by the user can be viewed by opening the C:\user\Win10\AppData\Local\Google\Chrome\UserData\Default\Top Sites file in DB Browser for SQLite. It provides URL along with data count etc. for the most viewed sites. However, ChromeAnalysis and hetman Internet spy softwares can also show these details, as seen in Figure 7 and 8.

ChromeAnalysis - Chrome Internet History Analysis

File Filter Sort Cache Help

Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache Session Tabs

URL Rank	URL	Title	Redirects	Last Updated (UTC, DST Enabled)
0	https://www.google.com/	Google	https://www.google.com/	9/4/2018 8:06:27 PM
1	http://igihe.com/	IGIHE Amakuru, Politiki, Ubukungu, ...	https://igihe.com/ http://igihe.com/	8/28/2018 8:16:09 AM
2	https://www.google.com/_chrome/newtab?e=UTF-8		https://www.google.com/_chrome/newtab?e=...	8/27/2018 9:42:25 PM
3	https://chrome.google.com/webstore?hl=en	Chrome Web Store	https://chrome.google.com/webstore?hl=en	8/27/2018 9:40:24 PM

Fig. 8: Top sites opened in ChromeAnalysis .

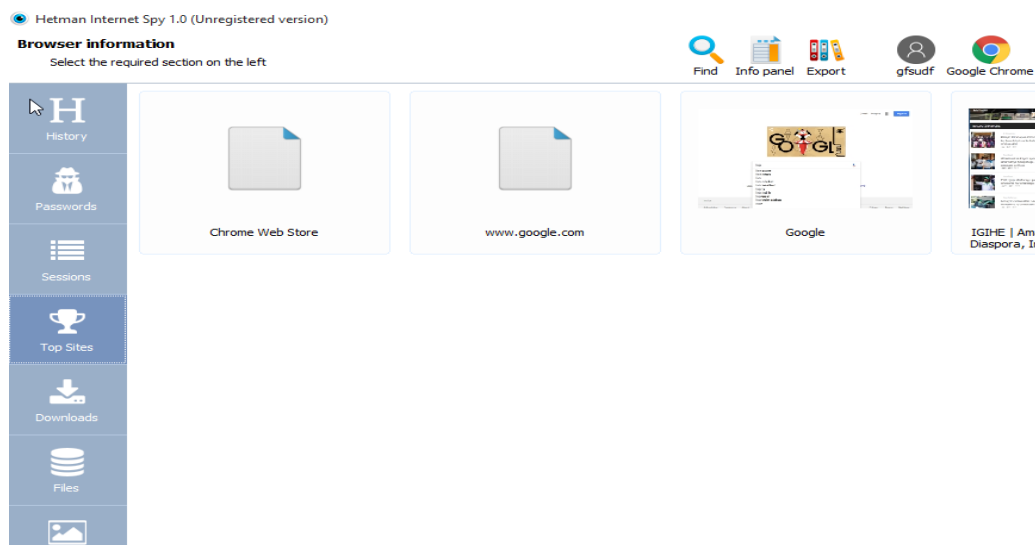


Fig. 9: Top sites opened in Hetman Internet spy.

5.1.1. E. Downloads

It is easy to show all download file in SQLite that downloaded by user. it will display current path, target path, start time of download, how many bytes received etc. Download folder is there in its default location in computer also, if user wants to change its default path then he/she can change that path.

ChromeAnalysis - Chrome Internet History Analysis									
File Filter Sort Cache Help									
Website History Bookmarks Cookies Downloads Search Terms Logins Most Visited Sites Favicons Archived Website History Cache Session Tabs									
<input type="checkbox"/> Filter download state Paused									
ID	URL	Full Path	Start Time (UTC, DST Enabled)	End Time (UTC, DST Enabled)	State	Bytes Downloaded	Total Bytes	Opened	
13	https://www.foxtonf...	C:\Users\gfsudf\Downloads\FoxAnalysis_v1.6.0_Trial.zip	9/5/2018 3:05:19 AM	9/5/2018 3:05:32 AM	Complete	1112032	1112032	No	
12	https://www.foxtonf...	C:\Users\gfsudf\Downloads\ChromeAnalysis_v1.7.2_Trial (2)...	9/5/2018 3:04:44 AM	9/5/2018 3:04:55 AM	Complete	1060005	1060005	No	
11	https://www.foxtonf...	C:\Users\gfsudf\Downloads\ChromeAnalysis_v1.7.2_Trial (1)...	9/5/2018 3:04:38 AM	9/5/2018 3:04:49 AM	Complete	1060005	1060005	No	
10	https://www.foxtonf...	C:\Users\gfsudf\Downloads\ChromeAnalysis_v1.7.2_Trial.zip	9/5/2018 3:03:57 AM	9/5/2018 3:04:10 AM	Complete	1060005	1060005	No	
9	https://hetmanrecov...	C:\Users\gfsudf\Downloads\hetman_internet_spy (1).exe	9/5/2018 3:00:11 AM		In Progr...	5390063	12052960	Yes	
8	https://hetmanrecov...	C:\Users\gfsudf\Downloads\hetman_internet_spy.exe	9/5/2018 3:00:01 AM	9/5/2018 3:02:05 AM	Complete	12052960	12052960	Yes	
7	https://www.foxtonf...	C:\Users\gfsudf\Downloads\BrowserHistoryViewer_v1.2.2.zip	9/5/2018 2:15:23 AM	9/5/2018 2:17:56 AM	Complete	15633889	15633889	No	
6	https://downloads.s...	C:\Users\gfsudf\Downloads\LiveViewPublicInstallerv0.7a.exe...	9/4/2018 8:49:21 PM	9/4/2018 8:49:22 PM	Complete	194	194	No	
5	https://downloads.s...	C:\Users\gfsudf\Downloads\LiveViewPublicInstallerv0.7a.exe...	9/4/2018 8:48:17 PM	9/4/2018 8:48:19 PM	Complete	194	194	Yes	
4	https://downloads.s...	C:\Users\gfsudf\Downloads\Chromensics 1.6 (2).zip	8/27/2018 11:24:35 PM	8/27/2018 11:25:57 PM	Complete	17897001	17897001	No	
3	https://downloads.s...	C:\Users\gfsudf\Downloads\Chromensics 1.6 (1).zip	8/27/2018 11:22:42 PM	8/27/2018 11:24:14 PM	Complete	17897001	17897001	No	
2	https://downloads.s...	C:\Users\gfsudf\Downloads\Chromensics 1.6.zip	8/27/2018 11:20:18 PM	8/27/2018 11:21:45 PM	Complete	17897001	17897001	No	
1	https://download.mo...	C:\Users\gfsudf\Downloads\Firefox Installer.exe	8/27/2018 9:42:36 PM	8/27/2018 9:42:41 PM	Complete	313768	313768	Yes	

Fig.10: Downloaded files, size and the path of their location opened in ChromeAnalysis

Hetman Internet Spy 1.0 (Unregistered version)

Browser information
Select the required section on the left

Find Info panel Export gfsudf Google Chrome

Website	File name	File size	Download start
www.foxtonforensics.com	FoxAnalysis_v1.6.0_Trial.zip	1,085.97 KB	9/4/2018 7:05 PM
www.foxtonforensics.com	ChromeAnalysis_v1.7.2_Trial (2).zip	1,035.16 KB	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis_v1.7.2_Trial (1).zip	1,035.16 KB	9/4/2018 7:04 PM
www.foxtonforensics.com	ChromeAnalysis_v1.7.2_Trial.zip	1,035.16 KB	9/4/2018 7:03 PM
hetmanrecovery.com	hetman_internet_spy (1).exe	11,770.47 KB	9/4/2018 7:00 PM
hetmanrecovery.com	hetman_internet_spy.exe	11,770.47 KB	9/4/2018 7:00 PM
www.foxtonforensics.com	BrowserHistoryViewer_v1.2.2.zip	15,267.47 KB	9/4/2018 6:15 PM
master.dl.sourceforge.net	LiveViewPublicInstallerv0.7a.exe (1).asc	0.19 KB	9/4/2018 12:49 PM
master.dl.sourceforge.net	LiveViewPublicInstallerv0.7a.exe.asc	0.19 KB	9/4/2018 12:48 PM
excellmedia.dl.sourceforge.net	Chromensics 1.6 (2).zip	17,477.54 KB	8/27/2018 3:24 PM
excellmedia.dl.sourceforge.net	Chromensics 1.6 (1).zip	17,477.54 KB	8/27/2018 3:22 PM

Fig. 11: Downloaded files opened in Hetman Internet Spy.

5.1.1. F. Other Internet Artifacts

There are also many files, opened by different tools, which have meaning in investigation process, because they hold artifacts that investigator use to identify and retrieve meaningful evidence. Figure 12 bellow show some of those file.

Hetman Internet Spy 1.0 (Unregistered version)

Browser information
Select the required section on the left

Find Info panel Export gfsudf Google Chrome

Name	Type	Size	Modified	Created
Current Session	SNSS File	58.81 KB	9/5/2018 2:25 AM	8/27/2018 1:40 PM
Current Tabs	SNSS File	61.03 KB	9/4/2018 7:11 PM	8/27/2018 1:42 PM
DownloadMetadata	File	1.16 KB	9/4/2018 7:05 PM	8/27/2018 3:21 PM
Favicons	SQLite Database	100.00 KB	9/4/2018 7:05 PM	8/27/2018 1:40 PM
History	SQLite Database	192.00 KB	9/4/2018 7:10 PM	8/27/2018 1:40 PM
History Provider Cache	File	2.28 KB	9/4/2018 12:05 PM	8/27/2018 2:24 PM
Last Session	SNSS File	532.33 KB	9/4/2018 1:17 PM	8/27/2018 1:40 PM
Last Tabs	SNSS File	17.61 KB	9/4/2018 1:17 PM	8/27/2018 1:42 PM
Login Data	SQLite Database	18.00 KB	9/4/2018 6:15 PM	8/27/2018 1:40 PM
Network Action Predictor	SQLite Database	96.00 KB	9/4/2018 7:06 PM	8/27/2018 1:40 PM
Network Persistent State	JSON File	27.45 KB	9/5/2018 2:26 AM	8/27/2018 1:41 PM

Fig.12. other artifacts files opened in hetman Internet spy.

5.1.1.G. Recover Deleted History

If however the culprit/user deletes the browsing history from the Chrome Menu> Clear History, all the history files present in the memory gets deleted. However, the downloads, cookies, and cache files are initialized to zeroes. (Junghoon, Seungbong & Sangjin, 2011).

In short, we observe that Google Chrome really stores a wealth of internet artifacts on the user's drive. Among all the files, the history file alone provides sufficient information to the forensic investigator to reconstruct the timeline of user's activity or at the least get the idea of his intention. This observation is important in cases of child pornography, electronic fraud, non-repudiation cases etc. Moreover, the forensic investigator must also analyze the cookie's file to get the session ID of the user, top sites file to look for suspect's most visited sites, login data file to note suspect's credentials for various websites, etc.

In terms of privacy, the regular mode of operation is not at all secure, since it stores almost all the surfing activity of the user on the hard drive. However, with the availability of various browser forensics tools in the market, the forensic investigation of web browsers has been made quite easy for the forensic investigators.

5.1.2. Mozilla Firefox

Mozilla Firefox is a free and open source web browser descended from the Mozilla application suite and managed by Mozilla Corporation. Firefox stores all browsing information in a SQLite database instead of a flat file. The database files that are required are places.sqlite, formhistory.sqlite, downloads.sqlite, cookies.sqlite, search.sqlite, etc. For Windows 10, Firefox stores its files and database in the following default locations in C drive.

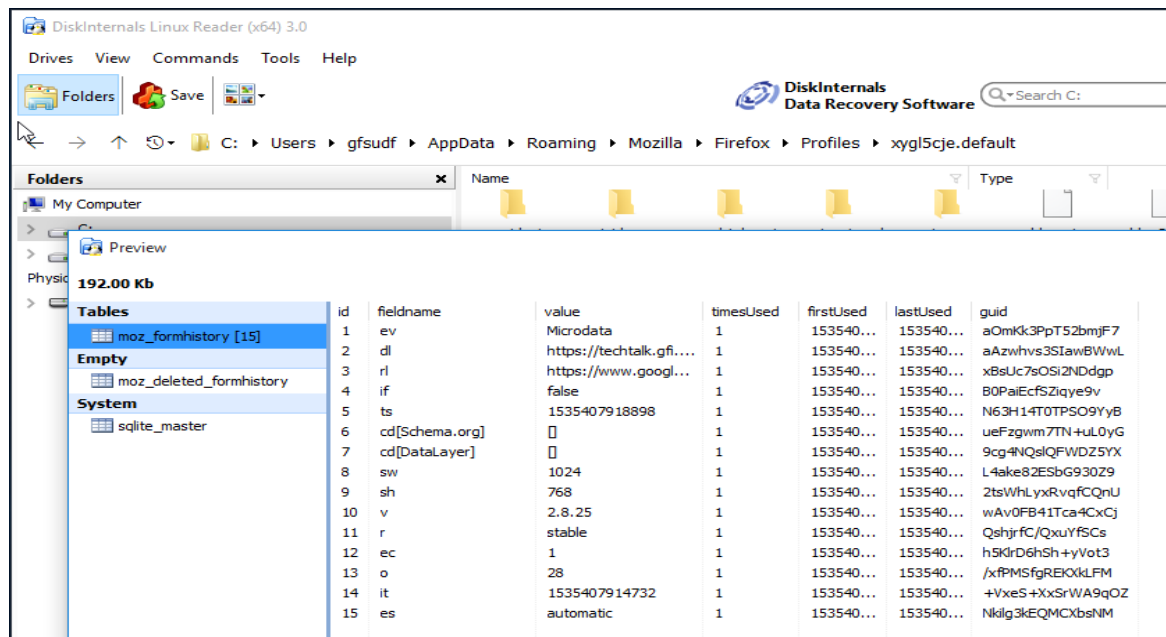
C:\users\[username]\AppData\Roaming\Mozilla\Firefox\Profile\< profile folder>

The profile folder contains files .i.e. places, sqlite, formhistory.sqlite, downloads.sqlite etc.

This section will discuss the analysis of the artifacts stores on disk in the Regular Browsing mode from the forensic point of view. Analysis of web activities for Mozilla Firefox done by opening the files present in the profile folder includes cookies.sqlite, formhistory.sqlite, etc, separately in various web forensic tools, in order to find significant internet evidence.

5.1.2. A. History

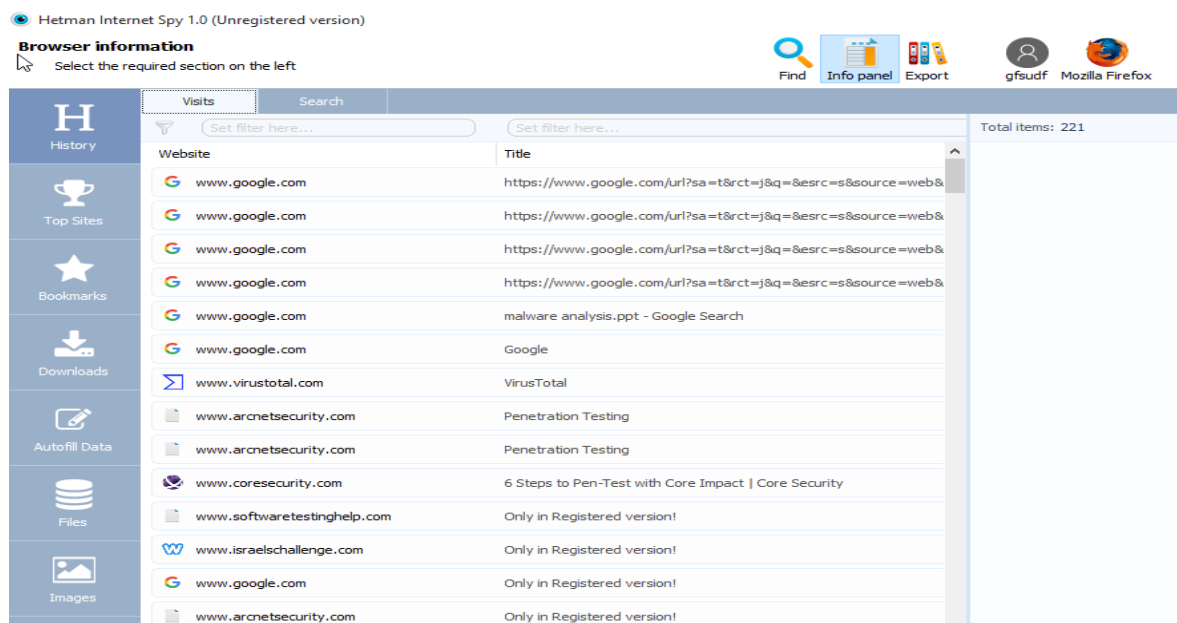
History file contains all browsing information of the users like visited links (URLs), downloads, search terms, and download chains etc. This history file can be viewed using DiskInternals Linux Reader and hetman Internet spy tools .Following figures 14,15 and 16 show list of the URL searched by user.



The screenshot shows the DiskInternals Linux Reader interface. The file path is C:\Users\gfsudf\AppData\Roaming\Mozilla\Firefox\Profiles\xygl5cje.default. The 'moz_formhistory [15]' table is selected, displaying a list of browsing history entries.

id	fieldname	value	timesUsed	firstUsed	lastUsed	guid
1	ev	Microdata	1	153540...	153540...	aOmKk3Pt52bmjF7
2	dl	https://techtalk.gfi...	1	153540...	153540...	aAzwhvs3SIawBWwL
3	rl	https://www.googl...	1	153540...	153540...	xBsUc7sOSi2NDdgp
4	if	false	1	153540...	153540...	B0PaIEcFSZiqye9v
5	ts	1535407918898	1	153540...	153540...	N63H14T0TPSO9Yy8
6	cd[Schema.org]	[]	1	153540...	153540...	ueFzgw7TN+uL0yG
7	cd[DataLayer]	[]	1	153540...	153540...	9cg4NQslQFWDZ5YX
8	sw	1024	1	153540...	153540...	L4ake82ESbG930Z9
9	sh	768	1	153540...	153540...	2tsWhLyxRvqfCQnU
10	v	2.8.25	1	153540...	153540...	wAv0FB41Tca4CxCj
11	r	stable	1	153540...	153540...	QshjrFC/QxuYfScs
12	ec	1	1	153540...	153540...	h5KlrD6hSh+yVot3
13	o	28	1	153540...	153540...	/xPMSfgREKxkLFM
14	it	1535407914732	1	153540...	153540...	+VxeS+XxSrWA9qOZ
15	es	automatic	1	153540...	153540...	Nklg3kEQMCXbsNM

Fig.13: History file opened in DiskInternals Linux Reader



The screenshot shows the Hetman Internet Spy interface. The 'Visits' section is active, displaying a list of browsing history entries. The total number of items is 221.

Website	Title
www.google.com	https://www.google.com/url?sa=t&rc=j&q=&esrc=s&source=web&
www.google.com	https://www.google.com/url?sa=t&rc=j&q=&esrc=s&source=web&
www.google.com	https://www.google.com/url?sa=t&rc=j&q=&esrc=s&source=web&
www.google.com	https://www.google.com/url?sa=t&rc=j&q=&esrc=s&source=web&
www.google.com	malware analysis.ppt - Google Search
www.google.com	Google
www.virustotal.com	VirusTotal
www.arcnetscurity.com	Penetration Testing
www.arcnetscurity.com	Penetration Testing
www.coresecurity.com	6 Steps to Pen-Test with Core Impact Core Security
www.softwaretestinghelp.com	Only in Registered version!
www.israelschallenge.com	Only in Registered version!
www.google.com	Only in Registered version!
www.arcnetscurity.com	Only in Registered version!

Fig.14: History file opened in hetman Internet spy.

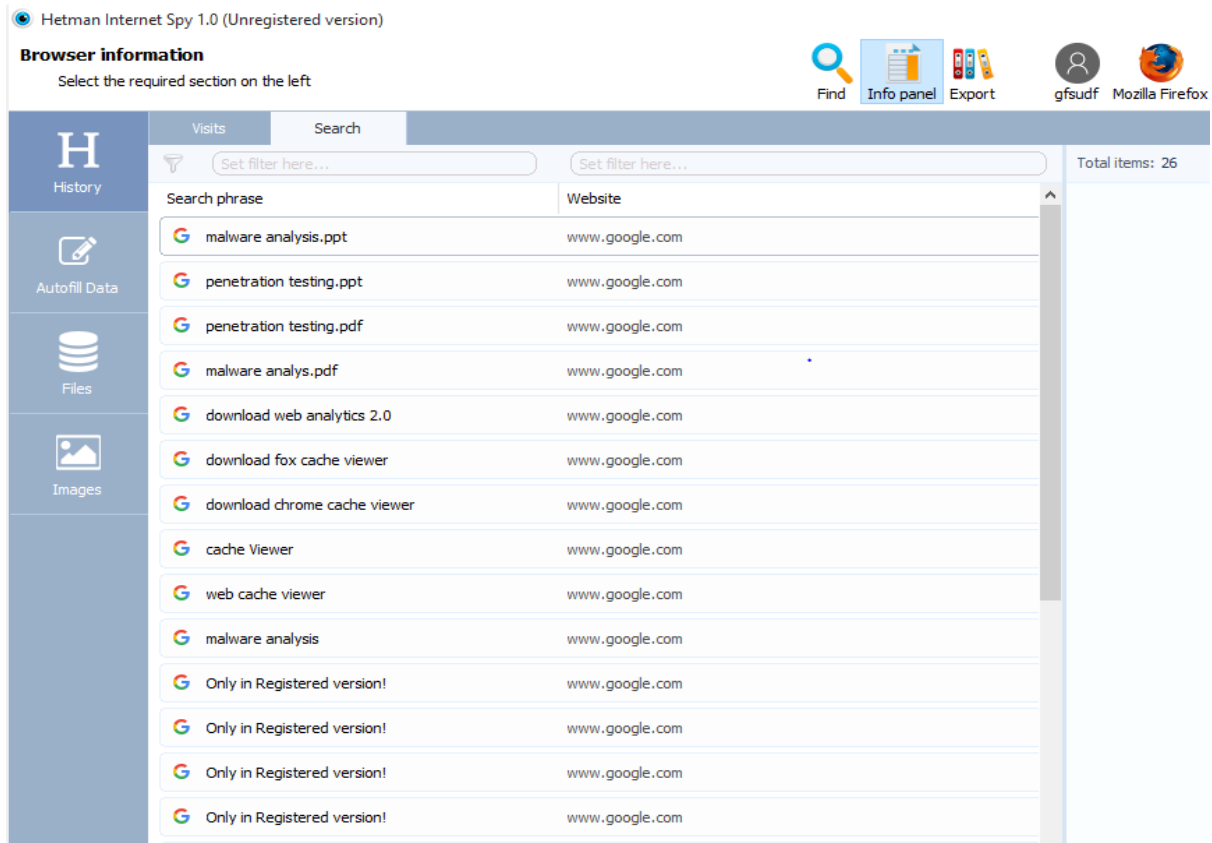


Fig.15: History file has part of searched phrase opened in hetman Internet spy

5.1.2. B. ANALYSIS OF COOKIES

Cookie are files which are created when user visit any website. Cookies store site preference and profile number. Two types of cookie will be generated when user visit any website and another being generated for the advertisement purpose.

Cookie help websites to track of user preferred setting, so that when user re-visits any website, cookie reload previous setting of the user for that same site. As shown in the Figures 17 and 18, we can get the information such as creation_utc, host_key, name, value, path, expires_utc etc.

DB Browser for SQLite - C:\Users\gfsudf\AppData\Roaming\Mozilla\Firefox\Profiles\xygl5cje.default\cookies.sqlite

File Edit View Help

Database Structure Browse Data Edit Pragma Execute SQL

Table: moz_cookies

	id	baseDomain	originAttributes	name	value	host	path	expiry	lastAccessed	creationTime	isSecure
1	1	mozilla.org		moz-stub-a...	c291cmNIP...	www.mozilla.org	/	1535489181	153540338...	1535402781208000	0
2	2	mozilla.org		moz-stub-a...	58fd65a42...	www.mozilla.org	/	1535489181	153540338...	1535402781226000	0
3	7	mozilla.org		_gat_UA-3...	1	.mozilla.org	/	1535402858	153540279...	1535402798308000	0
4	8	mozilla.org		_gali	skip-button	.mozilla.org	/	1535402833	153540280...	1535402803105000	0
5	12	google.co.in		NID	137=Vyhy1...	.google.co.in	/	1551173581	153611800...	1535402834542000	0
6	23	dataforensi...		_ga	GA1.2.3649...	.dataforensics.org	/	1598474900	153540308...	1535402900620000	0
7	24	dataforensi...		_gid	GA1.2.1610...	.dataforensics.org	/	1535489300	153540308...	1535402900620001	0
8	25	dataforensi...		_gat_gtag_...	1	.dataforensics.org	/	1535402960	153540290...	1535402900620002	0
9	26	acquirefore...		_ga	GA1.2.9534...	.acquireforensics.com	/	1598474909	153540290...	1535402909965000	0
10	27	acquirefore...		_gid	GA1.2.1332...	.acquireforensics.com	/	1535489309	153540290...	1535402909965001	0
11	28	acquirefore...		_gat	1	.acquireforensics.com	/	1535402969	153540290...	1535402909965002	0
12	39	github.com		_octo	GH1.1.2117...	.github.com	/	1598521536	153540731...	1535403589636001	0
13	40	github.com		logged_in	no	.github.com	/	2166515136	153540731...	1535403589636002	1
14	56	andreafor...		__cfduid	d70549228...	.andreaforuna.org	/	1566900665	153540512...	1535405120684000	1
15	57	andreafor...		_ga	GA1.2.1640...	.andreaforuna.org	/	1598477129	153540512...	1535405129028000	0

Fig.16: Cookie file opened in DB Browser for SQLite.

FoxAnalysis - Firefox Internet History Analysis

File Filter Sort Cache Help

Website History Bookmarks Cookies Downloads Form History Logins Cache Session Store Session Store Cookies Favicons

ID	Host	Path	Created (UTC, DST Enabled)	Last Accessed (UTC, DST Enabled)	Name	Expiry (UTC, DST Enabled)	Is Secure	Is HTTP Only	Base Domain	Value
520	.addthis.com	/	8/27/2018 10:29:42 PM	9/5/2018 4:28:35 AM	ssc	9/27/2019 11:11:40 PM	No	No	.addthis.com	google%3B4
1059	.addthis.com	/	9/5/2018 4:19:08 AM	9/5/2018 4:28:35 AM	na_id	10/6/2019 4:19:08 AM	No	No	.addthis.com	201809061912195401377
1068	.addthis.com	/	9/5/2018 4:19:08 AM	9/5/2018 4:28:35 AM	na_tc	10/5/2019 9:32:32 PM	No	No	.addthis.com	Y
1170	.addthis.com	/	8/27/2018 10:29:42 PM	9/5/2018 4:28:35 AM	uvce	10/5/2019 4:27:10 AM	No	No	.addthis.com	4%7C35%2C1%7C36
1175	.addthis.com	/	8/27/2018 10:29:50 PM	9/5/2018 4:28:35 AM	loc	10/5/2019 4:27:12 AM	No	No	.addthis.com	MDAwMDBBUQOR0oyMD
1181	.addthis.com	/	8/27/2018 10:42:50 PM	9/5/2018 4:28:35 AM	mus	10/1/2019 8:20:26 PM	No	No	.addthis.com	0
1182	.addthis.com	/	8/27/2018 10:29:42 PM	9/5/2018 4:28:35 AM	ouid	10/1/2019 8:20:26 PM	No	No	.addthis.com	5b83cf4100018fc4dce27f
1183	.addthis.com	/	8/27/2018 10:29:42 PM	9/5/2018 4:28:35 AM	uid	10/1/2019 8:20:26 PM	No	No	.addthis.com	5b83cf41674b4486
1226	.finecomb.com	/	9/5/2018 4:21:20 AM	9/5/2018 4:28:35 AM	_ga	9/4/2020 4:28:35 AM	No	No	.finecomb.com	GA1.2.1557298413.15361
1227	.finecomb.com	/	9/5/2018 4:21:20 AM	9/5/2018 4:28:35 AM	_gid	9/6/2018 4:28:35 AM	No	No	.finecomb.com	GA1.2.716996866.153611
1228	.finecomb.com	/	9/5/2018 4:28:35 AM	9/5/2018 4:28:35 AM	_gat_UA-64...	9/5/2018 4:29:35 AM	No	No	.finecomb.com	1
1225	.samsclass.info	/	9/5/2018 4:27:53 AM	9/5/2018 4:27:53 AM	__cfduid	9/6/2019 8:21:05 PM	No	Yes	.samsclass.info	da4ceb396b6bb29c7b010
1224	.google.com	/	8/27/2018 9:47:03 PM	9/5/2018 4:27:52 AM	1P_JAR	10/6/2018 8:21:04 PM	No	No	.google.com	2018-09-06-19
1223	www.google.com	/	9/5/2018 4:08:56 AM	9/5/2018 4:27:47 AM	DV	9/5/2018 4:37:47 AM	No	No	.google.com	c51FLO5Cz74f413wvEtbM
452	.google.com	/search	8/27/2018 9:47:50 PM	9/5/2018 4:27:45 AM	CGIC	2/26/2019 1:30:41 AM	No	Yes	.google.com	l90ZKh0L2h0bWwsYXBw
449	.google.com	/	8/27/2018 10:48:29 PM	9/5/2018 4:27:44 AM	OGP	9/26/2018 10:48:51 PM	No	No	.google.com	-5061451:
972	.google.com	/	8/27/2018 9:47:03 PM	9/5/2018 4:27:44 AM	NID	3/5/2019 7:02:07 PM	No	Yes	.google.com	138=q97T0ktINKU9sv9P2
451	.google.com	/com...	8/27/2018 9:47:50 PM	9/5/2018 4:27:34 AM	CGIC	2/26/2019 1:30:41 AM	No	Yes	.google.com	l90ZKh0L2h0bWwsYXBw
1219	.virustotal.com	/	9/5/2018 4:09:01 AM	9/5/2018 4:27:25 AM	_ga	9/4/2020 4:27:25 AM	No	No	.virustotal.com	GA1.2.245850578.153611
1220	.virustotal.com	/	9/5/2018 4:09:01 AM	9/5/2018 4:27:25 AM	_gid	9/6/2018 4:27:25 AM	No	No	.virustotal.com	GA1.2.759953847.153611
1221	.virustotal.com	/	9/5/2018 4:27:25 AM	9/5/2018 4:27:25 AM	_gat	9/5/2018 4:28:25 AM	No	No	.virustotal.com	1
1217	www2.secureau...	/	9/5/2018 4:27:23 AM	9/5/2018 4:27:23 AM	visitor_id182...	9/2/2028 4:27:23 AM	No	No	.secureauth.c...	257401881
1218	www2.secureau...	/	9/5/2018 4:27:23 AM	9/5/2018 4:27:23 AM	visitor_id182...	9/2/2028 4:27:23 AM	No	No	.secureauth.c...	d6d0e947c12c29419dc3e
1215	www.coresecurit...	/	9/5/2018 4:27:21 AM	9/5/2018 4:27:21 AM	visitor_id182...	9/2/2028 4:27:21 AM	No	No	.coresecurity....	257401881
1216	www.coresecurit...	/	9/5/2018 4:27:21 AM	9/5/2018 4:27:21 AM	visitor_id182...	9/2/2028 4:27:21 AM	No	No	.coresecurity....	5b7aee889fa30fcae56a4

Fig.17: Cookie file opened in FoxAnalysis tool.

5.1.2. C. Download

The table bellow shows (Figure -19) what type of stuffs downloaded by the user. It also gives information like name of file downloaded, type and the size of the file.

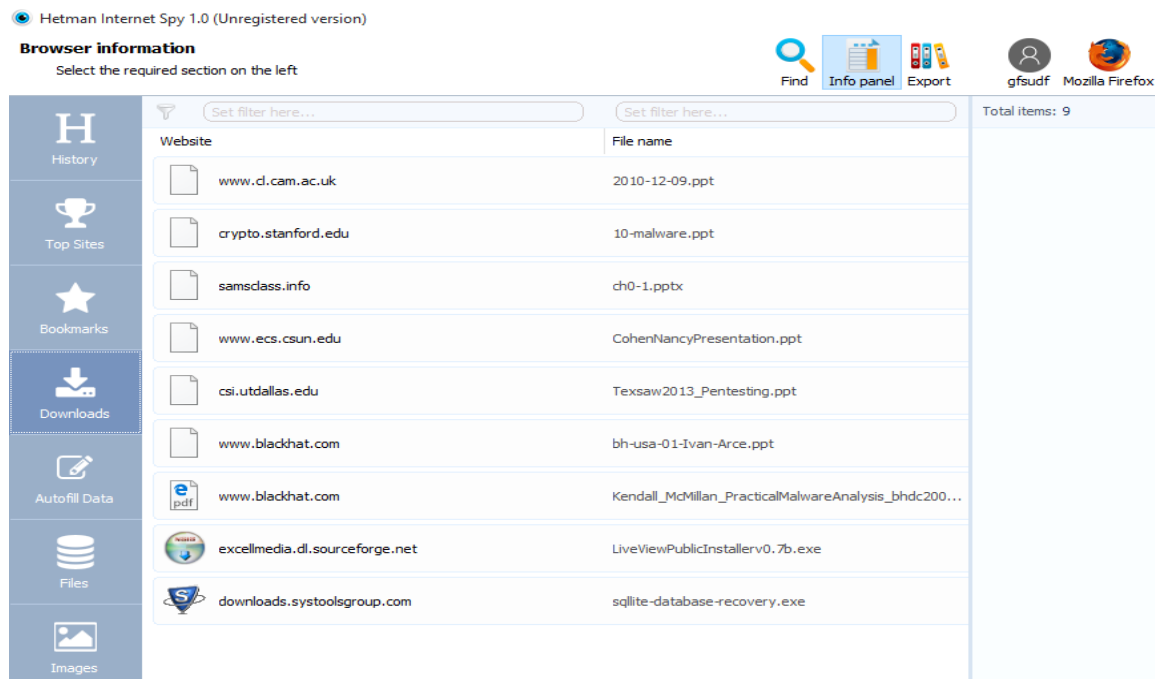


Fig.18: Downloaded files opened in hetman Internet spy.

5.1.2. D. Bookmarks

Bookmarks are URI's (Universal Resource Identifiers) that are basically the shortcuts to the favorite or saved pages. If the website has been bookmarked, the user doesn't need to remember the URL for opening it. Thus these bookmarks provide the forensic investigator idea of what kind of data or website does the user deems important. Bookmarked sites can be opened from the Mozilla Menu > Bookmarks.

Bookmarks tab only shows the URL of the websites that the user has bookmarked. This information is insufficient for a forensic analyzer to determine which bookmarks are recent. as seen in Figure 20 bellow.

FoxAnalysis - Firefox Internet History Analysis

File Filter Sort Cache Help

Website History Bookmarks Cookies Downloads Form History Logins Cache Session Store Session Store Cookies Favicons

	ID	Title	URL	Date Added (UTC, DST Enabled)	Last Modified (UTC, DST Enabled)
▶	20	CacheViewer - Add-ons for Firefox	https://addons.mozilla.org/en-US/firefox/addon/cacheview...	9/5/2018 4:21:40 AM	9/5/2018 4:21:40 AM
	19	Finecomb.com	https://www.finecomb.com/web?qsrc=999&qo=semQuery&...	9/5/2018 4:21:25 AM	9/5/2018 4:21:25 AM
	18	Introduction to Malware Analysis - intro-to-malwar...	https://zeltser.com/media/docs/intro-to-malware-analysis.pdf	9/5/2018 4:21:00 AM	9/5/2018 4:21:00 AM
	17	Kendall_McMillan_PracticalMalwareAnalysis_bhd...	https://www.blackhat.com/presentations/bh-dc-07/Kendall...	9/5/2018 4:20:48 AM	9/5/2018 4:20:48 AM
	16	https://www.google.com/url?sa=t&rct=j&q=&esrc=...	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=...	9/5/2018 4:20:29 AM	9/5/2018 4:20:37 AM
	14	Recent Tags	place.type=6&sort=14&maxResults=10	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	13	Most Visited	place.sort=8&maxResults=10	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	12	Getting Started	https://www.mozilla.org/en-US/firefox/central/	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	8	Help and Tutorials	https://support.mozilla.org/en-US/products/firefox	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	9	Customize Firefox	https://support.mozilla.org/en-US/kb/customize-firefox-cont...	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	10	Get Involved	https://www.mozilla.org/en-US/contribute/	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM
	11	About Us	https://www.mozilla.org/en-US/about/	8/27/2018 9:46:15 PM	8/27/2018 9:46:15 PM

Fig.19: Mozilla Firefox Bookmarks opened in FoxAnalysis Tool.

5.1.3. Internet Explorer

Internet Explorer is the most familiar browser amongst users and is default provision with windows OS. Internet Explorer also does the same and leaves behind traces of browsing activities on the end user's machine. Internet Explorer always leaves multiple piece of information about the web activities such as history of web pages visited, URLs, Bookmarks, Cookies, etc. Important files can be found in the internet Explorer folder located in user system. The default location of file is :

C:\users\[username]\AppData\local\Microsoft\Windows

In Internet Explorer have two main files in which investigator can focus while analyzing web browser activities. Those two files are index.dat and cache.

The index.dat files is database file and also is a repository of information such as web URL search queries and recently opened files. Its purpose is to enable quick access to data used by Internet Explorer. for instance, every web address visited is stored in the index.dat file, allowing Internet Explorer to quickly find autocomplete matches as the user types a web address. Separate index.dat file exist for internet Explorer history, cache, and cookies. The index.dat file is never resized or deleted. This file always being used by windows system . Even you clear Temporary Internet files on internet option of Internet Explorer, it will not delete index.dat file.

5.1.3. A. History

History file contains all browsing information of the users visited, when and how many times. It contains also c the record of a keyword searched, URL visited, paths, etc. Records can be found from in suspect's machine through the path mentioned bellow:

C:\user\[username]\ AppData\Local\Microsoft\ Windows\WebCache

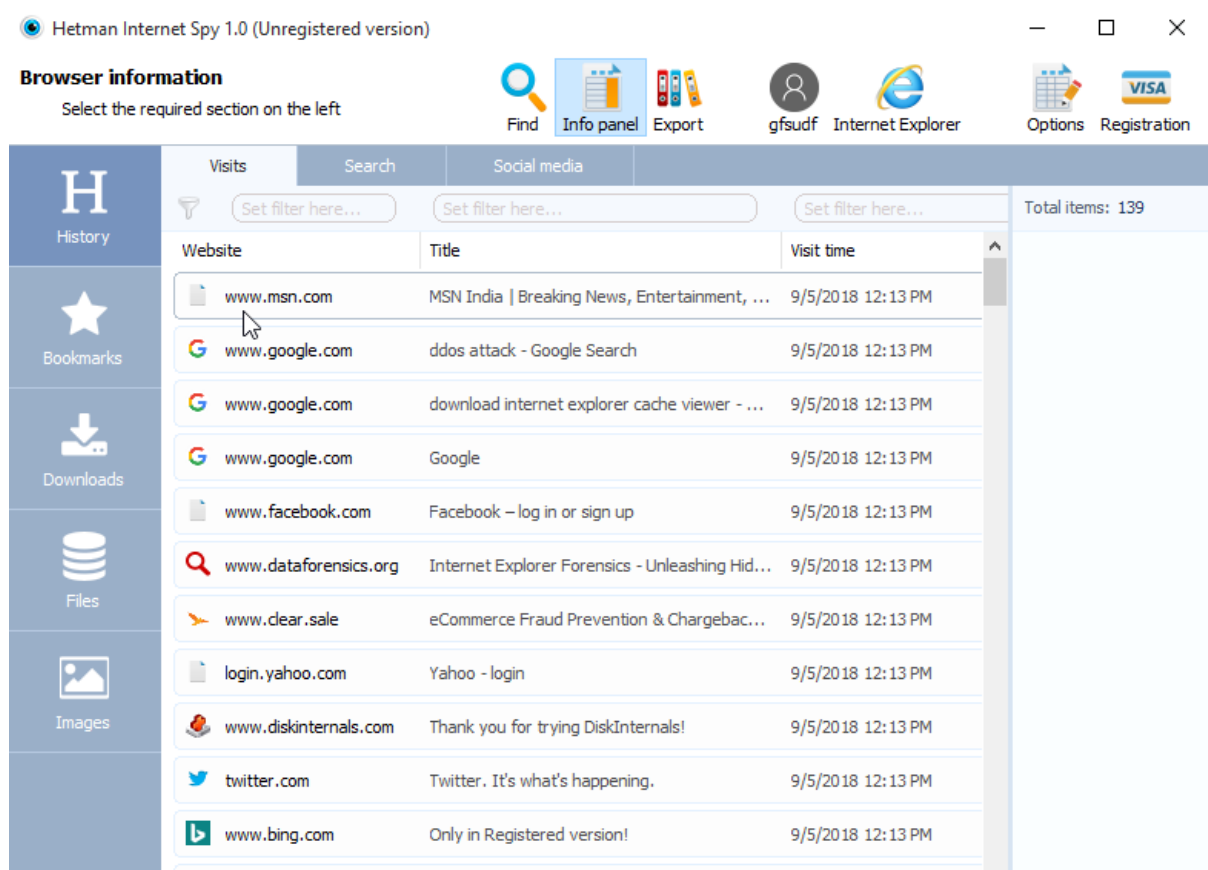


Fig.20: Above fig. Shows List of the URLs visited by user and time.

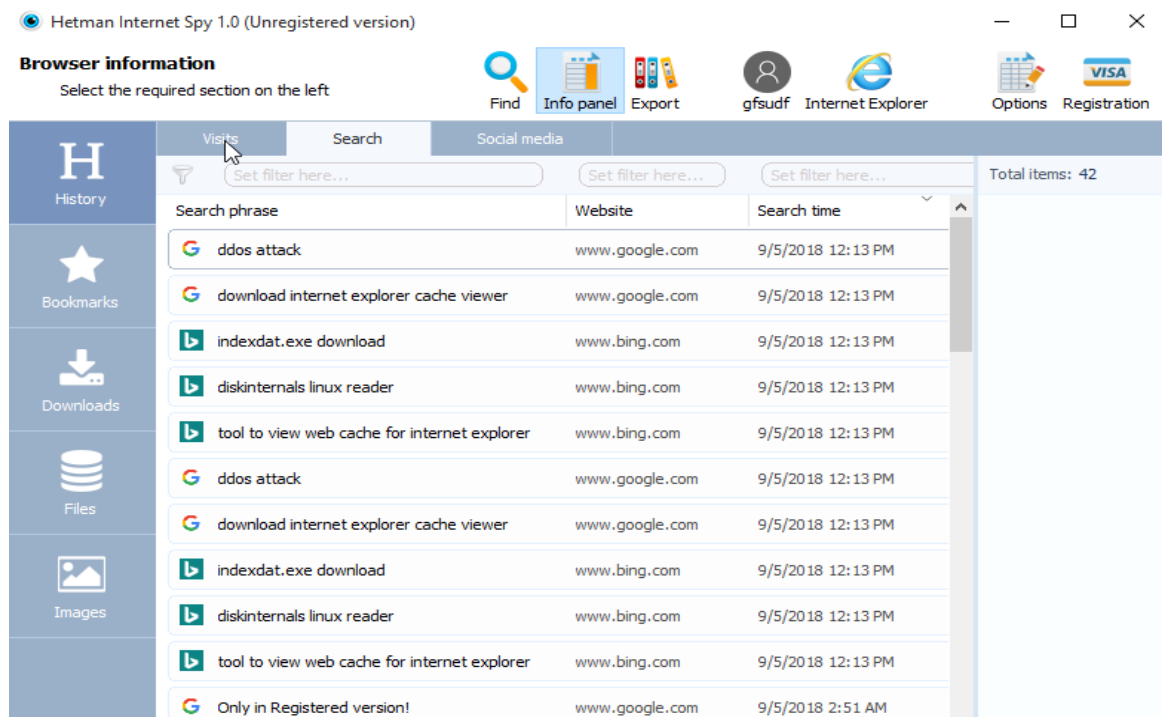


Fig.21: Above fig. Shows part of History that List of searched phrases, sites and time.

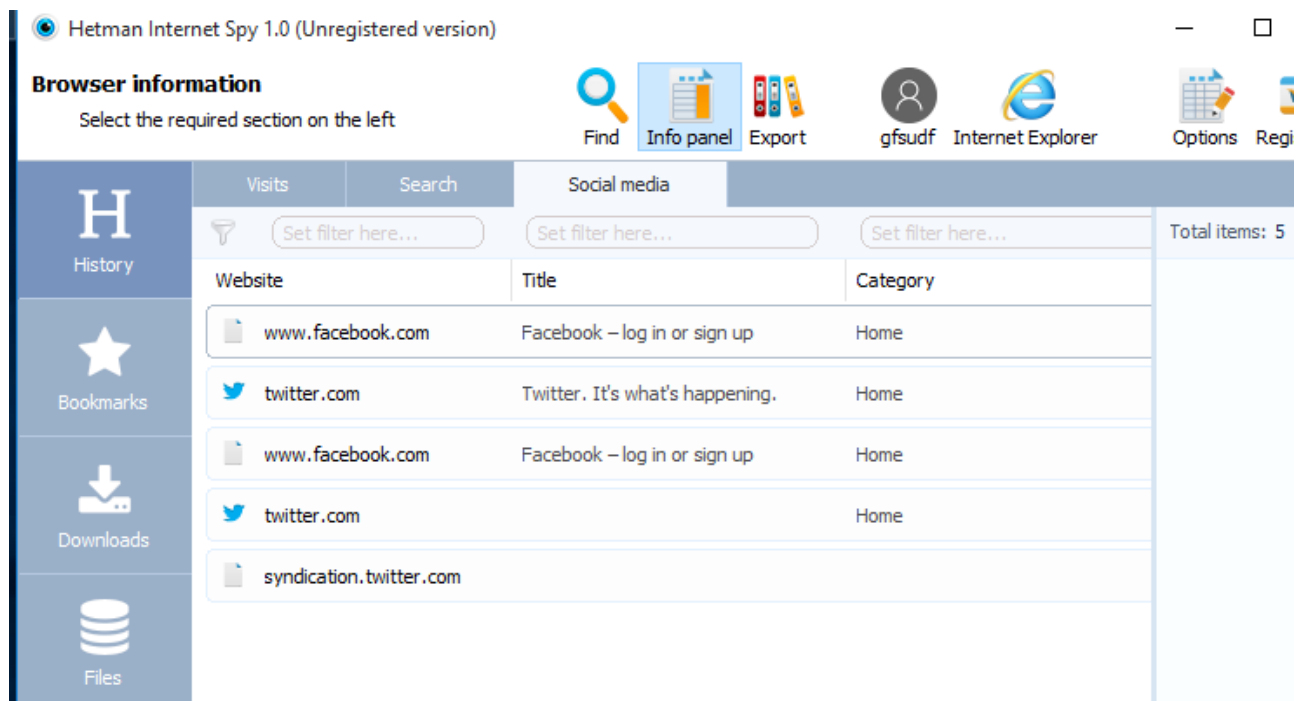
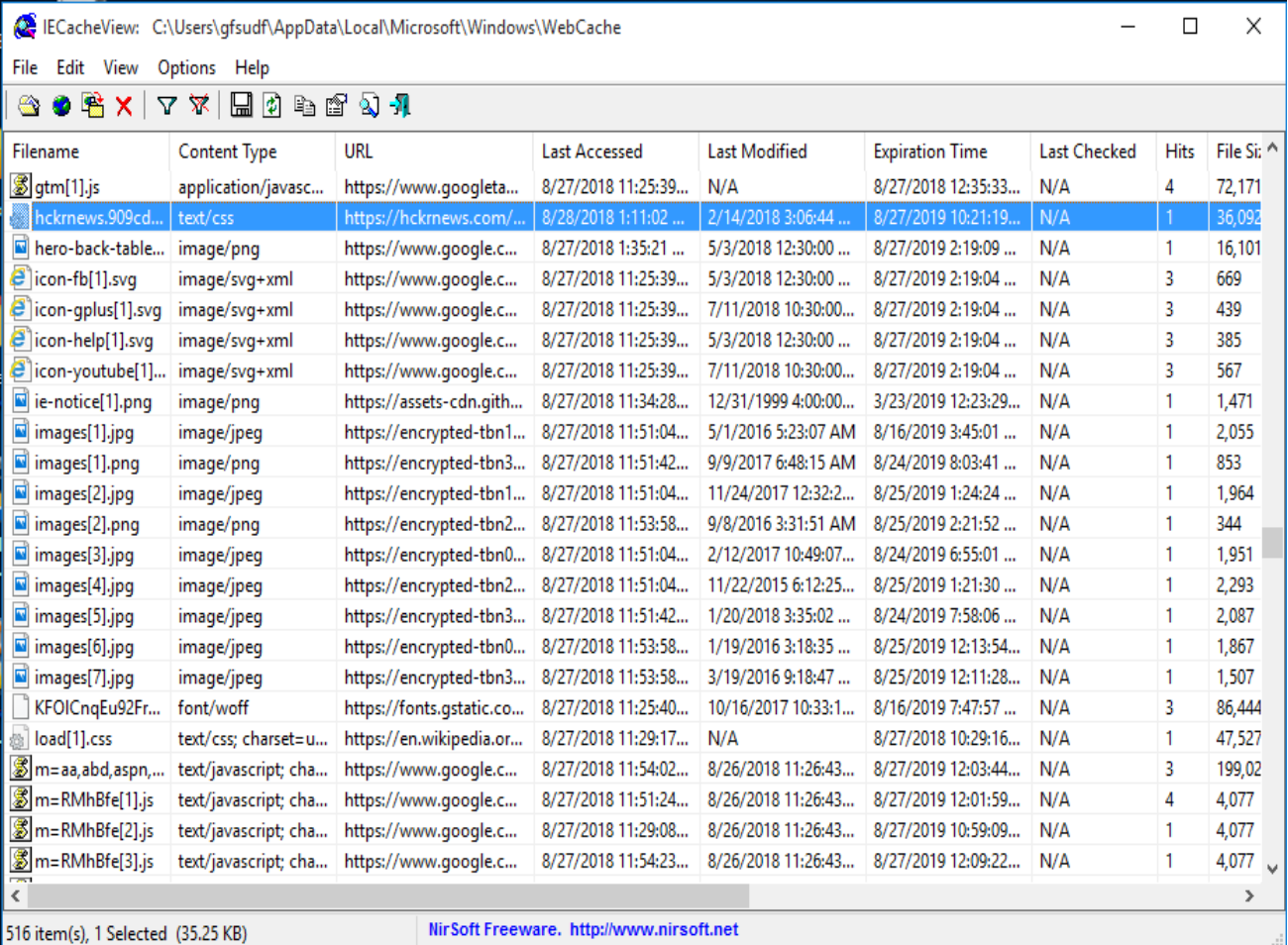


Fig.22: Above fig. Shows part of History that List of social media used by user.

5.1.3. B. Cache

Cache transparently stores website's data so that future requests for that data can be served faster. Cache contains files stored from different WebPages browsed by the user as shown on fig.24 bellow.

%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5



The screenshot shows the IECacheView application window. The title bar reads "IECacheView: C:\Users\gfsudf\AppData\Local\Microsoft\Windows\WebCache". The menu bar includes "File", "Edit", "View", "Options", and "Help". Below the menu is a toolbar with various icons. The main area displays a table of cached files with the following columns: Filename, Content Type, URL, Last Accessed, Last Modified, Expiration Time, Last Checked, Hits, and File Size. The table lists 20 items, including JavaScript files, CSS files, images, and fonts. The status bar at the bottom indicates "516 item(s), 1 Selected (35.25 KB)" and includes a link to "NirSoft Freeware. http://www.nirsoft.net".

Filename	Content Type	URL	Last Accessed	Last Modified	Expiration Time	Last Checked	Hits	File Size
gtn[1].js	application/javasc...	https://www.googlea...	8/27/2018 11:25:39...	N/A	8/27/2018 12:35:33...	N/A	4	72,171
hckrnews.909cd...	text/css	https://hckrnews.com/...	8/28/2018 1:11:02 ...	2/14/2018 3:06:44 ...	8/27/2019 10:21:19...	N/A	1	36,092
hero-back-table...	image/png	https://www.google.c...	8/27/2018 1:35:21 ...	5/3/2018 12:30:00 ...	8/27/2019 2:19:09 ...	N/A	1	16,101
icon-fb[1].svg	image/svg+xml	https://www.google.c...	8/27/2018 11:25:39...	5/3/2018 12:30:00 ...	8/27/2019 2:19:04 ...	N/A	3	669
icon-gplus[1].svg	image/svg+xml	https://www.google.c...	8/27/2018 11:25:39...	7/11/2018 10:30:00...	8/27/2019 2:19:04 ...	N/A	3	439
icon-help[1].svg	image/svg+xml	https://www.google.c...	8/27/2018 11:25:39...	5/3/2018 12:30:00 ...	8/27/2019 2:19:04 ...	N/A	3	385
icon-youtube[1]...	image/svg+xml	https://www.google.c...	8/27/2018 11:25:39...	7/11/2018 10:30:00...	8/27/2019 2:19:04 ...	N/A	3	567
ie-notice[1].png	image/png	https://assets-cdn.gith...	8/27/2018 11:34:28...	12/31/1999 4:00:00...	3/23/2019 12:23:29...	N/A	1	1,471
images[1].jpg	image/jpeg	https://encrypted-tbn1...	8/27/2018 11:51:04...	5/1/2016 5:23:07 AM	8/16/2019 3:45:01 ...	N/A	1	2,055
images[1].png	image/png	https://encrypted-tbn3...	8/27/2018 11:51:42...	9/9/2017 6:48:15 AM	8/24/2019 8:03:41 ...	N/A	1	853
images[2].jpg	image/jpeg	https://encrypted-tbn1...	8/27/2018 11:51:04...	11/24/2017 12:32:2...	8/25/2019 1:24:24 ...	N/A	1	1,964
images[2].png	image/png	https://encrypted-tbn2...	8/27/2018 11:53:58...	9/8/2016 3:31:51 AM	8/25/2019 2:21:52 ...	N/A	1	344
images[3].jpg	image/jpeg	https://encrypted-tbn0...	8/27/2018 11:51:04...	2/12/2017 10:49:07...	8/24/2019 6:55:01 ...	N/A	1	1,951
images[4].jpg	image/jpeg	https://encrypted-tbn2...	8/27/2018 11:51:04...	11/22/2015 6:12:25...	8/25/2019 1:21:30 ...	N/A	1	2,293
images[5].jpg	image/jpeg	https://encrypted-tbn3...	8/27/2018 11:51:42...	1/20/2018 3:35:02 ...	8/24/2019 7:58:06 ...	N/A	1	2,087
images[6].jpg	image/jpeg	https://encrypted-tbn0...	8/27/2018 11:53:58...	1/19/2016 3:18:35 ...	8/25/2019 12:13:54...	N/A	1	1,867
images[7].jpg	image/jpeg	https://encrypted-tbn3...	8/27/2018 11:53:58...	3/19/2016 9:18:47 ...	8/25/2019 12:11:28...	N/A	1	1,507
KFOICnqEu92Fr...	font/woff	https://fonts.gstatic.co...	8/27/2018 11:25:40...	10/16/2017 10:33:1...	8/16/2019 7:47:57 ...	N/A	3	86,444
load[1].css	text/css; charset=u...	https://en.wikipedia.or...	8/27/2018 11:29:17...	N/A	8/27/2018 10:29:16...	N/A	1	47,527
m=aa,abd,aspn,...	text/javascript; cha...	https://www.google.c...	8/27/2018 11:54:02...	8/26/2018 11:26:43...	8/27/2019 12:03:44...	N/A	3	199,02
m=RMhBfe[1].js	text/javascript; cha...	https://www.google.c...	8/27/2018 11:51:24...	8/26/2018 11:26:43...	8/27/2019 12:01:59...	N/A	4	4,077
m=RMhBfe[2].js	text/javascript; cha...	https://www.google.c...	8/27/2018 11:29:08...	8/26/2018 11:26:43...	8/27/2019 10:59:09...	N/A	1	4,077
m=RMhBfe[3].js	text/javascript; cha...	https://www.google.c...	8/27/2018 11:54:23...	8/26/2018 11:26:43...	8/27/2019 12:09:22...	N/A	1	4,077

Fig.23: Cache file opened by IECacheView tool.

5.1.3. C. Downloads

This table shows (Figure -25) what type of files downloads by the user.

Hetman Internet Spy 1.0 (Unregistered version)

Browser information
Select the required section on the left

Find Info panel Export gfsudf Internet Explorer

	Website	File name
History	www.cs.sjtu.edu.cn	C1610.pdf
Bookmarks	www.ijecs.in	873-Article Text-1498-1-10-20171230.pdf
Downloads	www.ijcttjournal.org	IJCTT-V8P109.pdf
Files	ijcsit.com	ijcsit20150602104.pdf
Images	usir.salford.ac.uk http://usir.salford.ac.uk/2595/1/bbs.pdf	BBS.pdf
	samsclass.info	ch0-1.pptx
	www.diskinternals.com	Linux_Reader.exe
	www.google-analytics.com	analytics.js
	www.myfavorit gadgets.info	IECacheView.zip
	dl1.pointstone.com	IndexDatViewerSetup.exe
	download.sqlitebrowser.org	DB.Browser.for.SQLite-3.10.1-win64.exe

Total items: 11

Fig.24: Downloaded files opened by hetman Internet spy.

5.2. Private Mode Analysis

5.2.1. Live Memory Capture

Live memory would be captured and imaged to recover and carve out browsing related information to see if data can be recovered from the physical memory itself.

Private browsing artifacts will be collected using RAM dump of the system. We visited Gmail, Facebook, Twitter and Google chrome, Mozilla Firefox, Internet Explorer in private mode and try to extract evidences related to same using RAM dump analysis. We took RAM dump of system using MagnetRAMCapture and analyzed RAM dump using tools and apply filter to find visited web sites related information.

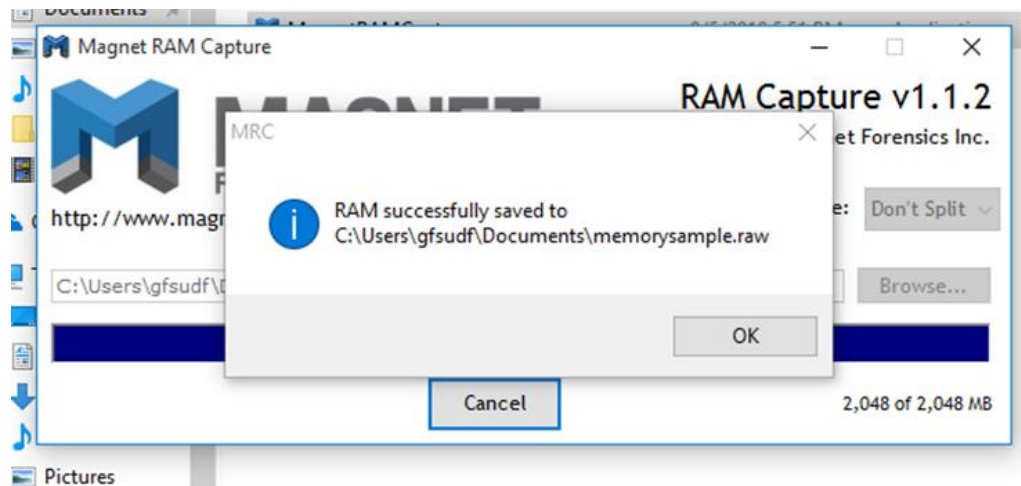


Fig.25: RAM Capture on Windows 10 Screenshot

5.2.2. Private Web Browser

All most popular web browsers discussed on this research paper, allow user to surf internet in Private mode. The private browsing feature of web browsers gives the user freedom of browsing the internet, without keeping any record of his browsing history, cookies, temporary Internet files, usernames/passwords, form data etc. The feature also helps prevent him from third party websites that usually track user's browsers activity. Thus, these types of browsing features tend to make the job of forensic expert or forensic investigator hard.

The private mode in all vendor browsers claim that all browsing history, temporary

Internet files, form data, cookies, usernames and passwords leave no traces or Evidence of the browsing or search history behind. Chrome, Firefox and also claim that they don't store download list entries.

Researchers earlier have performed similar analysis of private mode and have released papers related to the findings. The research performed by Donny and Narasimha in have used a tool called DaemonFS and was restricted to just Windows 7 operating system. They found that the Internet Explorer stored data on the file system as well as in the memory and the browsing data were recoverable using file recovery tools. Google Chrome and Firefox did not store any data on the file system but the data was recoverable from the memory.

a. Private Web Browser in Google Chrome.

For the user to start the private browsing in Chrome, press *Chrome Menu > New Incognito window*. Alternatively incognito window can be opened from Ctrl + Shift+ N shortcut. The user can enjoy private browsing unless he himself turns it off.

b. Private Web Browser in Mozilla Firefox.

To start the private mode in Firefox, go to *Firefox menu >New private window* or press Ctrl + Shift +N.

c. Private Web Browser in Internet Explorer.

To start Private mode in Internet Explorer, go to Internet Explorer menu > Safety > inPrivate Browsing or you can press Ctrl + Shift + P.

5.2.3. Detecting private mode:

Since the evidence extraction for private mode of operation is slightly different from the regular mode the forensic examiner needs to know whether the suspect uses private mode or not. A simple indication for private mode on an opened browser is the presence of Incognito sign and the absence of Recent tabs bar. But if the browser is closed, the forensic examiner can run Chrome Cross-mode Interference inspector application on the suspect's PC to see when the private mode was enabled and where was the data stored.

5.2.3.1. Web Activity

Private browsing mode though enabled keeps track of user internet activity. The browser was launched in incognito mode and websites were accessed .after accessing the sites, the browser was closed and RAM contents were captured using RAM capturer. The captured file was opened in different tools to perform analysis. During the analysis it was found that the browsed websites were stored in the RAM.

5.2.3.1. A. Google Chrome:

The browser was launched in incognito mode and websites were accessed. After accessing the site, the browser was closed and the RAM contents were captured using MagnetRAMCapture as shown earlier. The captured file was opened using Winhex to perform analysis. During the analysis it was found that the browsed websites were stored in the RAM.

memdump.mem		Cookies																			
[unregistered]		Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	ANSI ASCII	^		
Cookies	C:\Users\gfsudf\AppData\Local\Google\	0000D60B	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
		0000D61A	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
		0000D629	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
File size:	544 KB	0000D638	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
	557,056 bytes	0000D647	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
		0000D656	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
Default Edit Mode		0000D665	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
State:	original	0000D674	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
Undo level:	0	0000D683	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
Undo reverses:	n/a	0000D692	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
		0000D6A1	82	47	81	1F	10	06	37	13	0D	0F	06	09	09	06	09	,G 7			
Creation time:	08/27/2018	0000D6B0	09	09	84	18	08	00	2E	D3	08	66	72	D6	E9	2E	77	„ .ó frÖé.w			
	13:40:28	0000D6BF	77	77	2E	72	65	73	65	61	72	63	68	67	61	74	65	Ww.researchgate			
		0000D6CE	2E	6E	65	74	70	74	63	2F	00	2F	0C	65	7E	9A	96	.netptc/ / e~š-			
Last write time:	09/09/2018	0000D6DD	E9	00	2E	D3	08	66	72	D6	E9	01	00	00	00	D0	8C	é .ó frÖé DE			
	16:27:50	0000D6EC	9D	DF	01	15	D1	11	8C	7A	00	C0	4F	C2	97	EB	01	š Ń Ęz ÅÖÄ-ë			
Attributes:	A	0000D6FB	00	00	00	F4	EA	AF	5C	94	E6	BA	46	9D	B3	E6	48	ôê\"æ°F æH			
Icons:	0	0000D70A	31	0D	3C	2E	00	00	00	00	02	00	00	00	00	00	10	1 <.			
Mode:	Text	0000D719	66	00	00	00	01	00	00	20	00	00	00	6C	27	D0	2B	f 1'B+			
Offsets:	hexadecimal	0000D728	11	F6	60	D0	CA	9E	53	D1	78	2B	C4	BD	E6	A9	4E	ô`ÐËŠŠÑx+ÅæœN			
Bytes per page:	35x15=525	0000D737	C5	4F	9F	E0	19	C4	A2	7B	0A	50	49	50	1D	00	00	ÅÖÄ Åö(PIP			
Window #:	2	0000D746	00	00	0E	80	00	00	00	02	00	00	20	00	00	00	DC	€ Ů			
No. of windows:	2	0000D755	7F	BD	1A	05	9C	89	BA	0B	48	E8	12	61	78	85	5C	š æt° Hè æx...\			
		0000D764	96	AA	78	DF	42	22	64	A5	C0	A6	F8	3A	A0	27	37	-*xBB"dWÅ!ø: '7			
		0000D773	61	30	00	00	00	02	56	B2	EA	53	F9	E9	C6	AA	03	a0 V*èŠùéÆ*			
Clipboard:	available	0000D782	AC	65	62	C3	8C	AF	6E	AB	97	25	18	50	DB	5C	F8	-ebÅÆ n«-š PŮ/ø			
TEMP folder:	202 MB free	0000D791	A3	1A	81	53	E6	5A	68	F9	0E	47	29	BF	75	E7	8C	£ šæZhù G) iuçœ			
C:\Users\gfsudf\AppData\Local\Temp		0000D7A0	9E	A7	E3	A7	A6	E3	8C	23	40	00	00	00	5E	88	09	žššš!æœ# ^~			
		0000D7AF	39	9B	D1	AE	81	51	65	1F	A6	B6	AD	9F	68	02	9D	9>Ńø Qe !q-Yh			
		0000D7BE	2C	C9	8A	73	D6	3F	8A	E4	01	FA	3A	48	EC	D4	86	.Éššö?šä ú:Hiôt			

Fig. 26 : Chrome on Windows Winhex analysis Screenshot.

5.2.3.1. B. FireFox:

The browser was launched in Private mode and websites were accessed. After that the browser was closed and the physical memory was captured using MagnetRAMCapture as shown previously. Then the image file was opened using Winhex to perform analysis. During the analysis it was found that the browsing data existed in the captured memory file.

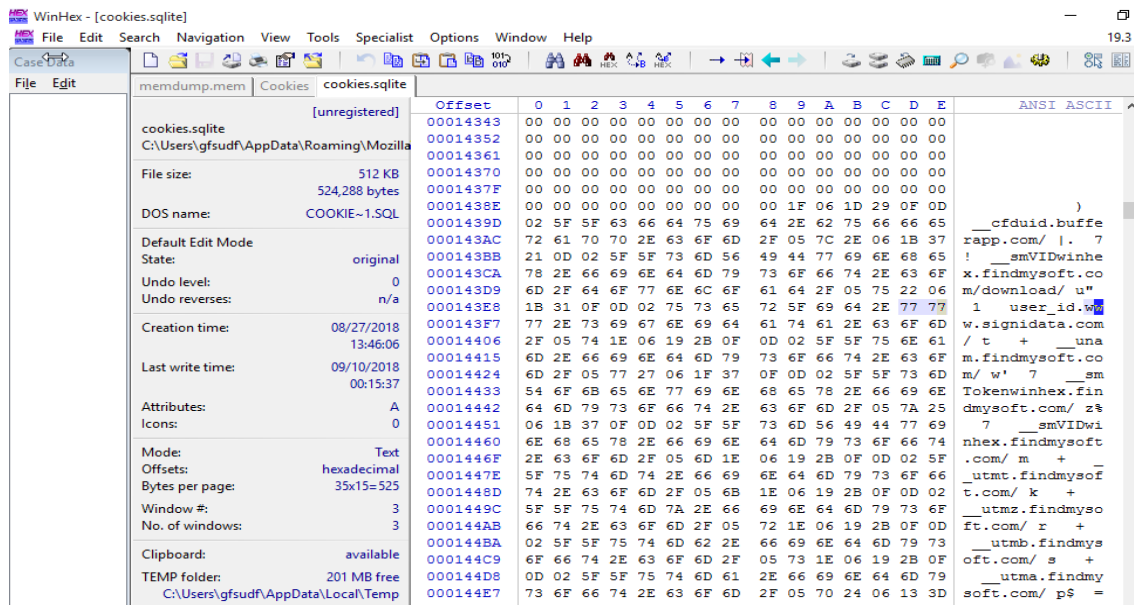


Fig.27: Firefox on Windows Winhex analysis Screenshot.

5.2.3.1. C. Internet Explorer:

The browser was launched in InPrivate mode and websites were accessed. The browser was closed after accessing websites. The physical memory contents were captured using MagnetRAMCapture as shown earlier. Analysis was performed by opening the image file in Winhex. It was found that the browsing information existed in the captured image.

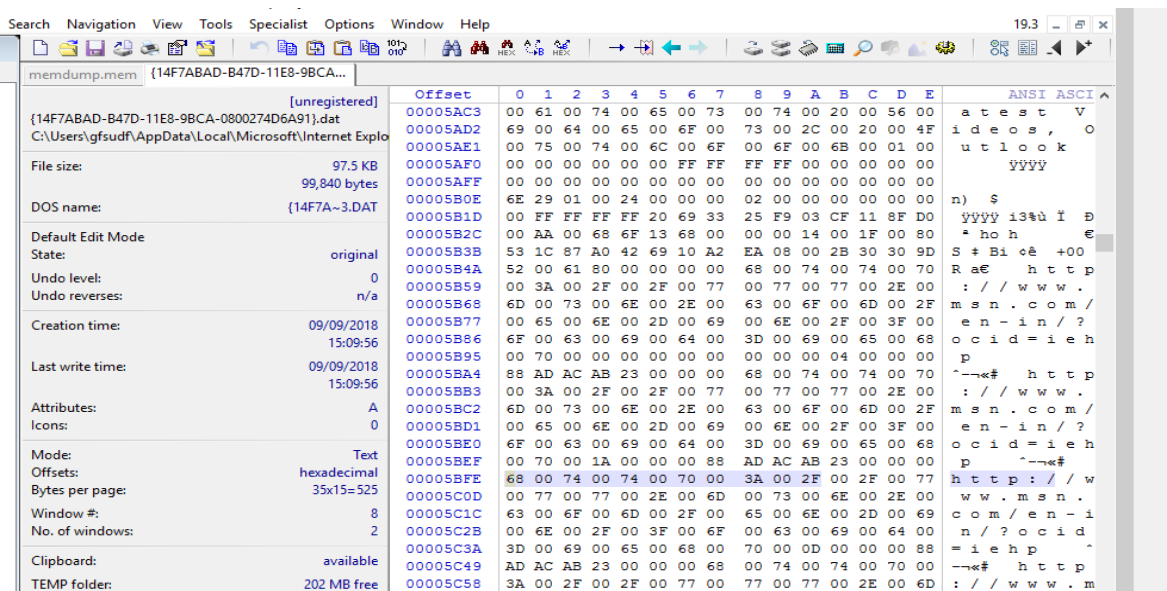


Fig . 28: IE Winhex analysis Screenshot

5.2.3.2. Cookies

In private browsing mode, the cookies are associated with a session time, and hence expire once the browser closes. They can thus only be copied, if the browser is left open.

5.2.3.3. Bookmarks

They can be easily seen, by just clicking the Bookmarks file present in Default folder, even after session expires. Thus, bookmarks need to be manually deleted by user.

5.2.3.4. Third Party Websites

Private browsing may temporarily hide the data from someone, trying to search for browsing activity in browser history, but the third party websites are still able to trace the IP, track user's activity and send malwares via links/pop-ups.

5.2.3.5. Downloads

The download list is cleared after the browser closes, but the downloaded files can still be seen in the downloads window and needs to be manually deleted.

5.2.3.5. Other Observations

Though data is deleted at the expiry of the session in private web browsing but this data certainly does not get wiped off the drive. The forensic examiner should therefore know all places and folders where the internet activity of the user and browser preferences gets stored. He may use any forensic tool e.g. FTK Toolkit etc.

5.3. Summary of Analysis in Private mode

Table.5. Recovery from file system method:

Browser	Analysis	Recover Data
Google chrome	The browser doesn't write anything to the filesystem and no data can be recovered.	NO
Mozilla Firefox	The browser doesn't write anything to the file system and no data can be recovered.	NO
Internet Explorer	Browsing related information is recoverable as the browser writes the data on the file system and then deletes it by a file system operation called "SetDispositionInformationFile".	YES

Table.6. Recovery from physical memory (RAM) method:

Browser	Analysis	Recover Data
Google chrome	Browsing related information is recoverable as the browser writes data on the RAM.	YES
Mozilla Firefox	Browsing related information is recoverable as the browser writes data on the RAM.	YES
Internet Explorer	Browsing related information is recoverable as the browser writes data on the RAM.	YES

6. Summary of Regular and Private Mode

The working of Google Chrome, Firefox and Internet Explorer in all two modes of operation is quite different. Table 3 below, summarizes the Web Browser activities analysis of them in Regular and private mode of operation.

Browser	Mode	Web Activities Analysis
Google Chrome	Regular Mode	<ul style="list-style-type: none">- Browsing history, cached websites, cookies, downloads, saved passwords etc. are stored in ..\Chrome\User Data Directory in C drive.
	Private Mode	<ul style="list-style-type: none">- Cookies, Bookmarks, History etc. gets stored in the Default Chrome folder- Browsed websites can be seen in RAM- New timestamp replaces chrome_shutdown_ms.txt on session expiry- User credentials and videos not stored.
Mozilla Firefox	Regular Mode	<ul style="list-style-type: none">- Browsing history and cookies get stored in C:\ drive of Mozilla Firefox folders.
	Private Mode	<ul style="list-style-type: none">- Browsed Websites can be seen in RAM.- It is recoverable.
Internet Explorer	Regular Mode	<ul style="list-style-type: none">- Browsing history and cookies get stored in C:\ drive of Internet Explorer folders.
	Private Mode	<ul style="list-style-type: none">- Internet Explorer stored data on the file system as well as in the memory RAM.

7. Future Trends

Web Browser forensics has become an important field of research for the forensic researchers. Today, most of the Web browser Forensic tools target any specific web browsers, and those few that are able to analyze multiple web browsers, lacks the accurate artifacts extraction.

In order to address this issue, a methodology should be designed to analyze multiple browsers simultaneously with one tool, and integrate their data according to the timestamps for integrated artifact analysis. Based on this designed methodology, a forensic tool should be developed for the forensic experts, to speed up their process of investigation. Moreover, since the web browsers are updated frequently, forensic analysts must be able to forensically analyze the newer versions too. Browser forensics should similarly be conducted on other Operating systems too.

However, since the trend of computer is gradually shifting towards the smartphone, the forensic investigator must also thoroughly carry out browser forensic of smart phones.

8. Conclusion.

As web browser is the only way to access the internet and cybercrime criminal uses or target the web browser to commit the internet related crime. Tracing evidence of Web browser use is an important process for digital forensic investigation. After analyzing a trace of Web browser use, it is possible to determine the objective, methods, and criminal activities of a suspect. When an investigator is examining a suspect's computer, the Web browser's log file will be one of his top concerns.

Browser Forensic Tools are the best source for the forensic experts to find the artifacts from web browser, in case of any suspected illegal Internet activity. The forensic experts can therefore utilize the efficiency of these forensic tools to find internet artifacts from various different locations in the computer's memory. Though the stored web data can be traced down to the exact folder, the deletion of any evidence by the culprit can seriously affect the progress of the case.

9. References

1. "WEB BROWSER FORENSICS: GOOGLE CHROME" Article · July 2017
<https://www.researchgate.net/publication/321534636>
2. Noorulla, Emad Sayed, "Web Browser Private Mode Forensics Analysis" (2014). Thesis. Rochester Institute of Technology. Accessed from
<https://www.writscholarworks@rit.edu>.
3. "Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools", Narmeen Shafqat, VOL.16 No.9, September 2016.
4. "Advanced Evidence Collection and Analysis of Web Browser Activity"
By Junghoon Oh, Seungbong Lee and Sangjin Lee
Digital Investigation 8(2011)
5. <http://digitalforensicsurvivalpodcast.com/2017/04/18/dfsp-061-firefox-forensics/>
6. Donny J Ohan, Narasimha and Shashidhar, Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions, EURASIP Journal on Information Security, December 2013, 2013:6
7. "Mozilla Firefox 3 History File Format - Forensics Wiki," accessed January 24, 2011,
http://www.forensicswiki.org/wiki/Mozilla_Firefox_3_History_File_Format.
8. <http://support.mozilla.com/en-US/kb/private%20browsing>.
9. Jones Keith j, Rohyt Blani. Web browser forensic. Security focus,
<http://www.securityfocus.com/infocus/1827>; 2005a.
10. Jones Keith J. Forensic analysis of internet explorer activity files. Foundstone,
http://www.foundstone.com/us/pdf/wp_index_dat.pdf; 2003
11. Mahendrakar, Aditya, James Irving, and Shivam Patel. "Forensic Analysis of Private Browsing Mode in Popular Browsers." < <http://mocktest.net/paper.pdf> > Web. 29 Sept. 2015.
12. Divyesh G, Nagoor A R. (2014). Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser. International Journal of Computer Applications. vol. 91, issue 4.

13. <http://digital-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/> Kristinn (2010). Google Chrome Forensics. SANS Digital Forensics and Incident Response Blog.
14. Jain, Ravi. *"Web Browser as a Forensic Computing Tool."* <<http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=6631f86a-42d0-458e-baf8-7b801f048534%40sessionmgr4004&vid=1&hid=4111> > Web. 29 Sept. 2015.
15. WEB BROWSER FORENSICS: GOOGLE CHROME Dr. Digvijaysinh Rathod
Institute of Forensic Science Gujarat Forensic Sciences University Gandhinagar,
Gujarat (India)
16. Forensic Analysis of Epic Privacy Browser on Windows Operating Systems by Alan Reed, Mark Scanlon, Nhien-An Le-Khac School of Computer Science, University College Dublin, Belfield, Dublin 4, Ireland.
17. Web Browser Forensics for Detecting User Activities by Mayur Rajendra Jadhav, Dr. Bandu Baburao Meshram.
18. COLLECTION OF EVIDENCE THROUGH WEB BROWSER & FORENSICS DIGITAL ANALYSIS VIA RECOVERABLE DATA by Nigam Pratap Singh and L S Maurya
19. Huwida Said, Noora Al Mutawa and Ibtesam Al Awadhi, Forensic analysis of private browsing artifacts, 2011 International Conference on Innovations in Information Technology, 25-27 April 2011
20. Murilo, T. P. (2009). Forensic analysis of the Firefox 3 internet history and recovery of deleted SQLite records. Digital Investigation, 5, 93-103.