Not as incognito as you might think: Use of Browser Forensics in Digital Forensics

Samriddhi

Northeastern University, Khoury College of Computer Sciences, 360 Huntington Ave, Boston, MA, USA 02115

lnu.samr@northeastern.edu

Abstract

Browser forensics, a branch of digital forensics, focuses on the analysis of web browser artifacts to uncover crucial information about a user's online activities. This paper explores the significance of browser forensics in digital forensics and its ability to shed light on seemingly incognito browsing sessions by examining browser caches, history, cookies, and other traces, forensic examiners can reconstruct a user's browsing behavior, reveal visited websites, and potentially discover evidence of illicit activities. The paper highlights the importance of browser forensics in the digital age, where online activities can hold the key to solving complex cases and bringing perpetrators to justice.

1. Introduction

In this digital age, web browsers have become indispensable tools for accessing information, communicating, and conducting various online activities. However, the convenience and ubiquity of web browsers also come with a trail of digital footprints that can provide valuable forensic evidence in criminal investigations. While some users may believe that their browsing sessions are incognito or private, the reality is that these digital traces can be recovered and analyzed by forensic experts. Browser forensics plays a crucial role in digital forensics as the evidence can be instrumental in various types of investigations, including cybercrime, fraud, intellectual property theft, and even traditional crimes where digital evidence may be present. Despite its significance, browser forensics faces several challenges, such as the ever-evolving nature of web technologies, the increasing use of privacy-enhancing tools, and the

complexity of recovering and interpreting browser artifacts. Forensic examiners must stay up-to-date with the latest developments in web browsers and employ advanced techniques and tools to ensure the effective collection, preservation, and analysis of digital evidence. This paper aims to explore the importance of browser forensics in digital forensics, highlighting its capabilities, challenges, and best practices. (1) By shedding light on this critical aspect of digital forensics, we can better understand the implications of our online activities and the potential for uncovering valuable evidence in criminal investigations.

2. Related Work

Several studies have explored the significance and techniques involved in this domain. Ohana and Shashidhar provided a comprehensive overview of browser forensics, highlighting the importance of analyzing browser artifacts such as history, cache, cookies, and form data. They discussed the potential of browser forensics in uncovering user activities, identifying visited websites, and recovering deleted data. Their work emphasized the need for forensic examiners to stay updated with the latest developments in web technologies and browser architectures. (2)

Mahaju and Atkison conducted a comparative analysis of various open-source tools for browser forensics, evaluating their effectiveness in extracting and analyzing browser artifacts. They highlighted the strengths and limitations of tools like Hindsight, BrowsingHistoryView, and WebBrowserPassView, providing valuable insights for forensic practitioners. (3)

In a study by Cusack and Khaleghparast, the authors explored the challenges associated with browser forensics, particularly in the context of privacy-enhancing technologies and anti-forensics techniques. They proposed a framework for mitigating these challenges and ensuring the effective collection and analysis of browser-related evidence. (4)

Researchers at the National Institute of Standards and Technology (NIST) developed a comprehensive test methodology for evaluating the performance of browser forensics tools.

Their work involved creating a controlled environment with known browsing activities and assessing the ability of various tools to accurately recover and interpret browser artifacts. These studies and others in the field of browser forensics have contributed to the understanding of the importance of this domain, the development of effective techniques and tools, and the identification of challenges and limitations. As web technologies continue to evolve, further research will be necessary to keep pace with the changing landscape of browser forensics.(4)

3. Proposed Methodology

To effectively leverage browser forensics in digital forensics investigations, we propose a comprehensive methodology that encompasses various stages of the forensic process. This methodology aims to ensure the effective collection, preservation, and analysis of browser artifacts while addressing the challenges associated with evolving web technologies and privacy-enhancing tools.

I. Identification and Preservation: The first step in the proposed methodology is the identification and preservation of potential sources of browser-related evidence. This includes identifying the devices and web browsers used by the subject of the investigation and ensuring that the devices are properly seized and preserved to maintain the integrity of the evidence. Forensic practitioners should follow established best practices for evidence handling, such as creating forensic images of the devices and storing them in a secure and controlled environment.

II. Data Acquisition: Once the devices have been secured, the next step is to acquire the relevant browser artifacts. This process involves the use of specialized forensic tools and techniques to extract data from various browser components, including:

- Browser history

- Cache files
- Cookies
- Bookmarks
- Saved passwords
- Form data
- Browser extensions and plugins

The data acquisition process should be conducted in a forensically sound manner, ensuring that the acquired data is not altered or contaminated during the process.

III. Data Analysis: After acquiring the relevant browser artifacts, the next step is to analyze the data to uncover valuable information and evidence. This stage involves the use of various analysis techniques and tools, such as:

Timeline analysis: Reconstructing the sequence of events and user activities based on timestamps and other metadata.

Keyword and pattern searching: Identifying relevant information by searching for specific keywords, URLs, or patterns within the browser artifacts.

Data correlation: Correlating browser artifacts with other digital evidence, such as email communications, social media activity, or financial transactions.

Visualization tools: Utilizing graphical representations and visualizations to identify patterns and relationships within the browser data.

IV. Reporting and Presentation: The final stage of the proposed methodology involves documenting the findings and presenting the evidence in logical manner. This includes generating detailed reports that outline the forensic process, the tools and

techniques used like AccessData FTK, Magnet Axiom along with the relevant findings and conclusions. Furthermore, forensic professionals need to be ready to present the evidence in court or during other legal proceedings, making sure that non-technical audiences can grasp what is being said. It is imperative to strictly adhere to recognized legal and ethical requirements, as well as acknowledged best practices in digital forensics, throughout the suggested technique. To guarantee the efficacy of the methodology, regular training and updates on the most recent advancements in browser forensics and web technologies are also crucial.

4. Analysis

The paper by Ohana and Shashidhar (2) provides a comprehensive forensic analysis of private and portable web browsing sessions. The authors examined various popular web browsers in private browsing mode to determine the traces of browsing activities that remain in physical memory and on disk.

- Private browsing modes in web browsers are designed to prevent the storage of browsing history, cached web content, cookies, and other artifacts on disk. However, the study found that remains of private browsing sessions can still be recovered from physical memory and other locations.
- Volatile memory (RAM) contained significant amounts of data related to private browsing sessions, including URLs visited, rendered web content, form data, and other sensitive information. This data persisted in memory even after the private browsing session was terminated.
- On disk, the authors found traces of private browsing activities in various locations, such as swap files, hibernation files, and prefetch files. These artifacts could potentially be recovered using forensic tools and techniques.

- The extent of recoverable data varied across different web browsers. Some browsers, like Google Chrome, were more effective at minimizing the footprint of private browsing sessions, while others left behind more substantial traces. Private browsing modes do not provide complete privacy or anonymity, as claimed by some web browser vendors. Forensic examiners can potentially recover valuable evidence from private browsing sessions using appropriate tools and techniques.

Memory forensics plays a crucial role in analyzing private browsing activities, as volatile memory can contain a wealth of information that may not be present on disk.

Forensic investigators are aware of the various locations where private browsing artifacts may reside, including swap files, hibernation files, and prefetch files, and employ appropriate techniques to recover and analyze these artifacts. The effectiveness of private browsing modes varies across different web browsers, and forensic examiners should be familiar with the specific behaviors and artifacts associated with each browser.

Like Google Chrome, Firefox uses SQLite databases to store the majority of its browser data. The browser cache is an exception to this, just like Chrome. Since 2008, the locations of Firefox artifacts have not changed. Firefox divides out the important objects and keeps them in separate locations, in contrast to Chrome. Firefox keeps its downloads, history, bookmarks, and auto-complete data in locations similar to those where SQLite keeps its data: \AppData\Roaming\Mozilla\Firefox\Profiles\\profile, or %USERPROFILE%. Similarly, cache is located at %USERPROFILE%\AppData\Local\Mozilla\Firefox\Profiles\.default\Cache, and Firefox cookies are saved in the same place within cookies.

5. Conclusion and Scope of Future Work

In conclusion, browser forensics proved to be significant in lieu of forensic investigations.

Despite the claims of privacy and anonymity as broadcasted by the incognito or private browsing modes, the paper demonstrated that remnants of these sessions can still be recovered from physical memory, swap files, and other locations. The suggested technique provides a thorough approach to browser forensics, including data collection, analysis, reporting, and source identification and preservation. Investigators can successfully gather, preserve, and analyze browser artifacts while tackling the problems provided by developing web technologies and privacy-enhancing capabilities by following this process and utilizing cutting-edge forensic tools and techniques.

The techniques of browser forensics will need to adjust and create new methods to keep up with the rapid evolution of online technologies. Future studies ought to concentrate on things like a need for automated and scalable solutions for browser forensics. Researchers should explore machine learning and artificial intelligence techniques to streamline the analysis of large datasets and identify patterns and anomalies more efficiently.

Overall, browser forensics in digital forensics can enhance the reliability, consistency, and efficiency of digital forensic investigations as this technology continues to develop and evolve.

6. References

(1) Is it Ever Really Gone? The Impact of Private Browsing and Anti-Forensic Tools - Rick Schroeder

https://sansorg.egnyte.com/dl/Y8A2ctm4WC

(2) Ohana, D. J., & Shashidhar, N. (2013). Do private and portable web browsers leave incriminating evidence?: A forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP Journal on Information Security, 2013(1), 6.

https://www.researchgate.net/publication/261264203_Do_Private_and_Portable_Web_Browsers_Leave_Incriminating_Evidence_A_Forensic_Analysis_of_Residual_Artifacts_from_Privat

e_and_Portable_Web_Browsing_Sessions/link/573f680d08ae9f741b321e93/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

(3) Comparative Analysis of Commercial And Open-Source Tools in The Examination And Analysis of Web Browser Data - Perefoti Timothy Komiti

https://www.researchgate.net/publication/369299223_Comparative_Analysis_of_Commercial_And_Open-Source_Tools_in_The_Examination_And_Analysis_of_Web_Browser_Data

(4) Cusack, B., & Khaleghparast, R. (2021). Browser forensics

https://focusinfotech.com/blog/browser-forensics/

(5) National Institute of Standards and Technology. (2020). Test methodology for browser forensics tools (NIST Special Publication 1800-35).

https://doi.org/10.6028/NIST.SP.1800-35

(6) A comparative forensic analysis of privacy enhanced web browsers Ryan M. Gabet

https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1925&context=open_access_theses