EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

# Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity

K.V.P.S Ganesh Majeti[1,*], Y.V.L Sai Sundar[1], Sai Shanmukh Ulichi[1], Sachi Nandan Mohanty[1], Sudha SV[1]

[1]School of Computer Science & Engineering (SCOPE), VIT-AP University, Amaravati, Andhra Pradesh, India
(ganeshmajeti712@gmail.com, saisundaryvl@gmail.com, ulichi.saishanmukh@gmail.com, sachinandan09@gmail.com, svsudha.mvenki@gmail.com)

## Abstract

Web browsers are the applications that the majority of computer users utilize the most. Users carry out a wide range of tasks, including accessing the internet, downloading files, and using social media programs, using a web browser to access email accounts. Many crimes committed using digital resources need to be investigated by looking at online browser history. Such information must be included in the reports of the examiners that will generate one of the data gathered, particularly about crimes involving entering the URL, downloaded files, access times, search phrases browser type, and times. Different methods are used by web browsers to store user data. Additionally, the locations where data is stored vary depending on the operating system being used. The analysis of web browsers on digital resources that are subject to criminal activity, data from various browsers on various operating systems, storage types, and data types that can be retrieved are all demonstrated in this study. Also, we demonstrated the capabilities and tools used in the web browser to review the records.

**Keywords:** Digital Forensics, Web Browser Forensic, Digital Evidence, Framework, Integrated Analysis, Search word analysis, URL decoding

Received on 15 February 2023, accepted on 20 April 2023, published on 29 June 2023



doi: 10.4108/eetsis.3357

## 1. Introduction

Browser forensics is primarily used to look at your computer's browsing history and general web activity looking for mysterious activity or content access. To obtain accurate information about the targeted system, this also relates to tracking website traffic and analyzing server-generated LOG files. The goal of computer forensics, a type of forensic investigation, is to characterize and analyze the digital evidence that is stored on computers and related storage media. Internet usage is practically universal, even among suspects under investigation. Suspects can use web browsers to gather information, cover up crimes, or find new ways to commit crimes. A key aspect of digital forensic investigations is often searching for web browsing-related data. Thus, during the usage of a web browser, most of the actions of the accused would be recorded. This data can therefore be helpful when a detective examines the culprit's computer. It is possible to examine evidence from a suspect's computer, including cookies, cache, history, and download lists, to determine the websites visited, the timing and regularity of usage, and the search engine terms the suspect used. Below is a list of various sources that investigators can find evidence in their browsers: 1. Surfing history 2. Bookmarks 3. Download 4. Cookies 5. Cache Therefore, an advanced methodology of existing research and tools is needed. So that the evidence collection from different browsers would be significantly easier. The tools like Autopsy and WEFA (Web Browser Forensic Analyzer) can be used for Web Browser

*Corresponding author. Email: ulichi.saishanmukh@gmail.com

Forensics. These tools are explained in detail in further parts of the paper.

## 2. Related research

### 2.1 Existing tools

The solutions for analysing Web browser log files that are available today are focused on a particular web browser or a particular piece of data. This method may produce skewed data that causes a digital forensics investigation to draw incorrect conclusions. Tools like Cache back and En case can be used to look into different web browsers and examine a variety of data. Encase does not, however, offer a comprehensive review of a variety of Web browsers. If the suspect utilizes several different Web browsers while committing the crime, it will be challenging for an investigator to find any activity. Although Cache back, another programme, uses a straightforward parsing procedure to evaluate cache and history files, it is feasible to do an integrated examination of several Web browsers using this application. Some of the other tools that are existing are briefly explained below

Table 1. Representative forensic tools for Web browsers

| Tool | Targeted Web Browser | Information to be Analyzed |
|---|---|---|
| Pasco | IE | *Index.dat* |
| Web Historian 1.3 | IE, Firefox Safari, Opera | History |
| Index.dat Analyzer 2.5 | *IE* | *Index.dat* |
| Firefox | Firefox | Cookies, History |
| Forensic 2.3 | | Download List Bookmarks |
| Chrome Analysis 1.0 | Chrome | History, Cookies Bookmarks Download List Search Words |
| NetAnalysis 1.52 | IE, Firefox, Chrome Safari, Opera | History |
| Cache Back 3.1.7 | IE, Firefox, Chrome Safari, Opera | Cache, History Cookies |
| Encase 6.13 | IE, Firefox, Safari, Opera | Cache, History Cookies, Bookmarks |
| FTK 3.2 | IE, Firefox, Safari | Cache, History Cookies, Bookmarks |

#### 2.1.1. Autopsy

For Windows and Linux, there is a digital forensic platform called Autopsy. It offers the ability for timeline analysis, web artifact analysis, and data carving. Web history, cookies, and bookmarks from Firefox, Chrome, and IE are extracted during the autopsy. Law enforcement, the military, and business examiners utilize it to look into computer-related incidents. Even recovering photographs from the memory card of your camera is possible with it.

#### 2.1.2. WEFA (Web Browser Forensic Analyzer)

A free online browser analysis tool is WEFA. Windows NT and later versions support it. Supports the following web browsers: Swing, Internet Explorer (11), Mozilla Firefox, Apple Safari, Opera, Chromium, Google Chrome, Google Chrome Canary, Comodo Dragon, and Cool Novo (Chrome Plus). WEFA provides several performance options for these browsers. Either an active system or an image disc can be analysed. These techniques involve obtaining the cache of the web browser. Cookies, download history, session data, transient internet files, and timesheet data are all examples of internet data, and information. The retrieved information can be viewed in timeline, HTML, or URL parameters views. Searches can be performed on collected data using regular expressions, dates, and keywords. Recovering destroyed data is also possible. The index.dat file can be thoroughly examined, and user behaviour can be categorized and analysed

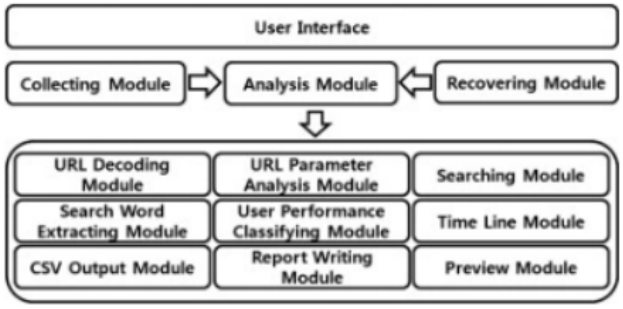



**Fig. 1.** WEFA structure.

#### 2.1.3. Net Analysis

The application Net Analysis allows for the extraction, analysis, and forensic evidence related to the Internet is presented by browser and user behaviour on desktop and mobile devices. Additionally, our Net Analysis package has sophisticated data. Recovery program created to restore erased browser history artifacts that may be studied and imported into Net Analysis. .Net Analysis is software that provides substantial advancements over current uses and methodologies.

#### 2.1.4. Browser History Examiner

The Browser History Examiner analyses web records for chrome, Firefox, and internet explorer web browsers on the Windows platform. Browser History Examiner is a forensic software program for capturing, extracting, and reading net records from the principal computer net browsers. Various information may be analysed together with internet site visits, searches, downloads, and cached files.

#### 2.1.5. Internet Evidence Finder

Internet Evidence Finder (IEF) is a computer forensics software program that can get better statistics from a problematic drive, RAM, or documents for Internet-associated evidence. IEF changed into being designed with virtual forensics examiners in mind; IEF is likewise used significantly by employees in IT facts security, digital discovery, cyber security, and company investigations

## 3. Literature Analysis

### 3.1 Browser Forensics

A web browser is a piece of software that enables users to find, access, and view web pages. Additionally, it is the only method used to access the internet for activities like accessing email, social networking, uploading and downloading files and videos, and other information that is normally found on a web page at a website on the World Wide Web (www) or a local network. A key aspect of digital forensic investigations is often searching for Web browsing-related data. Nearly all actions a suspect does while using a Web browser are recorded on the device, even looking for information in a Web browser. Therefore, this data can offer valuable information when a detective examines the suspect's computer. It is possible to examine evidence from a suspect's computer, such as cache, history, cookies, and download list, to determine the websites visited, the timing and frequency of access, and the search engine terms used.

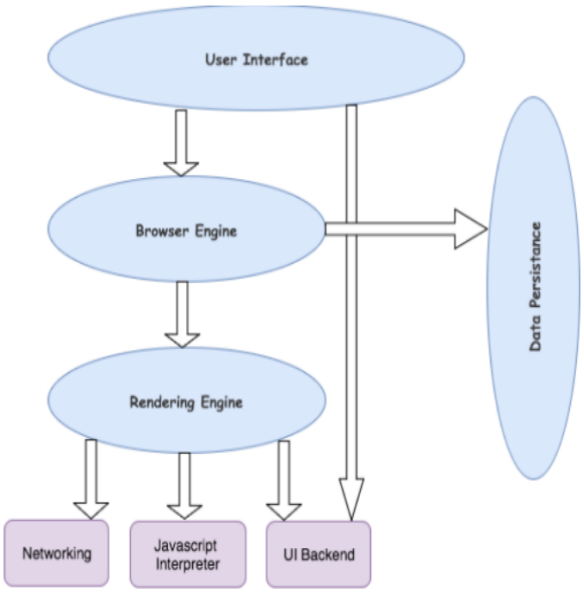



**Fig. 2.** Working of Web Browser

### 3.2 Steps in the digital forensic process

1. Examine the crime scene. In order to undertake an investigation, one must first receive the necessary authorization. This usually entails evaluating the circumstances, interviewing relevant parties, and recording the findings in an effort to pinpoint the crime and the location of the evidence. 2. The collection phase requires one to locate prospective data sources, such as computers, storage devices, routers, mobile phones, digital cameras, etc., and collect forensic data from them. Locating the evidence, determining its significance, accumulating the evidence, and preparing a chain of custody are the main steps in the collection phase. 3. Analyse the data/files gathered and identify the relevant proof. The method requires the computer forensic investigator to find, sort, and retrieve concealed data. 4. Report phase: The audience should be able to comprehend the information gathered throughout the phase of evidence gathering and analysis. The report creation step stores the supporting information that each analysis component has uncovered. It also keeps track of the time and offers hash values for the evidence that was gathered to prove the chain of custody. 5. The inquiry requires documentation, thus this phase is crucial. Integrity must be maintained for testimony to be trusted in court. The necessity for secure storage and tamper resistance. A court cannot claim that the evidence has been tampered with if there is a chain of custody. As soon as evidence is gathered, it needs to be categorized and collected. The investigator should keep a record of everything they do, including why they did it. All actions must be recorded, as well as integrity checked.

### 3.3 Keeping Records on Computers

Web browsers are used to store user activity in various areas of the operating system. Analyses are needed in many different fields in order to get user information. Additionally, data differs depending on the type of web browser. Web browsers maintain user data in four different places. These are cookies, cache records, and history records. Web browsers claim that the system keeps data in several folders and places. Examining data from various folders is crucial for the analysis process. In the four different record kinds stated above, folders should be looked for. Computer users frequently use the web browser Internet Explorer. Each user's own Internet activity history is kept in the user profile folder. According to the locations shown in the Table, data is stored individually in the Cookies, Cache, Download History, and history folders. Index.dat or container.dat database files contain the data that is stored in folders. This file contains data in binary format. Safari maintains web browser information in a binary file called History, under the web browser.

### 3.4. Clearing the Web Browser History

When web browser data was analysed, it appeared suspicious that browser data may have been wiped. Users of several web browsers have the ability to remove their cache, cookies, history, and downloaded files. Users will discard data that can be obtained in an inspection using a browser function if this information is deleted. To delete records, there are two methods. The old data is lost using the first technique, which involves overwriting the existing data when apps are launched. The second method is user-initiated data deletion from the menu or index of the browser. Accessing old data after the first technique is really difficult. By recovering and scratching the disc after the second procedure, data can be accessed.

Table 2. Lists the options and routes that permit browser users to delete records.

| Web Browser | Delete Options Path |
|---|---|
| İnternet Explorer | Settings/ Internet Options/ / Deletes |
| Firefox | Settings /Privacy/History<br>about:preferences#privacy |
| Google Chrome | Settings /History/Search Data<br>chrome://settings/clearBrowserData |
| Safari | Settings / Privacy / Delete All Web Site Data<br>Settings/History |
| Opera | Settings /History/Privacy and Security/Delete All Search Data<br>opera://settings/clearBrowserData |

## 4. Methodology

### 4.1 Social Media forensic extraction from digital devices

The goal of the digital forensic gathering method is to serve as evidence in a civil or criminal legal proceeding, secure electronic data is required. The information readily available on social media in the case of sites are easily reachable and completely understandable for regular users. Despite the requirement to adhere to the official procedure of purchase made in accordance with legal specifications for utilizing This process is primarily carried out by a person with sufficient expertise in legal and technical fields matters to guarantee the acquisition's legality. It is acknowledged that forensic artifacts are an important source of proof. through social media. Thus, the majority of research efforts are concentrated on acquiring forensic evidence. Initial studies on forensic extraction from social media were focused on the identification of individual devices and the retrieval of traces discovered on devices left by browsers and social media programs. The prerequisites for the general definition of forensic social media collecting are 1. Gathering pertinent information or content from many networks and media portals. 2. Gathering info from posts on social media. 3. During the forensic data collection procedure, make sure the data are accurate. Digital device social media forensic extraction

### 4.2 Analysing the methods

A Web browser is used by users to carry out a variety of tasks, including information retrieval, email, shopping, reading the news, online banking, blogging, and SNS. The forensic investigator should therefore be able to examine the user's actions when carrying out the information from a search engine that can be used. It's crucial to examine information retrieval activity. Additionally, data may be lost if a user uses numerous Web browsers generated by various Web browsers, which needs to be examined in an identical timeframe.

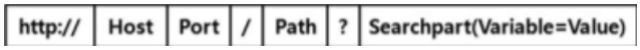
### 4.3. Integrated analysis

Web browsers are diverse, with every one having its characteristics. This permits customers to select their favourites or to strive for numerous Web browsers at an equal time. In This situation, it's far more difficult to hint at the websites that a person has visited if the forensic investigator can examine the simplest log files from a selected Web browser. Therefore, the investigator needs to be capable of observing all current Web browsers in a single machine and carrying out an integrated evaluation of more than one Web browser. For integrated evaluation, the important information, extra than all the different information, is time information. Every Web browser's log file includes time information, and consequently, it's feasible to construct a timeline array of the usage of this time information.

### 4.4. Timeline analysis

In a digital forensic investigation, it's far more important to stumble on the motion of the suspect alongside a timeline. By appearing in a timeline evaluation, the investigator can hint at the crook activities of the suspect in their entirety. The evaluation affords the path of movement from one Web page to any other and what the suspect did on every unique Web page. In addition, time region statistics should be considered. As described in Section 3.3, all 5 main Web browsers use UTC time. As a result, the time statistics extracted from the log file aren't always the suspect's neighbourhood time. For this reason, the investigator should observe a time region correction to the time information. Otherwise, the investigator can't recognize the exact neighbourhood time of the suspect's Internet behaviour. For instance, if the investigator is extracting log documents for a suspected New York (UTC/GMT ), the investigator ought to apply correction to New York's time region to the time statistics.

**Fig. 3.** General HTTP URL information structure.




## 4.5. Analysis of search history

Beyond the research of which Web websites the suspect has visited, it's crucial to analyse the hunt phrases he used in the hunt engine. These seek phrases can also additionally provide keywords for his crime, whether or not a single phrase or sometimes a sentence. In this case, seek phrases are proof of the suspect's efforts to acquire facts for his crime and may specify the purpose, target, and strategies of the crime. After the use of a search engine, search phrases are stored as HTTP URL information. The general HTTP URL information structure is shown in fig 2. The Path in this structure shows that the appropriate HTTP URL was utilized for search activities. The search terms are additionally provided by the variable name. For instance, if the search term "cyber security" is entered into the Google search bar, the following URL information is generated

https://www.google.com/search?q=cyber+security&sxsrf=ALiCzsY0oG4TBfHWIBhONxTqThD7WPeNFA%3A1668091000979&ei=eAxtY-y2O4W_8QOhvIrwDQ&oq=cyber&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAxgBMgQIABBDMgoIABCxAxCDARBDMgQIABBDMgcILhCxAxBDMgQIABBDMgQIABBDMgQIABBDMgcIABCxAxBDMgcIABCxAxBDOgcIIxDqAhAnOgQIIxAnOgUIABCRAjoICC4QgwEQsQM6CAgAELEDEIMBOgsIABCABBCxAxCDAToKCC4QgwEQsQMQQzoKCC4QsQMQgwEQQzoECC4QQzoFCAAQgAQ6CAgAEIAEELEDOgQILhAnOgoILhCxAxDUAhBDSgQITRgBSgQIQRgASgQIRhgAUJgHWPUwYPdFaAZwAXgAgAH5AYgB6AySAQUwLjkuMZgBAKABAbABCsABAQ&sclient=gws-wiz-serp

Many pieces of information can be gleaned from this HTTP URL, such as the host is google.com and the path is/search. This offers essential information about HTTP URLs related to search activity. After the variable q, the suspect's desired search terms are readily apparent. In other words, the search terms are the value of the variable q. The host, path, and variable are all referred to differently by each search engine. Consequently, an investigation of the HTTP URL architecture of various search engines is required. The top ten search engines in the world according to the authors' analysis were Google, Yahoo, Baidu, Bing, Ask, AOL, Excite, Lycos, Alta Vista, and MSN.

In HTTP URL addresses, several assumptions are made. First, the word "search" appears in the majority of host and path names across different search engines. The majority of search term variables go by the names q, p, or query. When it is possible to locate the word "search" in the host and path names as well as q or p as a variable name, these hypotheses allow an investigator to extract search words from an unknown HTTP URL. Search engines that are not accustomed to this technique must create and to extract search terms, a second signature database. Using this technique, a detective can get the search terms that a suspect employed, and you can infer their intent, target, and crime's technique

## 4.6 Analysis on URL encoding

For instance, if the search term "cyber security" is entered into the Google search bar, the following URL information is generated:
https://www.google.com/search?q=cyber+security&sxsrf=ALiCzsY0oG4TBfHWIBhONxTqThD7WPeNFA%3A1668091000979&ei=eAxtY-y2O4W_8QOhvIrwDQ&oq=cyber&gs_lcp=Cgxnd3Mtd2l6LXNlcnAQAxgBMgQIABBDMgoIABCxAxCDARBDMgQIABBDMgcILhCxAxBDMgQIABBDMgQIABBDMgQIABBDMgcIABCxAxBDMgcIABCxAxBDOgcIIxDqAhAnOgQIIxAnOgUIABCRAjoICC4QgwEQsQM6CAgAELEDEIMBOgsIABCABBCxAxCDAToKCC4QgwEQsQMQQzoKCC4QsQMQgwEQQzoECC4QQzoFCAAQgAQ6CAgAEIAEELEDOgQILhAnOgoILhCxAxDUAhBDSgQITRgBSgQIQRgASgQIRhgAUJgHWPUwYPdFaAZwAXgAgAH5AYgB6AySAQUwLjkuMZgBAKABAbABCsABAQ&sclient=gws-wiz-serp

If the variable q can be identified, search words can be found, however, the meaning of encoded search words cannot be determined using this method. Hexadecimal codes and the letter %, which is placed before each one-byte character, are used to express encoded characters in HTTP URLs. Each site uses a different encoding scheme. The vast majority of websites in the top 10 search engines worldwide employ UTF-8 encoding. Baidu mostly utilizes GB2312 encoding, however, when the search terms are not in Chinese, it switches to Unicode encoding.

Most search engines in East Asia employ an encoding that belongs to the encoding class known as DBCS (Double Byte Character Set). The format for DBCS encoding is not standardized. Moreover, Japanese search engines like Livedoor use Encoding with EUC-JP and Shift-JIS. As mentioned above, the majority of search engines select an encoding technique from the UTF-8, Unicode, or DBCS encoding classes for search words or any other characters. However, in rare circumstances, some search engines use various encoding methods for several words in a single HTTP URL. Considering these signatures. Since it's already there, the investigator can tell that the encoding is Unicode. The investigator can use UTF-8 encoding to use a distinct bit signature given for UTF-8 encoding in RFC 3629. UTF-8 encoding, however, also includes a form of two-byte encoding. Therefore, DBCS encoding cannot be recognized from two-byte UTF-8 encoding. For instance, a search engine-based technique of distinction or both decoding methods can be used to decode all the word techniques and print them. Using this approach, the researcher can tell the difference between encoding

techniques and employ the appropriate decoding encoding technique for words. This will aid in understanding the words that were encoded.

Table 3. Host, path, and search word locations for different search engines

| SearchEngine | Host | Path | Search Word Location |
|---|---|---|---|
| Google | google.com | #sclient | After variable *q* |
| Yahoo | search.yahoo.com | /search | After variable *p* |
| Baidu | baidu.com | /s | After variable *wd* |
| Bing | bing.com | /search | After variable *q* |
| Ask | ask.com | /web | After variable *q* |
| AOL | search.aol.com | /search/ | After variable *q* |
| Excite | msxml.excite.com | /results/ | After path/*Web*/ |
| Lycos | Search.lycos.com | | After variable *query* |
| Alta vista | altavista.com | /search | After variable *p* |
| MSN | bing.com | /search | After variable *q* |

## 4.7. Analysis of user activity

One HTTP URL is insufficient to identify a suspect's online activities in a trail of Web browser activity for an investigation. It would be simple to track the websites visited and estimate the suspect's movements over time if a suspect's movements could be categorized using HTTP URL information. To assess user activity, the investigator must visit all pertinent Web pages. This procedure compels the investigator to interact directly with the Web browser, which might take too much time. A method of calculating user activity from HTTP URL data is required to quicken the investigative process for digital forensic analysis

The person in charge of the website determines what is included in the HTTP URL information. The context of the Web page is included in information like domain and path in the HTTP URL. Typically, the HTTP URL contains a term that describes the activity that the Web page offers. This fact makes it possible to categorize the user's online activities using a specific term from the HTTP URL. Specific actions that a user can conduct with a web browser are categorized in Table 4. The activity is not entirely covered in this table. For instance, not all blog sites feature the word blog in their HTTP URL. In this instance. To manage the additional database construct, the particular phrase to describe the user's additional actions performed.

Table 4. User activities in a Web browser

| User Activity | Keyword in URL |
|---|---|
| Search | Existence of Searched words |
| Mail | Mail |
| Blogging | Blog |
| SNS | Facebook, Twitter… |
| News | News |
| Weather | Weather |
| Shopping | Shopping, Amazon… |
| Game | Game |
| Audio-Visual content | Video |
| Music | Music |
| Banking | Bank |

## 4.8. Recovery of deleted information

The majority of web browsers have a delete option for log data like the cache, history, cookies, and download list. Investigating whether a user used this function to delete log data will be challenging. There are two methods for deleting log data. The first entails overwriting or reinitializing log data. The log file is not removed in this instance. The second step entails erasing the pertinent log file. The log information cannot be recovered if the web user chose the first option, but the deleted file can be recovered and the log information can be extracted if the web browser selected the second option. The recovery method for deleted log information is as follows: It is possible to recover Internet Explorer, deleted cookie files, deleted weekly/daily index.dat files, and deleted temporary Internet files. This implies that the researcher can gather except for the weekly/daily index.dat files, all index.dat files are reinitialized and are not retrievable by Internet Explorer. The session log file is simply removed from Firefox. The investigator can extract some of the historical data from the destroyed session log file if it can be restored. Other log files have been reinitialized and are unrecoverable. Cache files are simply destroyed in Chrome, thus information can be retrieved from recovered cache files

Additionally, the monthly history file is only removed. As a result, deleted history data for the pertinent month can be recovered. Other log files have been reinitialized and are unrecoverable. It is feasible to extract data from a restored cookie file since Safari simply deletes the cookie file. Additionally, the session file is only removed. So, using a recovered session file, the investigator can extract a small portion of the history data. Other log files have been reinitialized and are unrecoverable. Due to the fact that Internet Explorer automatically moves history data from daily index.dat files to weekly index.dat files at the end of each week and deletes the daily index.dat files, there are a lot of deleted daily index.dat files in unallocated space.

Additionally, a lot of Firefox session files are stored in unallocated space because the session file is automatically deleted when Firefox is closed.

Table 5. Methods of erasing log information in five Web browsers

| Browser | Category | Erasing Method |
|---|---|---|
| IE | Cache | Initialization of *index.dat* file Deletion of Temporary Internet files |
| | History | Initialization of *index.dat* file Deleting daily and/or weekly *index.dat* files |
| | Cookie | Initialization of *index.dat* file Deletion of cookie files |
| | Download | IE has no download information |
| Firefox | Cache | Initialization |
| | History | Initialization |
| | Cookie | Initialization |
| | Download | Initialization |
| Chrome | Cache | Deletion |
| | History | Initialization |
| | Cookie | Initialization |
| | Download | Initialization |
| Safari | Cache | Initialization |
| | History | Initialization |
| | Cookie | Deletion |
| | Download | Initialization |
| Opera | Cache | Initialization |
| | History | Initialization |
| | Cookie | Initialization |
| | Download | Initialization |

Table 6. Recovery method for deleted information in five Web browsers.

| Browser | Category | Recovery Method |
|---|---|---|
| IE | Cache | Recovery of temporary Internet files |
| | History | Recovery of weekly/daily *index.dat* files<br>Recovery of *index.dat* file through carving method |
| | Cookie | Recovery of cookie files |
| | Download | IE has no download information |
| Firefox | Cache | N/A |
| | History | Recovery of session file through carving method |
| | Cookie | N/A |
| | Download | N/A |
| Chrome | Cache | Recovery of cache files |
| | History | Recovery of monthly history files |
| | Cookie | N/A |
| | Download | N/A |
| Safari | Cache | N/A |
| | History | Recovery of session files |
| | Cookie | Recovery of cookie files |
| | Download | N/A |
| Opera | Cache | N/A |
| | History | Recovery of session files |
| | Cookie | N/A |
| | Download | N/A |

## 5. Conclusions

Finding Web browser usage evidence is a crucial step in digital forensic investigations. It is feasible to identify the goal by examining a trace of Web browser usage. Procedures, as well as a suspect's criminal activity. One of the main things an investigator will focus on while looking at a suspect's computer is the Web browser's log file. The issues with the tools and studies that are now available for Web browser forensics have been examined in this work. In response, a cutting-edge methodology has been suggested to get rid of some of the restrictions this field possesses

It is required to do integrated analysis for several browsers at once when looking at Web browser usage evidence, and timeline analysis can be used to track a suspect's online activities over time. Additionally, it is important to look into the search terms the suspect used because they can reveal some of the suspect's traits and goals. In the event that the search terms are encoded, a decoding procedure is needed. In terms of digital forensics, investigation based on user behavior is equally essential. With the planned WEFA technology, forensic investigators will be able to conduct speedy analyses and assess the suspect's illegal operations as swiftly as possible. This study looked into Web browsers operating in a Windows environment. Future studies will include studying Web browser forensics on many operating platforms, including Linux, Mac, and mobile ones in addition to Windows.

### Acknowledgements.

The successful completion of this research would not have been possible without the generous assistance and support of others. I take great pleasure in expressing my sincere appreciation to all those who aided me, either directly or indirectly, throughout the course of my research. I take this opportunity to extend my sincere thanks to all those who were involved with our guide Dr. Sachi Nandan Mohanty (Associate Professor), Vellore Institute of Technology, Amaravati, for always encouraging me and providing me with his valuable support and guideline throughout the completion of the project. Lastly, but certainly not of least importance, I extend my deepest and most sincere gratitude to my parents and friends for their unwavering support, and for providing me with the opportunities and encouragement to pursue my aspirations.

## References

[1] **Article**: Berners-Lee T, Masinter L, M. Mc Cahill. RFC 1738:Uniform Resource. Uniform Resource Locators (URL). December 1994;Page 2,3. Locator (URL), http://tools.ietf.org/html/rfc1738.

[2] **Journal**: Jones Keith J. Forensic analysis of internet explorer activity files. Foundstone,2003, Url-http://www.foundstone.com/us/pdf/wp_index_dat.pdf

[3] **Journal**: Jones Keith j, Rohyt Blani. Web browser forensic. Security focus, 2005a,2005b. http://www.securityfocus.com/infocus/1827;

**[4]** **Book**: Humairu Arshad, Aman Jantan, Esther Omolara. Evidence collection and forensics on social networks

Research challenges and directions, Digital Investigation, Volume 28,2019,Pages 126-138,ISSN 1742-2876.

[5] **Article**: Jadhav, Mayur Rajendra, and Dr. Bandu Baburao Meshram. "Web Browser Forensics for Detecting User Activities." vol. 5, no. 7, 2018