Navya Harika Karaka
November 29, 2020

CY 5210 – Technical Paper

Introduction & Analysis of Web Browsers in Digital Forensics

Abstract

Nowadays, access to the internet via web browsers became less costly and very easy. Irrespective of age, lot of people spend most of their time accessing websites for entertainment purposes or to perform work-related activities or for other reasons. Due to this, web browser forensics is critical during a digital forensic investigation.

Since users have access to various browsers and therefore, access websites and perform activities on various websites, it's getting challenging for forensic analysts to gather evidence during a investigation.

Web browser artifacts play a key role in helping forensic analysts to gather information such as browser history, cache, sessions, cookies etc. and there are various tools such as Firefox Search Engine Extractor, Browser History Viewer, Web Browser Addons View, Nirsoft Web Browsers Tools, Hindsight etc. that can be used on these artifacts.

Although there are various challenges to web browser forensics, using these tools could help overcome some of them along with keeping up with any latest features that could be added to the web browsers along with any latest and advanced resources that could help during a forensic investigation.

Introduction

In this paper, I will be discussing about various web browsers, their artifacts along with an overview of it in digital forensics.

A web browser is a software that lets a user access the Internet by visiting websites and perform various activities such as accessing images, videos, games etc. It can also be used for communication purposes which can be performed via email[1].

The availability of web browser depends on the operating system of the computer. For example, Windows operating system uses Internet Explorer/Microsoft Edge and Mac OS operating system uses Apple's Safari by default[1]. Some of the most common browsers are Google's Chrome, Mozilla Firefox, Internet Explorer/Microsoft Edge, Apple's Safari etc.

Some of the features provided by these web browsers include letting a user to access the Internet via private mode where it won’t store any information about web pages that are accessed by the user. Most of the web browsers also encrypt sensitive data such as passwords, banking details etc. Some of the web browsers such as Google's Chrome provides easy synchronization between various user's devices[2]. Among the most common web browsers, Mozilla Firefox is considered to be more secure due to its advanced incognito mode and its ability to disable tracking of user's current location and other personal details[2].

For past few years, due to enhanced security integrated into these web browsers along with new advanced features, it's getting challenging for forensic analysts to analyze web browsers to gather proper evidence. Furthermore, I will be discussing some of these challenges and tools that can be used to overcome these challenges.

Challenges related to Web Browser Forensics

Some of the common challenges that forensic analysts face that are related to web browser forensics are as follows:

- **Encryption:** Various web browsers use different encryption methods to store sensitive data, so it takes more time than usual to extract that information.
- **Various browsers in one computer:** A user can have access to several browsers even though he could be using only one computer which means that information is stored in various places and there will be a lot of data to analyze.
- **Private mode or Incognito mode:** Most browsers let users to access the internet via private mode or incognito mode where some information such as visited websites, URLs, form values etc. won't be stored and hence, the forensic analyst won't have access to it.

Artifacts related to Web Browser Forensics

Forensic Artifacts are defined as the things that are found/left behind unintentionally and are hard to identify that would help a forensic analyst to gather evidence during a forensic investigation. Some of the common artifacts are registry keys, timestamps, event logs, link files, shell bags, prefetch files etc[3]. There are various tools such as Access Data Forensic Toolkit (FTK) v6.4, Access Data FTK Imager v3.4.2.6, Registry Ripper v3.0, Registry Viewer 1.8.05, Autopsy v4.6.0, LECmd 1.2.1.0, JLECmd 1.2.1.0, Shellbags Explorer 1.3.0.0, PECmd 1.2.0.2 etc. that can be used to analyze these artifacts.

Web Browser artifacts vary based on the version and type of the web broswer but the following types of artifacts can be found in most common web browsers: History, Sessions, Autofill values, URLs, Cache, Cookies, Downloaded files etc.

Following are some examples of artifacts from Windows Operating System:
1. Cookies:
\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cookies.db (Google Chrome, Windows)

2. Cache:
\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Cache\ (Google Chrome, Windows)

3. Downloaded files:
\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\History (Google Chrome, Windows)

4. URLs:

\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\History (Google Chrome, Windows)

5. Form Values:
\Users\%userprofile%\AppData\Local\Google\Chrome\User Data\Default\Web Data (Google Chrome, Windows)

Most of these files include timestamps such as date of creation, last accessed on and last accessed by which is useful during a digital forensic investigation if a user accessed certain websites to perform certain malicious activities.

Common tools to analyze web browser artifacts

To analyze some of the web browser artifacts mentioned above, following tools can be used:

- **Firefox Search Engine Extractor:** This tool can be used to extract a brief summary of the searches performed by the user. Mozilla Firefox stores the search information in a compressed format usually as "search.json.mozlz4" and this file can be used to extract the search information[5].
- **Browser History Viewer:** Web browser history plays a key role during a forensic investigation and this forensic tool can be used to extract and view internet history from the common web browsers such as Apple's Safari, Google's Chrome, Mozilla Firefox etc. Some of the key features of this tool are website activity timeline, its ability to display the images user might have accessed online and the web pages that user have seen previously in their original state etc[8].

- **Web Browser Addons View:** These days most web browsers let users to add various plugins/addons to their browsers for easy access or to block ads or for other purposes. This tool can be used to extract the information from these plugins/addons. It will look for any available addons and provides information such as name, version, description, timestamps, status etc[7].

- **Nirsoft Web Browsers Tools:** This is a very common tool in web browser forensics since its used to extract cookies, history data and cache information from most common web browsers such as Internet Explorer and Mozilla Firefox.

- **Hindsight:** This tool is most commonly used to analyze the browsing history of Google's Chrome along with Chromium-based applications. It helps in parsing various information such as URLs, download history, cache records, bookmarks, saved passwords etc. based on the artifacts[6].

Along these tools, there are various tools and resources that can be found helpful during a digital forensic investigation.

Conclusions

Web browsers and its artifacts play a key role during a digital forensic investigation. Similar to other areas of digital forensics such as Cloud Forensics or Windows operating system forensics etc., although there are various tools and resources available, forensic analysts still face quite a few challenges due to new advanced features and enhanced security that is integrated with latest web browsers or new versions of older web browsers.

In my opinion, to overcome these challenges gradually, forensic analysts should try to keep up their understanding on these latest features on most common web browsers or try to work with these major companies during a forensic investigation. Although, it's hard to perform these tasks since the major companies try not to reveal their security features to protect user's privacy, I think the major technological companies and the forensic investigation teams need to find a middle ground to help solve the security incidents that are increasing rapidly every day.

References:

[1] About your web browser
https://www.allaboutcookies.org/browsers/

[2] An Overview of Web Browser Forensics
https://www.digitalforensics.com/blog/an-overview-of-web-browser-forensics/

[3] What are Forensic Artifacts?
https://www.tetradefense.com/digital-forensics-services/what-are-forensic-artifacts-my-favorite-artifacts-part-0/#:~:text=Like%20the%20footprints%2C%20DNA%2C%20fingerprints,the%20bottom%20of%20an%20incident.

[4] Web Browser Forensics
https://nasbench.medium.com/web-browsers-forensics-7e99940c579a

[5] Firefox Search Engine Extractor
https://www.jeffersonscher.com/ffu/searchjson.html

[6] Hindsight
https://github.com/obsidianforensics/hindsight

[7] BrowserAddonsView v1.23
https://www.nirsoft.net/utils/web_browser_addons_view.html

[8] Browser History Viewer
https://www.foxtonforensics.com/browser-history-viewer/