International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 11 | Nov 2024 www.irjet.net p-ISSN: 2395-0072

Forensics of Chromium-Based Web Browsers in Windows Systems

Dija S, Veena Vijayan

Center for Development of Advanced Computing,
Thiruvanathapuram, India

Abstract - *Cybersecurity and digital investigations, Browser Forensics has become increasingly important due to the growing dependence on internet for everyday tasks. Browser Forensics is crucial in the Cybercrime investigation as they can reveal the user's online behaviour, establish a timeline and uncover potential criminal activities. This paper highlights the critical role of Browser Forensics in reconstructing user activity and uncovering digital evidence. The paper also examines the evolution of browser artifacts within Chromium-based web browsers on Windows systems, detailing the changes in artifact locations and retrieval methods over recent versions. The implications of these modifications for forensic analysis, emphasize the necessity for updated methodologies in digital investigations, by providing a comprehensive overview of the current state of browser artifacts, including history files, cookies, cache, and session data. The findings underscore the need for forensic professionals to adapt to these ongoing changes, ensuring effective retrieval and analysis of browser-related data in an ever-evolving digital landscape.*

Key Words: Browser Forensics, Internet Forensics, Web Browser Artifacts

1.INTRODUCTION

In today's digital world, the web browser remains the most mainstream means for accessing the Internet. From extremely business-critical operations to casual browsing, there exists a varied spectrum of activities. Some of the popular Chromium-based browsers—Google Chrome, Microsoft Edge, Opera, Maxthon, and Yandex—have gained huge adaptability due to their high speeds, super security features, and open-source architecture. These widely used browsers are an important area of focus for cybercrime investigations. Browser Forensics primarily concerns the identification, recovery, and analysis of digital artifacts left by the user, which may include a history of browsing, cookies, cache, autofill data, or records of downloads. Such artifacts can offer important information about user behavior, intent, and the online activities of the suspect.

Web browsers create reliable forensic traces of internet browsing activities on the storage media of computers. This paper specifically focuses on the forensic analysis of widely used web browsers, examining a range of artifacts such as Visited URLs, Searched Keywords, Downloads, Bookmarks, Favorites, Cookies, Cache, etc. These artifacts are vital for identifying user behavior and intentions. The frequent updates and new versions of these browsers change the locations and structures of digital artifacts stored on a user's system. As developers implement these updates, artifact locations can shift, complicating forensic analysis. This study emphasizes the importance of constant adaptation in forensic approaches to effectively detect and analyze digital traces left by users in modern browsing environments.

2.BROWSER FORENSICS

Browser Forensics is crucial in supplying forensically relevant information during Cyber Crime Investigations, as web browsers generate numerous files on the local system while users browse the Internet [2]. The purpose of Browser Forensics is to retrieve and analyze digital artifacts related to user Internet activity. Given that web browsers are now common place for all humans and organizations to access the Internet, they are a treasure trove of information on user's online actions, preferences, and interactions. When users access the internet, web browsers create specific local files that store information about their online activities.

These files are extremely useful for Cyber Forensics investigations as they may contain useful evidence related to the reported crime. As browser technology advances rapidly and developers release updates regularly, the locations and structures of the artifacts can quickly shift leading to the need for specialized skills and tools for navigating encrypted storage and proprietary file formats. Therefore, web browser analysis serves as an important forensic methodology overall.

2.1 Browser File Locations

Modern web browsers create different files to store information about the activities of user. These files are stored in specific file locations on a Windows system, sot the browser can monitor and keep records of the user's activities online. This paper explores the artifact locations of the browsers in local system and evaluate the changes in the locations as well as in the structures of these files after updates. It emphasizes how updates of browsers affect the storage and retrieval processes of forensics data and thus how investigators need to be constantly update on such changes for appropriate tracing of the digital trail left by users.

Below is an overview of popular web browsers, focusing on their relevance in digital forensics and the specific locations of their user activity data:

a) Google Chrome: Another popular internet browser around the world and developed on the Chromium platform is Google Chrome. Its popularity makes Chrome often at the center of digital forensic investigations. The browser saves a vast amount of user activity data locally, which is significant for reconstructing a user's browsing history, online interactions, and behavioral patterns [7]. These files are located within the user's profile directory, C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\.

b) Microsoft Edge: Another widely used web browser. Similar to Google Chrome, Microsoft Edge stores most of its artifacts in SQLite database files. These files are located within the user's profile directory, C:\Users\<username>\AppData\Local\Microsoft\Edge\User Data\Default\.

c) UC Browser: UC Browser, is another Chromium-based browser developed by mobile internet company UCWeb. It stores its artifacts in a structure similar to other Chromium browsers, with most of its data stored in SQLite database files. These files are located within the user's profile directory, C:\Users\\<username>\AppData\Local\ UCBrowser\User Data_i18n\Default.

d) Maxthon Browser: Maxthon stores critical user artifacts on the local system, making it a potential source of valuable evidence in digital forensic investigations. These artifacts are typically stored in SQLite database files, JSON files, and other formats within the user's profile directory. The forensic analysis of Maxthon can yield detailed information about the user's browsing behavior, including visited websites, downloads, cookies, etc. Maxthon's user data is located in, C:\Users\\<username>\AppData\Local\ Maxthon\Application\User Data\Default.

e) Yandex: Yandex Browser, developed by the Russian technology company Yandex. Like other browsers, Yandex stores its user artifacts in SQLite database files, JSON files, and other formats. Such artifacts are crucial to forensic investigations to unmask a user's browsing history, search queries, and interactions with online services. On a Windows system, Yandex Browser stores its data in, C:\Users\<username>\AppData\Local\Yandex\YandexBrowser\User Data\Default.

f) Opera: Opera is a multi-platform web browser developed by Opera Software. The majority of Opera web browser artifacts are maintained within SQLite database files, each containing multiple tables with information regarding the users' actions on the software. On 20 June 2023, Opera launched Opera 100, codenamed Opera One, a version of the browser built from the ground up around AI which was unveiled on 25 April 2023 [6]. Before the emergence of Opera One all the artifact files were directly stored in location, C:\Users\<username>\AppData\Roaming\Opera Software\Opera Stable. But after the launch of Opera One the artifact files were shifted to a profile folder Default and the new location is C:\Users\<username>\AppData\Roaming\Opera Software\Opera Stable\Default. However, the file structure of artifacts remained the same without any change.

Table -1: Comparison of Opera Artifact Locations

Browser Name	Browser Version	Location
Opera Old Version	95.0.4635.46	OS Drive:\Users\[Username] \AppData \Roaming\Opera Software\Opera Stable\<artifact files>
Opera One New Version	104.0.4944.23	OS Drive:\Users\[Username] \AppData \Roaming\Opera Software\Opera Stable\Default\<artifact files>
Cache		
Opera Old Version	95.0.4635.46	OS Drive: \Users\[Username]\App Data\ Local\Opera Software\Opera Stable\Cache\<cache_files>
Opera One New Version	104.0.4944.23	OS Drive: \Users\[Username]\App Data\ Local\Opera Software\Opera Stable\Default\Cache\ <cache_files>

This paper also describes the change in Opera's profile folder structure. The location of artifacts changed but the structure of artifact files remains the same. Opera browser versions prior to 100, namely 95.0.4635.46, created user artifacts in the path \\Users\UserName\AppData\Roaming\Opera Software\Opera Stable\ on the operating system drive, including cookies, history, and other pertinent artifact files. Files are saved to these paths in different formats. For cache data, the old location was \\Users\UserName\AppData\Local\Opera Software\Opera Stable\Cache.

Opera One, the most recent version, was made available as the 100th version on June 20, 2023 [6]. To improve

efficiency and organization, the user artifact storage structure has seen major modifications. This version consolidates forensically relevant artifacts into the Default folder, including cookies, history, and login information, etc. In TABLE I, a detailed comparison of artifact locations in different versions of the Opera browser is presented.

2.2 Analysis of Web Browsers

Open-source applications derived from the Chromium project serve as the core framework for many popular web browsers. Due to their shared technology, these browsers exhibit common features and architectural components. Artifacts generated by these browsers are primarily stored in SQLite database files, while bookmarks are stored in JSON file format. These artifacts are stored in specific user profile directory. Investigators must understand the storage architecture of these browsers to effectively recover and analyze the data for forensic purposes. Many Chromium-based browsers support multiple user profiles, each storing its own set of data. Understanding how these profiles are managed is essential, as it allows for a thorough analysis of user behavior across different profiles, which can be crucial in cybercrime investigations.

Recent versions of popular web browsers have shifted from a decentralized approach to user data storage. Instead of spreading artifacts across multiple directories, modern browsers now consolidate these artifacts into organized folders. For instance, Opera One 104.0.4944.23 the latest version of Opera browser, organizes all relevant artifacts such as cookies, history, and cache compartmentalized to a common profile folder named Default.

2.3 Important Artifacts

Web browsers may be used by the suspect to retrieve information or to conceal his/her criminal activities and to explore new crime techniques. Searching for evidence left by web browsing activity is typically a crucial component of digital forensic investigations. Each time a suspect engages with a web browser, it generates traces on the computer. This evidence can provide useful information to the investigator while examining the suspect's information. It is feasible to study this proof for websites visited, time and frequency of access, and search engine keywords used by the suspect after recovering data such as cache, cookies, and downloads list from a suspect's computer [4]. Table 2 summarizes browser types, database files, and related artifacts in Chromium-based browsers.

Some of the most important artifact files within the directories of popular web browsers include the following:

a) History: The History SQLite database is crucial for digital forensics as it logs all visited URLs, timestamps, and page titles. This data can provide insight into a user's online behavior, including what sites were accessed, when, and how frequently. Investigators can use this information to reconstruct a user's activities, establish timelines, and identify potentially relevant sites during an investigation. This SQLite database consists of several tables, Web History, Downloads, Search keywords, Web Visits, etc.

b) Searched Keywords: The searched keywords file, stored as an SQLite database, contains terms entered by the user in search engines or the browser's address bar. It reveals the user's search history, providing valuable insights into their interests, online activities, and potential connections to criminal behavior. This data can help forensic investigators identify key events or behaviors linked to specific searches.

c) Downloads: The downloads file, usually stored in SQLite database format, tracks details of files downloaded by the user, including file names, URLs, download times, and file paths. Examining this file helps investigators find suspicious files, track user actions, and gather evidence of illegal activities or unauthorized access. It is especially valuable in cases of intellectual property theft, malware distribution, or unlawful file sharing.

d) Bookmarks: The bookmarks JSON file shows the interest or sites of frequent visitation for the users and the types of activities they conduct online. From a forensic point of view, bookmark analysis will be very useful in giving context to user behavior and intent more so if relevant sites exist.

e) FavIcons: Favicons are small icons linked to websites, stored in the browser's cache or files. They help identify sites the user visited, even if history is deleted, and can provide evidence of online activities in forensic investigations.

f) Cookies: The cookies file is also a SQLite database file that contains crucial information regarding user sessions and tracking mechanisms. The analyst can look at the cookies to understand which sites the user visited and which data was shared. This data may be used in finding user preferences, login sessions, and tracking across various sites; therefore it forms an important aid in understanding user behavior and probable interaction with malicious content.

g) Login Data: This SQLite database file contains encrypted usernames and passwords from websites, hence this is highly important in forensic investigations. If decrypted, it would open up doors to accounts, which in turn reveal information and online activities from the account holder. Thus, such can be very important in identity theft cases or unauthorized access to some of the accounts.

h) Web Data: The Web Data file contains data for Autofill, which gives forensic investigators insight into personal information about the user such as addresses and credit card numbers. Data can also exhibit financial transactions or personal habits and even indicate

vulnerabilities in how sensitive information is shared by the user from online sites.

i) Cache: Cache stores copies of files temporarily. Such files would include images, scripts, and all other elements of web content meant for easing page loading. From a forensic point of view, though users might clear the history, there will be information contained within those files that can be evidence of previous access. Cache analysis will give you important artifacts such as recently viewed documents or media, which may have some relevance in cases of intellectual property or unauthorized access to information.

j) Topsites: The Top Sites file, usually stored in SQLite database format, keeps a record of the user's most frequently visited websites. This file helps forensic investigators understand browsing patterns, interests, and online activities. Even if other browsing history has been deleted, the Top Sites file can reveal essential online interactions, making it a valuable resource in criminal investigations.

Table -2: Artifact Overview for Chromium-Based Browsers

Sl. No	Browser Name	File Name	Artifacts
1	Google Chrome	Bookmarks Cookies Favicons Network-Action Predictor Topsites Webdata	Autofill URLs Cookies Downloads Searched-Keywords Network Activity Incognito Logins FavIcons Topsites
2	Microsoft Edge		
3	UC Browser		
4	Maxthon Browser		
5	Yandex		
6	Opera		

This paper has focused on the forensic analysis of the above-mentioned popular browsers built on the Chromium platform. Each one of these browsers creates essential artifact files, which significantly helps in making an insightful study of user actions. Important artifacts such as history (which logs the visited websites), cookies (which stores session and tracking data), cache (which holds the content of web pages temporarily), and download history (which records details of downloaded files) may be extracted from the suspect's system. By examining these files, investigators can reconstruct the user's browsing patterns, determine frequently visited sites, recover search engine queries, and assess download behavior, all of which are critical in building an evidence trail. One of the most important features of any Cyber Forensics Analysis Tool is keyword searching. However, identifying and finalizing the keywords to be searched during the analysis process in a particular Cyber Crime is always challenging for the investigators [2].

For instance, if a user searches for the word "terrorism," this search term is saved in the keyword_search_terms table of Google Chrome's History SQLite database file. In the process of investigation, one may find and analyze this table to obtain evident information such as the actual search term used ("terrorism"), the date and time it was executed, and the search engine used (for example, Google). This table might also identify similar patterns of searches or related terms for further contextual understanding of what a user was thinking of or trying to do. Fig 1 shows the searched keywords and URLs from browser artifacts.

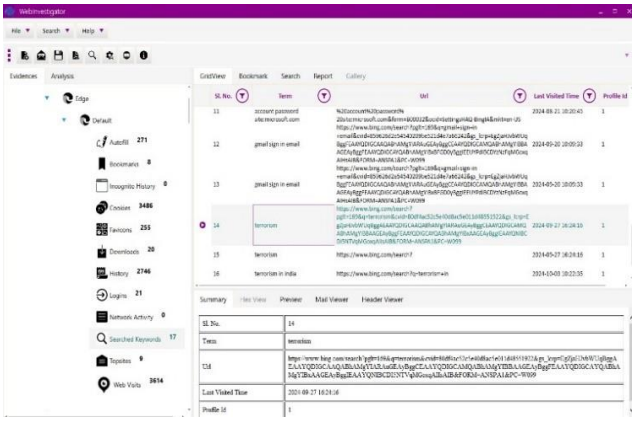

Fig -1: Searched Keywords and URLs from Browser Artifacts.

2.2 Forensic Relevance

Browser Forensics, particularly in Chromium-based browsers including but not limited to Google Chrome, Microsoft Edge, Opera, UC Browser, Maxthon, and Yandex, are of great importance in the forensic process of conducting digital investigations. With increased online usage, it is of grave importance for law enforcement, cybersecurity professionals, and digital forensic experts to explore the artifacts produced by such browsers. These browsers generate a large number of artifacts which include browsing history, cookies, cache files, and download records that altogether explain what the user has been doing. This information later becomes useful in reconstructing the suspect's online behaviors, including timelines and patterns of actions.

Every action performed by a user in a browser leaves some sort of digital footprint. The forensic specialist can trace the suspect's online activities over time by looking at these footprints. This is particularly critical because the suspects trying to cover their tracks, trying to delete the history of the browser, or using incognito modes. Also, analysis of artifacts in multiple browsers reveals inconsistencies and similarities between the activities of an individual. It may lead to insights about the suspect's surfing pattern and the potential use of multiple browsers to obfuscate activities.

Search queries from a browser's history can indicate whether a suspect was investigating illegal activities, such as drug trafficking or hacking. Cookies may reveal interactions with illicit websites, while download records can provide clues about relevant materials, including child exploitation or pirated software. Even when browser history is cleared, cached files can expose previously accessed content. Analyzing data from multiple browsers allows forensic analysts to develop a comprehensive view of a suspect's online presence, offering insights into their intent and motivations. This makes Browser Forensics an invaluable tool in both criminal and civil investigations.

3. CHALLENGES

Browser artifact analysis in the context of changing browser technology throws up many challenges to forensic investigators. One very common and frequent challenge has to do with the new releases of a version changing the locations of the artifacts each time the change is done in the browser. Another challenge is changes in the file structure, when browsers change from a single SQLite file to numerous files or entirely different formats, it tends to fragment the relevant evidence and makes it complicated to correlate data. In addition, changes in encoding procedures for artifacts can sometimes make interpretation difficult because forensic software packages are not always able to handle them. The use of cloud synchronization complicates evidence gathering, as artifacts may be stored in the cloud rather than locally, requiring access to cloud accounts for a complete picture. Altogether, these challenges require that forensic practitioners continue updating their knowledge and adjusting their techniques so that practitioners are best able to understand the new landscape of browser technologies even as they navigate successfully the emergence of new digital evidence.

4. FUTURE WORK

With evolving web browsers and adding synchronization of cloud and cross-devices, digital forensics must keep pace too. The efforts should continue to create tools that can successfully access and analyze data held on the cloud. Investigators will have to understand data synchronization across devices so that they can track the activities of a user with precise detail. It is, therefore, important that forensic analysts and browser developers collaborate to improve documentation on storage data and its synchronization. Future studies will concentrate on these changes' impact on the reliability of evidence in investigations as privacy issues and data security laws continue to increase. From such solutions, forensic analyzers will be in a better position to catch up with new technologies, and thus, digital investigations will be more effective.

5. CONCLUSIONS

This paper thus explored the important area of Browser Forensics, specifically Chromium-based browsers such as Google Chrome, Microsoft Edge, UC Browser, Maxthon, Yandex, and Opera. As the said browsers are being developed, new challenges in artifact locations, file structures, and synchronizations across the devices and cloud storage arise. Understanding all these changes will have a direct influence on forensic investigators, as these issues directly affect the recovery and analysis of evidence. In response to the complexities introduced by modern browser technologies, constant evolutions of forensic methodologies are inevitable so that investigations have a strong chance of turning out effective and reliable. The can contribute more appropriately toward a more robust framework of digital investigations, whereby one will be able to ensure that user behavior and activities may be scrutinized better with a progressively digital world.

REFERENCES

[1] S. Dija, V. Indu, A. Sajeena, and J. A. Vidhya, “A framework for Browser Forensics in live Windows systems,” in Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2017, pp. 1–5. (conference style)

[2] S. Dija, J. Ajana, V. Indu, and M. Sabarinath, “Web Browser Forensics for retrieving searched keywords on the internet,” in Proceedings of the 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), Greater Noida, India, 2021, pp. 1664–1668. (conference style)

[3] G. S. Suma, S. Dija, and A. T. Pillai, “Forensic analysis of Google Chrome cache files,” in Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 2017, pp. 1–5. (conference style)

[4] A. Nalawade, S. Bharne, and V. Mane, “Forensic analysis and evidence collection for web browser activity,” in Proceedings of the International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, 2016, pp. 518–522. (conference style)

[5] Reddit, “Reddit Opera Browser,” [Online]. Available: https://www.reddit.com/r/operabrowser/wiki/opera/new_profile_layout. [Accessed: Nov. 11, 2024]. (General Internet site)

[6] Wikipedia, “Opera (web browser),” [Online]. Available: https://en.wikipedia.org/wiki/Opera_(web_browser). [Accessed: Nov. 11, 2024]. (General Internet site)

[7] N. Malviya, "Browser Forensics: Google Chrome," InfoSec Institute, Sep. 2020. [Online]. Available: https://www.infosecinstitute.com/resources/digital-forensics/browser-forensics-google-chrome/. [Accessed: Nov. 11, 2024]. (General Internet site)