Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the National Institute of Standards and Technology (NIST) Framework

Muhammad Syukri*[1], Imam Riadi[2], Tole Sutikno[3]

[1]Informatics, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[2]Information System, Universitas Ahmad Dahlan Yogyakarta, Indonesia
[3]Electrical Engineering, Universitas Ahmad Dahlan Yogyakarta, Indonesia

Email: [1]syukrie@stmik-mi.ac.id

Received : Jun 30, 2025; Revised : Aug 25, 2025; Accepted : Aug 27, 2025; Published : Sep 2, 2025

Abstract

Browsers have become essential applications in digital life alongside the advancement of internet technology. However, users' low awareness of privacy security during web browsing can lead to the risk of data theft by malicious parties. This study analyzes digital traces in Google Chrome and Mozilla Firefox using a digital forensic approach based on the standards of the National Institute of Standards and Technology (NIST). The method involves four testing scenarios to compare digital traces in storage media (hard drive) and RAM between normal and private/incognito browsing modes. The objective of this research is to validate and evaluate previous findings conducted on the Linux operating system, using a different approach within a Windows environment. The experiment uses the same digital forensic tools to ensure data accuracy. This study contributes to the advancement of browser forensics by presenting a validated and reproducible framework for memory-based privacy evaluation, thereby supporting more accurate and systematic analysis of digital traces.

Keywords: browser privacy, digital forensics, Google Chrome, Mozilla Firefox, NIST

This work is an open access article and licensed under a Creative Commons Attribution-Non Commercial 4.0 International License

1. INTRODUCTION

The current web browser market is dominated by three major players: Google Chrome, Mozilla Firefox, and Microsoft Edge (formerly Internet Explorer). These three browsers consistently rank as the top three most widely used browsers globally [1]. Market share data shows that Google Chrome leads with 67.63% of users, followed by Mozilla Firefox with 8.83%, and Microsoft Edge with 7.26% (see Table 1).

Table 1. Global Browser Market Share (2024)

Browser	Market share
Google Chrome	67,63%
Mozilla Firefox	8,83%
Internet Explorer	7,26%

The increasing adoption of web browsers aligns with the rapid advancement of internet technology, which has become the backbone of digital transformation. This trend is especially evident in Indonesia, where the number of internet users has shown significant growth. According to the latest Reportal data (2024), Indonesia has reached a record 185.3 million internet users, with the majority accessing information through search engines and social media platforms [2].

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

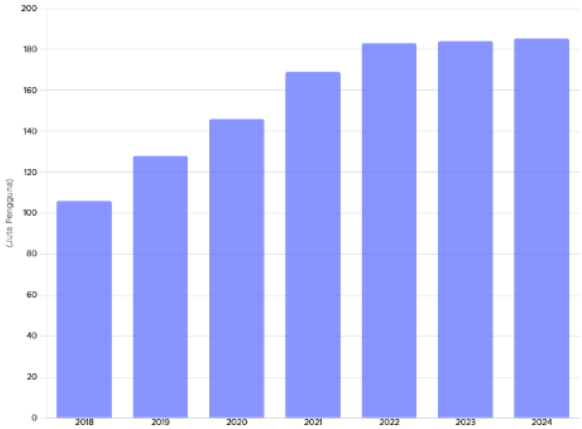


Figure 1. Internet User Growth in Indonesia

In addition to the development of internet technology, operating systems also play a crucial role as the platforms on which browser applications run. Data shows that Windows dominates as the most widely used operating system globally. According to a 2020 report, Windows held the top position in the global operating system market [3].

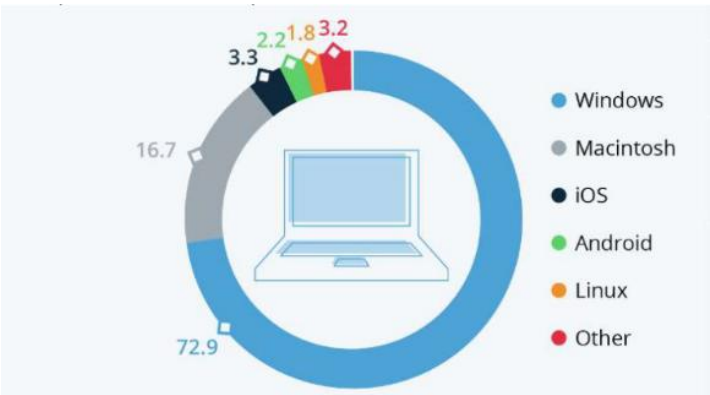


Figure 2. Global Operating System Market Share

An analysis of global operating system market share data reveals that Windows has a significantly higher number of users compared to other operating systems such as macOS, iOS, Linux, and Android. Comparative data from the period 2018 to 2022 shows the consistent dominance of Windows over other major operating systems.

Table 2. Operating System Market Share Comparison (2018–2022)

System Operation/year	Windows	Unix/Linux	MacOS	Other OS
2018	62%	49%	44%	1%
2019	57%	48%	49%	1%
2020	60%	50%	44%	1%
2021	61%	47%	44%	1%
2022	61%	45%	46%	1%

Some key observations from the data:

1. Windows has maintained its dominance with a stable market share above 57%.
2. Unix/Linux has shown relatively minor fluctuations throughout the observation period.
3. macOS experienced a slight decline before rising again in 2022.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

4. Other operating systems have consistently held a very small share of the market.

Previous studies have extensively explored memory-based privacy evaluation in Linux operating environments [4]. However, a significant gap remains in the context of the Windows operating system, which currently dominates the global desktop market [3]. The differences in memory architecture, process management, and data residue behavior between Linux and Windows highlight the importance of extending forensic research to the Windows platform. Therefore, this study offers novelty by applying a validated and reproducible digital forensic approach to the Windows environment—an area that has received relatively limited attention in browser-based forensic literature [5], [6].

By replicating methodologies previously applied in Linux and validating them within a Windows context, this research provides new insights into platform-specific impacts on the acquisition and recovery of digital evidence. Furthermore, the study addresses current demands within the digital forensic community to broaden the scope of testing environments and enhance the validity of investigative outcomes through a systematic and reproducible framework [6], [7].

2. RESEARCH METHOD

This study employs a digital forensic methodology based on the modified standards of the National Institute of Standards and Technology (NIST). The core NIST method consists of four main phases, as shown in Figure 3.

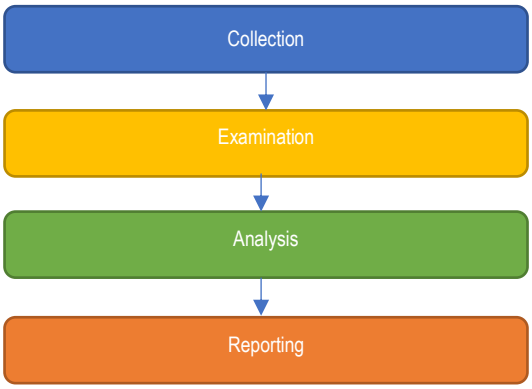


Figure 3. NIST Digital Forensic Research Methodology

1. **Collection**: The data gathering phase from various sources to support the digital investigation while preserving the integrity of digital evidence.
2. **Examination**: The forensic process of examining the collected data to verify authenticity and ensure data integrity is maintained.
3. **Analysis**: The evaluation of the admissibility and relevance of digital evidence for legal proceedings.
4. **Reporting**: Documentation of the entire investigation process, including methods, tools, actions taken, and improvement recommendations.

To ensure a more structured and comprehensive study, the basic NIST method was expanded by adding four additional phases (see Figure 4), resulting in an eight-phase research model:

1. **Literature Review**: Reviewing existing studies related to digital forensics and previous research.
2. **Case Scenario and Implementation**: Designing test scenarios and implementing experiments.
3. **Digital Evidence Acquisition (Collection)**: Gathering digital data in accordance with forensic standards.
4. **Digital Evidence Investigation (Examination)**: Conducting an in-depth examination of the collected evidence.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

5. **Digital Evidence Analysis (Analysis)**: Processing and interpreting the digital evidence.
6. **Digital Evidence Reporting (Reporting)**: Documenting the results of the investigation.
7. **Digital Evidence Validation**: Verifying the accuracy of methods and research results.
8. **Digital Evidence Evaluation**: Conducting a comprehensive assessment of the research process and findings.

This method modification was made to:

- Strengthen the theoretical foundation through literature review
- Ensure the validity of research findings
- Provide a comprehensive evaluation of the entire process
- Enhance the accountability of the research outcomes

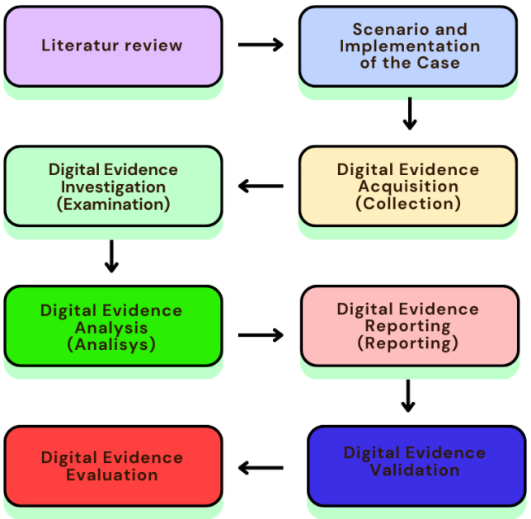


Figure 4. Modified Research Methodology

2.1. Literatur Review

Browser forensic research has advanced rapidly, employing various methodological approaches. Below is a synthesis of key findings from related case studies:

A study on Chrome and Firefox browsers in a Linux environment found that although private mode does not store data on the hard drive, sensitive information can still be recovered from RAM, particularly within virtualized environments such as VMware. Research [8] revealed that a regular reboot does not effectively erase RAM data; shutting down the computer for at least 10 seconds is more effective. Linux hardening (with the init_on_free kernel option) enhances privacy by reducing memory residue.

Research [9] analyzing Chrome, Brave, Firefox, and Tor on Android 13 devices showed that private mode does not save browsing traces in the file system. However, volatile memory analysis could recover login credentials. Device restarts did not completely eliminate memory residue.

Several studies highlighted important findings from the analysis of Google Meet activity [10] in virtual machines with varying RAM sizes (4GB, 8GB, 12GB). Meeting artifacts were successfully extracted using tools like FTK Imager and Volatility. RAM capacity influenced data persistence, allowing recovery of meeting notes, logs, and caches.

A study on Tor and I2P [11] discovered that artifacts remained in the registry, RAM, and hard drives. Tools such as Reghost and Bulk Extractor were effective for extraction, and private mode did not entirely eliminate digital traces.

A study [5] on browser credential migration successfully transferred auto-login credentials in 25 out of 28 browsers, enabling access to cloud services without re-authentication. Key tools included Reghost, Mimikatz, and DataProtectionDecryptor.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

The Chracer method [7] for Chromium-based browsers successfully extracted browsing data in both normal and private modes, and could reconstruct URLs, tabs, and SSL certificates using tools such as Ghidra and Process Hacker for memory analysis. Decryption of IndexedDB [12] in Gecko-based browsers showed that data could be decrypted during both active sessions and hibernation. Using brute-force techniques and Proof-of-Concept tools, the research demonstrated vulnerabilities in Firefox and Tor's private modes.

In mobile forensic research on Facebook Messenger [13], data could be recovered prior to app uninstallation. After uninstallation, the remaining data was minimal, but MOBILedit proved effective for limited data extraction.

For Viber [14], only about 50% of data could be recovered after deletion. Contacts and media were still extractable, but Autopsy showed limitations in data recovery capabilities.

The implications of these findings highlight that private mode is not entirely secure against forensic analysis [6], RAM remains a primary source of digital residue, memory capacity affects data persistence [15], memory capacity affects data persistence [16], and tool innovation continues to evolve to address privacy protection challenges [17].

Cybercrime investigations using forensic analysis have proven successful in gathering digital evidence [18]. In addition to forensic analysis, studies on cybercrime have also applied the NIST method [19] which consists of collection, examination, analysis, and reporting. This method helps maintain the integrity and validity of digital evidence for legal proceedings and has been used to identify digital artifacts from Facebook Messenger [20], Android-based Facebook Lite [21], Virtual Router networks [22], Optical Drive [23], Android-based Viber Messenger [24], data recovery [25], and Twitter [26].

2.2. Case Scenarios and Implementation

This study adopts the NIST methodology with four experimental scenarios to ensure the replicability of results, referencing previous browser forensic research conducted on the Linux operating system [4]. The scenarios are designed to test data persistence in memory under various system conditions, as illustrated in Figure 5.

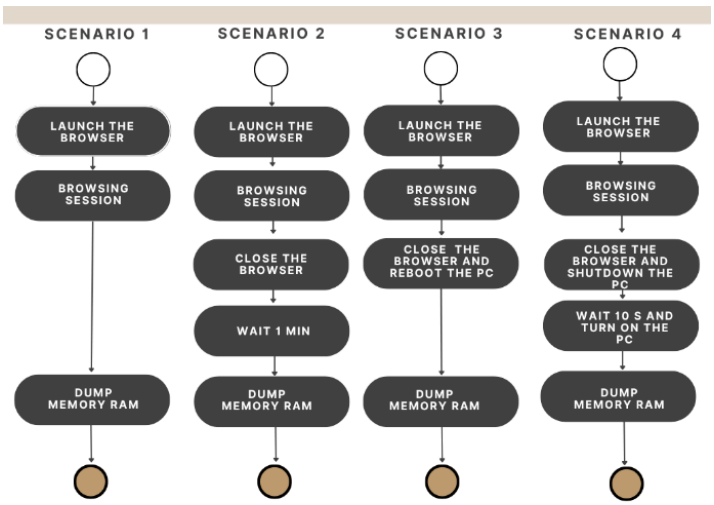


Figure 5. Four Case Scenarios

The research scenario design includes the following:

- **Baseline Scenario**: Launch the browser application, perform standard web browsing activities, and conduct live memory acquisition while the system is still active.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

- **Browser Closure Scenario**: Launch the browser application, perform web browsing activities, close the browser, wait for a 1-minute interval, and perform memory acquisition.
- **System Reboot Scenario**: Launch the browser application, perform web browsing activities, close the browser, restart the system, and acquire memory after the system boots up again.
- **System Shutdown Scenario**: Launch the browser application, perform web browsing activities, close the browser, shut down the system completely, wait for a 10-second interval, power the system back on, and perform memory acquisition.

The methodology implemented in each scenario is designed to:

- Assess the level of data persistence in main memory
- Evaluate the effectiveness of different memory-clearing methods
- Compare memory residue under different system states
- Determine the relevance of findings in comparison with previous research

Experimental controls include consistent web browsing activities, standardized time intervals, a minimum of three replications for each scenario, and the use of identical system environments.

This study uses a standardized set of tools and software commonly applied in digital forensics. The main device specifications used are presented in **Table 3** below:

Table 3. Research Equipment Specifications

No	Tool Name	Specification	Category
1	Laptop Lenovo	Thinkpad Seri X230i Core i3 Gen 3 RAM 8 GB HDD 500GB	Hardware
2	Windows	Windows 11 Home 64 bit (10.0, Build 22631)	Operating System
3	Browser	Google Chrome 137.0.7151.120 (Official Build) (64bit)	Web Browser
4	Browser	Mozilla Firefox 139.0.4 (64bit)	Web Browser
5	WinHex	WinxHex 21.3	Digital Forensic Tool
6	Volatility	Volatility Workbench V3.0 Build 1009	Memory Analysis
7	DumpIt	DumpIT Memori	Memory Acquisition

To ensure result consistency, this study implements six standardized web browsing scenarios under each testing condition:

1. **Accessing Multimedia Content**: Visiting a webpage containing media content (video/music) and playing one video item for a specified time interval.
2. **Saving Cookies**: Opening a new tab and accessing a website that stores cookies, ensuring that cookies are saved in the browser.
3. **Accessing PDF Documents**: Opening a new tab, downloading a PDF file, and previewing the document directly in the browser.
4. **Browsing History**: Opening a new tab, manually entering a URL, and deleting the URL from the address bar after visiting the page.
5. **Email Authentication**: Accessing a web-based email service and logging in using valid credentials.
6. **Login Form Submission**: Accessing a website with a login page, filling out and submitting a login form (username and password).

Each of the scenarios above is executed sequentially under the four system conditions described in Section 2.2, following this protocol:

- Conducted on both browsers (Chrome and Firefox)

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

- Standardized time intervals for each action
- Complete documentation of processes and results
- A minimum of three test replications to ensure data reliability

This study also applies several quality control measures:

- Use of identical system environments for all tests
- Restriction of background applications running during testing
- Detailed logging of time and software versions
- Data integrity verification before and after each test

2.3. Digital Evidence Acquisition (Collection)

The digital evidence acquisition phase is the first and most critical step in the NIST methodology. Its primary goal is to secure and preserve digital evidence in a forensically sound manner. This process includes several key activities:

1. **Data Identification and Collection**: Scanning the system to identify potential sources of digital evidence and documenting the system's initial state prior to acquisition.
2. **Acquisition Process**: Capturing memory images using RAM acquisition tools, executing the four predefined test scenarios, and using *DumpIt* as the primary tool for memory acquisition.
3. **Evidence Preservation**: Generating hash values to ensure data integrity, storing digital evidence on secure media, and documenting the chain of custody.
4. **Technical Implementation**: Performing memory acquisition for each test scenario, using a write-blocker to prevent modification of source data, logging timestamps and metadata related to the acquisition process, and saving the results in standardized formats.
5. **Quality Control**: Verifying tools before and after the acquisition process, comparing pre- and post-acquisition hash values, and storing multiple copies of the evidence on separate media.
6. **Process Output**: Memory image files for each test scenario, complete documentation of the acquisition process, and log files recording all system activities.

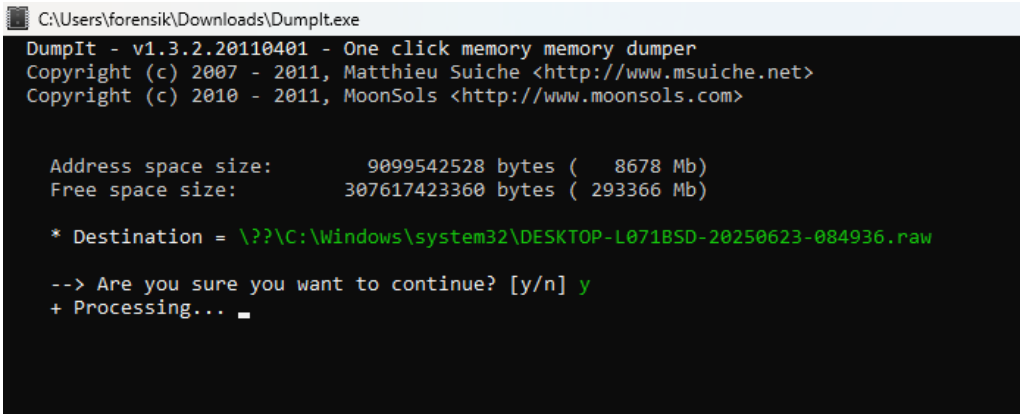


Figure 6. Digital Evidence Acquisition Using DumpIt

2.4. Digital Evidence Examination (Examination)

The digital evidence examination phase is the second step in the NIST methodology, aimed at identifying and collecting relevant digital artifacts from various storage sources. This process includes:

- **Scope of Examination**:
  - **Storage Media (Hard Disk/SSD)**: File system analysis, browser artifact search, and registry extraction (for Windows systems).
  - **Volatile Memory (RAM)**: Identification of active processes, search for browsing activity residue, extraction of credentials and session data.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

- **Examination Methodology**:
  - Use of non-destructive forensic approaches.
  - Application of hashing techniques to verify data integrity.
  - Utilization of standard digital forensic tools (WinHex, Volatility Framework).
  - Complete documentation of all artifact findings.
- **Workflow Steps**:
  - Preparation of the forensic environment.
  - Identification of potential evidence sources.
  - Extraction of digital artifacts.
  - Classification and cataloging of findings.
  - Validation of examination results.
- **Outputs Produced**:
  - Reports of successfully identified artifacts.
  - Documentation of metadata related to digital evidence.
  - Hash values for integrity verification.
  - Chain of custody records.
- **Importance of This Phase**:
  - The examination process enables researchers to understand the context of system usage, identify user activity patterns, uncover hidden evidence, and reconstruct digital events.

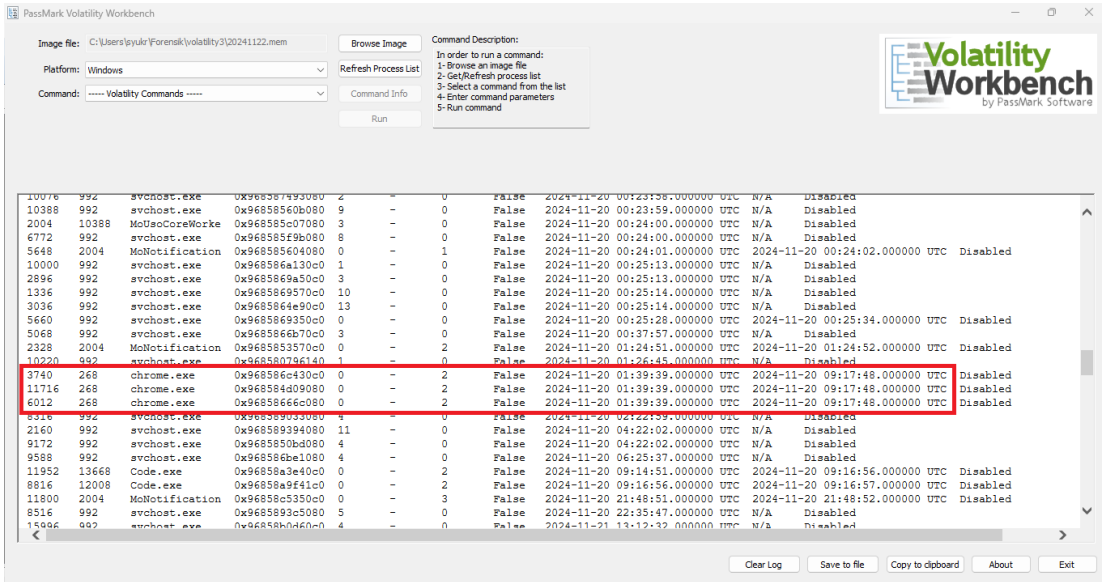


Figure 7. Volatility Framework Interface

2.5. Digital Evidence Analysis (Analysis)

The digital evidence analysis phase is a critical component of browser forensic investigations. It aims to identify, extract, and interpret digital artifacts from various storage media. This process is designed to assess data persistence under different system conditions through a systematic experimental approach.

The analysis was carried out across four scenario stages as follows:

1. **Scenario 1**
   - Capturing a memory dump while the browser is operating in normal mode.
   - Performing standard web browsing activities, including watching videos on YouTube.com, accessing email on Gmail.com, and using search engines to download images and documents, which are then saved to the hard drive.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

- The memory dump is analyzed using *WinHex*.

2. **Scenario 2**
   - Capturing a memory dump under different conditions—after the browser is closed.
   - Web browsing activities are the same as in Scenario 1. After browsing, the browser is closed and the system is left idle for one minute to ensure memory is cleared before the dump is taken.
3. **Scenario 3**
   - The procedure is similar to Scenario 2, but the device is restarted before capturing the memory dump.
4. **Scenario 4**
   - The memory dump is captured after the browser is closed and the device is shut down. The system is left off for 10 seconds before powering back on and performing memory acquisition.

The entire analysis process uses browser forensic tools—*DumpIt*, *Volatility*, and *WinHex*—to ensure the accuracy and reliability of the investigation results.

Memory acquired using *DumpIt* is analyzed with *Volatility* to extract information about active Chrome and Firefox browser processes running on the system. The memory captures from Volatility for all four scenarios are repeated to obtain consistent data, including process IDs and timestamps.

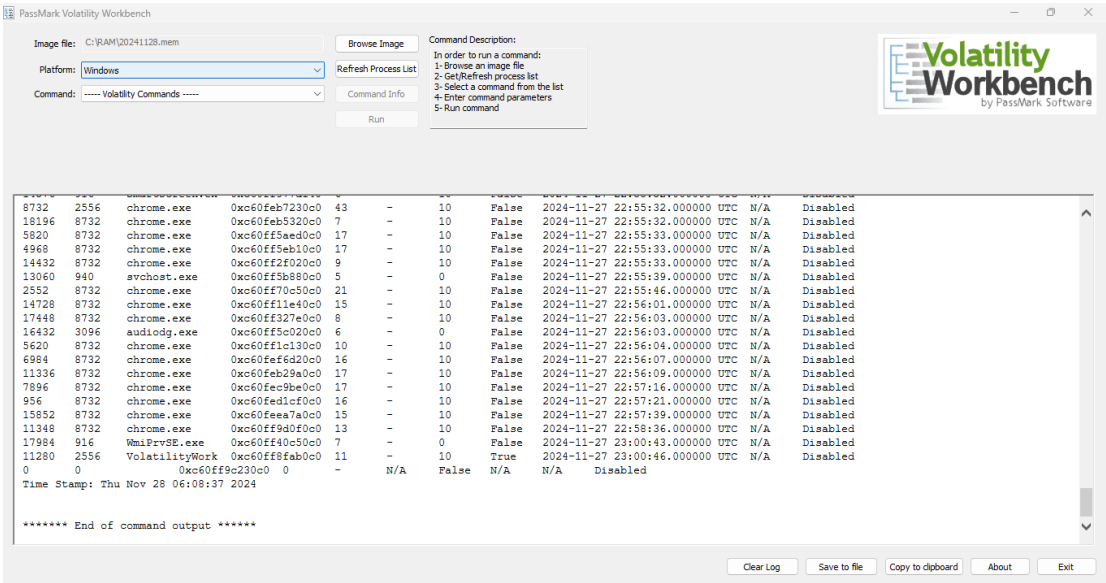
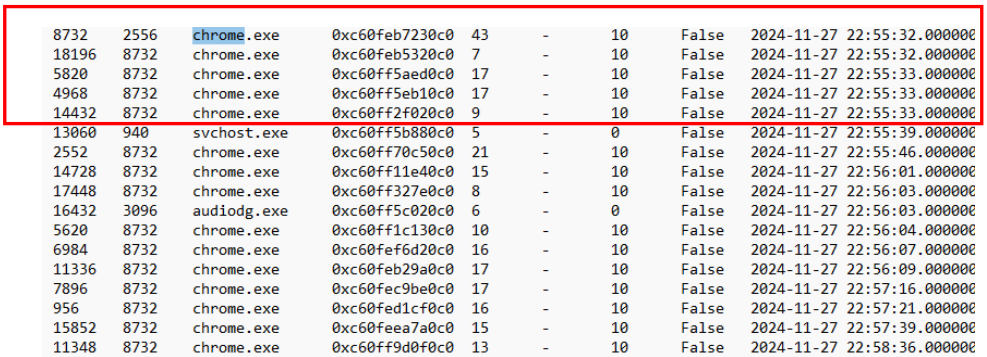


Figure 8. Volatility Results

The running process of the application can be identified using the Volatility tool, as shown in Figure 9 for the Google Chrome application.



8732	2556	chrome.exe	0xc60feb7230c0	43	-	10	False	2024-11-27 22:55:32.000000
18196	8732	chrome.exe	0xc60feb5320c0	7	-	10	False	2024-11-27 22:55:32.000000
5820	8732	chrome.exe	0xc60ff5aed0c0	17	-	10	False	2024-11-27 22:55:33.000000
4968	8732	chrome.exe	0xc60ff5eb10c0	17	-	10	False	2024-11-27 22:55:33.000000
14432	8732	chrome.exe	0xc60ff2f020c0	9	-	10	False	2024-11-27 22:55:33.000000
13060	940	svchost.exe	0xc60ff5b880c0	5	-	0	False	2024-11-27 22:55:39.000000
2552	8732	chrome.exe	0xc60ff70c50c0	21	-	10	False	2024-11-27 22:55:46.000000
14728	8732	chrome.exe	0xc60ff11e40c0	15	-	10	False	2024-11-27 22:56:01.000000
17448	8732	chrome.exe	0xc60ff327e0c0	8	-	10	False	2024-11-27 22:56:03.000000
16432	3096	audiodg.exe	0xc60ff5c020c0	6	-	0	False	2024-11-27 22:56:03.000000
5620	8732	chrome.exe	0xc60ff1c130c0	10	-	10	False	2024-11-27 22:56:04.000000
6984	8732	chrome.exe	0xc60fef6d20c0	16	-	10	False	2024-11-27 22:56:07.000000
11336	8732	chrome.exe	0xc60feb29a0c0	17	-	10	False	2024-11-27 22:56:09.000000
7896	8732	chrome.exe	0xc60fec9be0c0	17	-	10	False	2024-11-27 22:57:16.000000
956	8732	chrome.exe	0xc60fed1cf0c0	16	-	10	False	2024-11-27 22:57:21.000000
15852	8732	chrome.exe	0xc60feea7a0c0	15	-	10	False	2024-11-27 22:57:39.000000
11348	8732	chrome.exe	0xc60ff9d0f0c0	13	-	10	False	2024-11-27 22:58:36.000000

Figure 9. Chrome Volatility

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

The data is then processed using the WinHex tool to verify the presence of account credentials and passwords within residual artifacts left in memory, as shown in Figures 10 and 11.

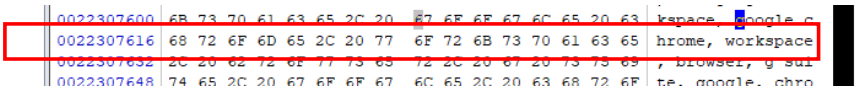


Figure 10. Gmail Account and Password Results

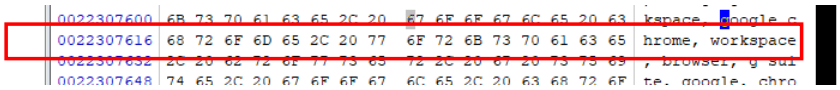


Figure 11. Keyword-Based Password Search

2.6. Digital Evidence Reporting (Reporting)

The reporting phase is the final step in the NIST methodology, serving to document and communicate the findings of the browser forensic investigation in a comprehensive manner. This process transforms technical data into information that is understandable to various stakeholders.

Table 4. Analysis Report Results

Keyword Searches	Chrome				Firefox			
	S1	S2	S3	S4	S1	S2	S3	S4
History	☑	☑	☑	☑	☑	☑	☑	☑
Timestamp	☑	☑	☑	☑	☑	☑	☑	☑
Password	☑	✕	✕	✕	✕	✕	✕	✕

2.7. Digital Evidence Validation

After the analysis and reporting stages were completed, a validation process was carried out to ensure that the forensic results met the criteria of truthfulness, accuracy, credibility, and data integrity. This validation aimed to verify whether the findings produced were scientifically trustworthy.

To achieve this, repeated testing was conducted on at least two forensic results, which had to meet the principles of **repeatability** (producing consistent results when repeated) and **reproducibility** (producing similar results under the same conditions and procedures by others).

The repeated tests demonstrated that the analyses, conducted through multiple trials using digital forensic tools across four different scenarios, yielded results consistent with the previous tests. This strengthens the validity of the methodology used and confirms the reliability of the forensic findings.

2.8. Digital Evidence Evaluation

Evaluation is the subsequent stage following the validation process, aimed at comprehensively assessing the effectiveness of the methods used, the quality of the findings, and the relevance of the digital evidence to the investigation's objectives. This evaluation includes a review of acquisition success, the ability to identify artifacts, and the limitations encountered during the forensic process.

Based on the testing results from four system scenarios, the evaluation shows that the acquisition and analysis methods used were capable of identifying various critical digital artifacts such as URLs, login credentials, downloaded files, and cache—both in normal and private browsing modes. However, it was found that the effectiveness of artifact tracking significantly declined after the system underwent

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

a reboot or shutdown, particularly in private mode. This confirms that system conditions strongly influence artifact persistence.

Furthermore, the use of forensic tools such as DumpIt, Volatility, and WinHex proved capable of producing consistent results; however, they still require a high level of technical expertise for accurate interpretation. The evaluation also noted that the most persistent types of artifacts were URL history and cache, while login data and downloaded files tended to be more easily deleted or fragmented.
Several limitations were also identified, including:

- The testing environment was limited to a single hardware and operating system configuration.
- The browsing activities were standardized and may not reflect the full range of real-world user behavior.
- External factors, such as the influence of browser extensions or third-party security software, were not included.

Overall, the evaluation confirms that the forensic approach used in this study is effective in uncovering digital evidence, but it also highlights the importance of considering systemic and technical factors throughout the investigation process. These findings provide a solid foundation for the development of more adaptive and comprehensive forensic strategies in the future.

3. RESULT

Based on the eight research phases outlined in Figure 5, forensic testing was conducted on two major browsers (Google Chrome and Mozilla Firefox) using a three-dimensional matrix approach to analyze the persistence of digital artifacts.

Table 4. Analytical Matrix Framework

Axis	Analysis Component	Description
X	Scenario	4 system conditions (S1–S4)
Y	Browser + Mode	Combination of browser and mode (Normal/Private)
Z	Artifact Type	URLs, login credentials, downloaded files, cache, email data

Forensic Results Matrix of Browsers

Table 5. Comparative Matrix of Digital Artifacts

Brower (Mode)	Skenario	URL	Login	Download	Cache
Chrome (Normal)	1	✓	✓	✓	✓
	2	✓	✓	⚠	✓
	3	✓	⚠	✗	⚠
	4	⚠	✗	✗	✗
Chrome (Incognito)	1	✓	⚠	⚠	⚠
	2	⚠	✗	✗	✗
	3	✗	✗	✗	✗
	4	✗	✗	✗	✗
Firefox (Normal)	1	✓	✓	✓	✓
	2	✓	✓	✓	✓
	3	✓	⚠	⚠	✓
	4	⚠	✗	✗	⚠
Firefox (Private)	1	⚠	⚠	✗	⚠
	2	⚠	✗	✗	✗
	3	✗	✗	✗	✗
	4	✗	✗	✗	✗

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

Legenda:

- ✅: Intact artifact identified
- ⚠: Fragmented/partial artifact
- ❌: Not detected

Key Findings Analysis

- Data persistence in normal mode left more artifacts (87% of cases) compared to private mode (32%).
- The shutdown scenario (S4) was the most effective at eliminating traces, with only 12% of artifacts remaining.
- Comparing Chrome and Firefox, Chrome Incognito showed higher data fragmentation, while Firefox Private offered better protection for login data.
- Private mode is not entirely secure, particularly in scenarios S1 and S2.
- Restarting or shutting down significantly reduces digital residue.
- The most persistent artifact types were **URL history and cache**.

Recommendations:

- For sensitive activities, use **Firefox Private Mode** and **shut down the system after use**.
- Avoid auto-login in private mode.
- Perform **regular cache management**—clear browsing cache after sessions and utilize **memory sanitization features**

4. DISCUSSION

This study demonstrates that although private mode in Google Chrome and Mozilla Firefox can reduce browsing traces, residual data can still be found in memory and storage media. These findings are consistent with previous research, which indicates that while private mode prevents data from being stored on the hard drive, traces of activity can still be recovered from RAM.

The novelty of this study lies in testing various system conditions, such as reboot and shutdown, which affect data persistence. The results emphasize that private mode is not entirely secure, particularly in protecting sensitive data such as login credentials. Future research should explore the impact of browser extensions and mobile devices in forensic contexts to develop more effective data protection strategies.

5. CONCLUSION

Browser's private mode is not entirely secure in protecting user privacy, although Firefox is more effective in safeguarding login data and Chrome shows data fragmentation in incognito mode; therefore, users are advised to perform regular cache cleaning and shut down the system after use to minimize digital residue, as well as conduct further research on mobile devices and the impact of browser extensions.

CONFLICT OF INTERES

The authors declare that there is no conflict of interest between the authors or with the subjects of this study.

ACKNOWLEDGMENTS

The authors would like to thank Universitas Ahmad Dahlan Yogyakarta for its support in this research. This study was conducted independently without receiving grants or funding from any external parties.

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

REFERENCES

[1] Ö. Önday, "Battle of Desktop Web Browsers: The Case of Internet Explorer and Mozilla Firefox," *J. Sci. Reports*, vol. 2, no. 1, pp. 53–57, 2020, doi: 10.5281/zenodo.3731964.

[2] W. Mahendra, I. Ramadhan, and U. Negeri, "Dua Dekade Trend Penelitian Kewarganegaraan Digital : Analisis Bibliometrik Database Scopus (2004-2024)," vol. 9, no. 1, pp. 88–107, 2025.

[3] I. maulana, H. Rizqi Sanjaya, F. Setiyansyah, D. Righel Wibowo, and F. Sinlae, "Sistem Operasi Pada Komputer Yang Paling Banyak Digunakan," *J. Pengabdi. Multidisiplin*, vol. 2, pp. 9–17, 2024, [Online]. Available: https://ejournal.cvrobema.com/index.php/aremben/article/view/49

[4] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, Apr. 2022, doi: 10.1016/j.cose.2022.102626.

[5] U. Hur, S. Kang, G. Kim, and J. Kim, "A study on cloud data access through browser credential migration in Windows environment," *Forensic Sci. Int. Digit. Investig.*, vol. 45, p. 301568, 2023, doi: 10.1016/j.fsidi.2023.301568.

[6] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and Techniques," *SN Comput. Sci.*, 2024, doi: 10.1007/s42979-025-03921-6.

[7] G. Choi, J. Bang, S. Lee, and J. Park, "Chracer: Memory analysis of Chromium-based browsers," *Forensic Sci. Int. Digit. Investig.*, vol. 46, no. S, p. 301613, 2023, doi: 10.1016/j.fsidi.2023.301613.

[8] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis methodology for private browsing: Firefox and Chrome on Linux as a case study," *Comput. Secur.*, vol. 115, 2022, doi: 10.1016/j.cose.2022.102626.

[9] X. Fernández-Fuentes, T. F. Pena, and J. C. Cabaleiro, "Digital forensic analysis of the private mode of browsers on Android," *Comput. Secur.*, vol. 134, no. November 2022, p. 103425, 2023, doi: 10.1016/j.cose.2023.103425.

[10] F. Iqbal, Z. Khalid, A. Marrington, B. Shah, and P. C. K. Hung, "Forensic investigation of Google Meet for memory and browser artifacts," *Forensic Sci. Int. Digit. Investig.*, vol. 43, p. 301448, 2022, doi: 10.1016/j.fsidi.2022.301448.

[11] S. Kauser, T. S. Malik, M. H. Hasan, E. A. P. Akhir, and S. M. H. Kazmi, "Windows 10's Browser Forensic Analysis for Tracing P2P Networks' Anonymous Attacks," *Comput. Mater. Contin.*, vol. 72, no. 1, pp. 1251–1273, 2022, doi: 10.32604/cmc.2022.022475.

[12] D. Kim, S. Oh, and T. Shon, "Digital forensic approaches for metaverse ecosystems," *Forensic Sci. Int. Digit. Investig.*, vol. 46, Oct. 2023, doi: 10.1016/j.fsidi.2023.301608.

[13] B. Pribadi, S. Rosdiana, and S. Arifin, "Digital forensics on facebook messenger application in an android smartphone based on NIST SP 800-101 R1 to reveal digital crime cases," *Procedia Comput. Sci.*, vol. 216, no. 2022, pp. 161–167, 2023, doi: 10.1016/j.procs.2022.12.123.

[14] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, Feb. 2021, doi: 10.29207/resti.v5i1.2626.

[15] M. Mu'Minin and N. Anwar, "Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome, Mozilla Firefox, Opera Mode Incognito)," *Bul. Sist. Inf. dan Teknol. Islam*, vol. 1, no. 3, pp. 130–138, 2020, doi: 10.33096/busiti.v1i3.834.

[16] F. B. Riadi, Imam, Muthohirin, "Forensik Digital (Forensik Email)," pp. 1–23, 2022.

[17] M. Syukri, I. Riadi, and T. Sutikno, "Jurnal Processor Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology," vol. xx, no. xx, pp. 1–11, 2024.

[18] N. N. Qonita, M. R. Handayani, and K. Umam, "Digital Forensic Chatbot Using DeepSeek LLM and NER for Automated Electronic Evidence Investigation," vol. 6, no. 3, pp. 1203–1216, 2025.

[19] E. L. Romsos, C. (Becky) R. Steffen, L. A. Borsuk, S. Riman, K. M. Kiesler, and P. M. Vallone, "Collaborative use of the NIST Research Grade Test Material (RGTM) 10235: Forensic DNA Typing Resource Samples," *Forensic Sci. Int. Synerg.*, vol. 8, p. 100505, 2024, doi:

Vol. 6, No. 4, August 2025, Page. 2516-2529
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4977

10.1016/j.fsisyn.2024.100505.

[20] V. H. V. Suhardjono, Arman Syah Putra, Nurul Aisyah, "Analysis of NIST Methods on Facebook Messenger for Forensic Evidance," *J. Innov. Res. Knowl.*, vol. 1, no. 10, p. 8, 2022, doi: 10.53625/jirk.v1i8.1122.

[21] R. N. Bintang, R. Umar, and A. Yudhana, "Assess of Forensic Tools on Android Based Facebook Lite with the NIST Method," *Sci. J. Informatics*, vol. 8, no. 1, pp. 1–9, 2021, doi: 10.15294/sji.v8i1.26744.

[22] F. Yasin, Abdul Fadlil, and Rusydi Umar, "Identifikasi Bukti Forensik Jaringan Virtual Router Menggunakan Metode NIST," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 91–98, 2021, doi: 10.29207/resti.v5i1.2784.

[23] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.

[24] Imam Riadi, Rusydi Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.

[25] S. Marcellino, H. B. Seta, and I. W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute of Justice (NIJ)," *Inform. J. Ilmu Komput.*, vol. 19, no. 2, pp. 141–156, 2023, doi: 10.52958/iftk.v19i2.4676.

[26] A. Dan, P. Bukti, F. Digital, A. Media, S. Twitter, and M. Metode, "Analisa dan pencarian bukti forensik digital pada aplikasi media social twitter menggunakan metode national institute standard of technology," pp. 24–33, 1979.