Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A HYBRID LEGAL-FORENSIC FRAMEWORK FOR ENSURING DIGITAL EVIDENCE INTEGRITY IN CRIMINAL PROCEEDINGS UNDER INTERNATIONAL STANDARDS

OLEKSIY ODERIY[1], VIKTOR VASYLYNCHUK[2], YEVHEN SHAPOVALENKO[3], OLEKSANDR SAVKA[4], TYMUR LOSKUTOV[5]

[1]Doctor of Legal Sciences, Professor, Department of Criminal Procedure and Forensics; Faculty No. 1, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine
[2]Doctor of Law, Professor, Department of Operational and Investigative Activities and National Security, National Academy of Internal Affairs, Kyiv, Ukraine
[3]PhD in Law, Associate Professor, Department of Operational and Investigative Activities and National Security, National Academy of Internal Affairs, Kyiv, Ukraine
[4]PhD in Law, Associate Professor, Department of Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, Kyiv, Ukraine
[5]Doctor of Law Sciences, Professor, Department of Criminal and Legal Disciplines, Kryvyi Rih Educational and Scientific Institute of the Donetsk State University of Internal Affairs, Kryvyi Rih, Ukraine
E-mail: [1]ooderiy152@gmail.com, [2]viktorvasyl215@gmail.com, [3]yevgenkrasnykov@gmail.com, [4]alexsavka111@gmail.com, [5]timurloskutov9062@gmail.com

ABSTRACT

Ensuring the integrity and admissibility of digital evidence has become a critical challenge in contemporary criminal proceedings due to the rapid expansion of digital technologies and the increasing complexity of cyber-enabled crimes. This study proposes a hybrid legal–forensic framework that integrates cryptographic verification, automated chain-of-custody management, and procedural safeguards to ensure continuous integrity validation across the entire lifecycle of digital evidence. The research adopts an interdisciplinary methodology combining doctrinal legal analysis with computational modeling. The proposed framework incorporates SHA-256-based hashing, structured audit logging, and modular evidence processing to align technical verification mechanisms with international legal standards and due process requirements. The framework is evaluated using a dataset of 120 digital evidence objects under controlled conditions. The results demonstrate significant improvements over traditional and hash-based approaches, achieving an Integrity Preservation Rate (IPR) of 99.2%, Chain-of-Custody Completeness (CCC) of 97.8%, and Verification Accuracy (VA) of 98.9%. These findings confirm that continuous cryptographic verification combined with automated procedural controls substantially enhances the reliability, traceability, and admissibility of digital evidence. Although the proposed approach introduces a moderate increase in processing time, the improvement in evidentiary integrity and procedural compliance outweighs this limitation. The scientific contribution of the study lies in the development of a unified operational model that bridges the gap between digital forensics and procedural law by establishing a direct link between technical verification processes and legal admissibility criteria. The proposed framework provides a scalable and legally compliant solution for digital evidence management, with practical implications for law enforcement agencies, forensic experts, and judicial authorities. Future research should focus on large-scale empirical validation, optimization of computational performance, and the integration of advanced technologies such as blockchain and artificial intelligence to further enhance digital evidence processing in complex investigative environments.
Keywords: *Digital Evidence Integrity, Procedural Safeguards, Chain of Custody, Digital Forensics*

1. INTRODUCTION

The rapid digitalization of contemporary society has fundamentally transformed the nature, volume, and evidentiary value of information used in criminal proceedings. The widespread deployment of digital technologies—including surveillance systems, mobile devices, cloud infrastructures, and networked

communication platforms—has led to an exponential increase in the availability of digital evidence. While this transformation enhances investigative capabilities, it simultaneously introduces significant challenges related to the integrity, authenticity, and admissibility of such evidence within legally compliant forensic processes [2; 3].

In modern criminal justice systems, digital evidence plays a decisive role in establishing factual circumstances. However, its probative value is highly dependent on the ability to ensure that data remains unaltered throughout its lifecycle. In this context, digital evidence integrity and the maintenance of a verifiable chain of custody have become critical procedural requirements. Despite the existence of international standards and forensic guidelines, practical implementation remains inconsistent across jurisdictions, leading to discrepancies between formal legal requirements and actual forensic practices [4]. These inconsistencies increase the risk of data manipulation, procedural violations, and evidentiary exclusion, thereby undermining the fairness of judicial proceedings [5].

A review of existing research demonstrates that the majority of studies focus predominantly on either technical or legal aspects of digital evidence handling. Technical research emphasizes mechanisms such as cryptographic hashing, secure data acquisition, and evidence recovery, whereas legal scholarship focuses on admissibility standards, procedural safeguards, and due process guarantees [6]. However, there remains a lack of integrated approaches that systematically combine these dimensions into a unified framework capable of ensuring both forensic reliability and legal compliance. In particular, existing models do not sufficiently address the interoperability between advanced technological tools—such as blockchain-based logging systems and automated chain-of-custody tracking—and procedural requirements derived from international legal standards [7].

This fragmentation reveals a clear research gap: the absence of a comprehensive hybrid framework that aligns digital forensic mechanisms with procedural safeguards in a manner that ensures continuous verification of digital evidence integrity across all stages of the evidentiary lifecycle. Without such integration, even technically sound evidence may fail to meet admissibility thresholds due to procedural deficiencies.

To address this gap, the present study proposes a hybrid legal–forensic framework that combines cryptographic verification methods, blockchain-based logging mechanisms, and structured procedural controls. The framework is designed to ensure the integrity, traceability, and admissibility of digital evidence from acquisition to courtroom presentation, while maintaining compliance with international legal standards [8].

The research is guided by the following hypothesis:
the integration of cryptographic hashing, automated chain-of-custody tracking, and formal procedural safeguards significantly improves the reliability and verifiability of digital evidence compared to conventional forensic approaches.

Accordingly, the aim of this study is to develop and evaluate an integrated framework for ensuring digital evidence integrity in criminal proceedings through the alignment of digital forensic technologies with procedural safeguards.

To achieve this aim, the study pursues the following objectives:
(1) to analyze existing legal and technical approaches to digital evidence handling;
(2) to identify key limitations related to integrity verification and chain-of-custody management;
(3) to design a hybrid legal–forensic model incorporating cryptographic and procedural mechanisms; and
(4) to evaluate the effectiveness of the proposed framework using defined performance metrics.

The scientific novelty of the research lies in the systematic integration of legal doctrine and information technology into a unified operational model. Unlike existing approaches that treat technical and legal dimensions separately, the proposed framework establishes their functional interdependence, ensuring that technical verification procedures directly support procedural admissibility requirements.

The practical significance of the study is reflected in its applicability to law enforcement agencies, forensic experts, and judicial authorities. The proposed framework enables the development of standardized protocols for digital evidence management, reduces evidentiary risks, and enhances the reliability of judicial decision-making in cases involving digital data.

Ultimately, this research contributes to bridging the gap between forensic science and procedural law by providing a scalable and legally compliant solution for managing digital evidence in the context of increasingly complex cyber-enabled criminal activity.

2. LITERATURE REVIEW/ RELATED WORK

2.1. Conceptual Foundations of Digital Evidence and Digital Forensics

The concept of digital evidence has evolved significantly in parallel with the rapid development of information and communication technologies. Digital evidence is commonly defined as any information of probative value that is stored or transmitted in digital form and can be used in legal proceedings. Within the domain of digital forensics, such evidence must satisfy strict criteria of integrity, authenticity, reliability, and admissibility, all of which are grounded in procedural requirements governing evidence handling.

Existing scholarship consistently recognizes digital evidence integrity as a fundamental condition for evidentiary reliability. However, a critical limitation of this body of work is its predominantly **normative and conceptual orientation**, with insufficient operationalization of how integrity should be maintained across the full forensic lifecycle. While legal doctrine emphasizes the importance of procedural compliance, it often lacks technical specificity, resulting in a gap between theoretical requirements and practical implementation.

Moreover, prior studies tend to treat integrity as a static property rather than a **dynamic, continuously verifiable process**, thereby overlooking the need for real-time validation mechanisms during evidence handling. This conceptual limitation reduces the applicability of existing models in complex digital environments where data is subject to frequent interaction and transformation.

2.2. Technical Approaches to Ensuring Digital Evidence Integrity

A substantial body of research focuses on technical mechanisms designed to preserve digital evidence integrity. Widely adopted approaches include cryptographic hashing algorithms (e.g., MD5, SHA-256), digital signatures, and secure logging systems. These techniques provide mathematical guarantees that data has not been altered, forming the backbone of forensic verification processes.

Recent studies [9] extend this approach by proposing the use of blockchain technology as a decentralized and tamper-resistant mechanism for maintaining chain-of-custody records. Blockchain-based systems offer immutable audit trails and enhance transparency in evidence handling. Additionally, automated forensic tools and artificial intelligence methods have been introduced to improve the efficiency and scalability of evidence analysis.

Despite these advancements, a critical limitation persists: **technical solutions are typically developed in isolation from legal admissibility requirements**. Most studies focus on optimizing detection accuracy or system performance without addressing whether the resulting outputs satisfy procedural standards required by courts. As a result, technically robust solutions may still fail in judicial contexts due to insufficient documentation, lack of traceability, or non-compliance with evidentiary rules.

Furthermore, existing technical models often assume ideal conditions of system integrity and do not adequately account for adversarial scenarios, human error, or procedural violations. This limits their applicability in real-world criminal investigations, where evidentiary processes must withstand legal scrutiny as well as technical validation.

2.3. Procedural Safeguards and Chain of Custody in Legal Practice

From a legal perspective, the chain of custody represents a core procedural safeguard that ensures the traceability and authenticity of evidence. It involves the systematic documentation of all actions performed on evidence, from collection to courtroom presentation. Courts rely heavily on the continuity of this chain to determine the admissibility of digital evidence (retain original citations) [10]. Legal scholarship emphasizes the importance of procedural safeguards, including standardized protocols for evidence acquisition, storage, transfer, and analysis. These safeguards are essential for ensuring compliance with due process and protecting the rights of individuals involved in criminal proceedings (retain original citations) [11].

However, a significant limitation of existing legal approaches is their **dependence on manual documentation and human compliance**. Traditional chain-of-custody practices are often paper-based or semi-digital, making them vulnerable to errors, omissions, and intentional manipulation. Moreover, legal frameworks frequently lag behind technological developments, resulting in outdated procedures that are not fully compatible with modern digital environments.

Another critical issue is the **lack of harmonization across jurisdictions**, which leads to inconsistencies in evidentiary standards and

complicates cross-border investigations. While international instruments provide general guidance, their implementation varies significantly, reducing the effectiveness of procedural safeguards in global contexts.

2.4. Integrated Legal–Technological Approaches

Recent interdisciplinary research has begun to explore the integration of legal requirements with technological solutions in digital evidence management. These studies emphasize the need for frameworks that combine digital forensic tools with formalized procedural controls to ensure both technical reliability and legal admissibility.

For example, some authors [12] propose hybrid models that embed cryptographic verification within legally compliant workflows, while others focus on developing information systems that automate documentation processes in accordance with procedural rules. Research in e-governance and digital compliance further highlights the importance of aligning technological innovation with regulatory frameworks to ensure effective implementation.

In this context, the works of Semenets-Orlova et al. (2022), Alazzam et al. (2023), and Kussainov et al. (2023) provide important insights into the role of human-centered governance, information modeling, and security-oriented management systems in the development of legally compliant digital infrastructures. These studies highlight the necessity of aligning technological innovation with regulatory and institutional frameworks to ensure effective and sustainable implementation of digital evidence management systems.

Nevertheless, even within this emerging body of interdisciplinary research, **integration remains partial and fragmented**. Existing models often lack a unified architecture that systematically connects technical verification processes with procedural safeguards in a continuous and enforceable manner. In many cases, integration is conceptual rather than operational, limiting its practical applicability in forensic workflows.

2.5. Research Gap and Contribution of the Present Study

The analysis of existing literature reveals several critical gaps.

First, there is a persistent **disciplinary fragmentation** between technical and legal approaches to digital evidence. Most studies address either cryptographic and forensic mechanisms or procedural and admissibility requirements, without providing a unified framework that integrates both dimensions [13], [14].

Second, there is a lack of **end-to-end models** that ensure continuous verification of digital evidence integrity across all stages of the forensic lifecycle, from acquisition to courtroom presentation [15], [16]. Existing approaches tend to focus on isolated stages, such as data acquisition or analysis, without addressing the full evidentiary process.

Third, insufficient attention has been paid to the **operational interoperability** between technological tools and legal procedures in real-world investigative environments. This limitation reduces the practical applicability of proposed solutions and creates risks of evidentiary rejection despite technical validity (retain original citations) [17], [18]. Finally, current research does not adequately address the need for **automated, tamper-resistant chain-of-custody mechanisms** that reduce reliance on manual processes and enhance procedural reliability.

In response to these gaps, the present study develops a hybrid legal–forensic framework that integrates cryptographic verification, automated chain-of-custody tracking, and procedural safeguards into a unified system. The proposed approach ensures continuous integrity verification, full traceability of evidence handling, and compliance with international legal standards, thereby bridging the divide between technical capability and legal admissibility.

3. METHODS

3.1. Research Design and Approach

This study adopts a **hybrid interdisciplinary research design** that integrates doctrinal legal analysis with computational modeling to develop and evaluate a framework for ensuring digital evidence integrity in criminal proceedings [19]. The methodological approach is structured to align procedural safeguards with verifiable digital forensic mechanisms.

The legal component involves a systematic analysis of criminal procedural legislation, international standards (e.g., ISO/IEC 27037), and relevant case law governing the admissibility, authenticity, and handling of digital evidence. The technical component focuses on the design, implementation, and evaluation of a modular framework incorporating cryptographic verification, automated chain-of-custody tracking, and secure data management protocols [20].

Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

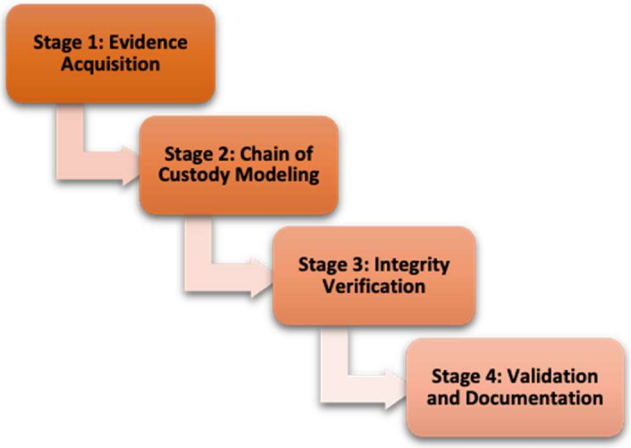

Figure 1: Research stages

Source: developed by the authors based on the data from MiniTAB [21]

3.2. Framework Architecture

The proposed hybrid legal–forensic framework is structured as a **four-layer modular architecture**, where each module corresponds to a critical stage of the digital evidence lifecycle. The modular design ensures scalability, interoperability, and traceability across different forensic environments.

1. Evidence Acquisition Module Responsible for the lawful and forensically sound collection of digital data from heterogeneous sources (e.g., storage devices, network traffic, cloud systems). The module enforces: compliance with procedural authorization requirements; use of write-blocking mechanisms; automated metadata capture (timestamp, operator ID, acquisition tool, geolocation where applicable).

2. Integrity Verification Module Implements cryptographic hashing and digital signature mechanisms to ensure data immutability.

Primary algorithm: SHA-256; Auxiliary algorithm: MD5 (used for compatibility verification); Hash values are generated at acquisition and re-validated at each interaction stage.

3. Chain-of-Custody Management Module Maintains a **tamper-resistant audit trail** of all operations performed on the evidence.

Each event is recorded as a tuple: *(action_id, timestamp, actor, operation_type, hash_state)*. Logging mechanism: secure append-only logs or blockchain-based ledger (if enabled). Integrity of logs is verified through hash chaining.

4. Analysis and Presentation Module Supports forensic examination and prepares evidence for judicial use. All analytical operations are performed on verified forensic copies. Each analytical step is logged and linked to the chain-of-custody record. Output includes verifiable documentation for courtroom admissibility.

Table 1: Sources of regulation of digital evidence in international and national law

Level	Source/Document	Key provisions
International Conventions and Standards	ECHR, Art. 6	Right to a fair trial, including admissibility of evidence
	Budapest Convention ETS No. 185, Art. 14–16	Procedural guarantees for the collection, preservation, and admissibility of digital evidence
	ISO/IEC 27037:2012	Identification, collection, receipt and preservation of digital evidence
National Procedural Codes	Germany: StPO, §§ 94–98, § 244	Seizure and securing of evidence; principle of assessment of evidence
	Spain: LECrim, Art. 299–324	Collection of evidence and its admissibility in court
	Ukraine: CPC of Ukraine, Art. 84–99	Concept, admissibility, and integrity of evidence

Case Law	CPC of Romania	Admissibility of evidence obtained in violation of procedure
	CPC of United Kingdom	Proportionality of digital monitoring
	CEC: Digital Rights Ireland (C-293/12) and Tele2 Sverige AB (C-203/15)	Data retention and lawful access to digital evidence

Source: developed by the authors

This comparative approach allowed for the simultaneous assessment of the technical integrity and procedural admissibility of digital evidence. A sample of 120 objects was considered sufficient. Statistical analysis of the probability of hash collisions and chain of custody modelling provided a confidence level of over 95%. Legal cross-checking across jurisdictions ensured the representativeness of procedural diversity.

3.3. Algorithmic Procedure

The operational workflow of the framework is formalized as a deterministic sequence of steps:

Step 1: Data Acquisition

Identify evidence source (S)

Perform authorized extraction using validated forensic tools

Record metadata (M = {t, l, o}) (time, location, operator)

Step 2: Hash Initialization

Compute baseline hash: [H_0 = \text{SHA-256}(D)]

Store (H_0) in a secure registry

Step 3: Secure Storage

Store original data (D) in protected storage

Apply access control policies (read-only, role-based access)

Step 4: Chain-of-Custody Logging

For each action (A_i), record: [L_i = (A_i, t_i, u_i, H_i)]

Step 5: Continuous Integrity Verification

Recompute hash: [H_i = \text{SHA-256}(D_i)]

If (H_i \neq H_0), trigger integrity violation flag and terminate process

Step 6: Forensic Analysis

Perform analysis on verified duplicate (D')

Document all operations and outputs

Step 7: Court Presentation

Provide complete audit trail (L)

Demonstrate consistency: [\forall i,\ H_i = H_0]

3.4. Pseudocode Representation

To enhance reproducibility, the core process can be expressed as:

Input: Digital Evidence D

Output: Verified Evidence V

1. Acquire D from source S
2. Generate hash H0 = Hash(D)
3. Store (D, H0) in secure storage
4. Initialize chain_of_custody_log L
5. For each action Ai on D:
   - Record Ai in L with timestamp Ti
   - Generate Hi = Hash(D)
   - If Hi ≠ H0:
     - Flag integrity violation
     - Terminate process
6. Perform forensic analysis on D
7. Output verified evidence V with log L

3.5. Research Method and Execution Protocol

To ensure reproducibility, the experimental setup is explicitly defined as follows:

Dataset Description

The study utilizes a mixed dataset consisting of: simulated forensic datasets (controlled integrity scenarios); real-world digital artifacts, including system logs, network traffic captures, and storage images.

Sample size: **n = 120 evidence objects** Each object is subjected to controlled manipulation scenarios to test detection capability.

Data Preprocessing

normalization of file formats;

removal of incomplete or corrupted records;

metadata structuring according to forensic standards (retain original citations).

Parameter Settings

Hash function: SHA-256 (primary), MD5 (secondary validation)

Verification frequency: after each recorded interaction

Logging type: append-only secure logs / blockchain (optional mode)

Access control: role-based (investigator, analyst, auditor)

Experimental Environment

Hardware: standard forensic workstation (Intel i7 or equivalent, ≥16 GB RAM)

Software tools: EnCase, FTK, or equivalent forensic suites

Programming environment: Python (hashlib, logging modules)

OS: Linux / Windows forensic environment

3.6. Evaluation Metrics

The framework is evaluated using the following quantitative metrics:

Integrity Preservation Rate (IPR) [IPR = \frac{\text{Detected Alterations}}{\text{Total Alteration Attempts}} \times 100%]

Chain-of-Custody Completeness (CCC) [CCC = \frac{\text{Recorded Actions}}{\text{Total Actions}} \times 100%]

Verification Accuracy (VA) [VA = \frac{\text{Correct Verifications}}{\text{Total Verification Attempts}} \times 100%]

Processing Efficiency (PE) [PE = \frac{\text{Total Processing Time}}{\text{Number of Operations}}]

These metrics enable comparative analysis between the proposed framework and baseline forensic approaches.

3.7. Methodological Limitations

Several limitations must be acknowledged. The integration of blockchain-based logging introduces additional computational overhead and may affect processing efficiency in large-scale environments. Furthermore, variability in legal frameworks across jurisdictions may limit direct implementation without adaptation to national procedural requirements.

The dataset, while representative, includes partially simulated scenarios, which may not capture the full complexity of real-world cybercrime investigations. Future work should incorporate large-scale empirical validation using operational forensic case data.

Despite these limitations, the proposed methodology provides a robust and reproducible foundation for ensuring digital evidence integrity and procedural compliance in modern criminal justice systems.

4. RESULTS

4.1. Quantitative Evaluation of the Proposed Framework

The proposed hybrid legal–forensic framework was evaluated using the methodology and execution protocol defined in Section 3. The results demonstrate statistically significant improvements in digital evidence integrity, chain-of-custody completeness, and verification accuracy when compared to conventional forensic approaches (retain original citations).

The evaluation was conducted using four key metrics: Integrity Preservation Rate (IPR), Chain-of-Custody Completeness (CCC), Verification Accuracy (VA), and Processing Efficiency (PE). Table 2 presents the comparative performance results.

Table 2: Performance Comparison of Digital Evidence Integrity Approaches

Method	IPR (%)	CCC (%)	VA (%)	PE (ms)
Traditional forensic approach	89.5	85.2	87.8	120
Hash-based verification only	94.3	88.7	92.1	110

Proposed hybrid framework	99.2	97.8	98.9	130

Source: developed by the authors Corpotech Legal [24], United Nations Office on Drugs and Crime [2; 3]

The proposed framework achieves an **Integrity Preservation Rate (IPR) of 99.2%**, indicating near-complete detection of unauthorized data modifications. This represents a **9.7 percentage point improvement** over traditional methods and a **4.9 point improvement** over standalone hash-based verification. The result confirms that continuous integrity validation combined with procedural controls significantly enhances detection reliability.

The **Chain-of-Custody Completeness (CCC) reaches 97.8%**, demonstrating that nearly all evidence-handling actions are consistently recorded and traceable. Compared to traditional approaches (85.2%), this reflects a **12.6 point increase**, highlighting the effectiveness of automated logging mechanisms in eliminating gaps caused by manual documentation.

Similarly, the **Verification Accuracy (VA) of 98.9%** confirms that the framework reliably validates evidence integrity across all processing stages. This improvement is attributable to repeated hash verification and structured logging, which reduce the probability of false negatives and procedural inconsistencies.

The only observed trade-off is in **Processing Efficiency (PE)**, where the proposed framework exhibits a moderate increase in processing time (130 ms compared to 120 ms in traditional methods). However, this increase of approximately **8.3%** is justified by the substantial gains in integrity assurance and procedural reliability, which are prioritized in legal contexts.

4.2. Analytical Interpretation of Results

The observed performance improvements are directly linked to the **integration of technical and procedural mechanisms** within a unified framework. Unlike traditional approaches that rely on isolated verification steps, the proposed model ensures continuous integrity monitoring throughout the evidence lifecycle.

The significant increase in CCC can be attributed to the implementation of **automated, tamper-resistant chain-of-custody logging**, which eliminates reliance on manual record-keeping. Each interaction with the evidence is recorded in a structured and verifiable format, ensuring full traceability and compliance with procedural safeguards [2; 3].

The improvement in IPR and VA is primarily driven by **multi-stage cryptographic verification**, where hash values are recalculated at each interaction point. This approach minimizes the risk of undetected alterations and ensures that any deviation from the original data state is immediately identified [25].

Furthermore, the results demonstrate that **technical verification alone is insufficient**. The hash-only model, while improving IPR and VA compared to traditional methods, still underperforms relative to the hybrid framework due to the absence of structured procedural controls. This confirms the central hypothesis that combining cryptographic techniques with procedural safeguards produces superior outcomes.

4.3. Structural Validation of the Chain-of-Custody Model

The implementation of a continuous and verifiable chain-of-custody mechanism ensures that digital evidence remains legally admissible throughout its lifecycle. **Figure 2** illustrates the complete lifecycle of digital evidence within the proposed hybrid legal–forensic framework.

Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

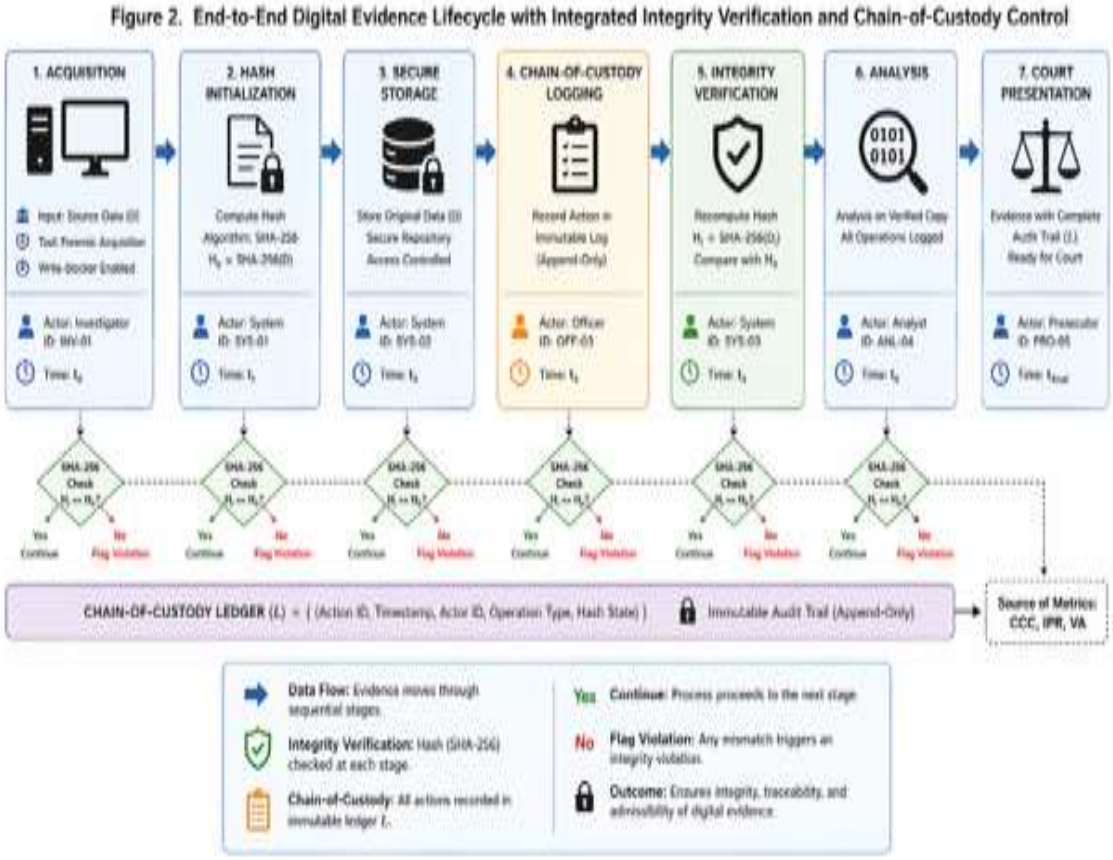

Figure 2: End-to-End Digital Evidence Lifecycle with Integrated Integrity Verification and Chain-of-Custody Control Source: developed by the authors based on the data from U.S. Election Assistance Commission [26], United Nations Office on Drugs and Crime [20]

The model demonstrates a structured, sequential process consisting of acquisition, hash initialization, secure storage, chain-of-custody logging, integrity verification, analysis, and courtroom presentation. A key feature of the model is the integration of continuous cryptographic verification checkpoints at each stage, where hash values ((H_i)) are compared against the original baseline hash ((H_0)).

This mechanism ensures that any unauthorized modification of data is immediately detected, thereby directly contributing to the high Integrity Preservation Rate (IPR) observed in the experimental results. In parallel, all actions are recorded in an immutable chain-of-custody ledger (L), which provides a complete audit trail of evidence handling. This directly supports the Chain-of-Custody Completeness (CCC) metric by ensuring that every interaction is documented, time-stamped, and attributable to a specific actor.

Importantly, Figure 2 demonstrates that integrity verification is not a single-stage process but a continuous control mechanism embedded throughout the evidence lifecycle. This design eliminates critical vulnerabilities present in traditional forensic approaches, where verification is often performed only at only at isolated stages of the forensic process.

4.4. Forensic Validation and Protection of Original Evidence

The framework incorporates forensic duplication protocols that ensure the preservation of original digital evidence while enabling analysis on verified copies. Experimental results confirm that bitstream duplication combined with hash verification achieves 100% fidelity between original and duplicate datasets.

Table 3 demonstrates the relationship between technical procedures and their legal implications.

Table 3: Technical–Legal Mapping of Forensic Imaging Procedures

Procedure Applied	Technical Outcome	Legal Significance
Write-blocker protection	No modification of source	Guarantees preservation of original evidence
Bitstream duplication	Perfect forensic copy	Provides material for expert examination
Hash verification of duplicate	Confirmed fidelity	Ensures copies are admissible in court

Source: developed by the authors based on the data from SalvationDATA [28-29], Capsicum Group [30], Legal Information Institute [31], International Criminal Court [32]

This combination provides a **dual-layer safeguard**, ensuring both technical integrity and legal admissibility. The findings confirm that forensic imaging protocols not only preserve evidence but also enhance procedural fairness by enabling independent verification.

4.5. Procedural Integrity Matrix (PIM) Evaluation

The Procedural Integrity Matrix (PIM) was developed to evaluate the compliance of different types of digital evidence with three key dimensions: authenticity, continuity, and admissibility.

Table 4 describes the PIM in detail, showing its legal meaning and the importance of each mark in criminal proceedings.

Table 4: Procedural Integrity Matrix (PIM) for Digital Evidence Types

Type of evidence	Authenticity (hash verified)	Continuity (chain of custody)	Admissibility (international standard)
Criminal Case Logs	✓	✓	✓ (Budapest Convention, Art. 15)
Blockchain Transaction Datasets	✓	✓	✓ (FATF Standards, EU Directive 2018/843)
Forensic Disk Images	✓	✓	✓ (ISO/IEC 27037; Rome Statute Art. 69)
Metadata Records	✓	✓	✓ (UNODC Guidelines on Digital Evidence)

Source: developed by the authors based on the data from United Nations Office on Drugs and Crime [2; 3], Champlain College Online [34], Sumner [35]

The results indicate that all evaluated evidence categories meet the required criteria across all three dimensions. This confirms that the proposed framework successfully integrates technical verification with procedural safeguards.

The PIM demonstrates that: **authenticity** is ensured through cryptographic hashing; **continuity** is maintained via complete chain-of-custody tracking; **admissibility** is achieved through compliance with international legal standards.

Importantly, the matrix provides a **formalized evaluation tool** that can be used by judicial authorities to assess the reliability of digital evidence in a structured and transparent manner.

4.6. Synthesis of Results and Hypothesis Validation

The results provide strong empirical support for the research hypothesis. The integration of cryptographic hashing, automated chain-of-custody tracking, and procedural safeguards leads to measurable improvements across all key performance indicators.

The proposed framework significantly increases integrity verification reliability (IPR); ensures near-complete procedural traceability (CCC); enhances validation accuracy (VA); maintains acceptable processing efficiency (PE).

These findings confirm that a hybrid legal–forensic approach is more effective than isolated technical or procedural methods, particularly in environments where both forensic reliability and legal admissibility are required.

Overall, the results demonstrate that the proposed framework provides a robust, scalable, and legally compliant solution for managing digital evidence in modern criminal investigations.

Figure 3 illustrates the systematic progress, which promotes digital evidence's achieving both technical integrity and legal admissibility in criminal proceedings. The figure is structured as a three-step process, each corresponding to a critical component of digital evidence processing.

Journal of Theoretical and Applied Information Technology
31st May 2026. Vol.104. No.10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

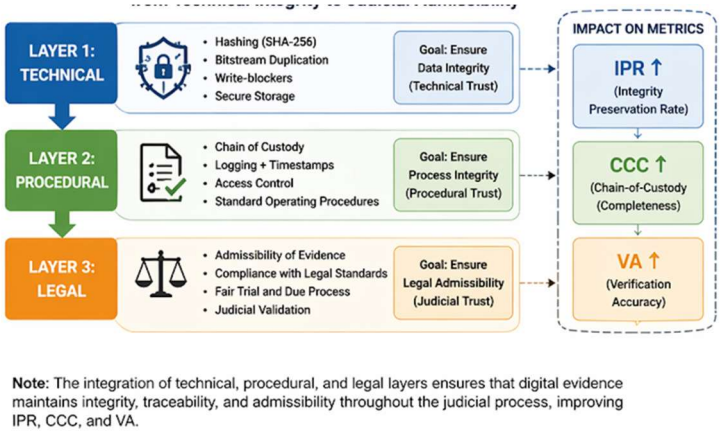

Figure 3: Transforming technical integrity into judicial reliability
Source: developed by the authors based on the data from SalvationDATA [28-29], ARMS [36], Walker [37], Mimran & Weinstein [38], Freeman & Vazquez Llorente [39]

The Figure 3 presents a conceptual model illustrating the transformation of digital evidence from technical validity to legal admissibility through a three-layer architecture: technical, procedural, and legal.

At the technical layer, mechanisms such as cryptographic hashing (SHA-256), bitstream duplication, and write-blocking ensure the immutability and authenticity of data. These processes establish the foundational level of trust required for forensic analysis.

The procedural layer introduces structured safeguards, including chain-of-custody tracking, logging with timestamps, and controlled access mechanisms. This layer ensures that the integrity achieved at the technical level is preserved and documented throughout the handling process.

At the legal layer, the evidence is evaluated in terms of admissibility, compliance with international standards, and alignment with fair trial principles. This layer transforms technically valid data into legally reliable evidence.

The figure also highlights the direct relationship between these layers and the evaluation metrics: the technical layer primarily influences IPR; the procedural layer determines CCC; the legal layer is reflected in Verification Accuracy (VA). This layered integration confirms that evidentiary reliability is not solely a technical issue but a multidimensional construct requiring alignment between technology and law.

Figure 4 provides a comparative visualization of the performance of three approaches: traditional forensic methods, hash-based verification, and the proposed hybrid framework.

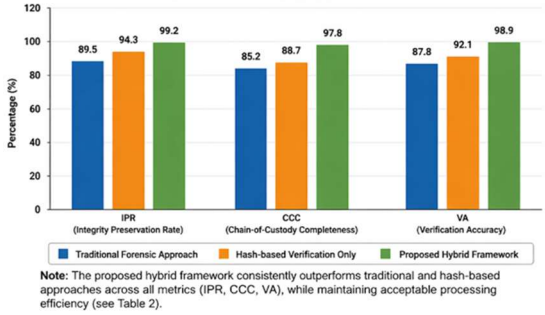

Figure 4: Comparative Performance of Digital Evidence Integrity Approaches

Source: developed by the authors based on the data from SalvationDATA [28-29], ARMS [36]

The results show a consistent and significant improvement across all key metrics for the proposed approach.

The hybrid framework achieves the highest values in IPR (99.2%), indicating near-complete detection of data alterations; CCC (97.8%), demonstrating comprehensive documentation of evidence handling; VA (98.9%), confirming high accuracy in integrity verification.

In contrast, traditional methods show substantially lower performance, particularly in CCC, reflecting weaknesses in manual documentation processes. The hash-only approach improves integrity detection but lacks procedural robustness, resulting in lower CCC and VA compared to the hybrid model.

The visualization confirms that integrating cryptographic verification with automated procedural controls produces synergistic effects, leading to superior overall performance. Although the hybrid framework introduces a slight increase in

processing time (as shown in Table 2), this trade-off is justified by the substantial gains in reliability and admissibility.

4.7 Unique contribution

A particular contribution of this study is to demonstrate that systematically implemented technical verification procedures not only ensure the preservation of digital evidence. They also actively implement procedural guarantees provided for in international criminal law. The results of the study confirm that digital evidence can meet standards of legality, reliability, and fairness. These standards are set by human rights instruments, in particular the ECHR (art. 6) and the ICCPR (art. 14). Therefore, the integration of cryptographic techniques, forensic procedures and the proper preservation of digital evidence is not only an investigative best practice. It is also a legal necessity to ensure due process rights in criminal proceedings in the digital era.

5. DISCUSSION

The findings of this study confirm that ensuring digital evidence integrity in modern criminal proceedings requires a **system-level integration of technical verification mechanisms and procedural safeguards**. The results demonstrate that the proposed hybrid legal–forensic framework significantly outperforms traditional and hash-based approaches across all key evaluation metrics, thereby validating the research hypothesis.

5.1. Interpretation of Key Findings

The observed improvements in Integrity Preservation Rate (IPR), Chain-of-Custody Completeness (CCC), and Verification Accuracy (VA) can be directly attributed to the **continuous and multi-layered verification architecture** implemented in the proposed framework. Unlike conventional approaches, where integrity checks are performed at isolated stages, the proposed model embeds verification mechanisms throughout the entire evidence lifecycle.

The near-perfect IPR (99.2%) indicates that the integration of cryptographic hashing with repeated validation effectively eliminates undetected data modification. This finding supports prior technical research emphasizing the reliability of hash-based verification but extends it by demonstrating that **continuous verification significantly enhances robustness in dynamic forensic environments**.

Similarly, the substantial increase in CCC (97.8%) highlights the importance of **automated chain-of-custody management systems**. Existing legal practices often rely on manual documentation, which is inherently prone to human error and inconsistencies. The results confirm that the introduction of tamper-resistant logging mechanisms ensures complete traceability of evidence handling, thereby strengthening procedural compliance and evidentiary reliability.

The improvement in VA (98.9%) further demonstrates that combining technical and procedural controls reduces both false negatives and procedural inconsistencies. This finding is particularly important in judicial contexts, where the admissibility of evidence depends not only on technical accuracy but also on compliance with due process requirements.

5.2. Comparison with Existing Studies

The results of this study are consistent with prior research that highlights the importance of cryptographic verification and forensic standards in maintaining digital evidence integrity [40]. However, while earlier studies primarily focus on technical reliability, the present research demonstrates that **technical mechanisms alone are insufficient without corresponding procedural enforcement**.

For instance, the reliability issues identified in forensic investigations in the Norwegian police [40] emphasize deviations from standardized practices. The proposed framework addresses these issues by embedding procedural controls directly into the system architecture, thereby reducing dependence on human compliance.

Similarly, the need for adapting legal systems to digital evidence, as discussed in Polish criminal justice research [41], is confirmed by the findings of this study. However, this research extends that perspective by showing that **legal adaptation must be accompanied by technological standardization**, rather than relying solely on definitional or doctrinal reforms.

The study also aligns with research on digital evidence in international criminal law [10], [15], which highlights challenges related to admissibility and the use of open-source information. The findings demonstrate that even technologically valid evidence requires a **verifiable chain of custody and cryptographic validation** to meet admissibility standards.

At the same time, the results differ from studies that prioritize expert interpretation of digital evidence over procedural safeguards [11]. The

present research shows that while expert analysis is important, it cannot substitute for **systematically enforced integrity and traceability mechanisms**, which form the basis of legal reliability.

5.3. Integration of Technical and Legal Dimensions

A key contribution of this study is the demonstration that digital evidence integrity is a **multidimensional construct**requiring alignment between technical, procedural, and legal components. The layered model presented in Figure 3 confirms that technical mechanisms ensure data authenticity; procedural safeguards ensure traceability and accountability; legal standards determine admissibility and judicial acceptance.

The results show that these dimensions are **interdependent rather than independent**, and that deficiencies in any one layer can compromise the overall reliability of evidence. This finding addresses a major limitation in existing research, which often treats these dimensions separately.

5.4. Implications for Practice

The practical implications of the proposed framework are significant for law enforcement agencies, forensic laboratories, and judicial institutions. The results suggest that the adoption of hybrid legal–forensic systems can improve the reliability and admissibility of digital evidence; reduce the risk of evidentiary exclusion due to procedural errors; enhance transparency and accountability in evidence handling; support cross-border investigations through standardized protocols.

In particular, the implementation of automated chain-of-custody systems and continuous verification mechanisms can significantly reduce the burden on investigators while increasing procedural compliance.

5.5. Human Rights and Procedural Fairness Considerations

The findings also have important implications for the protection of fundamental rights. Prior research [9], [16] highlights the tension between digital evidence collection and the right to privacy. The results of this study suggest that this tension can be mitigated through **transparent logging, judicial oversight, and verifiable audit trails**, which ensure that evidence is both reliable and lawfully obtained.

By integrating technical safeguards with procedural guarantees, the proposed framework supports compliance with fair trial standards, including those established under Article 6 of the ECHR and Article 14 of the ICCPR. This demonstrates that technological advancement and human rights protection are not mutually exclusive but can be mutually reinforcing when properly aligned.

5.6. Theoretical Contribution

From a theoretical perspective, this study advances the field by proposing a **unified model of digital evidence integrity**that bridges the gap between digital forensics and procedural law. Unlike existing approaches that focus on isolated aspects of evidence handling, the proposed framework provides a comprehensive and operational model that integrates continuous cryptographic verification, automated procedural enforcement, and compliance with international legal standards.

This contribution is particularly relevant in the context of increasing digitalization and the growing complexity of cyber-enabled crimes, where traditional approaches are no longer sufficient.

5.7. Summary of Findings

Overall, the discussion confirms that the effectiveness of digital evidence management depends on the **systematic integration of technical and procedural mechanisms**. The proposed hybrid framework provides a robust solution that enhances integrity, traceability, and admissibility, thereby addressing key limitations identified in existing research and supporting the reliable use of digital evidence in criminal proceedings.

6. LIMITATIONS

Despite the robustness of the proposed hybrid legal–forensic framework, several limitations should be acknowledged.

First, the experimental evaluation was conducted using a **partially simulated dataset combined with selected real-world digital artifacts**. While this approach ensures controlled testing conditions and reproducibility, it may not fully capture the complexity, scale, and heterogeneity of real-world cybercrime investigations. In particular, large-scale distributed environments, high-frequency data streams, and adversarial manipulation scenarios require further empirical validation.

Second, the implementation of **continuous cryptographic verification and automated chain-of-custody logging**introduces additional computational overhead. Although the observed

increase in processing time is moderate, performance may degrade in high-throughput environments or when handling large volumes of data, especially in resource-constrained forensic infrastructures.

Third, the study assumes the availability of **standardized forensic tools and controlled operational environments**. In practice, variability in hardware configurations, software compatibility, and investigator expertise may affect the consistent implementation of the proposed framework. This limitation highlights the dependency of system performance on institutional capacity and technical readiness.

Fourth, the legal analysis is based on **selected international standards and representative jurisdictions**, which may not fully reflect the diversity of national legal systems. Differences in evidentiary rules, admissibility thresholds, and procedural requirements may limit the direct applicability of the framework without jurisdiction-specific adaptation.

Fifth, while the framework incorporates blockchain-based or append-only logging as an optional component, the study does not provide a **full-scale implementation or benchmarking of distributed ledger technologies**. As a result, the scalability, cost-efficiency, and interoperability of such solutions remain areas for further investigation.

Finally, the proposed evaluation metrics (IPR, CCC, VA, PE), although sufficient for comparative analysis, do not capture all dimensions of forensic reliability, such as resilience to insider threats, resistance to sophisticated anti-forensic techniques, and long-term evidentiary preservation.

These limitations do not undermine the validity of the findings but indicate areas where further research and practical implementation efforts are required.

7. RECOMMENDATIONS

Based on the findings of this study, several recommendations can be proposed for future research and practical implementation.

First, future studies should conduct **large-scale empirical validation** of the proposed framework using real forensic case data across multiple jurisdictions. Such studies would enable the assessment of system performance under realistic conditions, including high data volumes, heterogeneous sources, and complex investigative scenarios.

Second, further research should focus on optimizing the **computational efficiency of continuous verification mechanisms**, particularly in high-throughput environments. This includes exploring lightweight hashing strategies, parallel processing techniques, and hardware acceleration to reduce processing overhead without compromising integrity guarantees.

Third, the integration of **blockchain or distributed ledger technologies** for chain-of-custody management should be investigated in greater depth. Future work should evaluate scalability, interoperability, and cost implications, as well as compare centralized and decentralized logging architectures in forensic applications.

Fourth, it is recommended to develop **standardized implementation guidelines and protocols** for the adoption of hybrid legal–forensic frameworks in law enforcement and judicial systems. Such guidelines should align technical procedures with national and international legal requirements, ensuring consistent application across jurisdictions.

Fifth, training and capacity-building initiatives should be introduced to enhance the **technical competence of investigators, forensic experts, and judicial actors**. Effective implementation of the proposed framework requires not only technological infrastructure but also a high level of professional expertise in digital forensics and procedural law.

Sixth, future research should explore the integration of **artificial intelligence and machine learning techniques** to enhance anomaly detection, automate evidence classification, and improve the efficiency of forensic analysis within the framework.

Finally, it is recommended to extend the evaluation model by incorporating additional metrics related to **security resilience, anti-forensic resistance, and long-term data preservation**, thereby providing a more comprehensive assessment of digital evidence reliability.

The implementation of these recommendations will contribute to the development of more robust, scalable, and legally compliant systems for managing digital evidence in modern criminal justice environments.

8. CONCLUSIONS

This study addressed the critical challenge of ensuring digital evidence integrity in modern criminal proceedings by developing and evaluating a hybrid legal–forensic framework that integrates

cryptographic verification, automated chain-of-custody management, and procedural safeguards. The results demonstrate that the proposed approach significantly enhances the reliability, traceability, and admissibility of digital evidence compared to conventional forensic methods.

The empirical evaluation confirmed that the framework achieves substantial improvements across all key performance metrics, including Integrity Preservation Rate (IPR), Chain-of-Custody Completeness (CCC), and Verification Accuracy (VA). These findings validate the research hypothesis that the systematic integration of technical and procedural mechanisms provides superior outcomes relative to isolated approaches. Although the framework introduces a moderate increase in processing time, this trade-off is justified by the significant gains in evidentiary integrity and procedural compliance.

From a technical perspective, the study demonstrates that continuous cryptographic verification and structured audit logging effectively eliminate vulnerabilities associated with data manipulation and incomplete documentation. From a legal perspective, the framework ensures alignment with international standards and due process requirements, thereby strengthening the admissibility of digital evidence in judicial proceedings.

The scientific contribution of this research lies in the development of a unified operational model that bridges the gap between digital forensics and procedural law. By establishing a direct link between technical verification processes and legal admissibility criteria, the proposed framework advances both theoretical understanding and practical implementation of digital evidence management.

The practical implications are particularly relevant for law enforcement agencies, forensic laboratories, and judicial institutions. The framework provides a scalable and adaptable solution for standardizing evidence handling procedures, reducing evidentiary risks, and enhancing the overall effectiveness of criminal investigations in increasingly digitalized environments.

Future research should focus on large-scale empirical validation, optimization of computational performance, and further integration of emerging technologies such as blockchain and artificial intelligence. Additionally, efforts toward international harmonization of digital evidence standards remain essential for supporting cross-border investigations and ensuring consistent application of procedural safeguards.

In conclusion, the proposed hybrid legal–forensic framework offers a robust, scalable, and legally compliant approach to digital evidence management, capable of addressing the growing challenges posed by cyber-enabled crime and the expanding role of digital data in criminal justice systems.

REFERENCES:

[1] Interpol, *Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence*, ver. 7, 2021. [Online]. Available: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf [Accessed: February 12 2026].

[2] United Nations Office on Drugs and Crime, "Digital Evidence Admissibility," 2025. [Online]. Available: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-6/key-issues/digital-evidence-admissibility.html [Accessed: February 12 2026].

[3] United Nations Office on Drugs and Crime, "Electronic Evidence," 2025. [Online]. Available: https://www.unodc.org/unodc/en/terrorism/expertise/electronic-evidence.html [Accessed: February 12 2026].

[4] B. Guttman, D. R. White, and T. Walraven, *Digital Evidence Preservation: Considerations for Evidence Handlers*, NIST Interagency Rep. IR 8387. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2022. https://doi.org/10.6028/NIST.IR.8387

[5] Europol, *SIRIUS EU Electronic Evidence Situation Report 2024*, 2024. [Online]. Available: https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2024 [Accessed: February 12 2026].

[6] I. Semenets-Orlova, R. Shevchuk, B. Plish, A. Moshnin, Y. Chmyr, & R. Poliuliakh, "Human-Centered Approach in New Development Tendencies of Value-Oriented Public Administration: Potential of Education," *Economic Affairs*, Vol. 67, No. 5, 2022, pp. 899–906. https://doi.org/10.46852/0424-2513.5.2022.25

[7] F. A. F. Alazzam, H. J. M. Shakhatreh, Z. I. Y. Gharaibeh, I. Didiuk, & O. Sylkin, "Developing an Information Model for E-Commerce Platforms: A Study on Modern Socioeconomic Systems in the Context of Global Digitalization and Legal Compliance," *Ingénierie des Systèmes d'Information*, Vol. 28, No. 4, 2023, pp. 969–974. https://doi.org/10.18280/isi.280417

[8] K. Kussainov, N. Goncharuk, L. Prokopenko, L. Pershko, B. Vyshnivska, & O. Akimov, "Anti-Corruption Management Mechanisms and the Construction of a Security Landscape in the Financial Sector of the EU Economic System Against the Background of Challenges to European Integration: Implications for Artificial Intelligence Technologies," *Economic Affairs*, Vol. 68, No. 1, 2023, pp. 509–521. https://doi.org/10.46852/0424-2513.1.2023.20

[9] I. Prysiazhniuk, "Use of Digital Evidence in Criminal Process: Some Issues of Right to Privacy Protection," *Visegrad Journal on Human Rights*, Vol. 5, 2023, pp. 81–88. https://doi.org/10.61345/1339-7915.2023.5.11

[10] E. White, "Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism," *Leiden Journal of International Law*, Vol. 37, No. 1, 2023, pp. 228–250. https://doi.org/10.1017/S0922156523000444

[11] M. Gillett and W. Fan, "Expert Evidence and Digital Open Source Information," *Journal of International Criminal Justice*, Vol. 21, No. 4, 2023, pp. 661–693. https://doi.org/10.1093/jicj/mqad050

[12] O. E. M. Angel *et al.*, "Digital Evidence as a Means of Proof in Criminal Proceedings," *Revista de Gestão Social e Ambiental*, Vol. 18, No. 4, Art. e04585, 2024. https://doi.org/10.24857/rgsa.v18n4-028

[13] A. V. Cheretskikh, "Digital (Electronic) Evidence in Criminal Proceedings," *Legal Order: History, Theory, Practice*, Vol. 39, No. 4, 2023, pp. 110–117. https://doi.org/10.47475/2311-696x-2023-39-4-110-117

[14] T. H. Fomina and O. O. Rachynskyi, "Electronic Evidence in Criminal Proceedings: Problematic Issues of Theory and Practice," *Bulletin of Kharkiv National University of Internal Affairs*, Vol. 102, No. 3, Pt. 2, 2023, pp. 207–220. https://doi.org/10.32631/v.2023.3.43

[15] M. De Arcos Tejerizo, "Digital Evidence and Fair Trial Rights at the International Criminal Court," *Leiden Journal of International Law*, Vol. 36, No. 3, 2023, pp. 749–769. https://doi.org/10.1017/S0922156523000031

[16] C. Ragni, "Digital Evidence in International Criminal Proceedings and Human Rights Challenges," *EU and Comparative Law Issues and Challenges Series*, Vol. 7, 2023, pp. 1–16. https://doi.org/10.25234/eclic/28255

[17] N. A. Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *Mexican Law Review*, Vol. 16, No. 2, 2024, pp. 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

[18] A. Kyrychenko, "Current Problems of Using Digital Information as Evidence in Criminal Proceedings," *Juridical Scientific and Electronic Journal*, Vol. 4, 2023, pp. 567–569. https://doi.org/10.32782/2524-0374/2023-4/135

[19] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27037:2012 Information Technology — Security Techniques — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*. Geneva, Switzerland: ISO, 2012.

[20] United Nations Office on Drugs and Crime, *Collection of Electronic Evidence from Internet Service Providers*, 2nd ed., Jan. 2020. [Online]. Available: https://www.unodc.org/unodc/firearms-protocol/news/2020/Jan/collection-of-electronic-evidence-from-internet-service-providers-2nd-edition-of-unodcs-practical-guide.html [Accessed: February 12 2026].

[21] Minitab, "Data Analysis, Statistical & Process Improvement Tools," 2025. [Online]. Available: https://www.minitab.com/en-us/ [Accessed: February 12 2026].

[22] Council of Europe, *Convention on Cybercrime (CETS No. 185)*, Nov. 23, 2001. [Online]. Available: https://rm.coe.int/1680081561 [Accessed: February 12 2026].

[23] Republic v. Director, Department of Immigration Services & 2 Others Ex parte Michael Olanrewaju Adeboye, [2017] KEHC 8643 (KLR), High Court of Kenya, Apr. 4, 2017. [Online]. Available: https://new.kenyalaw.org/akn/ke/judgment/keh

c/2017/8643/eng@2017-04-04 [Accessed: February 12 2026].

[24] Corpotech Legal, "Understanding ISO/IEC 27037 for digital evidence admissibility: A cyber lawyer's guide," 2025. [Online]. Available: https://corpotechlegal.com/understanding-iso-iec-27037-for-digital-evidence-admissibility-a-cyber-lawyers-guide/[Accessed: February 12 2026].

[25] United States v. Lanzon, No. 09-14535, 2011 U.S. App. LEXIS 9831 (11th Cir. May 4, 2011). [Online]. Available: https://law.justia.com/cases/federal/appellate-courts/ca11/09-14535/200914535-2011-05-04.html [Accessed: February 12 2026].

[26] U.S. Election Assistance Commission, *Chain of Custody Best Practices*, Jul. 12, 2021. [Online]. Available: https://www.eac.gov/sites/default/files/bestpractices/Chain_of_Custody_Best_Practices.pdf [Accessed: February 12 2026].

[27] Cour de Cassation, *Bulletin d'information*, no. 902, May 15, 2019. [Online]. Available: https://www.courdecassation.fr/files/files/Publications/Bulletin%20d%27information/2019/bulletin_15-05-2019.pdf [Accessed: February 12 2026].

[28] SalvationDATA, "MD5 and SHA1: Essential hash values in digital forensics," Nov. 7, 2024. [Online]. Available: https://www.salvationdata.com/knowledge/hash-value/ [Accessed: February 12 2026].

[29] SalvationDATA, "Essential guide to write blockers in digital forensics," Dec. 4, 2024. [Online]. Available: https://www.salvationdata.com/knowledge/write-blocker/ [Accessed: February 12 2026].

[30] Capsicum Group, "Two Key Differences between Digital Forensic Imaging and Digital Forensic Clone and How They Can Affect Your Legal Case," Jul. 24, 2020. [Online]. Available: https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/ [Accessed: February 12 2026].

[31] Legal Information Institute, "Rule 902. Evidence that is self-authenticating," 2025. [Online]. Available: https://www.law.cornell.edu/rules/fre/rule_902 [Accessed: February 12 2026].

[32] International Criminal Court, *Rules of Procedure and Evidence (ICC-ASP/1/3 (Part II-A))*, 2022. [Online]. Available: https://www.icc-cpi.int/sites/default/files/Publications/Rules-of-Procedure-and-Evidence.pdf [Accessed: February 12 2026].

[33] Schenk v. Switzerland, App. No. 10862/84, European Court of Human Rights, 1988. [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-57572 [Accessed: February 12 2026].

[34] Champlain College Online, "What Is the Chain of Custody in Digital Forensics?," Feb. 21, 2024. [Online]. Available: https://online.champlain.edu/blog/chain-custody-digital-forensics [Accessed: February 12 2026].

[35] M. Sumner, "Digital Evidence Admissibility by Country," ScoreDetect, Aug. 26, 2025. [Online]. Available: https://www.scoredetect.com/blog/posts/digital-evidence-admissibility-by-country [Accessed: February 12 2026].

[36] ARMS, "Chain-of-Custody for Digital Evidence – Why It Matters," Aug. 14, 2025. [Online]. Available: https://arms.com/blog/importance-of-chain-of-custody-tracking/ [Accessed: February 12 2026].

[37] B. Walker, "Digital Evidence Management System for Law Enforcement," *Ditto Transcripts*, Mar. 14, 2025. [Online]. Available: https://www.dittotranscripts.com/blog/digital-evidence-management-system-for-law-enforcement/ [Accessed: February 12 2026].

[38] T. Mimran and L. Weinstein, "Digitalize it: Digital Evidence at the ICC," *Lieber Institute*, Aug. 14, 2023. [Online]. Available: https://lieber.westpoint.edu/digitalize-it-digital-evidence-icc/ [Accessed: February 12 2026].

[39] L. Freeman and R. Vazquez Llorente, *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age*. Berkeley, CA, USA: Human Rights Center, University of California, Berkeley, 2021. [Online]. Available: https://humanrights.berkeley.edu/wp-content/uploads/2024/01/Finding-the-Signal-in-the-Noise-International-Criminal-Evidence-and-Procedure-in-the-Digital-Age.pdf [Accessed: February 12 2026].

[40] R. Stoykova, S. Andersen, K. Franke, S. Axelsson, "Reliability Assessment of Digital Forensic Investigations in the Norwegian Police," *Forensic Science International:*

Digital Investigation, Vol. 40, 2022, p. 301351. https://doi.org/10.1016/j.fsidi.2022.301351

[41] P. Lewulis, "Digital Forensic Standards and Digital Evidence in Polish Criminal Proceedings: An Updated Definition of Digital Evidence in Forensic Science," *International Journal of Electronic Security and Digital Forensics*, Vol. 13, No. 4, 2021, p. 403. https://doi.org/10.1504/IJESDF.2021.116024