Sienna (E -ISSN: 2745-9861 | P-ISSN: 2745-987X)
https://jurnal.umko.ac.id/index.php/sienna
DOI: https://doi.org/10.47637/sienna.v7i1.2377

Blockchain-Based Preservation Framework for Network Forensic Evidence Integrity

Mirza Sutrisno[1]*, Sunardi[2], Rusydi Umar[3]
2536083037@webmail.uad.ac.id[1], sunardi@mti.uad.ac.id[2], rusydi@mti.uad.ac.id[3]
[1,2,3]Universitas Ahmad Dahlan, Indonesia
[1]Universitas Muhammadiyah Jakarta, Indonesia
*Correspondence: mirza.sutrisno@umj.ac.id

Abstract

Network forensic investigations rely heavily on the integrity and traceability of Packet Capture (PCAP) files as primary digital evidence. Digital Forensic Research Workshop (DFRWS) implementations commonly employ centralized preservation mechanisms that remain vulnerable to unauthorized modification and provide limited provenance transparency. To address these limitations, this study proposes a blockchain-based preservation framework integrated into the preservation phase of the DFRWS model. The framework combines SHA-256 cryptographic hashing for integrity verification, blockchain-based provenance logging, and distributed ledger validation while maintaining off-chain evidence storage. Unlike many existing blockchain-based forensic frameworks that primarily emphasize provenance recording and chain-of-custody management, this study evaluates evidence preservation through an integrated validation approach consisting of controlled tampering simulation, cryptographic sensitivity analysis, and preservation latency measurement. Experimental evaluation using PCAP datasets representing attack and baseline traffic conditions demonstrated that unauthorized evidence modification was successfully detected through hash inconsistencies. Avalanche Effect analysis produced a value of 50.39%, confirming the strong cryptographic sensitivity of the SHA-256 mechanism to minimal data alteration. While SHA-256 enables reliable tampering detection, the integrated blockchain architecture provides tamper-resistant provenance recording, chain-of-custody traceability, and distributed verification of evidence integrity. The framework achieved an average preservation latency of 2.057 seconds within the experimental environment, providing preliminary evidence of feasibility for blockchain-assisted forensic logging under controlled conditions. Although no direct comparison with alternative preservation approaches was conducted, the findings provide a proof-of-concept validation and contribute empirical evidence regarding the potential of blockchain-supported provenance management to enhance trustworthiness and integrity assurance in network forensic workflows.

Article Status:
Accepted: 15-05-2026
Revised: 29-05-2026
Accepted: 02-06-2026

Keywords:
Blockchain;
Chain-of-Custody;
DFRWS;
Data Integrity;
Network Forensics

INTRODUCTION

Network forensics has become an essential component of modern digital investigations due to the exponential growth of cyber threats and the increasing complexity of network infrastructures. The rapid expansion of distributed systems, cloud environments, and Internet of Things (IoT) ecosystems has significantly amplified the volume and heterogeneity of network traffic, thereby increasing the difficulty of forensic evidence acquisition, preservation, and validation (Arif et al., 2025; Atlam et al., 2024). In Indonesia, this challenge is further reflected in the national cybersecurity landscape, where large-scale cyber incidents and traffic anomalies continue to rise, emphasizing the urgent need for reliable and trustworthy forensic mechanisms (Badan Siber dan Sandi Negara, 2024). A visual representation of Indonesia's Cybersecurity Landscape is provided in Figure 1 below.

Figure 1. Indonesia's Cybersecurity Landscape

Within this context, Packet Capture (PCAP) files play a central role as primary forensic artifacts, as they preserve detailed packet-level communication, including timestamps, payloads, and metadata required for reconstructing cyber incidents (Casey, 2020). Prior studies also emphasize the importance of structured investigation processes and systematic evidence handling in complex digital environments (Sunardi et al., 2019). Despite their evidentiary importance, PCAP files remain highly vulnerable to anti-forensic manipulation. Various forms of tampering, such as payload modification, timestamp alteration, replay injection, and metadata manipulation, can significantly distort forensic interpretation and compromise legal admissibility. These vulnerabilities are largely attributed to the reliance on centralized preservation mechanisms, which introduce single points of failure and enable unauthorized modification without transparent traceability (Chen, 2025; Riadi et al., 2022). In addition, the increasing sophistication of

cyberattacks, including multi-layer exploitation techniques such as Cross-Site Scripting (XSS), further complicates the integrity assurance of digital evidence, as conventional security mechanisms often fail to provide comprehensive protection across diverse attack vectors (Hartono & Sriyanto, 2022). Moreover, traditional chain-of-custody (CoC) practices often depend on manual documentation and centralized logging systems, which are prone to inconsistency, insider threats, and lack of verifiable auditability (Atlam et al., 2024; Wang et al., 2025). As a result, ensuring the integrity, transparency, and trustworthiness of digital evidence remains a fundamental challenge in contemporary network forensic investigations.

To address these limitations, blockchain technology has emerged as a promising approach for enhancing digital forensic processes. Blockchain provides a decentralized and immutable ledger that enables secure recording of evidence provenance, ensuring that any modification can be detected and verified across distributed nodes (Casino et al., 2019; Zheng et al., 2017). In particular, blockchain-based solutions have been widely explored for strengthening chain-of-custody management by enabling transparent, tamper-resistant, and verifiable tracking of evidence throughout its lifecycle (Lone & Mir, 2019; Machhi et al., 2024)

In cloud-based forensic infrastructures, the integration of distributed ledger technology has been shown to improve evidence management by eliminating reliance on centralized authorities and enabling decentralized validation processes (Al-Khateeb et al., 2019). Furthermore, within network forensic workflows, cryptographic hashing combined with blockchain recording mechanisms has been emphasized as a key approach to ensuring evidence integrity and detecting unauthorized modifications (Riadi et al., 2022). More broadly, recent systematic reviews confirm that blockchain technology offers substantial advantages in digital forensics, particularly in enhancing immutability, transparency, and distributed trust, although challenges related to scalability, performance, and implementation complexity remain significant (Atlam et al., 2024; Sunny et al., 2022).

Despite the growing adoption of blockchain technology in digital forensics, several important limitations remain in existing studies. First, many blockchain-based forensic frameworks, including ProvChain and Hyperledger-based chain-of-custody models, primarily focus on provenance architecture and evidence traceability. While these studies demonstrate the potential of distributed ledgers for forensic record management, they provide limited empirical validation regarding how effectively preserved evidence can resist anti-forensic manipulation under controlled experimental conditions. Second, previous studies generally evaluate blockchain functionality from a provenance or architectural perspective without examining the cryptographic sensitivity of the integrity verification mechanism itself. Third, operational performance aspects remain underexplored because relatively few studies report preservation latency measurements obtained from end-to-end forensic preservation workflows (Dorri et al., 2017; Wang et al., 2025).

Accordingly, the contribution of this study is not merely the adoption of blockchain for chain-of-custody management, but the integration of blockchain-based provenance preservation into the DFRWS preservation phase combined with three complementary validation perspectives: controlled tampering detection, Avalanche Effect-based cryptographic sensitivity analysis, and preservation latency measurement. Unlike ProvChain and most Hyperledger-based forensic preservation models, which primarily focus on provenance recording and chain-of-custody management, the proposed framework incorporates empirical validation of evidence integrity through controlled tampering experiments, evaluates the cryptographic sensitivity of the integrity

mechanism using Avalanche Effect analysis, and reports preservation latency obtained from an end-to-end preservation workflow. This combination provides an experimentally validated proof-of-concept that extends beyond architectural design and offers empirical evidence regarding blockchain-assisted network forensic workflows.

METHODS

Types of research

This study employed an experimental quantitative approach to evaluate the effectiveness of blockchain-based preservation mechanisms integrated into the Digital Forensic Research Workshop (DFRWS) framework. The proposed framework integrates blockchain technology into the preservation phase of the DFRWS model by combining SHA-256 cryptographic hashing, blockchain-based provenance recording, and distributed ledger verification mechanisms. This integration was intended to improve evidence immutability, chain-of-custody transparency, and resistance against anti-forensic manipulation.

The research workflow consisted of several stages, including network traffic acquisition, evidence hashing, blockchain recording, tampering simulation, hash verification, Avalanche Effect analysis, and performance evaluation through latency measurement. Experimental validation was performed using Packet Capture (PCAP) datasets representing both normal and attack-related traffic conditions.

Technical Implementation Environment

The framework was implemented using a private blockchain simulation environment deployed on Ubuntu Linux 22.04 LTS. The blockchain layer consisted of three logical node roles: Validator Node, Forensic Node, and Archive Node. The Validator Node was responsible for transaction validation and ledger synchronization. The Forensic Node performed evidence registration, hash generation, and verification requests, and the Archive Node maintained replicated provenance records to support distributed verification. Within this architecture, each preservation transaction followed a predefined workflow where an acquired PCAP file was processed using SHA-256 hashing. The generated hash value, timestamp, evidence identifier, and investigator identifier were encapsulated into a blockchain transaction to be validated and appended to the distributed ledger. Under this hybrid storage scheme, original PCAP evidence remained stored off-chain in a secure local directory, while metadata and integrity-related records were preserved on-chain.

Preservation transactions generated by the Forensic Node were validated by the Validator Node before being replicated to the Archive Node, ensuring consistent provenance records across the simulated blockchain environment. The software environment utilized Jupyter Notebook with Python 3.12 for automation and hash generation, Wireshark and tcpdump for network traffic capture, and a custom Python-based private blockchain simulator. Experimental execution for all three logical nodes was conducted on a workstation powered by an Intel Core Ultra 5 processor with 16 GB RAM and 512 GB SSD storage, representing a localized simulation environment designed for controlled performance and sensitivity evaluation.

Digital Forensic Research Workshop (DFRWS)

The proposed hybrid blockchain architecture was integrated into the Digital Forensic Research Workshop (DFRWS) framework to strengthen forensic evidence preservation, improve chain-of-custody transparency, and support distributed integrity verification during network forensic investigations. The implementation process was conducted through several interconnected investigation phases, as illustrated in Figure 2.

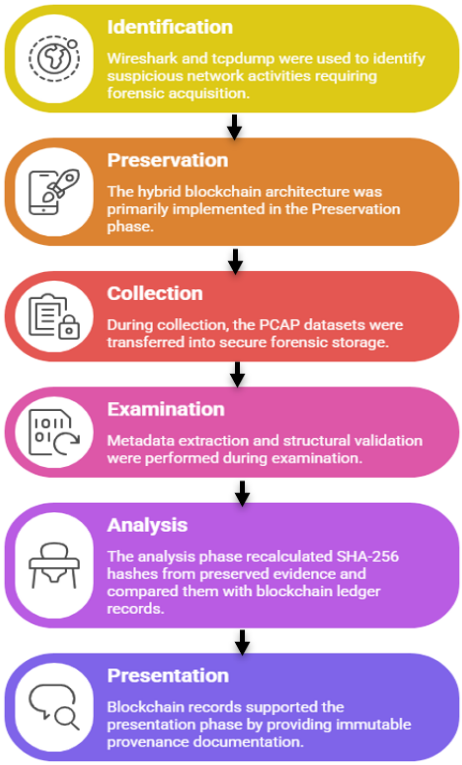

Figure 2. Digital Forensic Research Workshop (DFRWS) Framework

1. Identification

The identification phase focused on detecting suspicious network activities requiring forensic acquisition. Wireshark and tcpdump were utilized to monitor and identify anomalous traffic patterns within the simulated network environment. At this stage, blockchain mechanisms were not directly involved because the primary objective was incident recognition and traffic identification prior to forensic preservation.

2. Preservation

The preservation phase represented the core implementation stage of the proposed blockchain-based framework. After acquisition, each PCAP file was processed using the SHA-256 cryptographic hashing algorithm to generate unique hash values representing evidence integrity. The original PCAP files were stored in off-chain forensic storage, while hash values, timestamps, investigator identifiers, and provenance records were recorded as blockchain transactions within a private blockchain environment. This hybrid storage architecture was designed to maintain storage efficiency while ensuring immutable chain-of-custody preservation and distributed verification. Blockchain integration in this phase was designed to support forensic accountability through immutable provenance recording and distributed verification.

3. Collection

During the collection phase, acquired PCAP datasets were transferred into secure forensic repositories for further investigation. Blockchain technology supported this process by recording evidence transfer activities and preserving provenance continuity through distributed ledger transactions. Every collection event generated a verifiable transaction record to ensure traceability throughout the forensic lifecycle.

4. Examination

The examination phase involved metadata extraction, packet structure validation, and integrity inspection of the acquired evidence. Relevant metadata, including timestamps, source and destination addresses, communication protocols, and payload structures, were analyzed to support forensic interpretation. To evaluate the robustness of the proposed framework against anti-forensic manipulation, controlled tampering simulations were performed by modifying one byte within selected PCAP files. Blockchain records and previously generated hash values were subsequently used as integrity references to detect evidence alteration.

5. Analysis

The analysis phase recalculated SHA-256 hash values from the preserved evidence and compared them with hash records stored within the blockchain ledger. Any mismatch between recalculated and recorded hash values indicated integrity violations, tampering attempts, or inconsistencies within the chain-of-custody process. Avalanche Effect analysis was used as a supplementary validation mechanism to evaluate the sensitivity of the SHA-256 hashing algorithm against minimal evidence modification prior to blockchain preservation. A higher Avalanche Effect value indicated stronger sensitivity of the hashing mechanism to evidence alteration.

6. Presentation

The presentation phase compiled forensic verification results, blockchain provenance records, tampering detection outcomes, Avalanche Effect measurements, and preservation latency analysis into forensic reports. Blockchain records provided immutable provenance documentation that strengthened evidence transparency and supported legal admissibility during forensic reporting and verification processes. The overall integration of blockchain into the DFRWS framework was intended to provide a more reliable, transparent, and tamper-resistant preservation mechanism for network forensic evidence management.

Data Collection

The experimental dataset used in this study consisted of ten Packet Capture (PCAP) files generated within an isolated and controlled network environment. The datasets were designed to represent both normal and malicious network activities in order to evaluate the effectiveness of the proposed blockchain-based preservation framework under different forensic conditions. Five datasets were categorized as attack traffic scenarios, while the remaining five represented baseline network traffic without malicious activities.

The attack datasets contained various simulated cyberattack activities, including unauthorized access attempts, replay packet injection, abnormal payload transmission, and protocol anomalies. These scenarios were intentionally generated to emulate realistic anti-forensic and network intrusion conditions commonly encountered in forensic investigations. In contrast,

the baseline datasets represented normal operational traffic generated from standard communication processes within the simulated network environment.

The file sizes of the datasets varied significantly depending on traffic intensity and attack complexity. Attack-related PCAP files ranged from 15.2 MB to 33.0 MB, whereas baseline traffic datasets ranged from 64.8 KB to 65.7 KB. This variation allowed the proposed framework to be evaluated under different evidence scales and traffic conditions. Detailed characteristics of the experimental datasets are presented in Table 1.

Table 1. Experimental Dataset Characteristics

No	File Name	Type	File Size
1.	Attack_run01.pcap	Attack	33.0 MB
2.	Attack_run02.pcap	Attack	27.7 MB
3.	Attack_run03.pcap	Attack	21.0 MB
4.	Attack_run04.pcap	Attack	18.7 MB
5.	Attack_run05.pcap	Attack	15.2 MB
6.	Baseline_run01.pcap	Normal	65.7 KB
7.	Baseline_run02.pcap	Normal	65.7 KB
8.	Baseline_run03.pcap	Normal	65.5 KB
9.	Baseline_run04.pcap	Normal	65.0 KB
10.	Baseline_run05.pcap	Normal	64.8 KB

The acquisition process was conducted using Wireshark and tcpdump within a Linux-based forensic environment. All datasets were stored in a local forensic repository prior to integrity preservation and blockchain recording processes. The use of controlled and reproducible datasets ensured consistency during tampering simulation and verification experiments.

Procedure

The research procedure followed the Digital Forensic Research Workshop (DFRWS) framework, which consists of six primary phases: identification, preservation, collection, examination, analysis, and presentation (Casey, 2020). Blockchain integration was incorporated into several critical stages of the framework to support evidence immutability, improve chain-of-custody transparency, and support distributed integrity verification. The process began with the identification phase, where relevant network data sources and digital artifact types were determined. Packet Capture (PCAP) files and network logs generated within the simulated environment were identified as the primary forensic evidence used in the experiment. Wireshark and tcpdump were utilized to capture suspicious network activities and generate datasets representing both baseline and attack traffic scenarios. During the preservation phase, each acquired PCAP file was processed using the SHA-256 cryptographic hashing algorithm to generate unique hash values representing evidence integrity. The original evidence files were stored within local forensic storage, while the generated hash values, timestamps, investigator identifiers, and provenance records were recorded within a private blockchain environment through blockchain transaction mechanisms. The use of SHA-256 hashing was selected due to its high reliability and widespread adoption in integrity verification systems (Stallings, 2021).

The collection phase involved systematic evidence acquisition and secure transfer into the forensic repository. Blockchain transactions were used to record evidence transfer activities, thereby maintaining provenance continuity and ensuring transparent chain-of-custody

documentation throughout the investigation lifecycle. In the examination phase, metadata extraction and structural validation were performed on the acquired PCAP files. Relevant information such as timestamps, source and destination IP addresses, communication protocols, and payload structures were analyzed to support forensic interpretation. Controlled tampering simulations were subsequently conducted by modifying one byte within selected PCAP files in order to evaluate the sensitivity of the preservation mechanism against anti-forensic manipulation techniques. The analysis phase recalculated SHA-256 hash values from the preserved evidence and compared them with the corresponding records stored within the blockchain ledger. Any discrepancy between recalculated and recorded hash values indicated integrity violations or unauthorized evidence modification. In addition, Avalanche Effect analysis was conducted to measure the cryptographic sensitivity of the hashing mechanism against minor evidence changes.

Finally, the presentation phase compiled all forensic verification results, blockchain provenance logs, tampering detection outcomes, Avalanche Effect measurements, and preservation latency analysis into comprehensive forensic reports. Blockchain-based provenance records provided immutable documentation that strengthened evidence transparency and supported legal admissibility during forensic reporting processes. To evaluate the effectiveness of the proposed framework, this study employed a one-group pretest-posttest experimental design. Initial hash values were recorded before controlled evidence modification, followed by post-manipulation verification to identify integrity discrepancies. This experimental design enabled direct evaluation of the framework's capability to detect evidence tampering and preserve forensic integrity.

Data Processing

Data processing in this study focused on evaluating both the integrity preservation capability and operational performance of the proposed blockchain-based forensic framework. The processing stage consisted of cryptographic verification, tampering sensitivity analysis, and preservation efficiency measurement. Tampering sensitivity was evaluated using Avalanche Effect (AE) analysis, which measures the percentage of changed output bits resulting from minimal modifications to the input data. In cryptographic systems, secure hash functions are expected to generate substantially different outputs even when only minor changes occur in the original input, thereby ensuring strong resistance against manipulation attempts (Stallings, 2021; Upadhyay et al., 2022). In this study, Avalanche Effect analysis was performed by comparing binary differences between the original SHA-256 hash output and the hash generated after controlled tampering simulations on the PCAP files. The Avalanche Effect value was calculated using the following equation:

$$AE = \frac{Bflipped}{Btotal} x\ 100\%$$

where *AE* represents the Avalanche Effect percentage, *Bflipped* denotes the number of changed bits between the original and modified hash outputs, and *Btotal* represents the total number of bits produced by the SHA-256 algorithm, which equals 256 bits. According to cryptographic security standards, Avalanche Effect values approaching 50% indicate strong cryptographic sensitivity and effective resistance against anti-forensic manipulation (Upadhyay et al., 2022). In addition to cryptographic sensitivity analysis, system efficiency was evaluated

through preservation latency measurement. Preservation latency refers to the cumulative processing time required to secure, validate, and record digital evidence within the blockchain-based preservation framework. This metric combines SHA-256 hashing duration and blockchain transaction validation time, adapted from distributed ledger performance evaluation approaches proposed in previous blockchain forensic and lightweight blockchain studies (Al-Khateeb et al., 2019; Dorri et al., 2017). The preservation latency was calculated using the following equation:

$$Tpreservation = Thashing + Tblockchain$$

Thashing represents the processing time required to generate SHA-256 hash values, while *Tblockchain* denotes the time required for blockchain transaction validation and ledger recording processes. This dual-processing evaluation ensured that the proposed preservation framework not only provided strong cryptographic integrity protection but also maintained operational efficiency suitable for practical network forensic investigation environments.

RESULTS AND DISCUSSION

Blockchain Preservation Implementation

The implementation of the blockchain-based preservation framework demonstrates the potential of blockchain-assisted preservation for providing provenance transparency and distributed verification through distributed ledger mechanisms. By integrating SHA-256 cryptographic hashing with blockchain-based provenance logging, the proposed framework ensures that each forensic artifact is uniquely identified and immutably recorded within a distributed ledger. This design directly addresses the fundamental limitations of centralized systems, particularly the lack of transparency and vulnerability to unauthorized modification.

The findings are consistent with previous studies emphasizing that blockchain enables tamper-resistant and verifiable chain-of-custody management through decentralized consensus mechanisms (Casino et al., 2019; Zheng et al., 2017). Furthermore, recent developments in blockchain-based forensic architectures highlight that distributed ledger integration significantly enhances accountability and traceability in digital evidence management systems, particularly in multi-stakeholder environments (Al-Khateeb et al., 2019; Atlam et al., 2024).

In comparison to prior works such as ProvChain and Hyperledger-based forensic models (Liang et al., 2017; Lone & Mir, 2019), which primarily focus on architectural design, this study contributes by providing experimental validation within the DFRWS framework. The adoption of a hybrid architecture—combining on-chain provenance records with off-chain storage—also aligns with contemporary blockchain design principles aimed at improving scalability and efficiency (Xu et al., 2019). Additionally, recent studies in digital forensic frameworks emphasize that integrating blockchain with structured forensic models can significantly strengthen evidentiary reliability and legal admissibility, particularly when supported by automated provenance tracking mechanisms (Xu et al., 2025).

Tampering Simulation and Avalanche Effect Analysis

To evaluate tampering sensitivity, a controlled modification was performed by altering one byte within the attack_run01.pcap file using a hexadecimal editor. The integrity verification process generated two SHA-256 hash outputs corresponding to the original and modified

evidence. The original evidence hash ($H_{original}$) is represented as 4606fce06b36f2d97f23478df7d5c478a1bedaa53b49ba1f0034aaf3f7dba6a3. The modified evidence hash ($H_{modified}$) is represented as 7120dd19002e34134c581619ed113b8b372f413ba2b20f81b306d3729f354f5. Both hash values were converted into binary format and compared using the XOR operation to determine the number of differing bits between the two outputs. The comparison results indicate that *Bflipped*=129 bits. Since the SHA-256 algorithm produces a fixed output length of *Btotal*=256 bits. The Avalanche Effect (*AE*) value was calculated using the following equation:

$$AE = Bflipped/\ Btotal \text{ x } 100\%$$
$$AE = \frac{129}{256} \text{x } 100\%$$
$$AE = 50.39\%$$

The tampering simulation results demonstrate that the proposed framework effectively detects even minimal evidence modification. The obtained Avalanche Effect value of 50.39% confirms the strong diffusion property of the SHA-256 hashing algorithm, where minor input changes result in substantial output differences. This characteristic is essential in forensic applications to ensure that any unauthorized modification can be reliably detected. From a theoretical perspective, this finding is consistent with cryptographic security principles, which require hash functions to exhibit high sensitivity to input variation in order to prevent collision and manipulation attacks (Upadhyay et al., 2022).

It is important to note that the Avalanche Effect reflects the cryptographic behavior of the SHA-256 hashing algorithm rather than the blockchain layer itself. The role of blockchain in the proposed framework is to preserve hash records through tamper-resistant provenance logging and to enable distributed verification of integrity assessments across participating nodes. Consequently, the Avalanche Effect result should be interpreted as evidence of the sensitivity of the hashing mechanism, while blockchain contributes to the trustworthiness and traceability of the integrity verification process.

Compared to previous studies that focus primarily on blockchain-based provenance without evaluating cryptographic robustness (Liang et al., 2017; Lone & Mir, 2019), this study provides an additional validation layer by incorporating Avalanche Effect analysis. Recent research in forensic security systems also highlights that combining cryptographic validation with distributed ledger recording significantly enhances resistance against anti-forensic techniques, which often exploit weaknesses in centralized logging mechanisms (Chen, 2025; Rani et al., 2025; Riadi et al., 2022).

Integrity Verification Analysis

Integrity verification was performed by comparing recalculated SHA-256 hash values with the corresponding hash records stored in the blockchain ledger. The verification results are summarized in Table 2.

Table 2. Integrity Verification Results

No	File Name	Verification Result
1.	Baseline_run01.pcap	Valid

2.	Baseline_run02.pcap	Valid
3.	Baseline_run03.pcap	Valid
4.	Baseline_run04.pcap	Valid
5.	Baseline_run05.pcap	Valid
6.	**Attack_run01.pcap**	**Rejected**
7.	Attack_run02.pcap	Valid
8.	Attack_run03.pcap	Valid
9.	Attack_run04.pcap	Valid
10.	Attack_run05.pcap	Valid

The integrity verification results indicate that the proposed framework consistently differentiates between valid and tampered evidence. All non-manipulated datasets were successfully verified, while the modified dataset was correctly rejected due to hash inconsistency. This outcome demonstrates that the system enforces strict integrity validation through deterministic cryptographic hashing combined with immutable blockchain records. This result can be explained by the inherent properties of hash functions, where any alteration to the input data produces a completely different output. When these hash values are stored within a blockchain ledger, they serve as immutable references that cannot be altered without detection. This mechanism significantly enhances the reliability and trustworthiness of digital evidence, which is critical for forensic investigations and legal proceedings.

Furthermore, the findings highlight an important distinction between malicious content and evidence integrity. The presence of attack traffic does not inherently compromise data integrity unless post-acquisition manipulation occurs. This observation is consistent with network forensic principles, where integrity violations are primarily associated with unauthorized modification rather than the nature of the captured data itself (Riadi et al., 2022). Similar conclusions have been reported in recent forensic studies, which emphasize the importance of preserving evidence authenticity independently from attack characteristics (Atlam et al., 2024).

Latency Analysis

To provide an initial assessment of the operational characteristics of the proposed framework, preservation latency was measured across all experimental datasets. The resulting latency values are presented in Table 3.

Table 3. Preservation Latency Analysis

No	File Name	Category	*T_hash* (s)	*T_consensus* (s)	*T_total* (s)	Final Status
1.	baseline_run01.pcap	Normal	0.040	2.012	2.052	Valid
2.	baseline_run02.pcap	Normal	0.042	2.015	2.057	Valid
3.	baseline_run03.pcap	Normal	0.041	2.010	2.051	Valid
4.	baseline_run04.pcap	Normal	0.043	2.018	2.061	Valid
5.	baseline_run05.pcap	Normal	0.039	2.011	2.050	Valid
6.	attack_run01.pcap	Attack	0.046	2.005	2.051	Rejected
7.	attack_run02.pcap	Attack	0.045	2.022	2.067	Valid
8.	attack_run03.pcap	Attack	0.044	2.016	2.060	Valid
9.	attack_run04.pcap	Attack	0.047	2.010	2.057	Valid
10.	attack_run05.pcap	Attack	0.043	2.021	2.064	Valid

The experimental results show that the average preservation latency across all datasets was 2.057 seconds. The hashing process contributed only a small fraction of the total processing time, ranging from 0.039 to 0.047 seconds, whereas the blockchain consensus process accounted for the majority of the latency, with an average duration of approximately 2.01 seconds. Similar latency values were observed across both baseline and attack datasets, indicating that the traffic characteristics did not substantially affect processing time within the experimental environment.

Although these results indicate that the proposed preservation workflow can be completed within approximately two seconds per file, the findings should be interpreted with caution. The present study did not include a direct comparison with conventional non-blockchain preservation mechanisms or alternative blockchain implementations. Consequently, the relative performance impact introduced by blockchain integration cannot be conclusively determined.

Therefore, the reported latency values should be interpreted as preliminary evidence of feasibility within a controlled experimental environment rather than as definitive indicators of operational performance in real-world forensic deployments. Additional evaluations involving larger datasets, higher transaction volumes, and comparative benchmarking against alternative preservation approaches are required to provide a more comprehensive assessment of scalability and efficiency.

Nevertheless, the consistency of the observed latency values across all experimental scenarios suggests that the proposed framework can maintain stable processing behaviour under the tested conditions. This characteristic is important for forensic preservation workflows, where predictable evidence handling procedures contribute to process reliability and traceability.

Blockchain Verification Consistency

Blockchain verification consistency was evaluated to assess the reliability of distributed ledger synchronization across all participating nodes within the proposed framework. This evaluation focused on ensuring that cryptographic hashes, transaction records, and timestamps remained identical across validator, forensic, and archive nodes throughout the preservation process. Consistency in this context is critical for maintaining a trustworthy chain-of-custody, as any discrepancy between nodes may indicate data integrity issues or potential tampering. The consistency value was calculated using the following equation:

$$Cv = \frac{Nm}{Nt} \text{ x } 100\%$$

Cv represents the blockchain verification consistency (%), *Nm* denotes the number of matching transactions across all nodes, and *Nt* represents the total number of transactions processed during the preservation phase. The results of the consistency evaluation are presented in Table 4.

Table 4. Blockchain Verification Consistency

Node	Nm	Nt	$C_{v\,(\%)}$
Validator Node	10	10	100%
Forensic Node	10	10	100%
Archive Node	10	10	100%

All recorded transactions remained synchronized across participating nodes during the experimental evaluation, resulting in an observed consistency rate of 100% within the tested environment. This finding demonstrates successful ledger synchronization under the evaluated conditions. However, the result should not be generalized to large-scale deployments without further scalability testing. Blockchain systems are inherently designed to eliminate discrepancies through consensus protocols, thereby ensuring that all participants share the same version of the ledger (Zheng et al., 2017).

Compared to prior studies that report potential synchronization challenges in distributed environments, the absence of inconsistencies in this study indicates that the implemented configuration is sufficiently robust for forensic applications (Casino et al., 2019; Sunny et al., 2022). Moreover, recent forensic frameworks emphasize that distributed trust models significantly enhance transparency and reduce reliance on centralized authorities, thereby improving the credibility of digital evidence management systems (Rani et al., 2025).

Despite the strong consistency and reliability demonstrated by the proposed framework, several limitations should be acknowledged. The experimental evaluation was conducted in a controlled environment with a limited number of PCAP datasets, which may not fully represent large-scale and highly dynamic real-world network conditions. In addition, the use of a private blockchain configuration may influence performance characteristics, particularly in terms of scalability and consensus overhead. Therefore, further studies are needed to validate the proposed framework in more complex and real-time forensic environments.

CONCLUSION

This study demonstrates that integrating blockchain technology into the preservation phase of the DFRWS framework can support integrity assurance through immutable provenance logging, chain-of-custody traceability, and distributed verification. Experimental evaluation produced an Avalanche Effect value of 50.39%, confirming the strong cryptographic sensitivity of SHA-256 to minimal data modification. However, the primary contribution of the proposed framework lies not in the cryptographic sensitivity itself, but in its ability to provide immutable provenance logging, chain-of-custody traceability, and distributed verification through blockchain-based record management. The framework achieved an average preservation latency of 2.057 seconds within a controlled experimental environment, providing preliminary evidence of operational feasibility. Nevertheless, further validation under larger-scale and real-world conditions is required before broader deployment conclusions can be drawn.

Future research can extend this work by exploring the integration of real-time forensic acquisition with intrusion detection systems (IDS) and security information and event management (SIEM) platforms. Such integration would enable automated evidence capture and preservation directly from live network environments, improving responsiveness and reducing the risk of evidence loss during incident detection. In addition, the incorporation of machine learning techniques offers potential for enhancing anomaly-driven evidence preservation. By leveraging intelligent detection models, forensic systems could automatically prioritize and preserve high-risk network activities, thereby improving efficiency and scalability in large-scale environments. Further studies are also recommended to perform comparative benchmarking against centralized

preservation systems, Hyperledger-based implementations, and alternative permissioned blockchain architectures to quantify performance trade-offs and scalability characteristics.

REFERENCES

Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. In *Advanced Sciences and Technologies for Security Applications* (pp. 149–168). https://doi.org/10.1007/978-3-030-11289-9_7

Arif, T., Camacho, D., & Park, J. H. (2025). Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security. In *Journal of Network and Computer Applications* (Vol. 243, p. 104296). Academic Press. https://doi.org/10.1016/j.jnca.2025.104296

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. In *Electronics (Switzerland)* (Vol. 13, Issue 17, p. 3568). Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/electronics13173568

Badan Siber dan Sandi Negara. (2024). Lanskap Keamanan Siber Indonesia 2024. In *Direktorat Operasi Keamanan Siber* (Issue 70). bit.ly/44bzpHM

Casey, E. (2020). *Digital Evidence and Computer Crime*. Academic Press.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*(May 2018), 55–81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, X. (2025). Blockchain-Enhanced IoT Forensics: Advancing Security, Trust, and Efficiency in Digital Investigations. *Journal of Industrial Integration and Management*. https://doi.org/10.1142/s2424862225300054

Dorri, A., Steger, M., Kanhere, S., & Jurdak, R. (2017). BlockChain: A Distributed Solution to Automotive Security and Privacy. *IEEE Communications Magazine (In Press)*, *55*. https://doi.org/10.1109/MCOM.2017.1700879

Hartono, & Sriyanto. (2022). XSS Attack Detection and Mitigation Using Multi-Layer Security Mechanism (MLSM). *Sienna*, *3*(2), 1–14.

Liang, X., Shetty, S., Tosh, D., Kamhoua, C., Kwiat, K., & Njilla, L. (2017). ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability. *Proceedings - 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, CCGRID 2017*, 468–477. https://doi.org/10.1109/CCGRID.2017.8

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation*, *28*, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

Machhi, J., Madhavi, A., Kumar Maurya, A., Patil, S., & Savita Lade, P. (2024). Blockchain-Based Digital Forensic Evidence Management Chain of Custody. *International Research Journal of Modernization in Engineering Technology and Science*, *6*(4), 11799–11804. https://www.doi.org/10.56726/IRJMETS54596

Rani, D. R., Karthik, T., Narasimha, T., & Rajesh, K. (2025). Blockchain Based Framework for Securing Digital Evidence. *ScitePress : Science and Technology Publications*, 488–493. https://doi.org/10.5220/0013885300004919

Riadi, I., Sunardi, S., & Fitri, F. T. (2022). Spamming Forensic Analysis Using Network Forensics Development Life Cycle Method. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, *6*(1), 108–117. https://doi.org/10.29407/INTENSIF.V6I1.16830

Stallings, W. (2021). *Cryptography and Network Security*. Pearson.

Sunardi, Riadi, I., & Sugandi, A. (2019). Forensic analysis of Docker Swarm cluster using GRR Rapid Response framework. *International Journal of Advanced Computer Science and*

Applications, *10*(2), 459–466. https://doi.org/10.14569/ijacsa.2019.0100260

Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efat, M. I. A., & Islam, M. J. (2022). A Systematic Review of Blockchain Applications. *IEEE Access*, *10*, 59155–59177. https://doi.org/10.1109/ACCESS.2022.3179690

Upadhyay, D., Gaikwad, N., Zaman, M., & Sampalli, S. (2022). Investigating the Avalanche Effect of Various Cryptographically Secure Hash Functions and Hash-Based Applications. *IEEE Access*, *10*(October), 112472–112486. https://doi.org/10.1109/ACCESS.2022.3215778

Wang, S., Schlagwein, D., & Seymour, M. (2025). Socio-technical phenomena involving blockchain use: Literature review, conceptual framework, and research agenda. In *Journal of Strategic Information Systems* (Vol. 34, Issue 2, p. 101901). North-Holland. https://doi.org/10.1016/j.jsis.2025.101901

Xu, X., Pautasso, C., Lo, S. K., Zhu, L., Lu, Q., & Weber, I. (2025). An Extended Pattern Collection for Blockchain-Based Applications. *Lecture Notes in Computer Science*, *14630 LNCS*, 67–117. https://doi.org/10.1007/978-3-662-70810-1_2

Xu, X., Weber, I., & Staples, M. (2019). Architecture for Blockchain Applications. *Architecture for Blockchain Applications*, 1–312. https://doi.org/10.1007/978-3-030-03035-3/SAVE-RESEARCH

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2017). Blockchain Challenges and Opportunities : A Survey Shaoan Xie Hong-Ning Dai Huaimin Wang. *International Journal of Web and Grid Services*, *14*(4), 1–24. http://inpluslab.sysu.edu.cn/files/blockchain/blockchain.pdf