Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

Forensic Evaluation of the Effectiveness of Private Browsing Modes in Google Chrome and Mozilla Firefox Using the National Institute of Standards and Technology Framework Integrated with Artificial Intelligence

Muhammad Syukri[*1], Asep Ririh Riswaya[2], Dheni Apriantsani Budiman[3]

[1,2,3]Informatics Engineering, STMIK Mardira Indonesia, Bandung, Indonesia

Email: [1]syukrie77@gmail.com

Received : Dec 14, 2025; Revised : Jan 6, 2026; Accepted : Jan 6, 2026; Published : Apr 18, 2026

Abstract

As cyber threats and the misuse of personal data continue to increase, private browsing modes in web browsers such as Google Chrome and Mozilla Firefox are often perceived as solutions to enhance user privacy. However, these modes still leave traces of sensitive data in volatile memory (RAM), even though artifacts stored on disk-based storage are removed. This study evaluates the effectiveness of private browsing modes using the National Institute of Standards and Technology (NIST) framework integrated with Artificial Intelligence (AI) for forensic analysis. Simulation scenarios were conducted to assess the ability of private browsing modes to prevent data retention. The results indicate that although private browsing modes successfully eliminate disk-based traces, sensitive data such as account credentials can still be extracted from RAM. The integration of AI accelerates the detection of these artifacts. This research contributes to the field of digital forensics by providing a systematic framework for evaluating browser privacy mechanisms and offering insights for the development of real-time browser security tools.

Keywords : *AI, Digital Forensic, NIST, Private Mode.*

1 INTRODUCTION

Use privacy on the internet is increasingly important amid the rise of cybercrime [1] and the misuse of personal data [2]. Many browsers offer a private mode (private/incognito) [3] which is claimed to protect user data from local traces such a browsing history, cache, cookies, and other stored artifacts [4]. However, several studies have shown that private mode does not guarantee the complete removal of activity traces [5], as digital evidence may still appear in volatile storage (RAM) or system memory [6]. A browser is software designed to retrieve and display information resources from the internet [7]. Browser play a critical role in the digital ecosystem, as users cannot acess online content without them [8]. Modern browsers have undergone extensive developmnet in both quality and quantity, resulting in varying usage percentages among users [9]. According to statistical reports from survey platform StatCounter, Google Chrome, Internet Explorer and Firefox are the most widely used browsers [10], consistently ranking among the top three globally in overall market share [11].

Table 1. Top Three Web Browsers

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

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

The increasing adoption of web browsers aligns with the rapid advancement of internet technologies, which have become the backbone of digital transformation. This trend is particularly 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 of 185.3 million internet users, with the majority accessing information through search enginers and sosial media platforms [12]. See Figure 1.

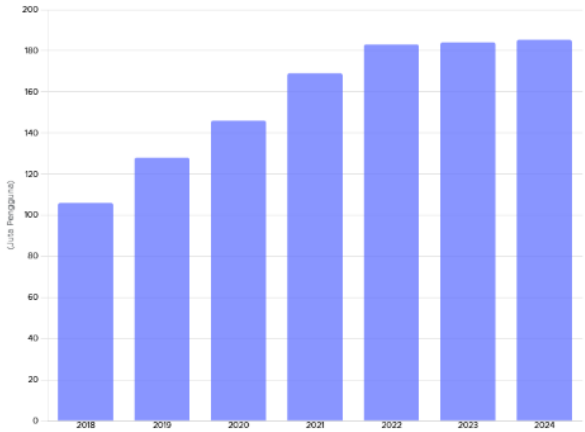

Figure 1. Internet Users in Indonesia

The process of handling cyber incidents through forensics analysis has proven effective in successfully collecting evidence of criminal activities [13]. The digital forensic investigation method developed by the National Institute of Standards and Technology (NIST) has been compared with the National Institute of Justice (NIJ) method in the context of MicroSD analysis, with findings indicating that the NIST method is more efficient for rapid investigations, while the NIJ method offers a more comprehensive and detailed approach [14].

Privacy mode features are widely implemented in many internet browsers, including Avant, Brave, Chrome, Chromium, Comodo IceDragon, Comodo Dragon, Edge, Epic, Falkon, Firefox, GreenBrowser, Internet Explorer, Konqueror, Links, Lynx, Maxthon, Midori, Netsurf, Opera, Pale Moon, Puffin, Seamonkey, Sleipnir, SlimJet, Tor Browser, Torch, US Browser, Vivaldi, and WaterFox, with increasing user awareness of their functions and intended purposes. However, further research is needed to understand their true effectiveness and ensure user data privacy [15].

Although numerous studies have evaluated the effectiveness of private browsing modes [6][16][15] independently, and other research has examined the application of AI [17][18][19] or the use of the NIST framework [20][21][22] in digital forensics, there is still no study that systematically integrates browser forensic analysis, the NIST framework, and AI modules into a single unified approach, particularly for evaluating data leakage in browser private modes. This lack of integration results in the absence of a comprehensive and adaptive evaluation framework capable of addressing modern investigative challenges that demand high speed and accuracy.

Based on this research gap, the present study aims to evaluate the effectiveness of private browsing modes in Google Chrome and Mozilla Firefox through a digital forensic approach based on the NIST framework, enhanced with AI modules [23]. This research examines residual digital artifacts [24] in both permanent storage and volatile memory, and assesses the contribution of AI [25] in accelerating and improving the accuracy of forensic analysis. The primary contribution of this study is the development of a systematic framework that integrates digital forensics, AI, and NIST standards to assess browser privacy security [26], thereby strengthening the novelty in the domain of modern browser [27] forensics.

2 LITERATUR REVIEW

A comparative study of forensic tools on Mozilla Firefox Private Mode revealed that even with private mode enabled, digital artifacs were still found in RAM, with tools such as Autopsy recovering up to 83% of browsing logs [4]. A case study involving Google Chrome, Mozilla Firefox, and Opera further demonstrated that incognito/private modes continue to leave digital traces, particulary within volatile memory (RAM) [10]. Studies on Google Chrome and Mozilla Firefox in a Linux environment show that although private mode does not store data on the hard disk, sensitive information can still be recovered from RAM [28].

Research analyzing Chrome, Brave, Firefox, and Tor on Android devices found that private mode does not store browsing traces in the file system; however, volatile analysis can recover login credentials, and devie restarts do not fully eliminate memory residues [27]. A study on Tor and P2P applications reported that artifacts remain stored in the registry, RAM, and hard disk, with tools such as Reghost and Bulk Extractor proving effective for extraction, indicating that private mode does not completely erase digital traces [29]. Research on browser credential migration demonstrated that automatic login credentials could be successfully migrated in 25 out of 28 browsers, enabling access to cloud services without re-authentication, using tools such as Rehost, Mimikatz, and DataProtectionDecryptor [30].

The implications of these findings highlight that private mode is not fully secure againts forensic analysis [31], RAM is the primary source of digital residue [10], memory capacity influences data persistence [26], and forensic tools continue to evolve to address privacy protection challeges [32].

In a broader context, the use of NIST-based forensic methods has proven effective in digital security investigations, both in file systems and mobile devices [33].

On the AI side, recent studies have begun exploring the adoption of AI and machine learning (ML) in digital forensics to automate artifact detection, evidence classification, and large-scale analysis [23]. Based on several studies, automation tools such as the MultiAgent Digital Investigation Toolkit (MADIK) and the Open Computer Forensic Architecture (OCFA) have been developed, utilizing machine learning (ML) based approaches in digital forensics. These approaches incorporate supervised, unsupervised, and reinforcement learning, enabling automated data classification and anomaly detection [34].

Research has been conducted to address the growing challenges in digital forensics resulting from the increasing complexity of cybercrime. Traditional manual methods are considered inefficient and prone to error. Therefore, recent studies propose AI based frameworks to automate evidance acquisition, analysis, and reporting, thereby improving both the speed and accuracy of investigations [18].

The application of AI in digital forensics [35], particularly for extracing digital evidence, has shown promising advancements. AI especially machine learning and deep learning [36], can enhance the efficiency of analyzing digital evidence such as emails and network data by automating the detection of suspicious patterns [37].

Another line of research applies AI to automate the evidence analysis phase in digital forensic through methods such as Answer Set Programming (ASP), which enables the objective resolution of complex investigation problem [38].

Despite these advancements, there remains a lack of literature that integrates all there aspects browser private mode, forensic analysis, and AI into a single systematic framework.

3 METHOD

This study employs an experimental approach by integrating digital forensic analysis based on the National Institute of Standards and Technology (NIST) framework with Artificial Intelligence (AI) modules to evaluate the effectiveness of private browsing modes in web browsers. The research

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

methodology is structured in a systematic and reproducible manner through six main stages, as illustrated in Figure 2.

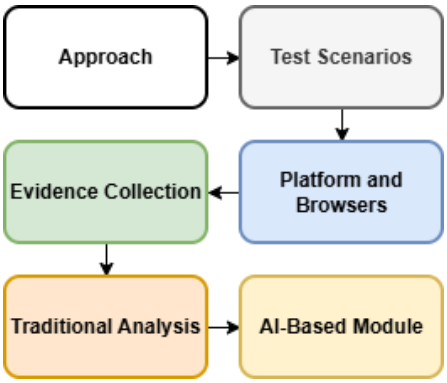

Figure 2. Research Stages

3.1 Research Framework

The research stages consist of: (1) a forensic and AI-based approach, (2) test scenario design, (3) testing platforms and environments, (4) digital evidence acquisition, (5) traditional forensic analysis, and (6) integration of AI modules for automated analysis. This approach ensures that the entire investigation process adheres to standard forensic procedures while simultaneously leveraging the advantages of AI to enhance the efficiency and accuracy of the analysis.

3.2 Integration of the NIST Framework

This study adopts the four main phases of the NIST framework—Collection, Examination, Analysis, and Reporting—which are integrated with AI modules in the Analysis phase.

a. Collection

This stage focuses on the collection and preservation of digital evidence from the test systems. The process is carried out by performing disk imaging and RAM capture after browsing sessions in both private and normal modes. Memory acquisition is conducted using live forensics techniques to maintain data integrity and minimize the loss of volatile artifacts.

b. Examination

At this stage, the collected digital evidence is examined using forensic tools such as Belkasoft Evidence Center and Autopsy. The examination includes the identification of browser artifacts such as cache, cookies, browsing history, login credentials, session tokens, and memory structures associated with browsing activities.

c. Analysis

The analysis stage is conducted using two approaches: traditional forensic analysis and AI-based analysis. Traditional analysis aims to manually identify the presence of artifacts, while AI-based analysis is used to automatically and systematically detect artifact patterns and potential data leakage.

d. Reporting

The final stage encompasses the documentation of the entire investigation process, the tools used, the results of both forensic and AI analyses, as well as recommendations for improving browser privacy security. The report is prepared in accordance with forensic soundness principles to ensure academic and legal accountability. Figure 3 illustrates the stages of the NIST methodology.

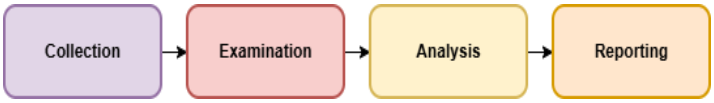

Figure 3. NIST Methodology

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

3.3 Testing Scenarios and Data Acquisition

To ensure reproducibility, this study employs four testing scenarios that represent common browsing activities, namely:

a. Website access and keyword searching,
b. Web-based account login and logout,
c. Social media interaction and email services,

Each scenario is executed on Google Chrome and Mozilla Firefox in private browsing mode. After each session, disk and RAM acquisition are performed to obtain consistent digital artifact datasets that can be compared across scenarios. See the test scenarios in Figure 4.

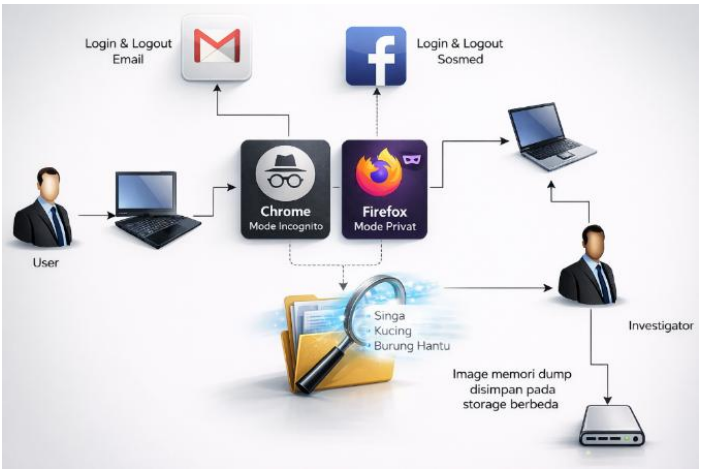

Figure 4. Four Case Scenarios and Their Implementation

3.4 Design and Integration of AI Modules

To clarify the AI-based data processing workflow, this study introduces a dedicated AI integration pipeline, as illustrated in Figure 5, which includes the following stages:

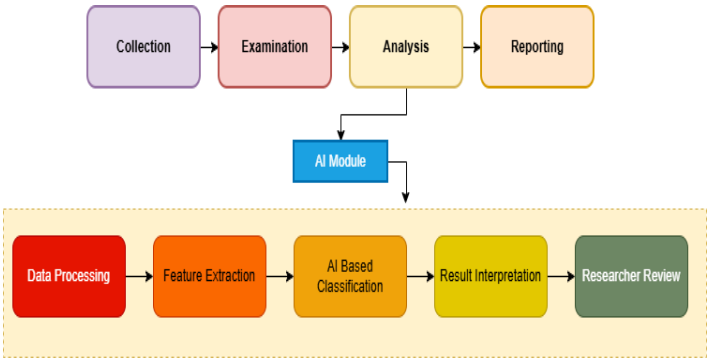

Figure 5. NIST Method Development with an AI Module

3.4.1 Data Processing

Artifacts obtained from the collection and examination phases are cleaned of redundant data, normalized, and converted into structured formats (CSV/JSON). This process includes noise removal, timestamp synchronization, and encoding of non-numeric attributes.

3.4.2 Feature Extraction

Extracted features include URLs, domains, timestamps, session IDs, authentication tokens, cache objects, memory metadata, and indicators of user activity. These features represent browsing behavior patterns and potential residuals of private browsing modes.

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

3.4.3 AI Modules and Algorithms

This study employs a supervised machine learning classification approach using the Random Forest algorithm due to its ability to handle heterogeneous data and reduce overfitting. The model is used to classify artifacts into the following categories:

a. Normal activity,
b. Residual artifacts of private browsing mode,
c. Potential leakage of sensitive data.

The model is implemented using the Scikit-learn library in a Python environment. See Figure 6 for the integration of the AI module in the Autopsy tool.

```
autopsy/
└── python_modules/
    └── ai_browser_forensic/
        ├── __init__.py
        ├── ai_browser_module.py
        └── model.pkl
```

Figure 6. Structure of the Autopsy Module Integrated with AI

An example of the Autopsy module framework (Python) is shown in Figure 7 below:

```python
from org.sleuthkit.autopsy.ingest import IngestModuleFactoryAdapter
from org.sleuthkit.autopsy.ingest import DataSourceIngestModule

class AIBrowserForensicModule(DataSourceIngestModule):

    def process(self, dataSource, progressBar):
        # Load AI model
        # Parse extracted artifacts
        # Run classification
        # Post results to Autopsy Blackboard
        pass
```

Figure 7. Autopsy AI Module Framework

3.4.4 Model Training and Validation

The dataset is divided into training and testing data with a 70:30 ratio. The training process is validated using k-fold cross-validation (k = 5) to ensure model stability. Model performance is evaluated using accuracy, precision, recall, and F1-score metrics.

3.4.5 Result Interpretation and Human Validation

The AI classification results are translated into forensic indicators that can be interpreted by analysts, such as leakage risk levels and confidence scores. Subsequently, forensic analysts perform manual validation to identify potential false positives and false negatives.

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

3.4.6 Reproducibility and Method Validity

To ensure research reproducibility, all testing environment configurations, activity scenarios, forensic tools, and AI model parameters are documented in detail. This approach ensures that the proposed method can be replicated and further developed in future studies with variations in browsers, operating systems, or AI algorithms.

4 RESULT

4.1 Overview of the Experiment

This experiment aims to evaluate the capability of integrating Autopsy with an external AI module in conducting browser forensic analysis on Google Chrome, particularly in scenarios involving email (Gmail) and social media (Facebook) login and logout activities, including private browsing (incognito) sessions. Forensic data were obtained from disk images, memory dumps, and browser artifacts (history, cache, and cookies). The entire process followed the stages of the NIST Digital Forensic Framework.

4.2 Data Acquisition Results (NIST – Collection)

4.2.1 Browser Artifacts Extracted by Autopsy

Autopsy successfully extracted browser artifacts as presented in Table 2.

Table 2. Autopsy Extraction Results of Browser Artifacts

Artifact Type	Quantity	Source
Web History	5 entries	History DB
Browser Cache	3 entries	Cache
Cookies	3 entries	Cookies DB
Memory Artifacts	3 entries	RAM Dump

Artifacts from incognito mode did not fully appear in the web history; however, they were successfully reconstructed from memory and cache, consistent with the characteristics of private browsing.

4.3 Autopsy Examination Results (NIST – Examination)

4.3.1 Gmail Login Activity

Autopsy identified the URL accounts.google.com along with supporting artifacts from history and cache. The session cookie (SID) was found in the memory dump. From a forensic perspective, this indicates a legitimate email login, with residual authentication evidence preserved in memory.

4.3.2 Facebook Login Activity (Incognito Mode)

Autopsy did not display Facebook login activity in the history database. However, several artifacts were identified, as shown in Table 3.

Table 3. Facebook Activity Artifacts

Artifact	Source
Session token	Memory
c_user cookie	Cache
Login timestamp	Memory

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

From a forensic interpretation, the Facebook login was performed using incognito mode; however, digital traces could still be reconstructed through volatile artifacts.

4.4 AI Engine Analysis Results (NIST – Analysis)

Initial integration testing attempted to embed the AI module directly into Autopsy through the ingest process. Although the integration was technically successful, it did not produce the expected analytical results during Autopsy execution. Therefore, an alternative approach was implemented by deploying an external AI engine. In this approach, artifacts extracted by Autopsy were exported into CSV files and subsequently processed by the AI engine. The processed data are shown in Table 4.

Table 4. Data Processed by the AI Engine

AI Feature	Source
URL & Domain	Web History
Login Patterns	Cookies & Cache
Access Time	Timestamp
Sensitive Strings	Memory Dump

4.4.1 AI Processing

The AI module performed feature extraction on the Autopsy output, followed by vectorization using TF-DF and risk classification using logistic regression. The resulting risk predictions are presented in Table 5.

Table 5. Risk Prediction Results

Domain	Activity	Risk Score	Risk Level
accounts.google.com	Email Login	0.62	Medium
facebook.com	Social Media Login (Incognito)	0.84	High

The AI classified the Facebook incognito activity as high risk due to the presence of active session artifacts that appeared only in memory and were not recorded in the history database.

4.5 Integration of Autopsy and AI within the NIST Framework

4.5.1 NIST Phase Mapping

The integration mapping between Autopsy and the AI module within the NIST framework is shown in Table 6.

Table 6. Integration Mapping of Autopsy and AI in the NIST Framework

NIST Phase	Implementation
Collection	Disk and memory acquisition
Examination	Artifact extraction by Autopsy
Analysis	AI-based risk classification
Reporting	AI result CSV and visualization
NIST Phase	Implementation
Collection	Disk and memory acquisition
Examination	Artifact extraction by Autopsy
Analysis	AI-based risk classification
Reporting	AI result CSV and visualization

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

The integration of AI with the Autopsy forensic tool strengthens the Analysis phase, which is traditionally manual in the NIST framework. Autopsy excels at artifact extraction, while AI enhances data correlation, risk assessment, and anomaly detection. The integration of both tools results in more comprehensive and objective forensic analysis.

In the context of private browsing, the findings demonstrate that private mode does not completely eliminate digital traces. Memory forensics, augmented by AI, is capable of uncovering hidden activities. These findings reinforce modern digital forensic literature.

Validation of the research results was conducted through manual investigator comparison, timestamp consistency checks, and cross-artifact verification. The AI results demonstrated analytical accuracy consistent with forensic investigators. Table 7 summarizes the forensic results of the AI-integrated NIST framework.

Table 7. Summary of Results

Aspect	Result
Autopsy	Successful artifact extraction
AI Engine	Successful risk classification
NIST Compliance	Fulfilled
Incognito Analysis	Successfully reconstructed

The results of this study confirm that private browsing mode in Google Chrome and Mozilla Firefox does not fully guarantee user anonymity. The primary vulnerability lies in Random Access Memory (RAM), which continues to store session artifacts, temporary credentials, and activity traces during browser execution. Technically, RAM is volatile but actively records application states, making it a critical weakness that private browsing mechanisms cannot fully eliminate.

Compared with previous studies reporting artifact recovery rates of up to 83% using Autopsy, this study demonstrates consistent forensic residue patterns with improved analytical precision through AI integration. AI enables cross-artifact correlation and systematic risk assessment, particularly for sensitive social media login activities.

From a computer science perspective, this research contributes a scalable hybrid NIST–AI framework for browser forensic automation. This framework supports the development of real-time security and privacy evaluation systems and has the potential to serve as a foundation for standardizing private browser forensic analysis within the computing discipline.

5 DISCUSSIONS

The results of this study confirm that private browsing mode in Google Chrome and Mozilla Firefox does not fully guarantee user anonymity. The primary vulnerability lies in Random Access Memory (RAM), which continues to store session artifacts, temporary credentials, and activity traces during browser execution. Technically, RAM is volatile in nature but actively records application states, making it a weakness that is difficult to eliminate through private browsing mechanisms.

When compared with previous studies, such as research reporting artifact recovery rates of up to 83% using Autopsy, the findings of this study demonstrate consistency in forensic residue patterns, while achieving improved analytical precision through AI integration. AI enables cross-artifact correlation and more systematic risk assessment, particularly for sensitive social media login activities.

From an informatics perspective, this research contributes by introducing a scalable hybrid NIST–AI framework for browser forensic automation. This framework supports the development of security and privacy systems based on real-time evaluation and has the potential to serve as a foundation for standardizing private browser forensic analysis within the field of computer science.

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

6 CONCLUSION

This study evaluated the effectiveness of private browsing mode in Google Chrome and Mozilla Firefox using a NIST-based digital forensic approach enhanced with AI. The results indicate that private mode provides only partial protection: while activity artifacts are removed from disk storage, digital residues such as URLs, timestamps, and session tokens can still be recovered from volatile memory (RAM).

The integration of AI in the analysis phase of the NIST framework was proven to improve efficiency and consistency in artifact detection compared to traditional forensic analysis. The hybrid NIST–AI approach enables a more systematic, scalable, and reproducible investigation process, particularly for complex browser memory analysis.

From the perspectives of informatics and computer science, this research contributes to the advancement of digital forensics and privacy engineering by providing a standardized AI-based framework for browser privacy evaluation. This framework has the potential to support browser security development and real-time forensic automation. Future research is recommended to extend testing to other operating systems such as Linux and Android, include additional browsers such as Brave and Tor Browser, and develop AI-based browser plugin prototypes for real-time data leakage detection.

The AI engine is executed externally to maintain forensic tool integrity, while Autopsy functions as the evidence acquisition and visualization platform.

CONFLICT OF INTEREST

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

ACKNOWLEDGEMENT

The author would like to express his gratitude for the support from the Ministry of Education and Science and Technology grant number: 125/C3/DT.05.00/PL/2025 and derivative Number: 8068/LL4/PG/2025.

REFERENCES

[1] D. Yuliana, T. Yuniati, and B. P. Zen, "Analisis Bukti Digital Cyberbullying Pada Media Sosial Menggunakan Metode National Institut of Standard and Technology (Nist) 800-101," *LEDGER J. Inform. Inf. Technol.*, vol. 1, no. 3, pp. 113–123, 2022, doi: 10.20895/ledger.v1i3.812.

[2] M. Syukri, I. Riadi, and T. Sutikno, "Analisis Forensik Keamanan Data Pribadi pada Mode Privasi Browser Menggunakan Metode National Institute of Standards and Technology (NIST)," *J. Process.*, vol. 20, no. 1, May 2025, doi: 10.33998/PROCESSOR.2025.20.1.2012.

[3] D. Kim, S. Lee, and J. Park, "Decrypting IndexedDB in private mode of Gecko-based browsers," *Forensic Sci. Int. Digit. Investig.*, vol. 49, no. S, p. 301763, 2024, doi: 10.1016/j.fsidi.2024.301763.

[4] J. Algoritma, S. Tinggi, and T. Garut, "Perbandingan Tool Forensik pada Mozilla Firefox Private Mode Menggunakan Metode NIST," pp. 283–291.

[5] M. Syukri, I. Riadi, and T. Sutikno, "Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the National Institute of Standards and Technology (NIST) Framework," vol. 6, no. 4, pp. 2516–2529, 2025.

[6] 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.

[7] H. A. Jannah, S. A. R. Laoh, E. Raup, T. Pangkey, N. Sumendah, and F. M. Monigir, "Internet Browsing," no. 6, 2024.

[8] H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic analysis of private browsing mechanisms: Tracing internet activities," *J. Forensic Sci. Res.*, vol. 5, no. 1,

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

pp. 012–019, Mar. 2021, doi: 10.29328/JOURNAL.JFSR.1001022.
[9] K. Hughes, P. Papadopoulos, N. Pitropakis, A. Smales, J. Ahmad, and W. J. Buchanan, "Browsers' private mode: Is it what we were promised?," *Computers*, vol. 10, no. 12, 2021, doi: 10.3390/computers10120165.
[10] M. Minin, "Live Data Forensic Artefak Internet Browser (Studi Kasus Google Chrome , Mozilla Firefox , Opera Mode Incognito)," vol. 1, no. 3, pp. 130–138, 2020.
[11] 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.
[12] 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.
[13] P. Binnar, S. Bhirud, and F. Kazi, "Security analysis of cyber physical system using digital forensic incident response," Jan. 2024, *KeAi Communications Co.* doi: 10.1016/j.csa.2023.100034.
[14] N. Anwar, A. M. Widodo, B. A. Sekti, M. B. Ulum, M. Rahaman, and H. D. Ariessanti, "Comparative Analysis of NIJ and NIST Methods for MicroSD Investigations: A Technopreneur Approach," *Aptisi Trans. Technopreneursh.*, vol. 6, no. 2, pp. 169–181, Jul. 2024, doi: 10.34306/att.v6i2.407.
[15] G. Horsman *et al.*, "A forensic examination of web browser privacy-modes," *Forensic Sci. Int. Reports*, vol. 1, no. October, p. 100036, 2019, doi: 10.1016/j.fsir.2019.100036.
[16] S. Alam, M. A. Aziz, and W. Iqbal, "Forensic Analysis of Edge Browser In-Private Mode," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. 9, pp. 256–263, 2016.
[17] V. Sharad, "AI-Enhanced Digital Forensics : Automated Techniques for Efficient Investigation and Evidence Collection," pp. 211–229, 2024.
[18] J. O. Ajayi *et al.*, "AI-Driven Digital Forensics : Automating Evidence Gathering and Analysis," vol. 6, no. 5, pp. 220–249, 2023.
[19] D. Dunsin, M. C. Ghanem, K. Ouazzane, and V. Vassilev, "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response," *Forensic Sci. Int. Digit. Investig.*, vol. 48, p. 301675, Mar. 2024, doi: 10.1016/J.FSIDI.2023.301675.
[20] 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.
[21] F. Breitinger and A. Jotterand, "Sharing datasets for digital forensic: A novel taxonomy and legal concerns," *Forensic Sci. Int. Digit. Investig.*, vol. 45, Jul. 2023, doi: 10.1016/j.fsidi.2023.301562.
[22] K. Chimmanee and S. Jantavongso, "Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN," *Expert Syst. Appl.*, vol. 249, Sep. 2024, doi: 10.1016/j.eswa.2024.123652.
[23] A. A. Solanke, "Forensic Science International : Digital Investigation Explainable digital forensics AI : Towards mitigating distrust in AI- based digital forensics analysis using interpretable models," *Forensic Sci. Int. Digit. Investig.*, vol. 42, p. 301403, 2022, doi: 10.1016/j.fsidi.2022.301403.
[24] A. A. Solanke and M. Angela, "Digital Forensics AI : Evaluating , Standardizing and Optimizing Digital Evidence Mining Techniques," *KI - Künstliche Intelligenz*, vol. 36, no. 2, pp. 143–161, 2022, doi: 10.1007/s13218-022-00763-9.
[25] C. Mitigation, "Digital Forensics and Incident Response (DFIR) Automation : Leveraging AI to Accelerate Breach Investigation , Evidence," vol. 01, no. 04, 2025, doi: 10.64235/tsvfvz27.
[26] 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.
[27] 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, Nov. 2023, doi: 10.1016/j.cose.2023.103425.
[28] 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,

Vol. 7, No. 2, April 2026, Page. 1639-1650
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2026.7.2.5577

p. 102626, Apr. 2022, doi: 10.1016/J.COSE.2022.102626.

[29] 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.

[30] 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.

[31] R. R. Chand, N. A. Sharma, and M. A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation of Emerging Tools and TechniquesNANo ranking found for 'SN Computer Science,'" *Springer*, vol. 6, no. 4, p. 355, Apr. 2025, doi: 10.1007/S42979-025-03921-6.

[32] Muhammad Rafi Ilmuna Ihsan and Apriade Voutama, "Penerapan Metode NIST Dalam Analisis Forensik Digital Pasca Serangan Siber (Studi Kasus : Pt.Analis Digital Forensik)," *Cyber Secur. dan Forensik Digit.*, vol. 8, no. 1, pp. 53–62, 2025, doi: 10.14421/csecurity.2025.8.1.5092.

[33] J. Teknologi, W. Agustiono, D. W. Suci, and N. Prastiti, "Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence," vol. 14, no. September, pp. 174–185, 2024, doi: 10.34010/jati.v14i2.

[34] O. Access, "We are IntechOpen , the world ' s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %".

[35] A. Jarrett, C. Security, S. Antonio, K. R. Choo, and C. Security, "Article Title : The Impact of Automation and Artificial Intelligence on Digital Forensics Article Type : Authors :," pp. 0–1, doi: 10.1002/wfs2.1418.

[36] C. Hargreaves, J. Sheppard, and M. Scanlon, "SoK : Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation," no. Ml, 2020, doi: 10.1145/3407023.3407068.

[37] A. Abdullahi, "Alma Mater Studiorum – Universitá di Bologna DOTTORATO DI RICERCA IN LAW , SCIENCE AND TECHNOLOGY Alma Mater Studiorum – University of Bologna Ph . D . PROGRAMME IN LAW , SCIENCE AND TECHNOLOGY," 2022.

[38] S. Costantini, G. De Gasperis, and R. Olivieri, *Digital forensics and investigations meet artificial intelligence*. 2019.