



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

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



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

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



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

%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\



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

- 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



Vidyavardhini's College of Engineering & Technology

Department of Computer Engineering

Output:

Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artifact Records

Artifact	Records
Bookmarks	1
Browser Settings	19
Cached Files	1942
Cached Images	823
Cached Web Pages	92
Cookies	384
Downloads	6
Email Addresses	6
Extensions	7
Favicons	66
Form History	5
Logins	4
Searches	134
Session Tabs	492
Site Settings	341
Site Storage	65
Thumbnails	4
Website Visits	48

Viewing 25/25 records

Last Fetched	Server Time	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
		image/png	https://cdn.openai.co		1717124	Edge (Default)
		image/peg	https://tpc.googlest		580098	Chrome (Profile 15)
		image/peg	https://i.ytimg.com/		180501	Chrome (Profile 10)
		image/webp	https://images.cfass		152446	Chrome (Profile 15)
		image/webp	https://images.cfass		147594	Chrome (Profile 15)
		image/png	https://www.netcad		147422	Edge (Default)
		image/peg	https://vcet.edu.in/wj		147375	Chrome (Profile 10)
		image/webp	https://i.ytimg.com/a		145022	Chrome (Profile 10)
		image/png	https://ssl.gstatic.co		140703	Chrome (Profile 10)
		image/png	https://ssl.gstatic.co		140703	Chrome (Profile 15)
		image/png	https://erp.vcet.edu.i		134260	Chrome (Profile 10)
		image/png	https://erp.vcet.edu.i		124261	Chrome (Profile 10)
		image/webp	https://i.ytimg.com/c		118760	Chrome (Profile 10)

Filter by keyword

Filter by date

From: Select a date 15

To: Select a date 15

Filter by time

From: Select a time

To: Select a time

Filter by web browser

All

Filter Undo Clear

Time zone: UTC Date format: mm/dd/yyyy

www.foxtonforensics.com

Browser History Examiner - Export Viewer

Time zone: UTC

Website Visits

Summary View (Top 1000) Detailed View

Show 50 entries

Search:

Date Visited	Title	URL	Visit Type	Visit Source	Visit Count	URL Record Count	Visited From	Web Browser (Profile)
2025-02-17 07:12:09		file:///C:/Users/admin/Pictures/Screenshots/Screenshot%20(3).png			1			Internet Explorer
2025-02-17 07:12:03		file:///C:/Users/admin/Pictures/Screenshots/Screenshot%20(2).png			1			Internet Explorer
2025-02-17 07:11:53		file:///C:/Users/admin/Pictures/Screenshots/Screenshot%20(1).png			1			Internet Explorer
2025-02-17 07:07:58		file:///C:/Users/admin/Downloads/BrowserHistoryExaminer_v1.21.0.zip			1			Internet Explorer
		file:///C:/Users/admin/Do						

Time zone: UTC

Conclusion:

In a digital forensics investigation, analyzing web browser logs with tools like **Browser History Examiner** helps uncover browsing activities, visited websites, and timestamps, offering vital evidence in a case. This evidence can link suspects to online actions or provide insights into their digital behavior..