Experiment No.5
To perform forensics investigation of web browser logs to detect evidence
Date of Performance:
Date of Submission:

Aim: To perform forensics investigation of web browser logs to detect evidence

Objective: To extract and analyze the evidence extracted from the various web browser logs using browser history examiner tool

Theory:

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.

On the personal computer, most of the web related activities are conducted through the web browser therefore the majority of the evidence consists of browser artifacts. Depending on the web browser used, the data will be stored differently but typically the cache, history, and cookies are your best sources of evidence. History and cookies will provide dates, times, and sites visited but the data of real evidentiary value is found in the cache. The cache stores web page components to the local disk to speed up future visits. Many emails read by the suspect are found in the cache folders and those locations vary depending on the operating system and browser used.

1)Internet Explorer

Since Internet Explorer (IE) is installed by default on most Windows installations, it’s likely the most commonly used and should always be searched when looking for webmail—or any browsing artifacts for that matter. Depending on the version of Windows and IE installed, the evidence will be stored in different locations. The locations are listed as below:

- Windows XP

%root%/Documents and Settings/%userprofile%/Local Settings/Temporary Internet Files/Content.IE5

- Windows Vista/7 %root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/Temporary Internet Files/Content.IE5

- Windows 8

%root%/Users/%userprofile%/AppData/Local/Microsoft/Windows/History

2)Mozilla Firefox

Firefox is a very popular browser and also stores its cache data in various locations based on the operating system installed. It's installed as the default browser on many Linux distributions and is available for MacOS operating system as well.

- Windows XP

%root%/Documents and Settings/%userprofile%/Local Settings/Application Data/Mozilla/Firefox/Profiles/*.default/Cache

- Windows 7/8

%root%/Users/%userprofile%/AppData/Local/Google/Chrome/User Data/Default/

- Linux

/home/%userprofile%/.config/google-chrome/Default/Application Cache/

- MacOS

/Users/%userprofile%/Caches/Google/Chrome/Default/

4) Opera

Opera web browser does not come with the desktop computers but it is default web browser in certain mobile handsets. Opera stores the user data in the following locations.

- Windows XP

C:\Documents and Settings\%USERNAME%\Local Settings\Application Data\Opera\Opera\

• Windows 7/8

C:\Users\%USERNAME%\AppData\Local\Opera\Opera\

• Linux

/home/$USER/.opera/

• MacOS

/Users/$USER/Library/Opera/cache

Apart from the browsing artifacts that show the evidence of site visited, the cache folders show the actual contents of the page or message, which is significantly more important when dealing with webmail artifacts.

Following Table gives the summary of the files used to maintain the web browser history, cookies, cache and their location in the Linux directory structure.

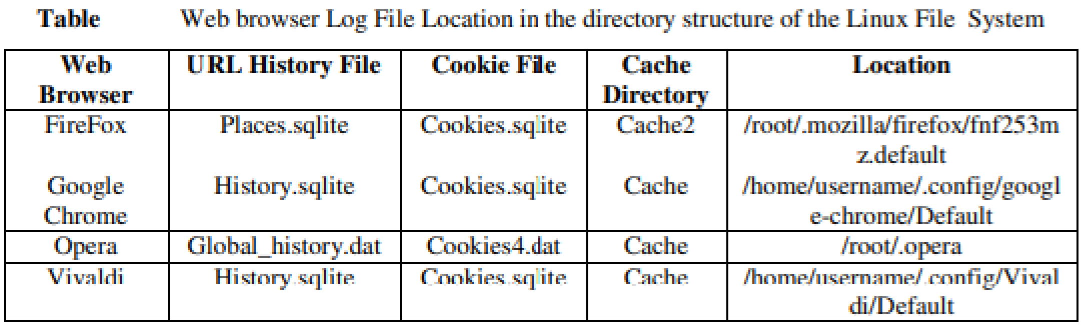

Table Web browser Log File Location in the directory structure of the Linux File System

Web Browser	URL History File	Cookie File	Cache Directory	Location
FireFox	Places.sqlite	Cookies.sqlite	Cache2	/root/.mozilla/firefox/fnf253mz.default
Google Chrome	History.sqlite	Cookies.sqlite	Cache	/home/username/.config/google-chrome/Default
Opera	Global_history.dat	Cookies4.dat	Cache	/root/.opera
Vivaldi	History.sqlite	Cookies.sqlite	Cache	/home/username/.config/Vivaldi/Default

Process:

Step 1. Install the Browser History Examiner from the website Browser History Examiner - Download | Foxton Forensics

Step 2. After successful installation, run the Browser History Examiner on your system

Step 3. Analyze the evidence extracted by Browser History Examiner

Conclusion:

The analysis of web browser logs using Browser History Examiner reveals critical evidence such as visited websites, search queries, timestamps, cached content, and cookies. These artifacts play a significant role in digital forensic investigations, as they provide insights into a suspect's online behavior, intent, and activities related to the crime. Cache data, in particular, can expose email contents or sensitive communications even if deleted. By examining this browser-related evidence, investigators can reconstruct timelines, confirm user actions, and gather supporting proof, making it invaluable in cybercrime and digital investigations.