Web Browser Forensics for Detecting User Activities

Mayur Rajendra Jadhav[1], Dr. Bandu Baburao Meshram[2]

[1]P.G. Student, Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai
[2]Professor, Department of Computer Engineering, Veermata Jijabai Technological Institute, Mumbai

---***---

Abstract - *The most widely used applications by the majority of user of computer are Web Browsers. A Web browser is an application program for accessing the Internet. Users performs their many activities such as, browsing on the internet, download files, use social media applications, accessing e-mail accounts via web browser. If user uses illegally the Internet as a source of information, the evidence related to the browser uses would be saved in the log file of the Web browser. Web browser's log file can help to collect information of criminal. After considering existing research and tools, this paper suggests a new evidence collection and analysis methodology and tool for forensic process.*

Key Words: Digital Forensic, Web Browser Forensic, Digital Evidence, Framework, Integrated Analysis, Search word analysis

1. INTRODUCTION

Browser forensic is mainly used for analyzing things like browsing history and general web activity of a pc to check for suspicious usage or content that has been accessed. This also refers to monitoring traffic on a webpage and analysis of LOG files from server to get actual information about targeted machine. Computers and their storage media is the object of investigative analysis, known as Computer Forensics, aimed at characterizing and interpreting the digital evidences present on the devices.

 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 crucial component of digital forensic investigations. Almost every movement of a suspect performed by using a web browser thus would leave a trace on a computer. Thus when an investigator analyzes the suspect's computer, this evidence can provide useful information. After retrieving data such as cookies, cache, history and download list from a suspect's computer, it is possible to analyze this evidence for web sites visited, time and frequency of access, and search engine keywords used by the suspect.

Following can be the different sources where an investigator can find evidences in browser.

1. Surfing history
2. Bookmarks
3. Download
4. Cookies
5. Cache

2. LITERATURE SURVEY

2.1 Browser Forensics

The Internet is used by almost everyone, including suspects under investigation. A suspect may use a Web browser to collect information, to hide his/her crime, or to search for a new crime method. Searching for evidence left by Web browsing activity is typically 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. Moreover, it is not sufficient to investigate a single file from a single browser because the evidence may be spread over several files. [17]

2.2 Steps in digital forensic process

1. Assess the crime scene- To conduct an investigation, one need to obtain proper authorization which would normally include assessing the case, asking people and documenting the results in an effort to identify crime and location of the evidence.

2. Collection phase- Here one would need to identify potential sources of data and acquire forensic data from them such as desktops, storage media, routers, cell phones, digital camera etc.. Finding the evidence, discovering their relevance, gathering the evidence, and

preparing a chain of custody are the main steps in collection phase.

3. Analysis phase- Examine the collected data/files and find out the actual evidence. The computer forensic investigator must trace, filter, and extract hidden data during the process.

4. Report phase- The audience should be able to understand the evidence data which has been acquired from the evidence collection and analysis phase. The report generation phase records the evidence data found out by each analysis component. Additionally, it records the time and provides hash values of the collected evidence for the chain-of-custody.

5. Documentation phase- Documentation is essential for the investigation. For evidence to be reliable in court, integrity has to be preserved. Safe storage and tamper protection is needed. Chain of custody prevents accusation in court that the evidence has been tampered with. Evidence needs to be labeled as soon as it is collected. All actions performed by the investigator should be documented, including the reasons for doing so. This means logging all actions and integrity checks. [16]

2.3 Challenges in Browser Forensic Process

1. Multiple browsers: Investigators will likely encounter numerous mainstream browsers. There may even be multiple browsers in use on the same machine.

2. Varied storage schemes: Once investigators determine which browsers are being used, they must realize that each browser may store different types of artifacts, differently and in different locations.

3. New/updated architectures: Browser developers may even completely change the architecture between versions, as Mozilla Firefox and Internet Explorer (IE) have done in the past.

4. Non-standard browsers: To further frustrate investigators, attackers may actually install a non-standard browser in an effort to obfuscate their activities.

2.4 Recovery methods of browser history

1. Recover deleted Internet history through

    i. Recover Data from Browser Cookies

Internet cookies are also another good method to access internet history. A cookie is a small text file that stored in your internet browser. They store your user information to for the web sites you visit. [1][13]

Fig 1: Cookies stored in Browser

    ii. Recover Data from Windows System Restore

The easiest method is to do a system restore. If the internet history was deleted recently system restore will recover it. To get system restore up and running you can go to the 'start' menu and do a search for system restore which will take you to the feature. Alternatively, go to 'Start' click on 'Programs' and then 'Accessories.'

You'll see a 'System Tools' option and 'System Restore' will be in there. Select the date you'd like to restore your computer to and sit back and wait until it does its thing. When finished the computer will reboot and if check your browser the internet history should be in there. [5]
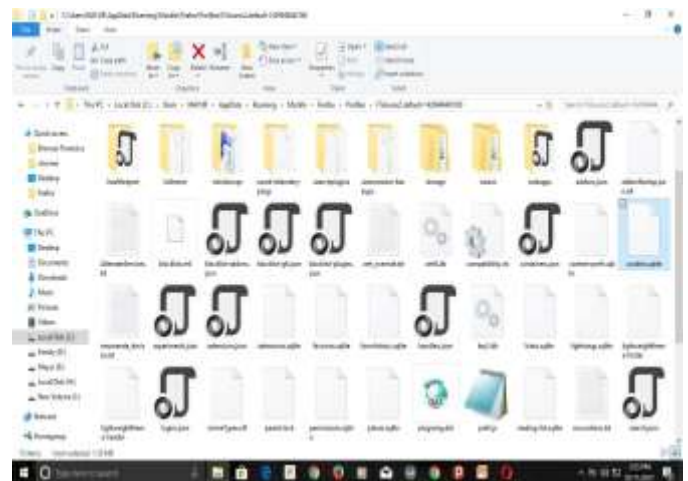

Fig 2: Evidences store in User System

2. Access deleted browning history with log files

Another method is to recover the history using log files. This method is suitable for histories that were deleted a long time ago. A word of warning though, while there is a simple step-by-step process to follow using this method some strange things can be thrown up such as warnings that you might lose other data. This isn't common but it's a point worth

nothing. All Windows computers have a file extension that stores arbitrary data. It's called Index.dat and is a file hidden on your computer that contains all of the web sites that you have ever visited. It lists every URL and every web page.

Possible evidences from these could include:

a) Surfing History could include typed URLs, redirects and also the number of visits to a particular site.

b) Bookmarks would mainly contain shortcuts or bookmarks created to specific websites by user.

c) For downloads, an investigator would mainly need to check for downloaded file in the default locations which can also include user defined locations or sometimes files that are downloaded to default locations and are then moved or copied to user defined locations.

d) Cookies are the files that contain a wealth of information about the user, it may contain information like usernames, passwords and web session information.

e) Cache is a temporary area on the disk which is used to store most recently visited web sites. [5]

3. Recover deleted browsing history from Google History

If you have Google Account and logged in everything when you browse websites, you will have a great chance to find and recover browser/internet history. When deleted history from browsers, the Google History is not deleted. It will store all browsing history including all pages that you've ever visited and even devices attached to your Google Account. Go to Google History, sign in with Google account. Then all of your browser/internet history will be displayed along with date/time.

This is by far the easiest method but it will only work if you were signed in to your account during the browsing session you wish to access. Sign into your Google Account.

Go to www.myactivity.google.com/myactivity. And enter the information for the account that you were browsing with. Review your browsing history. From this page you will be able to see your browsing history according to time and date. If you wish to delete your history, simply click on the cog icon in the upper-right hand corner of the screen and select "Remove Items."

Fig 3: View History using Google History

4. Using DNS Cache to find and view deleted browsing history

DNS, which is known as Domain Name System, can work as a fast method to restore searches or history for you. But when computer is restarted, it will not be able to help you find browsing history then. DNS cache can only work when almost everything is connected to the internet. Therefore, if you need to restore deleted browsing history for an app or video game, please do not shut down or restart the computer. You may still have a chance to view the deleted internet history. Open Command Prompt, type ipcongif/displaydns and click Enter. [14]
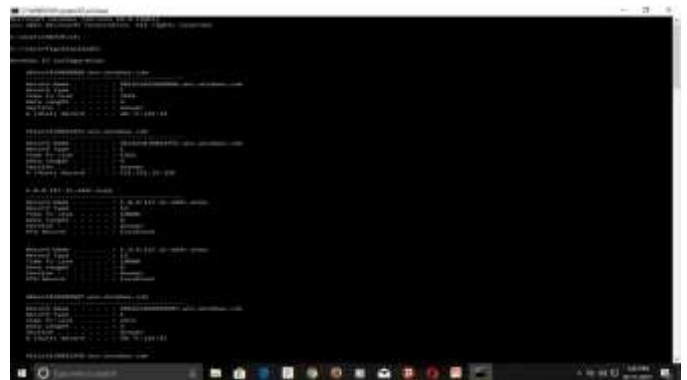
Fig 4: View History using DNS Cache

2.5 Existing Tools

1. Autopsy

Autopsy is a digital forensic platform for Windows and Linux. It provides the facility for data carving, timeline analysis, and web artifact analysis. The autopsy extracts the web history, cookies, bookmarks from Firefox, Chrome and IE. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

2. Browser History Examiner

The Browser History Examiner analyzes web history for chrome, Firefox, internet explorer web browser on the Windows platform. Browser History Examiner is a forensic software tool for capturing, extracting and analyzing internet history from the main desktop web browsers. Many types of data can be analyzed including website visits, searches, downloads and cached files. [5][8]

3. NetAnalysis

NetAnalysis is application for the extraction, analysis and presentation of forensic evidence relating to Internet browser and user activity on computer systems and mobile devices. Our NetAnalysis suite also includes advanced data recovery solution designed to recover deleted browser artefacts which can be imported into, and analyzed in NetAnalysis. NetAnalysis is a software product that offers significant improvements over existing applications and methodologies. [2][5][8]

4. Internet Evidence Finder

Internet Evidence Finder (IEF) is a computer forensics software product that can recover data from a hard drive, live RAM, or files for Internet-related evidence. IEF was designed with digital forensics examiners mind; IEF is also used extensively by personnel in IT information security, electronic discovery, cyber security, and corporate investigations. [5]

3. PROPOSED SYSTEM

3.1 Proposed System Component Diagram
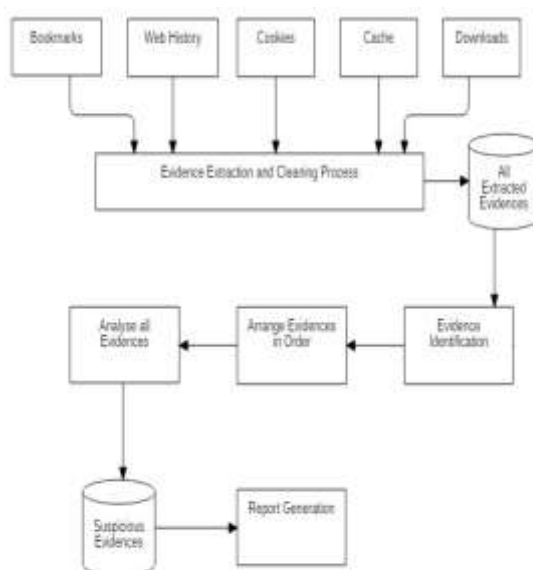
Fig 5: Proposed System Component Diagram

Description of Components:

1. Sources: Bookmarks, Web History, Cookies, cache, Downloads.

2. Evidence Extraction and cleaning process: Here all compressed data extracted in normal data.

3. All Extracted Evidences: All Extracted Evidences stored in database.

4. Evidence Identification: Find the illegal website evidences.

5. Arrange Evidences in Order: arrange all evidences in proper manner.

6. Analyze all evidences: Apply forensics process.

7. Suspicious Evidences: finding the suspicious data.

8. Report Generation: Generates the criminal's information.

3.2 Web Browsers Used in Proposed System

1. Firefox

Mozilla Firefox is another popular web browser which can be found on multiple platforms. Browsers like Mozilla and Chrome can also be found on mobile device working on platforms like android, iPads etc... Following could be the common areas where Firefox web browsing artifacts can be found and located:

a. SQLite database structure
b. Prefs.js(user preference)
c. Signons.txt(encrypted data for website authentication)
d. Form history(SQLite)
e. Cookies(SQLite)
f. Firefox cache
g. Places(bookmarks and history)
h. Downloads

Private Browsing features of Mozilla-

Private browsing mode allows users to surf the Internet without saving any information about visited sites or pages. Mozilla makes it clear that private browsing mode does not make users anonymous from web sites, ISPs, and networks. So private browsing is merely affected in the application layer recognized in the OS. Aside from other privacy features, there is an option to enable the Dot-Not Track feature in Firefox which requests that web sites do not track user browsing behavior. [3][7][8][10][15]

2. Google Chrome

Google Chrome is another very popular web browser that can be found on both Windows and Mac OS. Evidences from Chrome can be located in:

a. JSON(JavaScript Object Notation) structure- this is a text based open standard design for human readable data
b. Downloads
c. Bookmarks
d. Web data
e. Keyword search terms
f. Keywords
g. URL database
h. History index
i. Current and last sessions
j. Top sites database
k. Media cache

Chrome offers Incognito mode for users to browse the internet in a private setting. Incognito mode does not save or record any browsing or download histories, ad all created cookies will be removed when exiting a session completely. Additionally, if users are working in Chrome OS, surfing the internet under guest browsing also does the same thing. Once the guest session is closed, all browsing information is completely erased. [6][7][18]

3. Internet Explorer

Microsoft Internet Explorer is one of the most commonly used web browsers on Windows. A list of areas from where most IE browsing artifacts are located could be as follows

1. Cookies(index.dat)
2. History(index.dat)
3. Registry(typed URLs, search queries, auto-complete, protected storage)
4. Downloads
5. Temporary files and index.dat entries. [7]

4. Opera

Opera is another very popular web browser that can be found on both Windows and Mac OS. Evidences from Opera can be located in:

a. Downloads
b. Bookmarks
c. Web data
d. Keyword search terms
e. Keywords
f. URL database

3.3 Evidence Collection Analysis of Web Browser

Web Browsers are used by users for accessing the Websites, downloading and uploading the information on the web. Website developer makes use of Cookies to store the browsing information of user. This cookie store in Cache while subsequent use of same data or files by users information is send from cache, using this we can access the data faster than normal getting data from directly from server. It reduces the accessing time of website. [1]

1. Integrated Analysis

In this method user select a particular Web Browser depending on the requirements. The requirements can be high speed, easy to use, website compatibility. As there can be more than one browser used by the user on system therefore it becomes essential to do the forensic investigation of all the web browsers related log files. [1]

2. User Activity Analysis
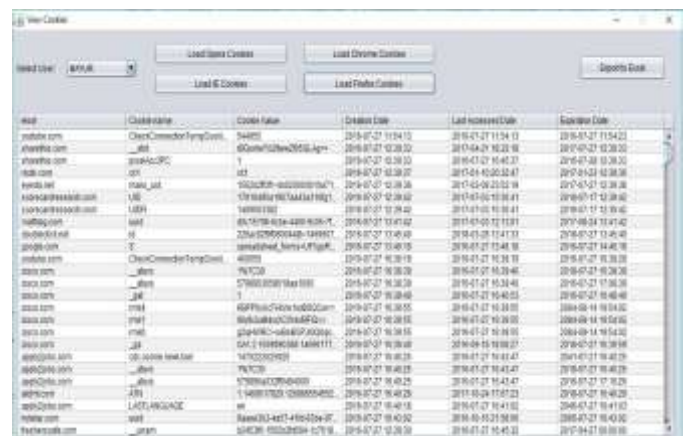
In this method, we get the analysis results on user activity details. The user performs various activities while using web browser. These web related activities can be categorized as web sites browsed, sending and receiving mails, uploading and downloading of the data. [1]

3. Timeline Analysis

By performing a timeline analysis, the investigator can trace the criminal activities of the suspect in their activities sequencing. The history log files for each web browser maintains the URL accessed by user along with the access time and date. The analysis provides the path of motion from one Web site to another and what the suspect did on each specific Web site. [1]

4. IMPLETATION RESULTS

Following are the implementation details of proposed system.

Fig 6: Analysis of Cookies

Fig 7: Analysis of Downloads History

Fig 8: Analysis of Browsing History

Fig 9: Analysis of Website Hosts Data

Fig 10: Analysis of Searched Keywords

5. CONCLUSIONS

This paper suggests the forensic method for various web browsers being used on windows platform. The tool such as Autopsy, NetAnalysis, and Internet Evidence finder performs forensic investigation of limited log files associated with the web browsers on windows platform. However, the proposed methodology includes the History, Cookies, Searched Keywords, Website Hosts, Download log files for various browsers to detect suspicious activities. A framework to detect the suspicious activity of the user based on the evidences collected from the log files of the web browser in proposed.

REFERENCES

[1] Junghoon Oh, Seungbong Lee, Sangjin Lee, "Advanced evidence collection and analysis of web browser activity", Digital Investigation 8, 2011, 8, PP. 62-70.

[2] Apurva Nalawade, Smita Bharne, Vanita Mane, "Forensic Analysis and Evidence Collection for Web Browser Activity", IEEE 2016.

[3] Murilo Tito Pereira, "Forensic analysis of the Firefox 3 internet history and recovery of deleted SQLite records", ScienceDirect, Digital Investigation 2009, PP. 93-103.

[4] Huwida Said, Noor Al Mutawa, Al Awadhi, Mario Guimaraes,"Forensic analysis of private browsing artifacts", Proceedings of International Conference on Innovations in Information Technology IEEE 2011, pp. 198-202.

[5] Erhan Akbal, Fatma Gunes, Ayhan Akbal, "Digital Forensic Analyses of Web Browser Records", Journal of software,2016,doi: 10.17706/jsw.11.7.631-637

[6] Andrew Marrington, Ibrahim Baggili, Talal Al Ismail, Ali Al Kaf, "Portable Web Browser Forensics -A forensic examination of the privacy benefits of portable web browsers", IEEE 2012.

[7] Donny J Ohana and Narasimha Shashidhar, "Do private and portable web browsers leave incriminating evidence?: a forensic analysis of residual artifacts from private and portable web browsing sessions", Springer

Open Journal 2013, http://jis.eurasipjournals.com/content/2013/1/6

[8] Sweta Mahaju, Travis Atkison, "Evaluation of Firefox Browser Forensics Tools", ACM 2017,

DOI: http://dx.doi.org/10.1145/3077286.3077310.

[9] Wade Alcorn, Christian Frichot, Michele Orru, "The Browser Hacker's Handbook".

[10] F.Aggarwal, E. Bursztein, C. Jackson, and D. Boneh, "An analysis of private browsing modes in modern browsers," In Proc. Of 19th Usenix Security Symposium, 2010.

[11] Jones Keith j, Rohyt Blani, Web browser forensic. Security focus, Available at,

http://www.securityfocus.com/infocus/1827 , 2005a.

[12] Jones Keith j, Rohyt Blani. Web browser forensic. Security focus, Available at,

http://www.securityfocus.com/infocus/1822, 2005b.

[13] Open Document, How to View Cookies

Available at, http://www.wikihow.com/View-Cookies

[14] Tracy King, How to Recover Browser/Internet History?

Available at, https://www.easeus.com/computer-instruction/recover-browser-internet-history.html

[15] Murilo Tito Pereira, "Forensic analysis of the Firefox3 internet history and recovery of deleted SQLite records", Science Direct, Digital Investigation, 2009, PP. 93-103.

[16] Natasa Suteva, Aleksandra Mileva, "Computer Forensic Analysis of Some Web Attacks", IEEE 2014.

[17] Divyesh G Dharan D, Nagoor Meeran A R, "Forensic Evidence Collection by Reconstruction of Artefacts in Portable Web Browser", IJCA 2014.

[18] Narmeen Shafqat, "Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools", IJCSNS 2016.