International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FORENSIC INTELLIGENCE: A HYBRID FRAMEWORK FOR AUTOMATED ARTIFACT COLLECTION AND ANALYSIS

Dr. Jaydevsinh B. Vala

Lecturer, Computer Engineering Department, A. V. Parekh Technical Institute (AVPTI),

Rajkot, Gujarat- 360001, India.

e-mail: jaydev.vala@gmail.com

Abstract

The increasing sophistication of cyber threats necessitates advanced digital forensic approaches for effective detection and investigation. This research presents a comprehensive framework that integrates memory forensics, digital artifact analysis, and automated evidence collection to enhance cybercrime investigations. By simulating real-world attack scenarios—including file manipulation, removable media interactions, and malicious downloads—diverse forensic artifacts were systematically extracted and analyzed. The proposed framework ensures evidence integrity, legal admissibility, and structured presentation through both live and dead forensic techniques. Python-based automation was employed to streamline IP tracing, social media profiling, and URL exploration, reducing manual effort and improving efficiency. Memory forensics was crucial in identifying volatile data such as rogue processes and network connections, supporting the reconstruction of malicious activities. Overall, this study advances digital forensics by introducing an automated, legally compliant, and comprehensive methodology for identifying and mitigating modern cyber threats.

Key Words and Phrases: Digital Forensics, Memory Forensics, Cybercrime Investigation, Artifact Analysis, Automated Evidence Collection, Python-Based Forensic Framework, Cyber Threat Detection.

1. Introduction

The rapid advancement of technology has revolutionized the digital landscape, transforming the way governments, organizations, and individuals operate. However, this technological progress has also created new vulnerabilities, giving rise to sophisticated cybercrimes such as ransomware attacks, data breaches, identity theft, and advanced persistent threats (APTs). These malicious activities exploit the interconnected and dynamic nature of modern digital ecosystems, posing severe challenges to cybersecurity and law enforcement agencies [1]. Addressing these threats requires specialized and systematic approaches, making digital forensics a critical discipline for uncovering, preserving, and analyzing electronic evidence.

Among the diverse branches of digital forensics, memory forensics and digital artifact analysis have emerged as vital methodologies for investigating complex cyber incidents [2]. Memory forensics focuses on examining a system's volatile memory (RAM) to uncover

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

evidence related to active processes, network connections, encryption keys, and traces of malicious activity that may not be present in persistent storage. Conversely, digital artifact analysis involves studying remnants of user activity—such as browser histories, log files, and metadata—to reconstruct timelines, identify user actions, and associate evidence with specific threat actors or behaviors [3].

The significance of memory forensics lies in its ability to extract volatile evidence that disappears upon system shutdown. This transient data often holds crucial insights into live attacks, fileless malware, and stealthy intrusions that bypass conventional disk-based investigations [4]. Similarly, analyzing digital artifacts provides contextual depth to forensic examinations, helping investigators piece together fragmented evidence and understand the full scope of cyber incidents. Together, these approaches offer a more comprehensive perspective on digital crimes, bridging the gap between live system analysis and post-event investigation.

However, modern computing environments have introduced new challenges for forensic investigators. Security mechanisms such as encryption, memory wiping, secure boot, and anti-forensic techniques—though vital for user privacy—make the retrieval of key evidence increasingly difficult [5]. Cybercriminals further complicate the process through obfuscation, anti-debugging, and evasion mechanisms designed to conceal malicious activity. As a result, traditional forensic tools and static methodologies often fall short when dealing with sophisticated, real-time cyberattacks.

To overcome these obstacles, recent research emphasizes the integration of automation and open-source technologies in forensic investigations. Python-based automation scripts and specialized forensic tools enhance the efficiency of data acquisition, anomaly detection, and artifact recovery, enabling investigators to process large datasets with greater accuracy and speed. This automation-driven approach minimizes manual effort while ensuring consistent and repeatable forensic workflows, a key requirement for legal admissibility and operational scalability.

In response to the growing complexity of cyber threats, this research aims to develop an improved framework for memory forensics and digital artifact analysis. The proposed approach focuses on advanced data acquisition, artifact reconstruction, and real-time forensic capabilities to address the limitations of existing methods. By leveraging automation and innovative analysis techniques, the study enhances the reliability, precision, and timeliness of cybercrime investigations. Ultimately, this work contributes to strengthening digital forensic practices and equipping investigators with robust tools to combat the evolving landscape of cyber threats.

2. Literature Survey

Digital forensics has witnessed rapid advancement in response to the growing complexity of cyber threats and the diversification of computing environments. Researchers have increasingly focused on developing specialized frameworks and methodologies for effective evidence acquisition, analysis, and preservation. This section reviews key contributions from

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

prior studies, emphasizing their findings, performance evaluations, and identified research gaps relevant to memory forensics and digital artifact analysis.

The study in [6] proposed an enhanced digital forensic framework designed for detecting and investigating Cross-Site Scripting (XSS) attacks within network traffic. Their work emphasized the necessity of adaptable forensic models tailored to specific cybercrime types. Although the framework demonstrated strong detection capability in network-based intrusions, its applicability was limited to certain categories of attacks, highlighting the need for more generalized forensic approaches.

In [7], the authors addressed challenges in cloud-based investigations by introducing the Cloud Forensic Investigation Model (CFIM), which operates under a Forensic-as-a-Service (FaaS) paradigm. This model effectively supported distributed and dynamic cloud environments, offering scalability and efficiency in forensic processes. However, handling the heterogeneity of cloud architectures and ensuring chain-of-custody compliance remain ongoing challenges.

A Secure Storage Model for Digital Forensic Readiness was introduced in [8], emphasizing encryption, integrity verification, and organizational preparedness for digital investigations. The model strengthened the chain of custody and ensured data soundness, yet its widespread organizational adoption is still limited. Similarly, the study in [9] investigated forensic procedures for compromised systems, including infected disks and volatile memory, revealing the pressing need for improved tools to analyze and report findings in ransomware and sophisticated malware cases.

Further, [10] provided a comprehensive review of existing cyber forensic tools, identifying inconsistencies in tool performance and cross-platform reliability. The study underscored the necessity of developing tools that maintain accuracy and stability across diverse operating systems and digital environments. [11] expanded on the concept of proactive forensics, suggesting that keystroke logging and hashing in cloud systems can enhance forensic readiness and rapid response to cyber incidents, though it raises ethical and privacy concerns.

A notable advancement was the Blockchain Cloud Forensic Logging (BCFL) framework proposed in [12], which utilized distributed ledger technology to ensure log integrity and establish a verifiable chain of custody. The BCFL system demonstrated improved admissibility and reliability of digital evidence but required further validation across heterogeneous cloud platforms. Similarly, [13] explored cutting-edge methods for remote digital forensic investigations, focusing on memory and live analysis. Their research highlighted the role of automated feature extraction and real-time evidence acquisition to manage distributed datasets effectively.

In [14], browser forensics was examined in the context of cloud computing, addressing challenges in recovering deleted or modified browsing data caused by malicious insiders. The study recommended authentication-driven validation techniques for ensuring evidence reliability. Complementarily, [15] analyzed forensic methods across multiple operating systems to recover web browser artifacts, while [16] evaluated forensic recovery and privacy

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

mechanisms within the Tor Browser on Windows and Android platforms, highlighting trade-offs between evidence accessibility and user anonymity.

Finally, [17] proposed the hystck framework, a synthetic dataset generation system that supports reproducible testing of forensic tools. By simulating realistic human-computer interactions, the framework enables ground truth validation of forensic methods, though future work should extend its capability to accommodate more complex and diverse attack scenarios.

Overall, as mentioned in Table 1, existing research demonstrates substantial progress in specialized forensic frameworks, automation, and cloud forensics. However, limitations persist in evidence recovery from volatile memory, artifact consistency across platforms, and forensic readiness for evolving attack vectors. This research addresses these gaps by proposing an automated, memory-focused, and artifact-driven forensic framework that enhances efficiency, scalability, and legal admissibility in modern cyber investigations.

Table 1: Summary of Key Studies in Digital Forensics

Research Study	Key Findings	Performance Analysis	Research Gap
[6]	Developed a framework for forensic investigation of XSS attacks.	Evaluated using network traffic analysis to detect intrusions.	Limited applicability to diverse cybercrime scenarios.
[7]	Introduced a Cloud Forensic Investigation Model (CFIM) supporting Forensic as a Service (FaaS).	Demonstrated effectiveness in cloud environments through case studies.	Challenges in handling dynamic and distributed cloud architectures.
[8]	Proposed a secure storage model integrating encryption and integrity verification for forensic readiness.	Assessed the security and forensic soundness of data storage.	Need for widespread implementation and organizational acceptance.
[9]	Detailed methodologies for digital forensics on infected disks and memory.	Tested with various malware, including ransomware, in controlled environments.	Improved tools required for efficient analysis and reporting.
[10]	Reviewed cyber forensic tools, highlighting mechanism challenges and emerging issues.	Evaluated tool performance across different operating systems.	Gaps in tool reliability and performance consistency.

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[11]	Explored proactive forensics through cloud-based keystroke logging and hashing.	Performance monitored in simulated cloud environments.	Ethical and privacy implications of proactive forensic readiness.
[12]	Designed a Blockchain Cloud Forensic Logging (BCFL) framework for log integrity and evidence management.	Case study showed improved admissibility and evidence integrity.	Scalability and adaptability to various cloud platforms.
[13]	Investigated remote forensic tools emphasizing live and memory analysis.	Focused on feature extraction and performance evaluation.	Integration and efficiency across distributed databases.
[14]	Studied browser forensics post-deletion of browsing data in cloud contexts.	Validated using simulated virtual environments.	Need for more advanced recovery tools for deleted browser data.
[15]	Proposed enhanced browser evidence collection across multiple operating systems.	Evaluated recovery of diverse browser data types.	Necessity to handle varied browser storage mechanisms.
[16]	Conducted forensic analysis of Tor Browser on Windows 10 and Android 10.	Assessed artifact recovery and privacy protection.	Methods needed to improve recovery without compromising privacy.
[17]	Introduced hystck framework for synthetic forensic dataset generation and validation.	Tested by simulating real-world user and network interactions.	Requires expansion to complex simulations and real-world cases.

3. Methodology

Despite notable advancements in cybercrime detection, several critical research gaps remain. Most existing studies focus on specific types of cybercrimes or isolated forensic methods, resulting in a fragmented understanding of the broader digital forensics domain. The rapid evolution of cyber threats and technological advancements further challenges the adaptability and effectiveness of forensic methodologies. Additionally, the lack of standardized procedures across jurisdictions limits the global applicability and consistency of digital forensic practices.

This research addresses these limitations by proposing a comprehensive and adaptive framework for cybercrime detection that leverages digital forensic artifacts to enhance investigative accuracy, reliability, and efficiency. The framework integrates multiple forensic

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

techniques, automated tools, and structured procedures to enable systematic evidence collection and analysis. Figure 1 illustrates the proposed Digital Artifact Collection Framework, which outlines the sequential process for acquiring, analyzing, and presenting forensic evidence.

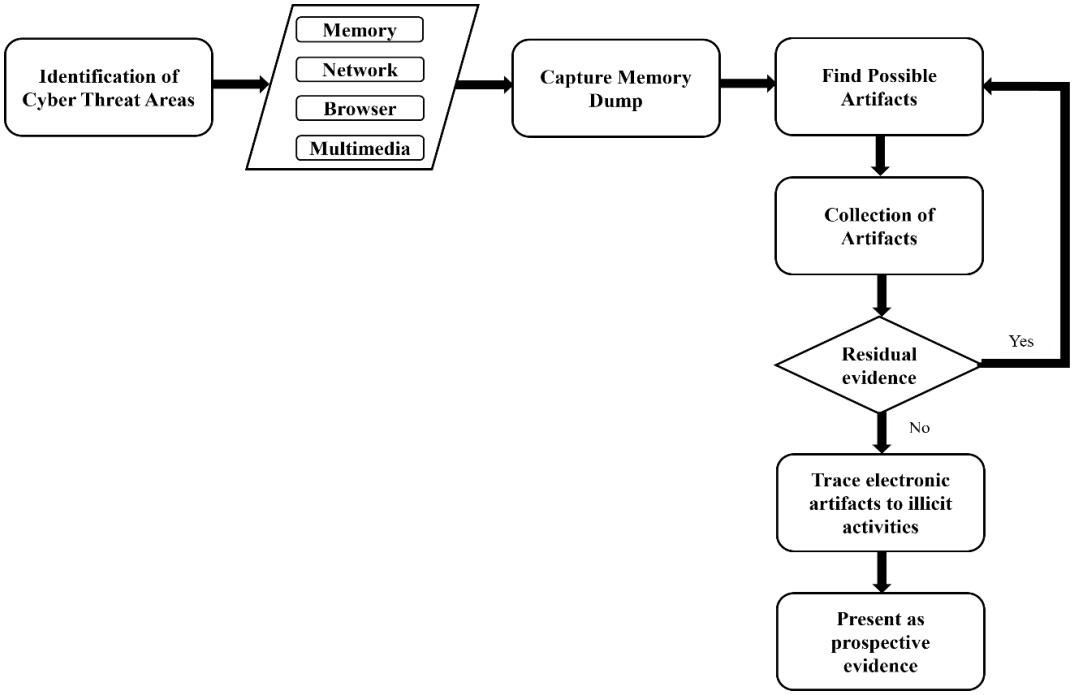

Figure 1: Proposed Digital Artifacts Collection Framework

The proposed artifacts collection framework shown in Figure 1 begins with the systematic identification of cyber threat areas across the target system, focusing on potential sources of compromise such as malware infections, unauthorized access points, suspicious user activities, or signs of data breaches. This initial step ensures that investigators concentrate their efforts on the most vulnerable and high-risk components, enabling a more efficient and targeted forensic examination. Following this, a complete memory dump of the system's volatile memory (RAM) is captured to preserve the live operational state of the machine. This snapshot contains invaluable information such as active processes, open network connections, running services, encryption keys, and other transient data that would otherwise be lost once the system is powered off. The captured memory and associated system data are then thoroughly analyzed to identify potential forensic artifacts, including suspicious executables, anomalous process behaviors, irregular registry changes, malicious scripts, hidden threads, or unusual network traffic patterns. Once these artifacts are detected, they are extracted in a systematic and controlled manner, ensuring that data integrity is maintained and that a clear chain of custody is established for each piece of evidence. Proper documentation accompanies this process to support the legal admissibility of the collected information. After primary extraction, residual or leftover evidence within the system is examined to uncover supplementary data that may provide additional context or reinforce the initial findings, ensuring that the forensic analysis is complete and comprehensive. The recovered artifacts are then correlated with known malicious activities or mapped to specific stages of the attack

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

lifecycle, enabling investigators to reconstruct how the intrusion occurred, determine the attack vector, and attribute actions to the responsible threat actors. Finally, all evidence, analytical findings, correlation results, and procedural documentation are compiled into a detailed and structured forensic report. This report is prepared with legal standards in mind to ensure admissibility in court and serves as an essential resource for supporting prosecutorial actions and strengthening the overall cybercrime investigation.

4. Results and Discussion

The forensic analysis of activity artifacts across multiple operating systems—Tails, Whonix, Mofo Linux, Windows, and BlackArch—in both live and dead system states revealed significant differences in the recoverability and persistence of digital evidence.

4.1 Comparative Artifact Analysis

As shown in Table 2, URL traces were the most consistently retrievable artifacts across all operating systems in the live state and in all systems except Tails in the dead state. This indicates that browsing activity leaves detectable traces in most environments, even after shutdown, whereas Tails effectively prevents post-mortem URL recovery due to its privacy-focused design.

Table 2: Live Vs Dead Forensic Artifacts

Activity Artifacts	Tails		Whonix		Mofo Linux		Windows		BlackArch	
	Live	Dead	Live	Dead	Live	Dead	Live	Dead	Live	Dead
URL	✓	X	✓	✓	✓	✓	✓	✓	✓	✓
Passwords	X	X	X	X	X	X	✓	X	✓	X
Social Searching	X	X	X	X	✓	X	✓	X	✓	X
Downloads	X	X	✓	✓	✓	✓	✓	✓	✓	✓
IP Address	X	X	✓	✓	✓	✓	✓	✓	✓	✓
Phone Numbers	X	X	X	X	X	X	X	X	X	X
Commands	X	X	X	X	✓	X	✓	X	✓	X

Password artifacts were found only in the live state of Windows and BlackArch, suggesting that these systems temporarily store credential data in volatile memory during active sessions. In contrast, Tails, Whonix, and Mofo Linux displayed no recoverable password traces, reflecting stronger in-memory data protection mechanisms.

Social searching activities were detected in the live states of Mofo Linux, Windows, and BlackArch, but were completely absent in the dead states across all systems. This highlights the transient nature of such data and its dependence on active memory processes.

Received: August 15, 2025

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Download activities were consistently recorded across all systems and both states, implying that downloaded files generate persistent traces within the file system and volatile memory, making them key indicators during forensic investigations.

IP address artifacts were identifiable in all systems except Tails, in both live and dead states, emphasizing that most systems inadvertently retain network-related information that can be exploited for attribution or timeline reconstruction.

Phone number artifacts were not detected in any operating system or state, indicating robust privacy and minimal retention of personal contact data.

Command execution traces were visible only in the live states of Mofo Linux, Windows, and BlackArch, showing that command-line activities are typically lost upon shutdown and are challenging to recover post-mortem.

4.2 Operating System-Level Findings

From Table 3, it is evident that Tails OS demonstrated the highest resistance to forensic recovery—no meaningful artifacts were found in either live or dead states, confirming its strong anonymity and anti-forensic architecture.

Table 3: OS vs Activity wise Artifacts

Operating System	**Live RAM Artifacts**	**Dead RAM Artifacts**
Tails	No artifacts found only junk data is there.	No artifacts found.
Whonix	IP, Mobile Number, plain URLs and onion URLs, Downloaded files	IP, Downloaded files, URLs
Mofo Linux	IP, social searching, downloaded files, plain URLs and onion URLs, Terminal Commands	IP, Downloaded files, URLs
Windows	URL, Password, Social Searching, Downloads, IP Address, Commands	URL, Downloads, IP Address
BlackArch	URL, Password, Social Searching, Downloads, IP Address, Commands	URL, Password, Downloads, IP Address, Commands

Whonix and Mofo Linux revealed a moderate level of traceability, with recoverable IP addresses, URLs, and downloaded file information in both states. Mofo Linux also exhibited traces of terminal commands and social search activity during live capture, signifying partial memory retention of user actions.

Windows and BlackArch proved to be the most artifact-rich environments. Both systems exposed multiple traces including URLs, passwords, download records, IP addresses, and executed commands in live memory. BlackArch also retained certain password and command

International Journal of Applied Mathematics
Volume 38 No. 12s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

traces even in the dead state, indicating weaker data sanitization mechanisms after shutdown.

4.3 Discussion

The comparative forensic analysis highlights that the extent of artifact recoverability is highly dependent on the operating system architecture, security protocols, and memory management mechanisms.

• Tails achieved complete anti-forensic resilience, offering no usable evidence post-capture.

• Whonix and Mofo Linux provided limited recoverable data, balancing privacy with usability.

• Windows and BlackArch retained the highest number of forensic artifacts, making them more transparent but also more vulnerable in forensic investigations.

Overall, the findings demonstrate that privacy-centric operating systems like Tails and Whonix effectively minimize forensic traceability, while general-purpose and penetration-testing systems like Windows and BlackArch maintain extensive memory and disk-level traces.

This comparative insight can assist forensic analysts, cybersecurity researchers, and law enforcement in selecting appropriate forensic tools and prioritizing evidence acquisition strategies based on the target environment.

4.4 Comparison of time for analysis in different operating systems

The Figure 2 is a line graph comparing the time taken for two types of analysis—Live State Analysis and Dead State Analysis—across five different operating systems: Tails, Whonix, Mofo Linux, Windows, and BlackArch. The x-axis represents the operating systems, while the y-axis denotes the time taken (in minutes) for the analysis. Two lines represent the data:

- The blue line corresponds to Live State Analysis.
- The orange line corresponds to Dead State Analysis.

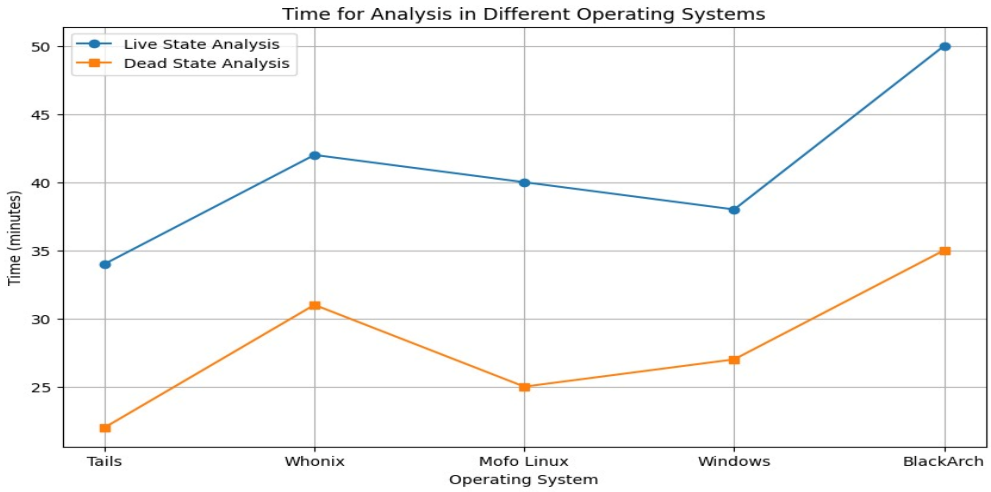

Figure 2: Time for analysis in different operating systems

Received: August 15, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Following are key observation derived from above Figure 2.

• For Live State Analysis, the time increases steadily across the operating systems, reaching a peak with BlackArch at 50 minutes.

• Dead State Analysis generally requires less time compared to Live State Analysis across all operating systems, with the time ranging between 25 and 35 minutes.

• Tails shows the smallest difference between the two types of analysis, while BlackArch exhibits the largest difference.

• Whonix shows a notable peak in Dead State Analysis time at 35 minutes, followed by a decline for Mofo Linux.

Conclusion and Future work

This research introduced a structured framework for the systematic collection and analysis of digital forensic artifacts to enhance cybercrime detection. The comparative analysis across Tails, Whonix, Mofo Linux, Windows, and BlackArch revealed distinct variations in artifact persistence and forensic traceability. Tails exhibited strong privacy and anti-forensic measures, while Windows and BlackArch retained the widest range of recoverable artifacts, including URLs, passwords, and network data. These findings highlight how system design and security configurations influence forensic visibility.

The proposed framework ensures reliable evidence acquisition, preservation, and analysis, supporting both technical investigations and legal admissibility. Overall, this study contributes a practical and adaptable approach for digital forensic investigations across diverse environments. Future work will focus on integrating AI-driven forensic intelligence to automate artifact correlation, strengthen real-time detection, and enhance accuracy in cybercrime attribution.

References

[1] J. Choi, J. Yu, S. Hyun, and H. Kim, Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. *Digital Investigation*, vol. 28, pp. S50–S59, Apr. 2019, doi: 10.1016/j.diin.2019.01.011.

[2] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, A review of mobile forensic investigation process models. *IEEE Access*, vol. 8, pp. 173359–173375, 2020, doi: 10.1109/ACCESS.2020.3014615.

[3] Y. Cheng, X. Fu, X. Du, B. Luo, and M. Guizani, A lightweight live memory forensic approach based on hardware virtualization. *Information Sciences*, vol. 379, pp. 23–41, Feb. 2017, doi: 10.1016/j.ins.2016.07.019.

[4] N. Usman *et al.*, Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. *Future Generation Computer Systems*, vol. 118, pp. 124–141, May 2021, doi: 10.1016/j.future.2021.01.004.

[5] A. Pichan, M. Lazarescu, and S. T. Soh, Cloud forensics: Technical challenges, solutions

Received: August 15, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and comparative analysis. *Digital Investigation*, vol. 13, pp. 38–57, Jun. 2015, doi: 10.1016/j.diin.2015.03.002.

[6] S. Kumar, S. Pathak, and J. Singh, An enhanced digital forensic investigation framework for XSS attack. *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1009–1018, May 2022, doi: 10.1080/09720529.2022.2072424.

[7] E. E. D. Hemdan and D. H. Manjaiah, An efficient digital forensic model for cybercrimes investigation in cloud computing. *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 14255–14282, Apr. 2021, doi: 10.1007/s11042-020-10358-x.

[8] A. Singh, R. A. Ikuesan, and H. Venter, Secure storage model for digital forensic readiness. *IEEE Access*, vol. 10, pp. 19469–19480, 2022, doi: 10.1109/ACCESS.2022.3151403.

[9] A. Al-Sabaawi, Digital forensics for infected computer disk and memory: Acquire, analyse, and report. in *Proc. IEEE Asia-Pacific Conf. Computer Science and Data Engineering (CSDE)*, Dec. 2020, doi: 10.1109/CSDE50874.2020.9411614.

[10] V. Fernando, Cyber forensics tools: A review on mechanism and emerging challenges. in *Proc. 2021 11th IFIP Int. Conf. New Technologies, Mobility and Security (NTMS)*, Apr. 2021, doi: 10.1109/NTMS49979.2021.9432641.

[11] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, Proactive forensics: Keystroke logging from the cloud as potential digital evidence for forensic readiness purposes. in *Proc. IEEE Int. Conf. Informatics, IoT, and Enabling Technologies (ICIoT)*, Feb. 2020, pp. 200–205, doi: 10.1109/ICIOT48696.2020.9089494.

[12] K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem. *Future Generation Computer Systems*, vol. 122, pp. 1–13, Sep. 2021, doi: 10.1016/j.future.2021.03.001.

[13] K. U. Maheswari and G. Shobana, The state of the art tools and techniques for remote digital forensic investigations. in *Proc. 2021 3rd Int. Conf. Signal Processing and Communication (ICSPC)*, May 2021, pp. 464–468, doi: 10.1109/ICSPC51351.2021.9451718.

[14] B. H. AlOwaimer and S. Mishra, Analysis of web browser for digital forensics investigation. *International Journal of Computer Applications in Technology*, vol. 65, no. 2, pp. 160–172, 2021, doi: 10.1504/IJCAT.2021.114987.

[15] K. V. P. S. G. Majeti, Y. V. L. S. Sundar, S. S. Ulichi, S. N. Mohanty, and S. SV, Digital forensic advanced evidence collection and analysis of web browser activity. *EAI Endorsed Transactions on Scalable Information Systems*, vol. 10, no. 5, pp. 1–8, Jun. 2023, doi: 10.4108/eetsis.3357.

[16] M. R. Arshad, M. Hussain, H. Tahir, S. Qadir, F. I. Ahmed Memon, and Y. Javed, Forensic analysis of Tor browser on Windows 10 and Android 10 operating systems. *IEEE*

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Access, vol. 9, pp. 141273–141294, 2021, doi: 10.1109/ACCESS.2021.3119724.

[17] T. Göbel, T. Schäfer, J. Hachenberger, J. Türr, and H. Baier, A novel approach for generating synthetic datasets for digital forensics. *IFIP Advances in Information and Communication Technology*, vol. 589, pp. 73–93, 2020, doi: 10.1007/978-3-030-56223-6_5.

[18] R. Nelson, A. Shukla, and C. Smith, Web browser forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle. *Studies in Big Data*, vol. 61, pp. 219–241, 2020, doi: 10.1007/978-3-030-23547-5_12.

[19] H. Kim, I. S. Kim, and K. Kim, AIBFT: Artificial intelligence browser forensic toolkit. *Forensic Science International: Digital Investigation*, vol. 36, p. 301091, Mar. 2021, doi: 10.1016/j.fsidi.2020.301091.

[20] F. Iqbal, Z. Khalid, A. Marrington, B. Shah, and P. C. K. Hung, Forensic investigation of Google Meet for memory and browser artifacts. *Forensic Science International: Digital Investigation*, vol. 43, p. 301448, Sep. 2022, doi: 10.1016/j.fsidi.2022.301448.

Received: August 15, 2025