CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 32. Núm. Ordinario (2026), pp. 405-428
·ISSN 2340-860X - ·ISSNe 2386-5229

Procedural reliability of digital evidence in pre-trial criminal proceedings: A forensic-legal assessment framework

Serhii Holovkin[1,*]
Donetsk State University of Internal Affairs
Dina Drobenko[2]
Donetsk State University of Internal Affairs
Maryna Kulyk[3]
National Academy of Internal Affairs
Vadym Butenko[4]
Interregional Academy of Personnel Management
Assol Shulzhenko[5]
Sumy National Agrarian University

[1] PhD in Juridical Sciences, Senior Research Officer, Associate Professor, Associate Professor of the Department of Criminal Procedure and Criminalistics, Faculty of Training Specialists for Pre-Trial Investigation Bodies, National Police of Ukraine, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine. ORCID: 0000-0002-3204-2286; gsvvsg79@gmail.com (corresponding author).
[2] Senior Lecturer, Department of Criminal Procedure and Criminalistics, Faculty for the Training of Specialists for Pre-Trial Investigation Bodies, National Police of Ukraine, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine. ORCID: 0009-0005-9950-6283; d.drobenko@gmail.com.
[3] PhD in Legal Sciences, Associate Professor, Professor of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine. ORCID: 0000-0003-1373-6749; kulyk_m@ukr.net.
[4] PhD in Legal Sciences, Associate Professor, Department of Civil Law and International Law, Interregional Academy of Personnel Management, Kyiv, Ukraine. ORCID: 0009-0006-0836-2120; butenko_v@gmail.com.
[5] Doctor of Philosophy, Associate Professor of the Department of Justice and Philosophy, Sumy National Agrarian University, Sumy, Ukraine. ORCID: 0000-0003-0161-6926; assol_shulzhenko@ukr.net.

Abstract: This study examines procedural reliability of digital evidence during pre-trial criminal proceedings and addresses the gap between technical integrity, evidentiary authenticity, and procedural legality. Existing legal and forensic approaches focus on judicial admissibility or technical verification, while the development of reliability during investigations remains underexplored. The research defines reliability as an autonomous procedural-legal category formed through compliance with legal safeguards throughout the lifecycle of digital evidence. The study applies a doctrinal-empirical legal-forensic methodology combining doctrinal analysis, procedural reconstruction of evidentiary processes, and adversarial validation modeling. Its empirical basis includes 72 cases involving digital evidence handling at the pre-trial stage. The analysis identifies key reliability criteria: procedural legality, continuity of custody, integrity, authenticity, technical verifiability, and institutional accountability. To operationalize these factors, the study develops the Comprehensive Reliability Index (CRI), a framework for reliability assessment in investigative and prosecutorial practice. Findings indicate that reliability depends primarily on procedural transparency, continuity, and documentation quality rather than technological sophistication alone. The study also shows that technically imperfect evidence may remain reliable when deviations are traceable, justified, and documented. Special attention is given to AI-assisted forensic systems, including explainability, algorithmic accountability, and procedural transparency. The proposed framework supports investigators, prosecutors, forensic specialists, and courts.

Keywords: Digital Evidence, Procedural Reliability, Pre-Trial Criminal Proceedings, Chain Of Custody, Forensic Integrity, Algorithmic Accountability, Criminal Procedure

1. Introduction

Digital evidence has become a central component of contemporary criminal proceedings, particularly at the pre-trial stage, where investigators and prosecutors make critical procedural decisions concerning evidentiary strategy, qualification of offenses, and prosecutorial viability.[6] The rapid expansion of digital technologies—including cloud infrastructures, mobile communications, distributed networks, and

[6] ROMANIUK, V. V.; ABLAMSKYI, S. Y. "Criteria for the admissibility of digital (electronic) evidence in criminal proceedings", Law And Safety, v. 93, n. 2, p. 140–150, 2024. https://doi.org/10.32631/pb.2024.2.13

automated information systems—has fundamentally transformed the evidentiary environment of modern criminal justice systems. As digital interaction increasingly permeates social, economic, and institutional activity, criminal investigations now routinely depend on electronically stored information derived from personal devices, communication platforms, online services, surveillance systems, and network infrastructures. This transformation has significantly increased both the evidentiary value and procedural complexity of digital materials used in criminal proceedings.[7]

Despite the growing centrality of digital evidence, its legal evaluation remains conceptually fragmented. Existing approaches predominantly focus either on judicial admissibility or on technical forensic integrity, emphasizing such elements as authenticity, data preservation, and system reliability.[8] Although these approaches provide important analytical foundations, they insufficiently address a critical intermediate dimension: the procedural formation of evidentiary reliability during pre-trial proceedings.[9,10]

This doctrinal gap has substantial practical consequences. Procedural violations occurring during the acquisition, preservation, transfer, or analysis of digital evidence frequently produce irreversible evidentiary vulnerabilities that cannot be fully remedied at the trial stage.[11] At the same time, legal doctrine continues to lack a coherent operational framework capable of determining when digital evidence may be considered procedurally reliable before judicial evaluation takes place.

As a result, reliability is often reduced to technical correctness or treated as a derivative element of admissibility, while its independent procedural dimension remains underdeveloped.[12,13] Such an approach inadequately reflects the realities of contemporary digital investigations, where evidentiary reliability depends not only on technological integrity, but also on procedural transparency, institutional accountability, and continuity of evidentiary handling. This study proceeds from the premise that reliability should be conceptualized as an autonomous procedural-legal category distinct from both admissibility and authenticity. Within this framework, reliability is understood not as an inherent property of digital data, but as a

---

[7] United Nations Office on Drugs and Crime. "E4J University Module Series: Cybercrime. Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics", 2019. Available at: https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html (accessed on 21 January 2026).

[8] Masaar. New judicial trend: Criminal court overturns conviction due to invalidity of digital forensic evidence, 2025. Available at: https://masaar.net/en/court-overturns-conviction-due-to-invalidity-of-digital-forensic-evidence/ (accessed on 21 January 2026).

[9] LYTVYN, N.; ANDRUSHCHENKO, H.; ZOZULYA, Y. V.; NIKANOROVA, O. V.; RUSAL, L. M. "Enforcement of court decisions as a social guarantee of protection of citizens rights and freedoms", PRAWO I WIĘŹ, v. 1, n. 39, p. 80–102, 2022. https://doi.org/10.36128/priw.vi39.351

[10] MARTINENGO, L.; NG, M. S. P., DE RONG NG, T.; ANG, Y.; JABIR, A. I.; KYAW, B. M.; CAR, L. T. "Spaced digital education for health professionals: Systematic review and meta-analysis", Journal of Medical Internet Research, v. 26, e57760, 2024. https://doi.org/10.2196/57760

[11] Supreme Court of Ukraine. A Supreme Court judge analyzed the criteria for admissibility and reliability of electronic evidence in criminal proceedings. Judiciary of Ukraine, 2025. Available at: https://court.gov.ua/press/news/1751426/ (accessed on 21 January 2026).

[12] YERMACHENKO, V. "Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects", Economic Affairs, v. 68, n. 1, p. 617-633, 2023. https://doi.org/10.46852/0424-2513.1.2023.29

[13] KIENER-MANU, K. E4J University Module Series: Cybercrime. Module 4: Introduction to Digital Forensics, 2026. Available at: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html (accessed on 21 January 2026).

procedurally constructed legal status formed through compliance with legally established safeguards throughout the entire lifecycle of evidence.[14,15,16,17]

The research addresses this conceptual and methodological gap through development of a structured forensic-legal framework for assessing digital evidence reliability at the pre-trial stage. The proposed framework integrates several interconnected evaluative criteria: procedural legality; continuity of custody; integrity; authenticity; technical verifiability; institutional accountability.

Unlike conventional approaches oriented primarily toward retrospective judicial evaluation, the framework developed in this study enables prospective assessment of evidentiary reliability during investigative practice itself.

The scientific novelty of the research lies in three interrelated contributions. First, the study conceptualizes digital evidence reliability as an autonomous procedural-legal construct within criminal proceedings. Second, it systematizes the principal criteria affecting evidentiary reliability into a coherent analytical structure applicable to diverse categories of digital evidence. Third, the study develops the Comprehensive Reliability Index (CRI) as an operational framework designed to support structured reliability assessment during pre-trial proceedings.

The purpose of this study is to formulate a legally grounded and operationally applicable framework for assessing the procedural reliability of digital evidence prior to judicial review in order to strengthen procedural fairness, evidentiary transparency, and legal certainty within criminal proceedings.

To achieve this objective, the study pursues the following research tasks: (1) to define the legal nature of digital evidence reliability as an independent procedural category at the pre-trial stage; (2) to examine the interaction between procedural legality, continuity of custody, integrity, and technical verification in the formation of reliable digital evidence; (3) to identify systemic procedural risks affecting different categories of digital evidence throughout the evidentiary lifecycle; (4) to develop and validate an operational model for reliability assessment applicable within investigative and prosecutorial practice.

The study therefore seeks to contribute not only to doctrinal discussions concerning digital evidence, but also to the development of more transparent, accountable, and methodologically consistent evidentiary practices within contemporary criminal justice systems.

2. Literature review

The legal and forensic understanding of digital evidence has evolved significantly over the past decade, reflecting the increasing centrality of digital data in criminal proceedings. However, this evolution has not been accompanied by a coherent conceptual framework capable of clearly distinguishing between

[14] BÉRUBÉ, M.; BEAULIEU, L.-A., ALLARD, S.; DENAULT, V. "From digital trace to evidence: Challenges and insights from a trial case study", Science Justice, v. 65, n. 5, 101306, 2025. https://doi.org/10.1016/j.scijus.2025.101306

[15] LASAGNI, G. "Admissibility of Digital Evidence from Part I - Collecting Digital Evidence", In V. Franssen S. Tosza (Eds.), The Cambridge Handbook of Digital Evidence in Criminal Investigations. Cambridge: Cambridge University Press, 2025, p. 126–152. Available at: https://www.cambridge.org/core/books/abs/cambridge-handbook-of-digital-evidence-in-criminal-investigations/admissibility-of-digital-evidence/7F8292A7652FF16F5EA850B2984EE0E5 (accessed on 21 January 2026).

[16] SHCHOKIN, R.; OLIINYK, V.; AMELIN, O.; BONDARENKO, Y.; MAZIYCHUK, V.; KYSLENKO, D. "Methods of combating offenses in the field of ecology", Journal of Environmental Management and Tourism, v. 14, n. 1, 5, 2023, p. 5-15. https://doi.org/10.14505/jemt.v14.1(65).01

[17] NAIK, S.; AGARWAL, S. When digital evidence fails: The corporate cost of ignoring metadata. LiveLaw, 2026. Available at: https://www.livelaw.in/amp/articles/digital-evidence-indian-corporation-519181 (accessed on 21 January 2026).

admissibility, authenticity, and reliability—three categories that remain inconsistently defined and frequently conflated in both legal doctrine and forensic practice.

2.1. Admissibility-oriented approaches

Early scholarship on digital evidence was predominantly concerned with its admissibility, focusing on whether electronically stored information could be incorporated within existing evidentiary frameworks. These approaches, reflected in both doctrinal analysis and institutional guidance, emphasize compliance with formal legal requirements governing the introduction of evidence in court.[1819] However, contemporary scholarship increasingly shifts attention toward the reliability of such evidence, recognizing that admissibility alone does not guarantee evidentiary validity in practice.

Within this paradigm, admissibility is treated as a threshold judicial determination, dependent on legality of acquisition, relevance, and procedural compliance. However, such approaches are inherently retrospective, as they evaluate evidence at the stage of judicial review rather than during its formation. As a result, they provide limited guidance for assessing the quality or reliability of evidence during pre-trial proceedings.[20,21] Moreover, admissibility-based models often implicitly assume that evidence satisfying formal criteria is substantively reliable.[22] This assumption has been increasingly challenged in both judicial practice and academic literature, which demonstrate that formally admissible digital evidence may nevertheless be procedurally flawed or technically compromised.

2.2. Technical reliability and authenticity models

A second line of research conceptualizes digital evidence primarily through its technical properties, focusing on authenticity, integrity, and system reliability. Within this framework, authenticity is generally understood as the ability to verify that data originate from a particular source, while integrity refers to the preservation of data in an unaltered state.

Scholars such as Angel et al.[23] identify authenticity, integrity, and contextual coherence as core elements of evidentiary evaluation. Similarly, forensic research emphasizes risks of contamination, tool limitations, and data manipulation as central threats to evidentiary validity.[24] While these approaches provide valuable insights into the technical vulnerabilities of digital evidence, they exhibit two critical limitations. First, they tend to treat reliability as a derivative of technical

---

[18] Romaniuk, V. V.; Ablamskyi, S. Y. "Criteria for the admissibility of digital (electronic) evidence in criminal proceedings". 2024. Ibid.

[19] United Nations Office on Drugs and Crime. "E4J University Module Series: Cybercrime. Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics". 2019. Ibid.

[20] Lasagni, G. "Admissibility of Digital Evidence from Part I - Collecting Digital Evidence", In V. Franssen S. Tosza (Eds.), The Cambridge Handbook of Digital Evidence in Criminal Investigations. 2025. Ibid.

[21] Supreme Court of Ukraine. A Supreme Court judge analyzed the criteria for admissibility and reliability of electronic evidence in criminal proceedings [Press release]. 2025. Ibid.

[22] KIENER-Manu, K. Cybercrime module 4: Key issues — Standards and best practices for digital forensics. 2026. Ibid.

[23] ANGEL, O. E. M., MERCEDES, C. F. Y. M., ELISA, Q. L. A., JOAQUIN, D. J.; DE OLIVEIRA DIAZ DENY GIOVANNA, C.; BEATRIZ, G. Q. G. "Digital evidence as a means of proof in criminal proceedings", Revista De Gestão Social E Ambiental, v. 18, n. 4, e04585, 2024. https://doi.org/10.24857/rgsa.v18n4-028

[24] GRUBER, J.; HARGREAVES, C. J.; FREILING, F. C. "Contamination of digital evidence: Understanding an underexposed risk", Forensic Science International Digital Investigation, v. 44, 301501, 2023. https://doi.org/10.1016/j.fsidi.2023.301501

correctness, thereby neglecting the role of procedural legality in evidentiary formation. Second, they often assume that technical validation mechanisms—such as hash verification—are sufficient to guarantee evidentiary reliability, overlooking the legal significance of how evidence is collected, documented, and transferred.

Consequently, authenticity and integrity, although necessary conditions, cannot be considered sufficient indicators of reliability in a legal sense.

2.3. Procedural and hybrid approaches

More recent scholarship attempts to bridge the gap between legal and technical perspectives by emphasizing the procedural construction of digital evidence. Within this approach, reliability is understood as the outcome of a sequence of legally regulated actions, including acquisition, preservation, analysis, and documentation.

Stoykova[25] introduces the concept of a "right to procedural accuracy," arguing that evidentiary validity depends on demonstrable compliance with procedural safeguards throughout the evidence lifecycle. Similarly, studies on cross-border investigations highlight how fragmentation of procedural standards undermines the consistency and reliability of digital evidence[26].

Blockchain-based models and other technological solutions have been proposed to enhance traceability and control over the chain of custody[27]. While these approaches contribute to improving evidentiary management, they reveal a fundamental tension between technological guarantees and legal legitimacy. Technological systems may strengthen data integrity but cannot substitute for procedural compliance or institutional accountability[28].

Despite their contributions, procedural and hybrid approaches remain underdeveloped at the operational level. They lack structured criteria and evaluative models that could be applied consistently in investigative practice, particularly at the pre-trial stage.

2.4. Emerging challenges: Artificial intelligence and automated forensic systems

Recent developments in artificial intelligence (AI) and automated forensic technologies have significantly transformed the evidentiary landscape of criminal proceedings. AI-based systems are increasingly used for data extraction, facial recognition, predictive analysis, pattern detection, and automated classification of digital information. These technologies expand investigative capacities and enable the processing of large-scale datasets that would otherwise exceed human analytical capabilities. However, they also generate substantial legal and procedural challenges regarding reliability, transparency, and accountability.

Contemporary scholarship increasingly emphasizes that automated forensic systems may undermine procedural fairness where algorithmic operations remain

---

[25] Stoykova, R. "A new right to Procedural accuracy: a governance model for digital evidence in criminal proceedings", Computer Law Security Review, v. 55, 106040, 2024. https://doi.org/10.1016/j.clsr.2024.106040

[26] Casino, F.; Pina, C.; LÓPEZ-Aguilar, P.; Batista, E.; Solanas, A.; Patsakis, C. "SoK: cross-border criminal investigations and digital evidence", Journal of Cybersecurity, v. 8, n. 1, 2022. https://doi.org/10.1093/cybsec/tyac014

[27] Loffi, L.; Camillo, G. L.; DE Souza, C. A.; Westphall, C. M.; Westphall, C. B. "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature review", IEEE Access, v. 13, p. 77804–77832, 2025. https://doi.org/10.1109/ACCESS.2025.3560191

[28] AL-Billeh, T.; AL-Hammouri, A.; Khashashneh, T.; Makhmari, M. A.; Kalbani, H. A. "Digital evidence in human rights violations and international criminal justice", Journal of Human Rights Culture and Legal System, v. 4, n. 3, p. 842–871, 2024. https://doi.org/10.53955/jhcls.v4i3.446

insufficiently transparent or independently verifiable[29]. In particular, concerns have been raised regarding algorithmic opacity, limited explainability, data bias, and the inability of defense parties to meaningfully challenge automated evidentiary conclusions[30]. Unlike traditional forensic methods, AI-driven analytical systems may rely on probabilistic models and adaptive computational processes that are not fully reproducible or interpretable by investigators, courts, or legal representatives.

These concerns have contributed to the emergence of the explainable AI paradigm, which seeks to ensure that algorithmic decisions remain understandable, auditable, and contestable within legal proceedings[31]. From an evidentiary perspective, explainability functions not merely as a technical requirement but as a procedural safeguard directly connected to adversarial fairness and equality of arms. Where automated systems cannot provide transparent reasoning or reproducible analytical pathways, the reliability of the resulting evidence becomes procedurally vulnerable.

Recent legal scholarship further highlights that algorithmic accountability requires the existence of institutional oversight mechanisms capable of documenting system architecture, validation procedures, training datasets, and error rates[32]. Accordingly, evidentiary reliability increasingly depends not only on data integrity but also on the procedural transparency of the technological environment through which evidence is generated and processed[33].

From the perspective of the present study, these developments directly affect two central criteria of the CRI: technical verifiability (T) and procedural legality (L). Automated forensic outputs may satisfy technical integrity requirements while nevertheless failing to meet procedural standards of transparency and contestability. Consequently, reliability cannot be presumed solely on the basis of technological sophistication or computational accuracy.

The growing integration of AI into investigative practice therefore reinforces the need for a procedural model of reliability capable of evaluating both technological and legal dimensions of evidentiary formation. In this context, the CRI framework proposed in this study provides a structured mechanism for assessing whether automated evidentiary processes remain sufficiently transparent, accountable, and procedurally verifiable to support reliable legal use in pre-trial proceedings.

2.5. Structural gaps in existing research

Despite the diversity of approaches, several fundamental limitations persist in the literature. First, there is a systematic conflation of key concepts, particularly reliability, admissibility, and authenticity. These categories are often used

---

[29] Billah, M. "Developing an explainable AI system for digital forensics: enhancing trust and transparency in flagging events for legal evidence", International Journal of Latest Technology in Engineering Management & Applied Science, v. 14, n. 7, p. 6–16, 2025. https://doi.org/10.51583/ijltemas.2025.1407000002

[30] Dufeniuk, O.; Melnyk, N.; Nahorniak, Y.; Melnyk, S. "Innovative potential of 3D technologies in crime investigation", Social Legal Studios, v. 7, n. 4, p. 222–230, 2024. https://doi.org/10.32518/sals4.2024.222

[31] European Union Agency for Fundamental Rights. "Assessing high-risk AI: Fundamental rights risks". Publications Office of the European Union, 2025. Available at: https://privacy-web.nl/wp-content/uploads/2025/12/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf (accessed on 21 January 2026).

[32] Van Krimpen, F., De Bruijn, H., & Arnaboldi, M. "Machine Learning Algorithms and Publicdecision-making: A Conceptual Overview", In The Routledge Handbook of Public Sector Accounting (1st ed., pp. 124–138). Routledge - Taylor & Francis Group. 2023. https://doi.org/10.4324/9781003295945-12

[33] Rosenstrauch, D., Mangla, U., Gupta, A., & Masau, C. T. "Correction to: Artificial Intelligence and ethics", In: Meyers, A. (eds) Digital Health Entrepreneurship. Health Informatics. Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33902-8_17

interchangeably, leading to analytical ambiguity and inconsistent legal application. Second, most existing frameworks are retrospective, focusing on judicial evaluation at trial rather than on the procedural formation of evidence during the pre-trial phase. This limits their practical relevance for investigators and prosecutors. Third, current models lack operational tools capable of structuring reliability assessment in a consistent and reproducible manner. While individual criteria are identified in the literature, they are rarely integrated into a coherent evaluative system. Finally, the growing role of AI and complex digital infrastructures introduces challenges that are insufficiently addressed within existing doctrinal frameworks, particularly in relation to transparency, accountability, and cross-jurisdictional consistency.

2.6. Contribution of the present study

This study addresses the identified gaps by conceptualizing reliability as an autonomous procedural-legal category, distinct from both admissibility and authenticity. Unlike existing approaches, it focuses on the pre-trial stage, where reliability is formed through compliance with procedural requirements.

Furthermore, the research develops a structured system of forensic-legal criteria and introduces the CRI as an operational model for evaluating digital evidence. This model provides a transparent and reproducible framework capable of supporting decision-making in investigative practice.

By integrating legal doctrine, forensic methodology, and procedural analysis, the study establishes a coherent analytical foundation for assessing digital evidence reliability and contributes to the development of more consistent and accountable evidentiary standards.

In addition, the study contributes to emerging debates on technologically mediated evidence by integrating procedural legal analysis with contemporary concerns regarding algorithmic accountability and explainability in digital forensic systems. This enables the proposed framework to remain applicable not only to conventional digital evidence, but also to increasingly automated evidentiary environments shaped by AI-assisted investigative technologies.

3. Methods

3.1. Research design and analytical framework

This study employs a doctrinal–empirical legal-forensic research design aimed at conceptualizing and operationalizing the procedural reliability of digital evidence at the pre-trial stage of criminal proceedings. The methodological framework combines legal analysis with forensic reconstruction in order to examine how reliability is formed through procedural practice rather than merely inferred from technical integrity.

The research design integrates three interrelated methodological components: (1) doctrinal legal analysis; (2) procedural reconstruction of evidentiary processes; (3) adversarial validation modeling. The doctrinal component focuses on the interpretation of criminal procedural norms governing the acquisition, preservation, transfer, and evidentiary use of digital materials. The analysis includes national criminal procedure legislation, judicial practice, international legal instruments, and forensic standards applicable to digital evidence handling. Particular attention is devoted to procedural safeguards established within the framework of the Convention on Cybercrime (Budapest Convention)[34] and United Nations[35] guidance

[34] COUNCIL OF EUROPE. Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe, 2001. Available at: https://rm.coe.int/1680081561 (accessed on 21 January 2026).

concerning digital evidence and cybercrime investigations.

The empirical component is based on procedural reconstruction of the digital evidence lifecycle across recurrent investigative scenarios. These scenarios include: seizure of personal digital devices; acquisition of data from electronic service providers; extraction of cloud-based information; interception of electronic communications; collection of network metadata; voluntary submission of digital materials.

Procedural reconstruction was conducted using authentic procedural documentation, forensic audit logs, transfer protocols, and technical verification records. This approach enabled identification of legally significant procedural stages, evidentiary transformation points, and recurrent procedural risks affecting reliability.

The third methodological component—adversarial validation modeling—simulates procedural objections commonly raised by defense parties during pre-trial and early trial stages. These objections include allegations of unlawful acquisition, procedural discontinuity, data contamination, incomplete documentation, and lack of technical verifiability. The purpose of this stage is to assess whether the proposed reliability framework remains sufficiently robust under adversarial scrutiny and exclusion-oriented procedural review.

The integrated methodological structure allows the study to bridge doctrinal legal analysis with applied forensic evaluation, thereby treating reliability not as a purely technological characteristic of data, but as a procedurally constructed legal status.

3.2. Dataset formation, sampling strategy, and jurisdictional scope

The empirical basis of the study consists of 72 documented cases involving digital evidence handling during pre-trial criminal proceedings. Cases were selected through purposive (criterion-based) sampling designed to ensure analytical representativeness rather than statistical generalizability.

The sampling strategy was intended to capture recurrent procedural configurations relevant to reliability assessment across multiple categories of digital evidence.

The inclusion criteria were: availability of complete procedural documentation, including seizure records, transfer protocols, and forensic reports; presence of verifiable technical metadata, including hash values, timestamps, and audit logs; representation of distinct categories of digital evidence; completion of the pre-trial procedural phase.

The exclusion criteria included: classified or restricted-access materials; incomplete evidentiary chains; ongoing investigations lacking finalized procedural documentation.

The dataset primarily reflects Ukrainian investigative and judicial practice from 2019–2024, supplemented by international procedural standards and comparative forensic guidance. Although jurisdictionally concentrated, the selected materials reflect procedural structures broadly comparable to continental criminal procedure systems influenced by European evidentiary standards.

The sample size was determined according to the principle of analytical saturation. During the reconstruction process, additional cases ceased to produce substantially new categories of procedural variation, indicating sufficient coverage for model development and evaluative consistency.

Several methodological limitations must nevertheless be acknowledged. The concentration on a single jurisdiction introduces potential jurisdictional bias. In

[35] UNITED NATIONS. "Report of the Secretary-General on the work of the Organization 2025: Combating drugs, crime and terrorism", United Nations, 2025. Available at: https://www.un.org/sites/un2.un.org/files/sg_annual_report_2025_drugs-crime-terrorism_en.pdf (accessed on 21 January 2026).

addition, reliance on well-documented cases may favor investigations characterized by comparatively high procedural quality. These limitations are addressed by positioning the study as normative and model-oriented rather than statistically predictive. The purpose of the research is to construct a transferable analytical framework capable of supporting reliability assessment across diverse procedural contexts.

3.3. Methods of analysis

The study employs an integrated combination of legal and forensic analytical methods.

The legal analytical methods include: doctrinal interpretation of procedural norms; comparative analysis of international legal standards; case-based reasoning derived from judicial practice; normative assessment of procedural safeguards.

The forensic analytical methods include: reconstruction of the digital evidence lifecycle; hash-based integrity verification using SHA-256; simulation of chain-of-custody continuity; metadata and audit-log analysis; identification of procedural vulnerability points; adversarial stress-testing of evidentiary configurations.

The combination of these methods enables simultaneous evaluation of technical forensic processes and their procedural-legal significance. Accordingly, reliability is assessed not merely as a technological condition of data preservation, but as a legally mediated evidentiary status formed through procedural compliance.

3.4. Technical forensic processes and their legal significance

The reliability of digital evidence depends on the interaction between technical forensic operations and procedural legal safeguards. Technical processes generate evidentiary indicators, while procedural rules determine their legal significance.

Core forensic operations examined in this study include: hash-based integrity verification (SHA-256); metadata and system-log analysis; forensic extraction and imaging procedures; audit logging of investigative actions; chain-of-custody documentation.

Hash verification mechanisms were used to identify potential data alteration and preserve evidentiary integrity throughout the evidence lifecycle. Metadata analysis enabled reconstruction of data origin, transfer history, and system interactions. Forensic extraction procedures included both logical acquisition and bit-by-bit imaging depending on the nature of the evidentiary source.

However, the study demonstrates that technical indicators do not independently establish legal reliability. Their evidentiary value depends on procedural conditions under which they were generated, recorded, preserved, and documented.

For example: (1) hash values confirm integrity only when incorporated into a properly documented chain of custody; (2) metadata supports authenticity only where acquisition procedures are legally authorized and reproducible; (3) forensic extraction results remain reliable only if investigative tools and analytical procedures are transparent and independently verifiable.

Accordingly, technical forensic processes operate as procedurally mediated evidentiary elements rather than autonomous indicators of reliability.

3.5. CRI: Structure, operationalization, and practical applicability

To operationalize the proposed procedural framework, this study introduces the CRI as a structured legal-analytical model for assessing digital evidence reliability during pre-trial proceedings.

The CRI consists of five core evaluative criteria:

L — Procedural legality (lawfulness of acquisition and authorization);

C — Continuity of custody (traceability of evidence handling and transfer);

I — Integrity (preservation of data without unjustified alteration);

A — Authenticity (attribution of data to an identifiable source);

T — Technical verifiability (possibility of independent procedural and technical verification).

Each criterion is evaluated using a trichotomous legal scale:

1 — fully satisfied;

0.5 — conditionally satisfied (procedural deviation justified and documented);

0 — not satisfied.

The CRI score is calculated as the arithmetic mean of all criteria.

All criteria are assigned equal weight based on the doctrinal premise that procedural reliability constitutes a composite legal status in which deficiencies in any dimension may affect overall evidentiary validity. The model therefore reflects the interdependence of procedural safeguards rather than imposing rigid hierarchical prioritization.

Interpretative thresholds are defined as follows: High reliability: CRI ≥ 0.8; Moderate reliability: 0.5 ≤ CRI < 0.8; Low reliability: CRI < 0.5.

Importantly, the CRI is not intended to function as a statistical metric or automated evidentiary algorithm. Rather, it serves as a structured decision-support instrument designed to enhance transparency, consistency, and procedural accountability in evidentiary assessment.

From a practical perspective, the CRI framework may be applied by investigators, prosecutors, forensic specialists, and judicial actors during different stages of pre-trial proceedings. In investigative practice, the model can function as an internal procedural screening mechanism enabling early identification of evidentiary vulnerabilities. Prosecutors may employ CRI assessment to evaluate evidentiary sustainability prior to indictment, while defense parties may use the framework to identify procedural deficiencies affecting reliability.

The model is particularly useful in investigations involving cloud infrastructures, multi-actor evidence transfer, and complex digital ecosystems where procedural fragmentation frequently undermines evidentiary continuity.

Accordingly, the CRI is designed not only as a theoretical construct, but also as an operational procedural framework capable of supporting standardized reliability assessment within real investigative practice.

3.6. Validation strategy and model robustness

The CRI model was validated through three complementary analytical procedures: cross-case consistency analysis; adversarial stress testing; applied procedural modeling.

Cross-case consistency analysis examined whether similar procedural configurations generated comparable CRI outcomes across different categories of digital evidence. Adversarial stress testing evaluated the relationship between CRI scores and simulated procedural objections typically raised by defense parties, including allegations concerning unlawful acquisition, evidentiary contamination, incomplete documentation, and chain-of-custody discontinuities. Applied procedural modeling tested the framework against reconstructed investigative scenarios involving varying levels of procedural compliance and technical complexity.

Validation results demonstrate that: critical procedural violations consistently produce low CRI scores; minor procedural deviations do not necessarily undermine reliability where properly documented and justified; the framework reliably differentiates between curable procedural irregularities and structurally disqualifying evidentiary defects.

These findings confirm the methodological robustness and practical applicability of the CRI framework as a procedural tool for reliability assessment.

3.7. Technical tools and forensic environment

Digital forensic analysis was conducted using established professional forensic platforms, including: EnCase Forensic; FTK (Forensic Toolkit); Autopsy; Cellebrite UFED; Oxygen Forensic Detective; Wireshark.

Cloud-based forensic acquisition modules were additionally employed for remote data extraction and synchronization analysis.

Data integrity verification was performed using SHA-256 hashing implemented both within forensic platforms and through independent verification tools, including OpenSSL and HashCalc. Hash values were generated and recorded at each stage of the evidence lifecycle to ensure procedural traceability and reproducibility.

All forensic tools produced audit logs and procedural reports documenting investigative actions, extraction procedures, and evidentiary transformations. These records were integrated into the reconstruction and validation process in order to support both technical verification and procedural accountability.

4. Results

4.1. Procedural architecture of digital evidence collection

The procedural reconstruction of the dataset demonstrates that digital evidence handling follows a relatively stable procedural architecture consisting of four interconnected stages: (1) lawful authorization; (2) procedural execution; (3) documented transfer; (4) formal evidentiary fixation.

Although this structure remains generally consistent across all investigated categories of digital evidence, the degree of procedural complexity and vulnerability differs substantially depending on the nature of the evidentiary source.

The analysis identifies six principal categories of digital evidence: personal digital devices; service provider servers; cloud storage systems; network metadata; surveillance systems; voluntarily submitted digital materials. Table 1 presents the comparative procedural architecture associated with each category and illustrates how variations in procedural complexity directly affect evidentiary reliability.

Table 1. Procedural architecture of digital evidence acquisition and its impact on reliability.

Evidence category	**Total procedural acts**	**Legally relevant access points**	**Third-party control**
Personal devices	Moderate	Limited	Absent
Service provider servers	High	Multiple	Present
Cloud storage systems	High	Multiple	Present
Network traffic/metadata	High	Distributed	Present
Surveillance systems	Low	Fixed	Absent
Voluntary materials	Low	Single	Absent

Source: developed by the author based on data from the Supreme Court of Ukraine,[36] Forensic Focus[37].

[36] Supreme Court of Ukraine. Cybercrime and electronic evidence: Supreme Court judge explains the assessment of electronic evidence in criminal proceedings, 2024. Available at: https://court.gov.ua/eng/supreme/pres-centr/news/1594957/ (accessed on 21 January 2026).

[37] Forensic Focus. Forensic Focus legal update July 2021: Reliability and credibility of digital evidence, 2021. Available at: https://www.forensicfocus.com/legal/forensic-focus-legal-update-july-2021-reliability-and-credibility-of-digital-evidence/ (accessed on 21 January 2026).

The results demonstrate a direct relationship between procedural complexity and evidentiary vulnerability. Evidence involving third-party participation—particularly cloud infrastructures, provider-controlled systems, and distributed network environments—requires a significantly larger number of procedural actions and legally relevant access points. This increases the probability of procedural fragmentation and complicates maintenance of evidentiary continuity.

From the perspective of the CRI, such environments create heightened risks for procedural legality (L) and continuity of custody (C), especially where evidence passes through multiple institutional or technical intermediaries.

In contrast, categories characterized by limited actor involvement, such as personal devices and voluntarily submitted materials, display comparatively stable evidentiary chains and reduced procedural uncertainty. These categories more consistently achieve high CRI scores due to simplified documentation requirements and lower exposure to procedural disruption.

Importantly, the findings indicate that evidentiary reliability depends less on technological sophistication than on the procedural environment within which digital evidence is acquired and managed. This confirms one of the central arguments of the study: procedural architecture is a more decisive determinant of reliability than technological complexity itself.

4.2. Lifecycle distribution of procedural risk

The reconstruction of the digital evidence lifecycle demonstrates that procedural risks are unevenly distributed across different stages of evidentiary handling. Reliability is therefore not established at a single procedural moment, but progressively constructed throughout the entire lifecycle of evidence. Figure 1 illustrates the distribution of legally significant procedural actions across five principal stages: acquisition; preservation; transfer; analysis; submission.

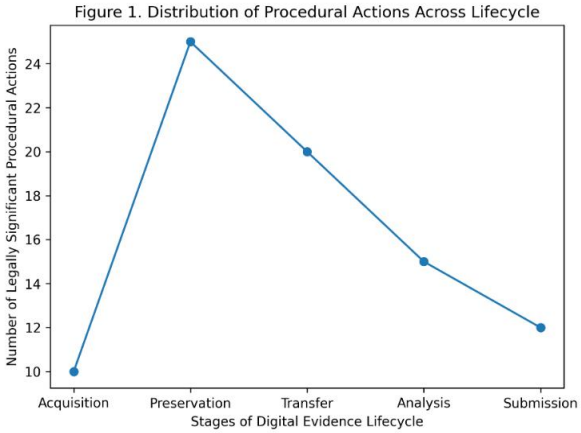

Figure 1. Distribution of legally significant procedural actions across the lifecycle of digital evidence. Source: developed by the author based on data from Meinheit,[38] MindMeister,[39] Loux[40].

[38] MEINHEIT, A. "From bytes to bench: Leveraging digital forensics in the litigation lifecycle", Complete Legal, 2025. Available at: https://completelegal.us/from-bytes-to-bench-leveraging-digital-forensics-in-the-litigation-lifecycle/ (accessed on 21 January 2026).

[39] MindMeister, Online mind mapping tool, 2026. Available at: https://www.mindmeister.com (accessed on 21 January 2026).

[40] LOUX, M.; LOUX, B. "How is digital evidence preserved in modern investigations?", American Military University, 2025. Available at: https://www.amu.apus.edu/area-of-study/criminal-justice/resources/how-is-digital-evidence-preserved/ (accessed on 21 January 2026).

The results reveal that the highest concentration of procedural vulnerability occurs during preservation and transfer stages rather than during initial acquisition. Although acquisition is essential for establishing procedural legality (L), subsequent stages expose evidence to repeated handling, institutional interaction, system synchronization, and potential undocumented transformations.

Preservation and transfer phases therefore create elevated risks for disruptions in continuity of custody (C) and integrity (I). These stages involve multiple actors, repeated procedural interventions, and interactions between forensic systems, all of which increase the likelihood of evidentiary fragmentation.

For multidisciplinary audiences, this finding is particularly significant because it demonstrates that digital evidence may become procedurally unreliable even after lawful acquisition. In other words, reliability is not guaranteed by judicial authorization alone; it depends on continuous procedural control throughout all subsequent stages of evidence handling.

The analysis further demonstrates that late-stage procedural deficiencies frequently exert disproportionate influence on overall CRI outcomes. Even relatively minor undocumented transformations occurring during transfer or preservation may substantially reduce reliability scores if procedural traceability cannot be maintained.

Accordingly, the findings support the conclusion that evidentiary reliability must be understood as a cumulative procedural condition requiring continuous monitoring across the entire evidentiary lifecycle.

4.3. Comparative reliability profiles across evidence categories

Application of the CRI across the dataset enabled comparative classification of digital evidence categories according to their procedural reliability profiles. Table 2 summarizes the average CRI performance observed across the analyzed categories of digital evidence.

The results reveal clear procedural stratification among evidentiary categories. Surveillance systems and voluntarily submitted materials demonstrate consistently high reliability due to procedural simplicity, stable evidentiary documentation, and limited involvement of external actors.

By contrast, provider-controlled and cloud-based evidence categories display significantly greater procedural variability. Their moderate reliability scores reflect the influence of cross-system dependencies, jurisdictional fragmentation, and multi-actor evidence management.

Table 2. Comparative reliability profiles of digital evidence categories based on CRI.

Evidence category	**Mean CRI**	**Range**
Personal devices	High	Moderate–High
Provider servers	Moderate	Low–High
Cloud storage systems	Moderate	Low–High
Network metadata	Moderate – High	Moderate–High
Surveillance systems	High	High–High
Voluntary materials	High	Moderate–High

Source: developed by the author based on Forensic Focus data[41].

An especially important finding concerns network metadata. Despite high technical complexity, these data frequently achieve comparatively strong reliability outcomes due to standardized logging protocols, automated traceability mechanisms, and relatively stable documentation practices.

[41] Forensic Focus. Forensic Focus legal update July 2021: Reliability and credibility of digital evidence. 2021. Ibid.

For legal practitioners, these findings illustrate that technological complexity alone does not necessarily reduce evidentiary reliability. Instead, the decisive factor is the extent to which procedural safeguards remain transparent, reproducible, and institutionally controllable.

The findings therefore reinforce the broader doctrinal conclusion that reliability is primarily shaped by procedural transparency and continuity rather than by the technological nature of the evidentiary source itself.

4.4. Integrity verification: Legal interpretation of hash analysis

Hash-based integrity verification was applied across all reconstructed evidentiary scenarios as a core technical mechanism for detecting unauthorized data alteration. However, the results demonstrate that the legal interpretation of hash verification differs substantially from its purely technical meaning.

Table 3 presents the relationship between hash consistency outcomes and their procedural-legal interpretation.

Table 3. Legal interpretation of hash-based integrity verification.

Evidence category	**Hash consistency**	**Legal implication**
Personal devices	Full	Legally preserved
Provider servers	Partial	Documented procedural justification
Cloud storage systems	Partial	Documented procedural justification
Network metadata	Full	Legally preserved
Surveillance systems	Full	Legally preserved
Voluntary materials	Full	Legally preserved

Source: developed by the author based on data Mossé Cyber Security Institute[42].

The results demonstrate that full technical consistency generally corresponds to maximum integrity scores within the CRI framework. Nevertheless, partial hash inconsistencies do not automatically render evidence procedurally unreliable where deviations remain traceable, justified, and properly documented.

This finding establishes an important distinction between technical and legal understandings of integrity. From a technical perspective, integrity implies strict immutability of data. From a legal perspective, however, integrity is satisfied where evidentiary transformations remain procedurally transparent and institutionally accountable.

Consequently, the legal significance of hash discrepancies depends not solely on the existence of technical deviations, but on the procedural context in which those deviations occur.

For example: documented system synchronization; authorized forensic conversion procedures; traceable cloud-based replication processes; may justify limited technical inconsistencies without undermining overall evidentiary reliability.

Conversely, even technically minor inconsistencies may become legally significant where documentation is incomplete or procedural traceability is disrupted.

The findings therefore confirm that hash verification functions as an evidentiary indicator rather than an autonomous determinant of reliability. Technical integrity acquires legal significance only when embedded within a procedurally verifiable evidentiary chain.

[42] Mossé Cyber Security Institute. "Preparing documentation and evidence". Mossé Cyber Security Institute Library, 2023. Available at: https://library.mosse-institute.com/articles/2023/08/preparing-documentation-and-evidence.html (accessed on 21 January 2026).

4.5. Chain of custody violations and their impact on reliability

The analysis of evidentiary continuity identified three principal categories of chain-of-custody violations: temporal violations; subject violations; functional violations.

Figure 2 presents the typological distribution of these violations and their relative impact on evidentiary reliability.

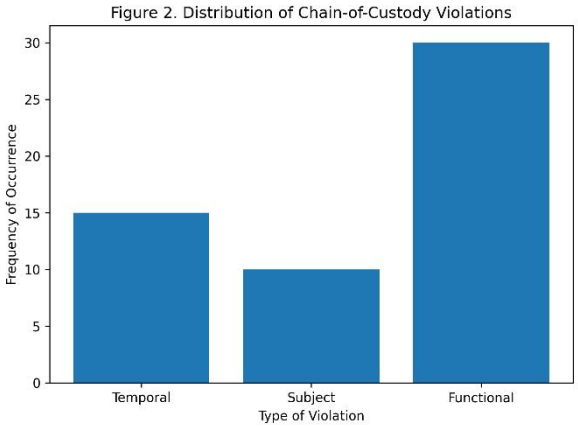

Figure 2. Typology of chain-of-custody violations and their impact on reliability. Source: developed by the author based on data from Cantelli-Forti et al.,[43] Griffiths,[44] Lucoveis et al.[45].

Temporal violations involve delays, interruptions, or gaps in procedural documentation. Subject violations arise through participation of unauthorized or undocumented actors. Functional violations involve unrecorded evidentiary transformations, undocumented processing actions, or opaque analytical procedures.

Among these categories, functional violations demonstrate the most severe impact on CRI outcomes because they directly compromise procedural traceability and interpretability of evidence.

Temporal violations generally affect continuity of custody (C), but may often be remedied through supplementary procedural records or corroborative documentation. Subject violations produce broader procedural risks by potentially affecting both legality (L) and continuity (C).

Functional violations, however, frequently generate irreversible evidentiary opacity. Because unrecorded transformations undermine both integrity (I) and technical verifiability (T), they consistently produce the lowest reliability scores across the dataset.

For investigators and prosecutors, this distinction has important operational implications. Not all procedural defects possess equal evidentiary significance. The

[43] CANTELLI-FORTI, A.; LONGO, G.; LUPIA, F.; RUSSO, E. "WEFT: A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence", International Journal of Information Security, v. 24, 81, 2025. https://doi.org/10.1007/s10207-025-00991-8

[44] GRIFFITHS, C. "The digital forensics project". Counsel: The Magazine of the Bar of England and Wales, 2025. Available at: https://www.counselmagazine.co.uk/articles/the-digital-forensics-project (accessed on 21 January 2026).

[45] LUCOVEIS, M. L.; GAMBA, M.; SILVA, E. Q.; PINTO, L. A.; SACCO, I. C. "The effects of the use of customized silicone digital orthoses on pre-ulcerative lesions and plantar pressure during walking in people with diabetic neuropathy: A study protocol for a randomized controlled trial", Contemporary Clinical Trials Communications, v. 37, 101247, 2024. https://doi.org/10.1016/j.conctc.2023.101247

findings demonstrate that certain irregularities remain procedurally curable, while others fundamentally compromise evidentiary reliability.

Accordingly, the typology developed in this study provides a practical analytical framework for distinguishing between correctable procedural defects and structurally disqualifying evidentiary violations.

4.6. Adversarial validation and procedural robustness

The adversarial modeling stage evaluated the resilience of digital evidence under simulated procedural challenges commonly raised by defense parties during pre-trial and early trial proceedings.

The analysis focused on: allegations of unlawful acquisition; evidentiary contamination; chain-of-custody discontinuities; lack of technical verifiability; insufficient procedural documentation.

Table 4 summarizes the relative resistance of different evidentiary categories to adversarial challenge.

Table 4. Adversarial resistance of digital evidence across categories.

Evidence category	**Resistance level**
Personal devices	Strong
Provider servers	Moderate
Cloud storage systems	Moderate
Network metadata	Strong
Surveillance systems	Very Strong
Voluntary materials	Very Strong

Source: developed by the author based on data from Loux,[46] Champlain College Online[47].

The results demonstrate that procedural transparency and documentation quality constitute the primary determinants of adversarial resistance. Categories characterized by minimal procedural ambiguity—particularly surveillance systems and voluntarily submitted materials—display the highest resilience to procedural challenge. In contrast, cloud-based and provider-controlled evidence demonstrates comparatively moderate resistance due to increased exposure to jurisdictional fragmentation, third-party involvement, and evidentiary discontinuities.

Importantly, the analysis identifies a strong correlation between CRI outcomes and adversarial sustainability. Higher CRI scores consistently correspond to greater resistance against exclusion-oriented procedural objections. This finding confirms the practical utility of the CRI framework as a predictive procedural tool capable of identifying evidentiary vulnerabilities before judicial review occurs. For investigative agencies, such predictive capacity may improve evidentiary screening, strengthen procedural planning, and reduce the likelihood of later evidentiary exclusion.

4.7. Synthesis of findings

Across all analytical dimensions, the results converge on several central conclusions. First, reliability emerges as a cumulative procedural construct formed throughout the entire lifecycle of digital evidence rather than at a single procedural stage. Second, procedural compliance exerts greater influence on reliability than

[46] LOUX, M.; LOUX, B. "How is digital evidence preserved in modern investigations?" 2025. Ibid.

[47] Champlain College Online. "Digital forensics and the chain of custody: How is electronic evidence collected and safeguarded?", 2026. Available at: https://online.champlain.edu/blog/chain-custody-digital-forensics (accessed on 21 January 2026).

technological perfection. Legally justified technical deviations do not necessarily undermine evidentiary reliability, whereas undocumented procedural actions consistently reduce reliability outcomes. Third, the CRI provides a coherent and operational framework capable of distinguishing between: fully reliable evidence; conditionally reliable evidence; procedurally defective evidence.

The study further demonstrates that CRI functions not merely as a descriptive classification tool, but as an integrative analytical mechanism linking empirical evidentiary observations with procedural legal evaluation.

Across heterogeneous evidentiary categories, the framework consistently standardizes reliability assessment while preserving sensitivity to context-specific procedural variations. This confirms that procedural reliability may be operationalized as a measurable evidentiary condition applicable within real investigative practice.

Overall, the findings establish a direct empirical foundation for the doctrinal conclusions developed in the subsequent Discussion section and confirm the practical applicability of the proposed forensic-legal reliability framework.

5. Discussion

5.1. Reliability as a procedural-legal construct

The findings of this study confirm that the reliability of digital evidence at the pre-trial stage should be understood as an autonomous procedural-legal category rather than as a derivative element of technical integrity or judicial admissibility.

The analysis demonstrates that reliability is progressively formed through the procedural lifecycle of evidence and depends on the transparency, continuity, traceability, and institutional accountability of investigative actions. This perspective differs fundamentally from approaches that equate reliability exclusively with technical authenticity or evidentiary admissibility.

The study therefore supports a three-dimensional differentiation of evidentiary concepts: admissibility functions as a retrospective judicial determination governing the possibility of evidentiary use in court; authenticity concerns attribution of data to a particular source or origin; reliability reflects the procedural quality and legal sustainability of evidentiary formation throughout pre-trial proceedings.

This distinction is not merely terminological. It has direct procedural significance because evidentiary reliability may be compromised long before judicial admissibility is formally evaluated. Procedural deficiencies occurring during acquisition, preservation, transfer, or analysis frequently generate irreversible evidentiary vulnerabilities that cannot be fully remedied at trial. Accordingly, the study argues that reliability should be treated as an independent object of procedural evaluation during investigative practice rather than solely as a matter for subsequent judicial review.

5.2. Relationship between technical integrity and procedural reliability

The results demonstrate that technical integrity constitutes a necessary but insufficient condition for procedural reliability. Although forensic verification mechanisms—particularly hash validation, metadata analysis, and audit logging—remain essential components of digital evidence evaluation, their legal significance depends on the procedural environment within which they operate.

The analysis of hash-based verification illustrates this distinction particularly clearly. Technical inconsistencies did not automatically produce evidentiary unreliability where procedural continuity and documentation remained transparent and reproducible. Conversely, even technically accurate data frequently became procedurally vulnerable where evidentiary transformations were insufficiently documented or institutional accountability was disrupted.

These findings challenge technologically deterministic approaches that equate evidentiary validity with computational accuracy alone. From a procedural perspective, digital evidence derives legal reliability not exclusively from technological precision, but from the ability to reconstruct, verify, and contest the evidentiary lifecycle in a transparent procedural context.

The study therefore proposes a procedural interpretation of technical evidence according to which forensic indicators acquire legal relevance only through demonstrable compliance with procedural safeguards.

5.3. Theoretical contribution of the CRI

One of the principal contributions of this research lies in the development of the CRI as an operational framework for evaluating procedural reliability[4849]. Existing doctrinal and forensic models generally identify individual reliability-related factors—such as integrity, chain of custody, or authenticity—but rarely integrate them into a coherent evaluative structure capable of systematic application during pre-trial proceedings[50].

The CRI framework addresses this limitation by organizing reliability assessment around five interconnected procedural criteria: legality; continuity; integrity; authenticity; technical verifiability.

Importantly, the model does not attempt to replace judicial discretion or automate evidentiary evaluation. Instead, it functions as a structured analytical instrument designed to enhance consistency, transparency, and procedural accountability within investigative practice.

The findings demonstrate that the framework remains sufficiently flexible to accommodate complex evidentiary environments while simultaneously preserving methodological coherence across heterogeneous categories of digital evidence.

In this respect, the CRI model contributes not only to forensic methodology, but also to broader discussions concerning procedural rationality, evidentiary governance, and institutional accountability in contemporary criminal proceedings.

5.4. Practical applicability in investigative and prosecutorial practice

The study further demonstrates that the proposed framework possesses significant practical applicability for investigative agencies, prosecutors, forensic specialists, and judicial actors.

Within investigative practice, the CRI model may function as an internal procedural assessment mechanism capable of identifying evidentiary vulnerabilities before materials are transferred for prosecutorial review or judicial examination. Early-stage procedural assessment is particularly important in investigations involving: cloud infrastructures; cross-border data acquisition; distributed network systems; multi-actor evidentiary environments; AI-assisted forensic analysis.

For prosecutors, the framework may assist in evaluating the procedural sustainability of digital evidence prior to indictment decisions. The structured nature of CRI assessment additionally facilitates identification of evidentiary weaknesses requiring supplementary procedural verification or documentation.

From the perspective of defense practice, the framework provides a transparent analytical structure for identifying procedural deficiencies affecting evidentiary

---

[48] Stoykova, R. "A new right to Procedural accuracy: a governance model for digital evidence in criminal proceedings". 2024. Ibid.

[49] Loffi, L.; Camillo, G. L.; DE Souza, C. A.; Westphall, C. M.; Westphall, C. B. "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature review". 2025. Ibid.

[50] Gruber, J.; Hargreaves, C. J.; Freiling, F. C. "Contamination of digital evidence: Understanding an underexposed risk". 2023. Ibid.

reliability. This contributes to strengthening adversarial equality by improving the ability of defense parties to contest procedurally defective digital evidence.

The model may also support institutional standardization of evidentiary handling procedures within investigative agencies by establishing clearer evaluative benchmarks for procedural compliance.

A practical implementation scenario may involve preliminary CRI screening immediately following forensic acquisition. Investigators or forensic specialists could conduct structured evaluation of legality, continuity, integrity, authenticity, and technical verifiability before evidentiary materials enter subsequent procedural stages. Such screening would enable early detection of procedural vulnerabilities and reduce the risk of later evidentiary exclusion. Accordingly, the study confirms that procedural reliability can be operationalized not only as a theoretical legal construct, but also as a practical evidentiary management instrument within contemporary investigative systems.

5.5. AI-based forensic systems and algorithmic accountability

The increasing integration of AI-assisted forensic technologies significantly complicates traditional approaches to evidentiary reliability. Automated analytical systems enhance investigative capacity and permit large-scale processing of digital information, but they simultaneously generate new procedural and doctrinal challenges.

The study demonstrates that AI-driven forensic systems directly affect several core components of the CRI framework, particularly technical verifiability, authenticity, and institutional accountability. Algorithmic opacity may undermine the ability of investigators, courts, and defense parties to independently reconstruct the analytical logic underlying automated forensic conclusions.

This problem becomes especially significant where evidentiary conclusions rely on proprietary machine-learning systems lacking sufficient explainability or reproducibility. In such contexts, procedural reliability may be weakened despite the technical sophistication of the analytical process itself.

The findings therefore support contemporary scholarship emphasizing the importance of explainable AI, procedural transparency, and algorithmic accountability in digital forensic practice. From a procedural perspective, evidentiary systems must remain contestable, reproducible, and institutionally reviewable regardless of their technological complexity.

Accordingly, the study argues that future development of digital evidentiary standards should incorporate explicit procedural safeguards governing: explainability of automated forensic systems; auditability of algorithmic processes; transparency of forensic software architecture; independent verification of AI-generated analytical outputs. These safeguards are necessary to preserve procedural fairness and maintain confidence in technologically mediated evidentiary systems.

5.6. Comparative and cross-jurisdictional implications

Although the empirical dataset is primarily derived from Ukrainian investigative practice, the analytical framework developed in this study possesses broader comparative relevance.

The procedural problems identified in the research—fragmented chain of custody, multi-actor evidence handling, cloud-based evidentiary environments, and algorithmic opacity—are characteristic of digital investigations across many contemporary criminal justice systems. The CRI framework may therefore contribute to harmonization of procedural reliability assessment within jurisdictions

influenced by European evidentiary standards and adversarial procedural safeguards.

This comparative applicability is particularly important in cross-border cybercrime investigations, where evidentiary continuity frequently depends on cooperation between multiple institutional and jurisdictional actors. In such contexts, standardized procedural reliability criteria may strengthen legal certainty and improve interoperability between investigative systems. The study therefore contributes not only to national procedural doctrine, but also to broader international discussions concerning digital evidence governance, procedural accountability, and transnational evidentiary standards.

5.7. Limitations of the study

Several limitations of the present research should be acknowledged. First, the empirical dataset is jurisdictionally concentrated and primarily reflects Ukrainian investigative practice. Although the procedural structures examined are broadly comparable to continental criminal procedure systems, direct generalization to all jurisdictions should be approached cautiously. Second, the purposive sampling strategy prioritizes analytical depth rather than statistical representativeness. The objective of the study was to construct a normative and operational framework rather than to quantify empirical prevalence of procedural defects. Third, rapidly evolving forensic technologies—particularly AI-assisted analytical systems and cloud-based infrastructures—may generate new procedural challenges requiring further adaptation of reliability criteria. Finally, the CRI framework remains a decision-support instrument rather than an automated evidentiary algorithm. Its practical effectiveness depends on consistent procedural implementation, institutional training, and appropriate forensic documentation practices.

5.8. Directions for future research

Future research should focus on several interconnected areas. First, comparative cross-jurisdictional validation of the CRI framework would strengthen its applicability within different procedural systems and legal traditions. Second, further research is needed concerning the interaction between AI-assisted forensic systems and procedural safeguards governing explainability, transparency, and algorithmic accountability. Third, empirical evaluation of CRI implementation within investigative agencies could provide additional insight into operational effectiveness, institutional adaptability, and procedural standardization. Finally, future studies may explore the possibility of integrating procedural reliability assessment into digital case-management systems and forensic workflow architectures in order to improve evidentiary governance within technologically complex investigations.

Overall, the findings confirm that procedural reliability represents an essential and autonomous dimension of digital evidence evaluation. By integrating doctrinal analysis, forensic methodology, and operational assessment, the present study establishes a coherent framework capable of supporting more transparent, accountable, and procedurally sustainable evidentiary practices in contemporary criminal proceedings.

6. Conclusion

This study examined the procedural reliability of digital evidence at the pre-trial stage of criminal proceedings and demonstrated that reliability should be understood as an autonomous procedural-legal category distinct from both technical authenticity and judicial admissibility.

The findings confirm that the reliability of digital evidence is not an inherent property of digital data itself, but rather the result of procedurally regulated

evidentiary formation occurring throughout the entire lifecycle of evidence. Reliability emerges through the interaction of procedural legality, continuity of custody, integrity, authenticity, technical verifiability, and institutional accountability.

The research established that procedural compliance exerts greater influence on evidentiary reliability than technological sophistication alone. Even technically imperfect evidence may retain procedural reliability where deviations remain transparent, justified, and properly documented. Conversely, undocumented procedural actions and disruptions in evidentiary traceability significantly undermine reliability regardless of technical accuracy.

A central contribution of the study lies in the development of the CRI as a structured legal-analytical framework for assessing digital evidence during pre-trial proceedings. The CRI model integrates five interconnected evaluative criteria and provides a transparent mechanism for distinguishing between reliable, conditionally reliable, and procedurally defective evidence.

The practical applicability of the framework was confirmed through procedural reconstruction, adversarial validation, and comparative analysis across multiple categories of digital evidence. The results demonstrate that the CRI model may support investigators, prosecutors, forensic specialists, and judicial actors in identifying evidentiary vulnerabilities prior to judicial review and in strengthening procedural accountability within investigative practice.

The study further highlighted the growing importance of explainability, transparency, and algorithmic accountability in the context of AI-assisted forensic systems. The increasing use of automated analytical technologies requires the development of procedural safeguards capable of ensuring reproducibility, contestability, and institutional oversight of digital forensic processes.

Although the empirical basis of the research is primarily derived from Ukrainian investigative practice, the proposed framework possesses broader comparative relevance for jurisdictions confronting similar challenges associated with cloud infrastructures, cross-border investigations, distributed digital environments, and technologically complex evidentiary systems.

Overall, the study contributes to contemporary scholarship on criminal procedure and digital forensics by establishing a coherent procedural framework for reliability assessment and by advancing a more transparent, accountable, and operationally applicable model of digital evidence evaluation in modern criminal proceedings.

7. References

AL-Billeh, T.; AL-Hammouri, A.; Khashashneh, T.; Makhmari, M. A.; Kalbani, H. A. "Digital evidence in human rights violations and international criminal justice", Journal of Human Rights Culture and Legal System, v. 4, n. 3, p. 842–871, 2024. https://doi.org/10.53955/jhcls.v4i3.446

Angel, O. E. M., Mercedes, C. F. Y. M., Elisa, Q. L. A., Joaquin, D. J.; DE OLIVEIRA DIAZ DENY Giovanna, C.; Beatriz, G. Q. G. "Digital evidence as a means of proof in criminal proceedings", Revista De Gestão Social E Ambiental, v. 18, n. 4, e04585, 2024. https://doi.org/10.24857/rgsa.v18n4-028

Bérubé, M.; Beaulieu, L.-A., Allard, S.; Denault, V. "From digital trace to evidence: Challenges and insights from a trial case study", Science Justice, v. 65, n. 5, 101306, 2025. https://doi.org/10.1016/j.scijus.2025.101306

Billah, M. "Developing an explainable AI system for digital forensics: enhancing trust and transparency in flagging events for legal evidence", International Journal of Latest Technology in Engineering Management & Applied Science, v. 14, n. 7, p. 6–16, 2025. https://doi.org/10.51583/ijltemas.2025.1407000002

CANTELLI-Forti, A.; Longo, G.; Lupia, F.; Russo, E. "WEFT: A consistent and tamper-proof methodology for acquisition of automatically verifiable forensic web evidence",

International Journal of Information Security, v. 24, 81, 2025. https://doi.org/10.1007/s10207-025-00991-8

Casino, F.; Pina, C.; LÓPEZ-Aguilar, P.; Batista, E.; Solanas, A.; Patsakis, C. "SoK: cross-border criminal investigations and digital evidence", Journal of Cybersecurity, v. 8, n. 1, 2022. https://doi.org/10.1093/cybsec/tyac014

Champlain College Online. "Digital forensics and the chain of custody: How is electronic evidence collected and safeguarded?", 2026. Available at: https://online.champlain.edu/blog/chain-custody-digital-forensics (accessed on 21 January 2026).

COUNCIL OF EUROPE. Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe, 2001. Available at: https://rm.coe.int/1680081561 (accessed on 21 January 2026).

Dufeniuk, O.; Melnyk, N.; Nahorniak, Y.; Melnyk, S. "Innovative potential of 3D technologies in crime investigation", Social Legal Studios, v. 7, n. 4, p. 222–230, 2024. https://doi.org/10.32518/sals4.2024.222

European Union Agency for Fundamental Rights. "Assessing high-risk AI: Fundamental rights risks". Publications Office of the European Union, 2025. Available at: https://privacy-web.nl/wp-content/uploads/2025/12/fra-2025-assessing-high-risk-ai-fundamental-rights-risks_en.pdf (accessed on 21 January 2026).

Forensic Focus. Forensic Focus legal update July 2021: Reliability and credibility of digital evidence, 2021. Available at: https://www.forensicfocus.com/legal/forensic-focus-legal-update-july-2021-reliability-and-credibility-of-digital-evidence/ (accessed on 21 January 2026).

Griffiths, C. "The digital forensics project". Counsel: The Magazine of the Bar of England and Wales, 2025. Available at: https://www.counselmagazine.co.uk/articles/the-digital-forensics-project (accessed on 21 January 2026).

Gruber, J.; Hargreaves, C. J.; Freiling, F. C. "Contamination of digital evidence: Understanding an underexposed risk", Forensic Science International Digital Investigation, v. 44, 301501, 2023. https://doi.org/10.1016/j.fsidi.2023.301501

KIENER-Manu, K. E4J University Module Series: Cybercrime. Module 4: Introduction to Digital Forensics, 2026. Available at: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/standards-and-best-practices-for-digital-forensics.html (accessed on 21 January 2026).

Lasagni, G. "Admissibility of Digital Evidence from Part I - Collecting Digital Evidence", In V. Franssen S. Tosza (Eds.), The Cambridge Handbook of Digital Evidence in Criminal Investigations. Cambridge: Cambridge University Press, 2025, p. 126–152. Available at: https://www.cambridge.org/core/books/abs/cambridge-handbook-of-digital-evidence-in-criminal-investigations/admissibility-of-digital-evidence/7F8292A7652FF16F5EA850B2984EE0E5 (accessed on 21 January 2026).

Loffi, L.; Camillo, G. L.; DE Souza, C. A.; Westphall, C. M.; Westphall, C. B. "Management of the Chain of Custody of Digital Evidence Using Blockchain and Self-Sovereign Identities: A Systematic Literature review", IEEE Access, v. 13, p. 77804–77832, 2025. https://doi.org/10.1109/ACCESS.2025.3560191

Loux, M.; Loux, B. "How is digital evidence preserved in modern investigations?", American Military University, 2025. Available at: https://www.amu.apus.edu/area-of-study/criminal-justice/resources/how-is-digital-evidence-preserved/ (accessed on 21 January 2026).

Lucoveis, M. L.; Gamba, M.; Silva, E. Q.; Pinto, L. A.; Sacco, I. C. "The effects of the use of customized silicone digital orthoses on pre-ulcerative lesions and plantar pressure during walking in people with diabetic neuropathy: A study protocol for a randomized controlled trial", Contemporary Clinical Trials Communications, v. 37, 101247, 2024. https://doi.org/10.1016/j.conctc.2023.101247

Lytvyn, N.; Andrushchenko, H.; Zozulya, Y. V.; Nikanorova, O. V.; Rusal, L. M. "Enforcement of court decisions as a social guarantee of protection of citizens rights and freedoms", PRAWO I WIĘŹ, v. 1, n. 39, p. 80–102, 2022. https://doi.org/10.36128/priw.vi39.351

Martinengo, L.; Ng, M. S. P., DE RONG Ng, T.; Ang, Y.; Jabir, A. I.; Kyaw, B. M.; Car, L. T. "Spaced digital education for health professionals: Systematic review and meta-analysis", Journal of Medical Internet Research, v. 26, e57760, 2024. https://doi.org/10.2196/57760

Masaar. New judicial trend: Criminal court overturns conviction due to invalidity of digital forensic evidence, 2025. Available at: https://masaar.net/en/court-overturns-conviction-due-to-invalidity-of-digital-forensic-evidence/ (accessed on 21 January 2026).

Meinheit, A. "From bytes to bench: Leveraging digital forensics in the litigation lifecycle", Complete Legal, 2025. Available at: https://completelegal.us/from-bytes-to-bench-leveraging-digital-forensics-in-the-litigation-lifecycle/ (accessed on 21 January 2026).

MindMeister, Online mind mapping tool, 2026. Available at: https://www.mindmeister.com (accessed on 21 January 2026).

Mossé Cyber Security Institute. "Preparing documentation and evidence". Mossé Cyber Security Institute Library, 2023. Available at: https://library.mosse-institute.com/articles/2023/08/preparing-documentation-and-evidence.html (accessed on 21 January 2026).

Naik, S.; Agarwal, S. When digital evidence fails: The corporate cost of ignoring metadata. LiveLaw, 2026. Available at: https://www.livelaw.in/amp/articles/digital-evidence-indian-corporation-519181 (accessed on 21 January 2026).

Romaniuk, V. V.; Ablamskyi, S. Y. "Criteria for the admissibility of digital (electronic) evidence in criminal proceedings", Law And Safety, v. 93, n. 2, p. 140–150, 2024. https://doi.org/10.32631/pb.2024.2.13

Rosenstrauch, D., Mangla, U., Gupta, A., & Masau, C. T. "Correction to: Artificial Intelligence and ethics", In: Meyers, A. (eds) Digital Health Entrepreneurship. Health Informatics. Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33902-8_17

Shchokin, R.; Oliinyk, V.; Amelin, O.; Bondarenko, Y.; Maziychuk, V.; Kyslenko, D. "Methods of combating offenses in the field of ecology", Journal of Environmental Management and Tourism, v. 14, n. 1, 5, 2023, p. 5-15. https://doi.org/10.14505/jemt.v14.1(65).01

Stoykova, R. "A new right to Procedural accuracy: a governance model for digital evidence in criminal proceedings", Computer Law Security Review, v. 55, 106040, 2024. https://doi.org/10.1016/j.clsr.2024.106040

Supreme Court of Ukraine. A Supreme Court judge analyzed the criteria for admissibility and reliability of electronic evidence in criminal proceedings. Judiciary of Ukraine, 2025. Available at: https://court.gov.ua/press/news/1751426/ (accessed on 21 January 2026).

Supreme Court of Ukraine. Cybercrime and electronic evidence: Supreme Court judge explains the assessment of electronic evidence in criminal proceedings, 2024. Available at: https://court.gov.ua/eng/supreme/pres-centr/news/1594957/ (accessed on 21 January 2026).

United Nations Office on Drugs and Crime. "E4J University Module Series: Cybercrime. Module 6: Practical Aspects of Cybercrime Investigations and Digital Forensics", 2019. Available at: https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/digital-evidence-admissibility.html (accessed on 21 January 2026).

UNITED NATIONS. "Report of the Secretary-General on the work of the Organization 2025: Combating drugs, crime and terrorism", United Nations, 2025. Available at: https://www.un.org/sites/un2.un.org/files/sg_annual_report_2025_drugs-crime-terrorism_en.pdf (accessed on 21 January 2026).

Van Krimpen, F., De Bruijn, H., & Arnaboldi, M. "Machine Learning Algorithms and Publicdecision-making: A Conceptual Overview", In The Routledge Handbook of Public Sector Accounting (1st ed., pp. 124–138). Routledge - Taylor & Francis Group. 2023. https://doi.org/10.4324/9781003295945-12

Yermachenko, V. "Theory and practice of public management of smart infrastructure in the conditions of the digital society' development: Socio-economic aspects", Economic Affairs, v. 68, n. 1, p. 617-633, 2023. https://doi.org/10.46852/0424-2513.1.2023.29