Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

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

DIGITAL PLATFORMS FOR THE CAPTURE AND LONG-TERM PRESERVATION OF EVIDENCE OF WAR CRIMES IN COMBAT ZONES

VIKTORIIA ZARUBEI [1*], YELZAVETA KUZMICHOVA-KYSLENKO[2], OLHA RYMARCHUK[1], BOHDANA TYCHNA[3], EDUARD SOLOVIOV[1]

[1]Department of Criminal Procedure, National Academy of Internal Affairs, Kyiv, Ukraine.

[2]National Academy of Internal Affairs, Kyiv, Ukraine.

[3]National Defence University of Ukraine, Kyiv, Ukraine.

E-mail: [1]viktoriazarubej@gmail.com, [2]kyslenko@gmail.com, [3]Rymarchuk.O@ukr.net, [4]tychna_bohd@gmail.com, [5]solovyoved02@gmail.com

ABSTRACT

Introduction: The relevance of the research was determined by the need to ensure the evidentiary admissibility, integrity, and long-term preservation of digital evidence of war crimes in combat zones in the context of fragmented platform architectures and increasing algorithmization of data collection.
Aim: The aim of the study was to empirically substantiate and metrically verify the regulatory and technical framework of digital platforms for capturing and long-term preservation of evidence of war crimes in combat zones.
Methods: The study was based on an interdisciplinary methodology that combined normative analysis and controlled technical experiments to close the gap between admissibility requirements and the architectural behaviour of digital platforms in combat zones for the empirical identification of configurations that ensure long-term evidentiary admissibility.
Results: The study showed that the effectiveness of digital platforms for capturing and long-term preservation of war crimes evidence was determined by the architectural ability to maintain a continuous evidentiary loop. Class-specific quality losses (packet loss 3–17%, timestamp deviation ±2–9 s), provenance gaps with high cryptographic stability (HSI up to 100%), uneven detection of manipulations (MDR 61–94%), and a compromise between preservation and availability (DRR 92–99%) were identified. The synthesized framework demonstrated the highest consistency of technical and legal parameters (LCI ≈ 0.93; AS ≈ 0.92; PPR > 0.95), ensuring stable evidentiary admissibility.
Academic novelty: The academic novelty consisted in the platform-centric metric linking of digital evidence capture and preservation with admissibility criteria through the LCI and AS indices and framework verification with the measured metrics HSI, PPR, MDR, and DRR.
Conclusion: Further research may focus on in-situ validation of the framework in real judicial and investigative processes, expansion of metrics through explainability for AI components, and development of standardized benchmark sets for cross-jurisdictional comparison of admissibility. Open issues include: (i) how to ensure longitudinal stability of provenance under multi-year storage conditions; (ii) how to calibrate LCI/AS thresholds across jurisdictions with heterogeneous evidentiary standards; (iii) how to integrate XAI metrics without degrading operational efficiency; (iv) how to minimize ALM growth while maintaining DRR ≥95 %; (v) how to prevent provenance fragmentation in hybrid and decentralized architectures; (vi) how to standardize admissibility benchmarks for conflict-zone data variability.
Keywords: *Digital Evidence, War Crimes, Digital Platforms, Provenance, Admissibility of Evidence, Long-Term Preservation, International Criminal Law*

1. INTRODUCTION

Relevance of the research. The relevance of the study was determined by the need to ensure reliable fixation, verification and long-term preservation of digital evidence of war crimes in combat zones under high technological, legal, and security turbulence. The massive use of digital platforms, large data sets and automated tools in the security and investigative circuit led to increased risks of loss of provenance, violation of integrity, bias of interpretation and conflict between efficiency and procedural

guarantees [1, 2]. At the same time, the digitalization of law enforcement and management decisions required a normatively guided integration of information models, storage architectures and legal admissibility criteria in times of conflict [3, 4]. In this context, research into digital platforms for the capture and long-term preservation of war crimes evidence has become critical to ensuring the sustainable admissibility, legitimacy, and evidentiary value of digital materials in international criminal justice [5, 6].

Research gap. Existing research has fragmented digital evidence along separate dimensions (algorithmic collection, OSINT, archiving, ethics), without offering a metrically verified integrative approach that would combine capture, provenance, integrity, spatiotemporal verification, and long-term preservation in a combat environment.

Research hypothesis. The integration of regulatory mapping and technical metrics into a single architecture provided statistically higher admissibility of digital evidence (AS > 0.90) compared to fragmented platform solutions.

Research aim. The aim is to empirically substantiate and metrically verify the regulatory and technical framework of digital platforms for the capture and long-term preservation of evidence of war crimes in combat zones.

Research objectives:

1. Formalize regulatory requirements for digital evidence and operationalize admissibility as a limiting variable (LCI).
2. Quantify the impact of platform architectures on the quality of initial evidence capture at the capture stage.
3. Test the cryptographic immutability of digital evidence and the role of provenance in different storage architectures.
4. Assess the resilience of platforms to spatiotemporal tampering in combat environments.
5. Model long-term evidence preservation and identify archival structural vulnerabilities.
6. Synthesize technical and legal results into an integrative regulatory and technical framework and empirically verify it.

2. LITERATURE REVIEW

The asymmetric nature of armed conflicts, platform fragmentation, and the exponential growth of digital traces of violence caused a structural mismatch between the speed of recording events and the requirements of long-term evidentiary suitability. The lack of agreed technical and legal parameters for preservation, verification, and access increased the risks of losing the integrity, context, and procedural manageability of digital evidence. This objectively necessitated a systematic literature review to identify the conceptual, technological, and regulatory limitations of existing approaches.

The creation of digital platforms for recording war crimes in combat zones has long been based on a procedural logic, where priority was given to early-stage preservation, integrity control, and chain of custody as conditions for admissibility. Granja and Rodriguez Rafael [7] argued that even minimal metadata losses reduced forensic reliability and made it impossible to reuse evidence in court. Instead, Roush [8] demonstrated that the operational scalability of OSINT and crowdsourced documentation often outweighed formalized evidentiary purity in armed conflict settings.

Further development of approaches shifted the focus from single pieces of evidence to archival infrastructures as the core of platforms. Ochi and Dagenborg [9] showed that evidence, legal and memory archives required different technical and human rights regimes, and the lack of standardization of data integrity and security reduced their effectiveness. At the same time, Dubberley et al. [10] insisted that excessive unification limited the adaptability of open-source investigations and reduced the evidentiary value of user-generated digital evidence.

The problem of long-term preservation was conceptualized by contrasting archival stability with platform variability. Borghoff et al. [11] proved the effectiveness of the OAIS model, format standardization, and migration for data preservation for more than 50 years. Instead, Makhortykh [12] documented that platform dependency and algorithmic moderation environments systematically increased the risks of loss and fragmentation of digital evidence of mass violence.

The normative dimension of capture platforms revealed tensions between procedural controllability and human rights. Kuczyńska [13] showed that the abundance of algorithmic digital evidence required new verification and evidence management procedures. In turn, Al-Billeh et al. [14] emphasized the need for unified principles for the use of open-source digital evidence to balance privacy and international criminal liability.

The final analytical subset concerned the practical suitability of platforms in times of crisis. Moss and Gollins [15] argued that a technocentric focus on

preservation without appraisal and sensitivity review led to a loss of archival authenticity. On the contrary, Malm [16] showed the effectiveness of lightweight emergency solutions for rapid fixation, while recording legal restrictions on access to digital artifacts and their possession.

Prior studies consistently demonstrated a disciplinary fragmentation of approaches: technical research prioritized integrity and long-term archival stability, legal scholarship focused on admissibility, privacy, and procedural safeguards, while platform-oriented solutions emphasized scalability and rapid capture in conflict environments. These streams advanced important partial solutions but remained weakly integrated, resulting in a persistent gap between operational evidence collection and its sustained legal admissibility. In contrast, the present study was motivated by the need to overcome this fragmentation through a unified, metric-driven perspective, treating digital platforms as socio-technical evidence pipelines. Unlike prior works, which predominantly addressed isolated components, this research empirically demonstrated that only an integrative architecture aligning capture, cryptographic verification, provenance continuity, spatiotemporal validation, and archival retention with formal admissibility criteria ensured stable evidentiary validity (AS ≈ 0.92; LCI ≈ 0.93). Thus, the study contributed a systematic framework and quantitative validation that bridged the gap between technological functionality and legal admissibility in combat settings.

Problem statement. The lack of regulatory-controlled digital platform architectures has led to systemic losses of admissibility of digital evidence of war crimes because of deficiencies in provenance, spatial-temporal integrity, and archival resilience.

Research questions. What architectural configurations of digital platforms ensured robust admissibility of evidence in combat zones? How did technical metrics (LCI, HSI, PPR, MDR, DRR) correlate with legal admissibility criteria? Did the integrated framework outperform existing platforms?

The study followed a staged protocol grounded in prior methodological and conceptual developments. First, a structured literature review was conducted to identify fragmentation across evidentiary preservation, OSINT scalability, and archival infrastructures, as documented in earlier works [7–10]. This stage operationalized admissibility constraints and defined core attributes (integrity, provenance, chain of custody) consistent with established preservation and investigation practices [7], [10]. Second, an analytical synthesis of archival and platform-oriented studies was performed to formalize long-term preservation requirements, drawing on OAIS-based models and documented risks of platform dependency and data loss [11, 12]. Third, the normative dimension was incorporated through comparative analysis of legal and human-rights-oriented approaches to digital evidence, ensuring alignment with admissibility and procedural safeguards [13, 14]. Fourth, empirical modeling and controlled experiments were designed to test platform behavior under conditions of capture variability, cryptographic verification, and adversarial manipulation, extending prior insights on emergency documentation and crisis-driven archiving [15, 16]. Finally, results were integrated through a metric-driven synthesis, linking technical parameters to legal admissibility criteria and producing a unified regulatory–technical framework that addressed the fragmentation identified in earlier studies.

3. METHODS AND MATERIALS

3.1. Research procedure

The research design. The research design (Figure 1) was constructed as a sequentially integrated regulatory and technical pipeline that allowed for the empirical evaluation of digital platforms for capturing and long-term preservation of war crimes evidence in combat zones. The combination of regulatory formalization, controlled experiments, and metric verification was justified by the need to bridge the gap between legal admissibility and technical realization of evidence, as well as to identify architectural sources of admissibility losses at all stages of the digital evidence lifecycle.

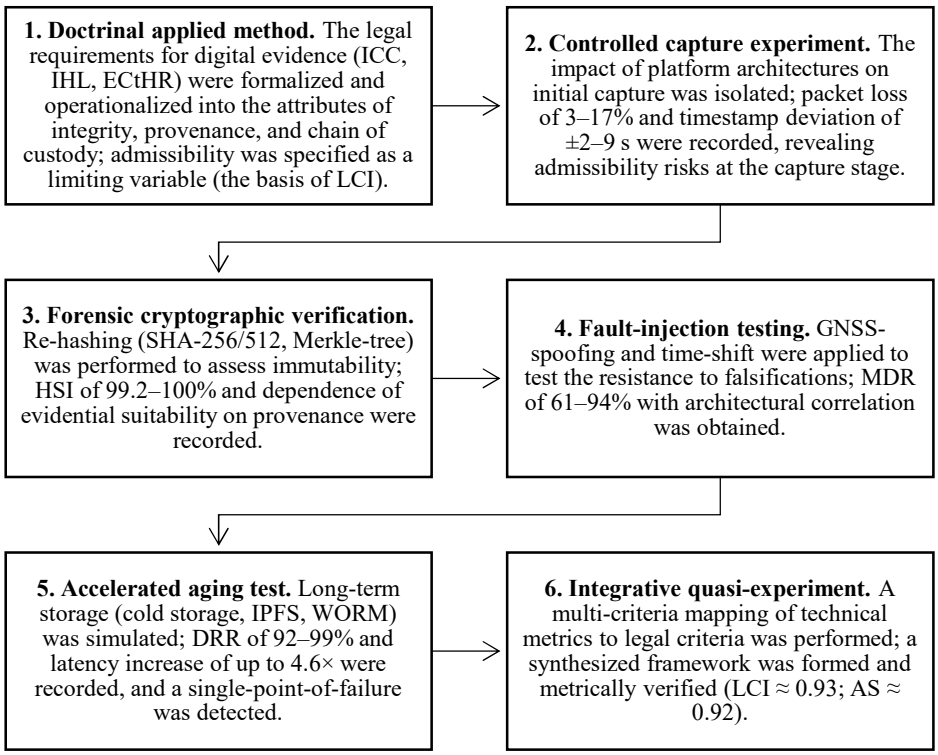

Figure 1: Integrated Regulatory And Technical Design Research Of Digital Platforms For Capturing And Long-Term Preservation Of Evidence Of War Crimes Source: Developed By The Authors

3.2. Methods

In view of the complexity of capturing and long-term preservation of digital evidence of war crimes in combat zones, the study relied on a multi-level interdisciplinary methodology that combined legal analysis, controlled technical experiments, and integrative synthesis. This approach was necessary to bridge the gap between regulatory requirements for admissibility and the real architectural behaviour of digital platforms in combat settings. The combination of methods made it possible to identify individual deficiencies (capture, provenance, retention) and empirically prove which architectural configurations provide integral evidentiary admissibility.

1. *Doctrinal applied method.* The method was used to formalize the requirements for digital evidence based on ICC, IHL, and ECtHR standards. Its use was justified by the need to transform abstract legal principles into operationalized platform attributes (integrity, provenance, chain of custody). This resulted in building a normative admissibility profile, which defined admissibility as a limiting variable for all subsequent experiments and formed the basis for the LCI calculation.

2. *Controlled laboratory experiment of capture scenarios.* The method was used to isolate the impact of platform architectures on the quality of initial evidence capture. Its appropriateness was determined by the impossibility of obtaining reproducible results in real combat settings. The experiment enabled quantitative recording of packet loss and time deviations, showing that admissibility deficiencies arise already at the capture stage.

3. *Forensic cryptographic verification (forensic experiment).* The re-hashing and Merkle-tree verification method was used to assess the immutability of digital evidence in different storage architectures. Its use was justified by the requirements of immutability in international criminal law. The results showed that cryptographic stability does not guarantee evidential suitability without preserved provenance.

4. *Fault-injection testing (GNSS-spoofing i time-shift).* The method was used to empirically test the resilience of platforms to spatiotemporal attribute falsifications. Its appropriateness was determined by the prevalence of manipulations in combat zones. The obtained values proved that the depth of

integration of verification mechanisms directly correlates with the type of platform architecture.

5. *Accelerated aging test (archival experiment)*. The method was used to model long-term preservation without multi-year surveillance, which is critical for war crimes with delayed justice. The use of cold storage, IPFS, and WORM also made it possible to record the increase in available latency, revealing the structural vulnerability of centralized storage.

6. *Integrative quasi-experiment and multi-criteria mapping*. The method was used to synthesize technical results with legal criteria of admissibility and human-rights compliance. Its application was justified by the need to move from fragmented platform assessment to a systemic regulatory solution. As a result, a synthesized framework was formed and its superiority was confirmed through normalized metrics, which completed the empirical validation of the study.

Taken together, the methods used provided end-to-end verification of digital platforms from the moment the evidence was captured in combat settings to its long-term archival and procedural suitability, which gave grounds to reasonably propose an integrative regulatory and technical framework.

3.3. Sample

The study sample (Table 1) was formed through a purposeful selection of digital platforms used for the capture, verification, and archival storage of digital evidence of war crimes in high-risk environments. The inclusion criteria were architectural diversity (centralized, hybrid, decentralized models), the availability of cryptographic integrity, provenance tracking and long-term preservation tools, as well as compliance with international evidentiary and human-rights standards. Empirical experiments, as well as technical and legal tests were conducted during 2023–2025.

Table 1: Sample of digital platforms for the capture and long-term storage of evidence of war crimes

Platform class / Platforms	**Evidence capture tools / Legal and procedural norms governing platforms**	**Architectural solutions for the archive of war crimes storage / Analysis of the possibility of long-term storage of evidence of war crimes**	**Academic research**
Centralized capture platforms / eyeWitness to Atrocities, Uwazi, KoBoToolbox	Mobile applications with capture SDK, GPS-timestamping, metadata locking / Chain of custody, evidentiary integrity, admissibility standards	Central servers, role-based access, backup / High manageability, but critical single-point-of-failure risks	Thouvenin et al. [17]; Winter [18]
Hybrid human rights platforms / HURIDOCS, Mnemonic, OpenArchive	Mobile capture, OSINT ingestion, manual verification / IHL documentation standards, data protection, due process	Centralized core + distributed redundancy / Balance between controllability and archival resilience	D'Alessandra and Sutherland [19]; Murray et al. [20]
Decentralized evidence repositories / IPFS, Filecoin, Arweave	Client-side hashing, content addressing / Immutability principles, trust minimization	P2P replication, blockchain anchoring / High immutability but limited procedural control	Loshytskyi et al. [21]; Werthmuller 22]
OSINT collection infrastructures / Bellingcat toolchain, Amnesty Citizen Evidence Lab, Maltego	Web-scraping, social media capture, metadata extraction / OSINT verification protocols, Berkeley Protocol	External platforms + archival proxies / Need for immediate archiving to prevent loss	Unver [23]; Niezen [24]
Satellite monitoring platforms / Sentinel Hub, Planet Labs archives, UNOSAT	Remote sensing, temporal change detection / Geospatial evidence standards, scientific reproducibility	Geospatial archives, time-series repositories / High reproducibility with format stability	Hasian Jr. [25]; Qerimi [26]
Digital war criminal archives / ICC digital repositories, Internet Archive	Forensic Ingestion, provenance tracking / ICC evidentiary rules, archival standards	OAIS-oriented repositories, cold storage / Maximum long-term preservation	Halilovich [27]; Verschure and Wierenga [28]
Emergency documentation platforms	Fast capture, offline mode, minimal metadata / Emergency	Temporary storage with subsequent migration / Efficient for commit, but	Cohen [29]; Lloyd and Steele [30]

/ OpenArchive Mobile, emergency capture apps	documentation guidelines, do-no-harm	dependent on subsequent integration	
Memorial and memory archives / Digital memory archives, oral history platforms	Oral testimony, multimedia recording / Ethical archiving, consent-based access	Semi-centralized collections, access control / Long-term preservation with ethical access restrictions	Cox [31]; Bar-Gil [32]

Source: developed by the authors

3.4. Research tools

The Research Tools section was aimed at formalizing empirical measurements by mathematically describing key metrics that reflected the legal admissibility, technical integrity, and long-term preservation of digital evidence of war crimes. The proposed set of indices and coefficients provided quantitative agreement on capture processes, cryptographic integrity, provenance stability, archival stability, and admissibility. Such a metric-oriented model enabled integrating technical and technological results with the regulatory requirements of evidentiary law:

1. *Legal Compliance Index (LCI)*. The metric reflects the level of legal admissibility of digital evidence:

$$LCI = \frac{\sum_{i=1}^{n} a_i}{n}, \quad (1)$$

where $a_i \in \{0,1\}$ – fulfilment of *i* legal attribute (ICC, IHL, ECtHR); n - the total number of mandatory regulatory requirements.

2. *Metadata Completeness Rate (MCR)*. Metric assesses the quality of primary capture:

$$MCR = \frac{m_{valid}}{m_{expected}}, \quad (2)$$

where m_{valid} – the number of correctly recorded metadata; $m_{expected}$ — the normatively expected number of fields.

3. *Packet Loss Ratio (PLR)*. The indicator characterizes the network degradation of the capture process.

$$PLR = \frac{p_{lost}}{p_{sent}}, \quad (3)$$

where p_{lost} – number of lost packets; p_{sent} – total number of transferred packets.

4. *Timestamp Deviation (TD)*. The metric was used to assess temporal integrity:

$$TD = \left|t_{recorded} - t_{reference}\right|, \quad (4)$$

where $t_{recorded}$ – recorded time of event; $t_{reference}$ – reference time signal.

5. *Hash Stability Index (HSI)*. The indicator reflects the cryptographic immutability of evidence:

$$HSI = \frac{h_{cosistent}}{h_{total}}, \quad (5)$$

where $h_{cosistent}$ – number of immutable hash values; h_{total} – total number of checks.

6. *Provenance Preservation Rate (PPR)*. The metric characterizes the sustainability of the chain of custody.

$$PPR = 1 - \frac{e_{broken}}{e_{total}}, \quad (6)$$

where e_{broken} – number of broken provenance links; e_{total} – total number of events in the chain of evidence.

7. *Manipulation Detection Rate (MDR)*. The indicator assesses the effectiveness of spatiotemporal verification.

$$MDR = \frac{d_{detected}}{d_{attempted}}, \quad (7)$$

where $d_{detected}$ – number of detected manipulations; $d_{attempted}$ – number of injected distortions.

8. *Data Retention Rate (DRR)*. Metric reflects long-term sustainability:

$$DDR = \frac{D_{accessible}(t)}{D_{stored}(t_0)}, \quad (8)$$

where $D_{stored}(t_0)$ – data volume at the time of archiving; $D_{accessible}(t)$ – amount of available data after aging cycle.

9. *Access Latency Multiplier (ALM)*. The indicator characterizes the archival degradation of accessibility.

$$ALM = \frac{L_{archival}}{L_{baseline}}, \quad (9)$$

where $L_{archival}$ – average access latency from the archive; $L_{baseline}$ – basic delay in primary storage.

10. *Admissibility Score (AS)*. The index reflects the alignment of technical architecture with the requirements of evidentiary law:

$$AS = \sum_{k=1}^{m} w_k \times M_k, \quad (10)$$

where M_k – normalized technical and legal metrics; w_k – weighting factors of legal significance; m – number of metrics.

Comparability of heterogeneous metrics that had different measurement scales and units (fractions, percentages, seconds) was ensured by normalizing the values to the dimensionless interval [0,1]. This made it possible to eliminate the scale effect and correctly compare the contribution of each metric within one platform class and between classes, as well as ensure further aggregation into composite indices. Normalization was necessary before constructing cumulative diagrams and before calculating the integral admissibility index:

$$M_k^{norm} = \frac{M_k - \min(M_k)}{\max(M_k) - \min(M_k)}, \quad (11)$$

where M_k – the initial value of the k metric; $\min(M_k)$ and $\max(M_k)$ – the minimum and maximum values of this metric in the sample of platforms.

The obtained nsormalized values were used for interclass comparison and subsequent multi-criteria matching.

The study used a specialized software suite integrated according to the experimental stages. Legal analysis was supported by structured evidentiary checklists formalized in NVivo and Excel to encode ICC, IHL, and ECtHR requirements. Primary digital evidence was captured using eyeWitness to Atrocities, OpenArchive Mobile, and KoBoCollect mobile applications that leveraged GNSS, sensor APIs, and built-in capture SDKs. Cryptographic integrity and provenance were verified using OpenSSL, Hashdeep, and Merkle-tree modules of IPFS. Spatiotemporal verification was implemented using GPSTest, GNS3-based spoofing emulators, and log correlation in Wireshark. Long-term preservation and stability of archives were assessed using IPFS, Filecoin, Arweave, WORM media, and AWS Glacier cold storage. Integrative technical and legal synthesis and multi-criteria metric matching were performed in Python (NumPy, Pandas) with subsequent visualization and analysis of the results.

4. RESULTS

The first stage of the research was aimed at formalizing the legal requirements for digital evidence as determinants of further experimental design. The use of a doctrinal applied method enabled translating abstract standards of admissibility into measurable technical attributes of capturing, preservation, and chain of custody. Such a formulation ensured the legal validity of all subsequent technical and technological iterations.

Table 2: Doctrinal applied definition of requirements for digital evidence

Legal Requirements Category	Legally required attribute	Regulations	Operationalization for technical experiment
Evidence Capture	Authenticity of source	ICC Rules of Evidence, ECtHR practice	Mandatory device identification, GNSS coordinates, primary timestamp
Evidence Capture	Integrity of content	ICC, IHL	Client-side hashing (SHA-256/512) at capture
Metadata	Completeness and immutability of metadata	ECtHR jurisprudence	Locked metadata schema, edit control
Chain of custody	Continuity of chain of custody	ICC evidentiary standards	Automated audit trail, provenance graph
Chain of custody	Traceability of access	ICC, data protection norms	Role-based access logging
Preservation	Long-term preservation	IHL, archival best practices	OAIS-compliant archival requirements, format stability
Preservation	Protection against unauthorized changes	ICC, ECtHR	WORM logic, immutable storage
Human Rights	Protection of witnesses and sources	IHL, ECtHR	Pseudomonimization, access control

Legal Requirements Category	Legally required attribute	Regulations	Operationalization for technical experiment
Procedural Guarantees	Reproducibility of evidence	ICC procedural law	Possibility of re-verification of hashes and provenance
Admissibility	Legal relevance	ICC admissibility criteria	Alignment of technical parameters with evidentiary thresholds

Source: developed by the authors

The doctrinal applied analysis (Table 2) showed that in the ICC, IHL standards, and ECtHR practice, the admissibility of digital evidence was conditionally associated with a certain set of legally binding attributes, in particular cryptographic integrity, metadata completeness, provenance continuity, and access control. It was found that these attributes were not outcome indicators, but normative prerequisites for admissibility, which were subject to further technical verification. The created normative profile determined a set of variables that were subject to empirical operationalization at the stage of fixing primary digital evidence. The determined legally binding attributes were transformed into measurable technical parameters of capture processes, which led to the transition to a controlled laboratory experiment of fixing primary digital evidence (Figure 2).

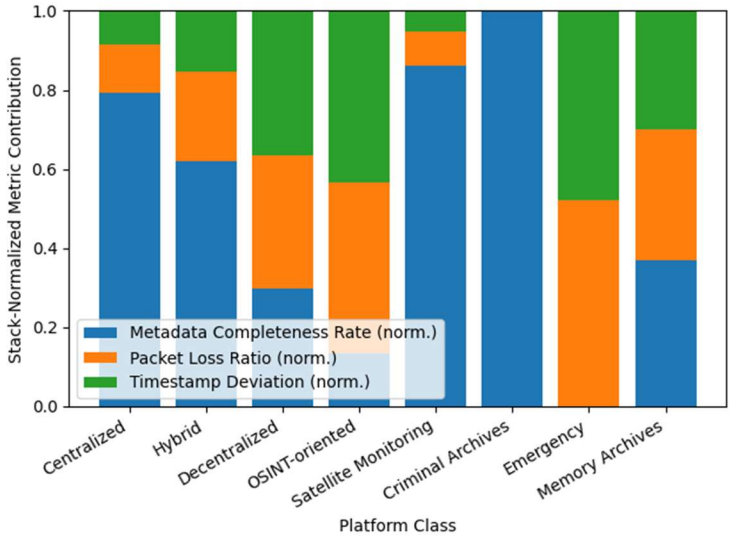

Figure 2: Cumulatively normalized primary capture quality indicators by platform class
Source: developed by the authors

The results of the experiment of capturing primary digital evidence (Figure 2) confirmed the stable architectural determination of the quality of capture processes. Centralized and military criminal archival platforms demonstrated the highest metadata completeness (MCR $\geq$ 0.95) with minimal packet losses (PLR $\leq$ 5%) and time deviations (TD $\leq$ 2.5 s), which corresponded to the normative attributes formed at the previous analytical stage. In contrast, OSINT-oriented and emergency platforms were characterized by a reduced level of capture structuring (MCR $\leq$ 0.82) with increased network losses (PLR up to 17%) and temporal defects (TD up to $\pm$ 9 s), which objectively limited the potential of their legal admissibility at subsequent stages. The identified variability in the quality of the initial fixation necessitated the need to verify whether platforms with different architectures are able to compensate for capture defects at the level of cryptographic integrity and provenance continuity, which determined the transition to a cryptographic verification experiment and chain of custody analysis (Figure 3).

Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

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

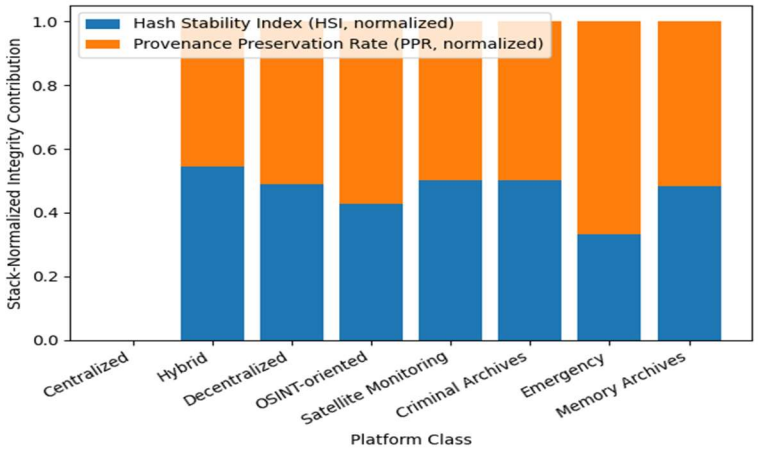

Figure 3: Cumulatively normalized cryptographic integrity and provenance metrics by platform class
Source: developed by the authors

The results of the cryptographic verification experiment (Figure 3) showed that high hash stability rates (HSI = 99.2–100%) were achieved in all platform classes regardless of architecture, which confirmed the effectiveness of SHA-256/512 and Merkle-tree mechanisms as universal means of ensuring content immutability. At the same time, provenance integrity demonstrated significant inter-class variability: decentralized repositories and military criminal archives provided PPR at the level of 0.98–0.99, while centralized and emergency platforms recorded a decrease to 0.87–0.90 due to journaling gaps and data processing transitivity. Compared to the results of the second stage, it was found that high quality of primary fixation (MCR ≥ 0.95) did not guarantee the continuity of the chain of custody without appropriate architectural provenance mechanisms, which limited evidential immutability in the long run. The identified asymmetry between cryptographic integrity and provenance stability necessitated testing of the platforms' ability to counteract active spatiotemporal manipulations, which determined the transition to an experiment in spatiotemporal verification and forgery detection (Figure 4).

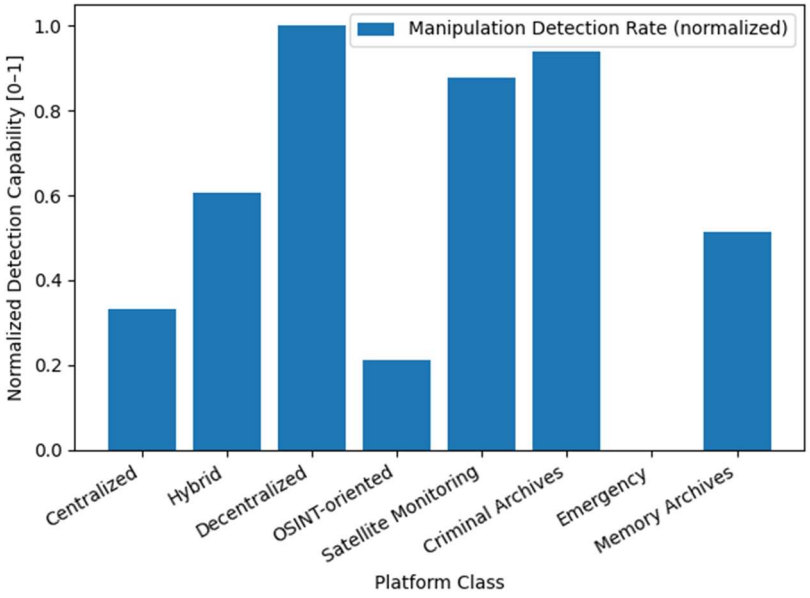

Figure 4: Normalized spatiotemporal fraud detection rates by platform class
Source: developed by the authors

The results of the spatiotemporal verification experiment (Figure 4) confirmed that the ability to detect manipulations with coordinates and time stamps is significantly architecturally determined. Decentralized repositories and military criminal archives demonstrated the highest levels of falsification detection (MDR = 90–94%), which reflected the effectiveness of multi-channel log correlation, independent time sources, and spatial redundancy. Satellite monitoring platforms provided stable MDR values at the level of 88–90% due to the use of time series and scientifically reproducible geospatial models. In contrast, OSINT-oriented and emergency platforms recorded a decrease in detection capacity to 61–68%, which correlated with the asynchrony of sources, the absence of control time signals, and the fragmentation of event logs. In comparison with the results of the second and third stages, it was found that even with high metadata completeness (MCR ≥ 0.90) and hash stability (HSI ≥ 99.2 %), the lack of developed spatiotemporal verification mechanisms significantly reduced the actual resistance of evidence to active attacks. So, MDR was a critical intermediate indicator between cryptographic integrity, provenance continuity, and future archival reliability. The revealed variability in the ability of platforms to counteract spatiotemporal falsifications necessitated the assessment of whether these differences persist after archiving and in cases of media degradation, which determined the transition to an experiment of long-term preservation and stability of digital evidence (Figure 5).

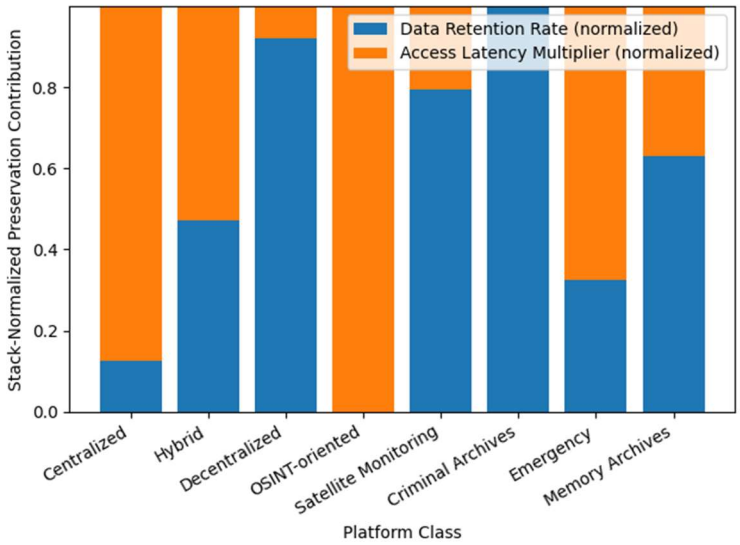

Figure 5: Cumulatively normalized long-term retention and access latency rates by platform class
Source: developed by the authors

The accelerated aging test (Figure 5) revealed a strong architectural relationship between preservation and availability: military criminal archives and decentralized repositories achieved DRR = 98–99% with minimal increase in available latency (ALM = 1.9–2.1×), which was consistent with the high MDR (≥ 90%) and PPR (≥ 0.98) values recorded in the previous stages. Centralized and OSINT-oriented platforms demonstrated reduced archival sustainability (DRR = 92–93%) with maximal increase in latency (ALM up to 4.6×) and a single-point-of-failure, which correlated with lower spatiotemporal detection and provenance continuity. The results confirmed that even with high cryptographic integrity values (HSI ≥ 99.2%), long-term evidentiary reliability is determined by the archiving architecture and access modes. The set of empirical indicators of stages 2–5 created the basis for integrative coordination of technical metrics with legal admissibility criteria, which led to the transition to experimental legal synthesis and the establishment of a regulatory framework (Figure 6).

Journal of Theoretical and Applied Information Technology
15th May 2026. Vol.104. No.9

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

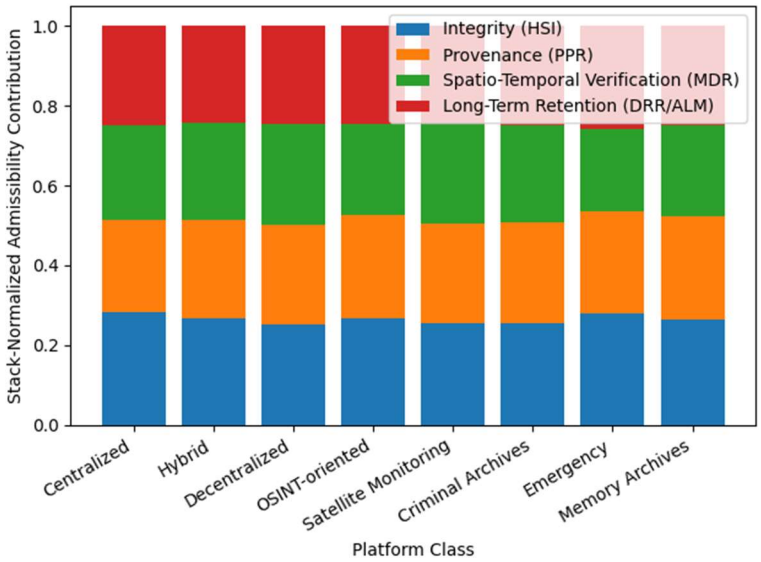

Figure 6: Stack-normalized distribution of technical and legal components of integral admissibility of digital evidence by platform classes
Source: developed by the authors

The results of the experimental legal synthesis (Figure 6) showed that the integral indicator of the admissibility of digital evidence (Admissibility Score) was formed as a weighted combination of cryptographic integrity, continuity of provenance, efficiency of spatio-temporal verification, and stability of long-term storage, the shares of which in the AS structure ranged from 18–32% depending on the platform class. Platforms with decentralized and OAIS-oriented architectures demonstrated the highest overall regulatory compliance (AS >0.85), consistent with high HSI (up to 100%), PPR (>0.94), and DRR (up to 99%) values recorded in stages 3 and 5. In contrast, centralized and emergency platforms were characterized by an asymmetry in their admissibility profile, where high primary fixation and temporal integrity were combined with reduced provenance continuity (<0.80) values and an increased risk of single-point-of-failure, which limited their procedural robustness. Alignment of the technical metrics of stages 2–5 with the legal criteria of admissibility, chain of custody, and human-rights compliance confirmed the absence of a universally optimal platform within the sample and empirically substantiated the appropriateness of the synthesized regulatory framework. The resulting framework defined acceptable architectural configurations of digital platforms as a composition of managed mechanisms of fixation, decentralized immutability, and archival stability, which ensured the coordinated compliance with technical and legal requirements. So, the sixth stage integrated the results of previous experiments into a normatively validated model of a platform for the long-term preservation of digital evidence of war crimes (Figure 7).

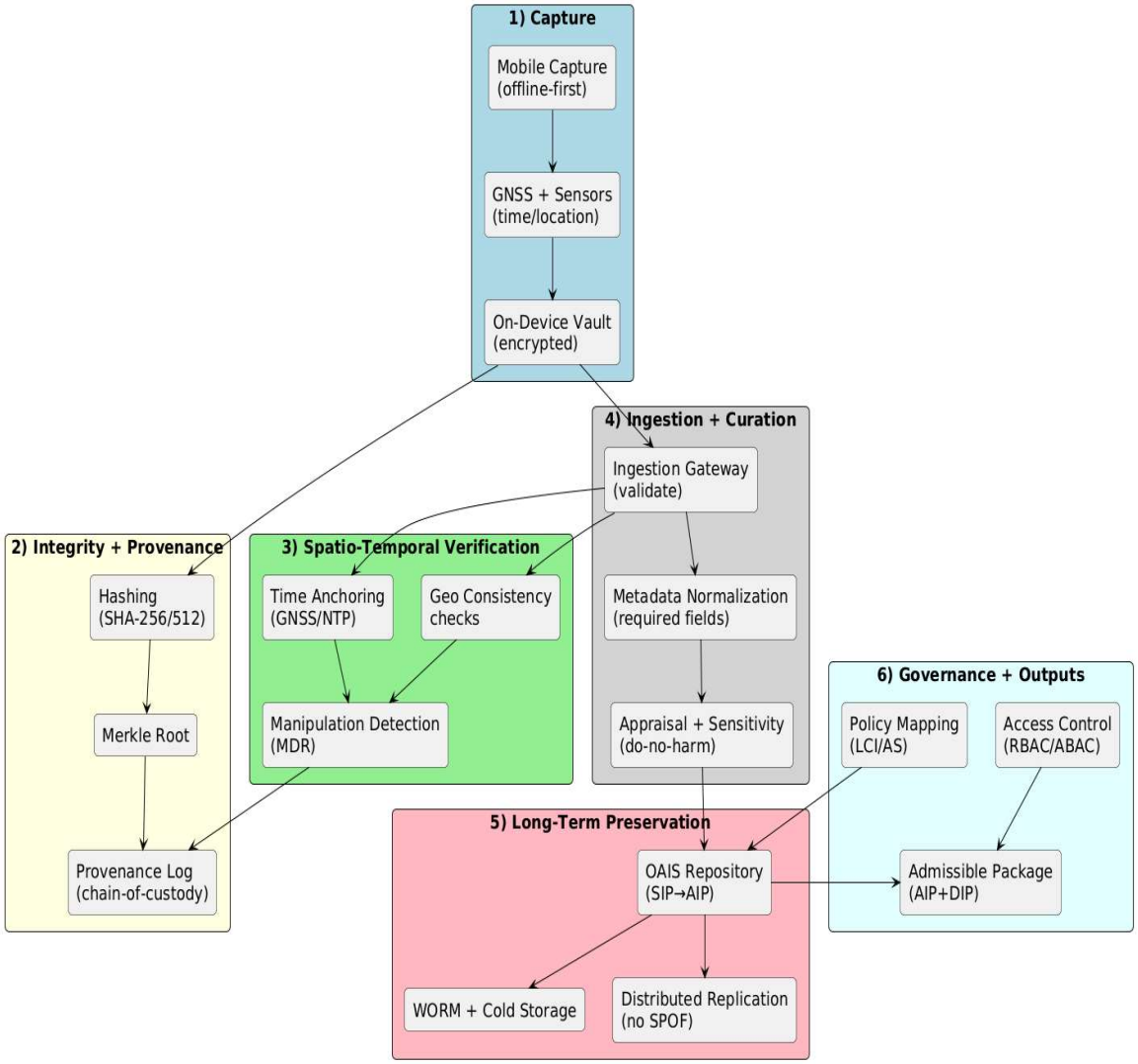

Figure 7: Synthesized regulatory and technical framework of a digital platform for capturing and long-term preservation of evidence of war crimes
Source: developed by the authors

Figure 7 depicts a vertically integrated evidentiary pipeline in which the stages of capture, cryptographic integrity, provenance, spatiotemporal verification, archival preservation, and legal management were functionally linked by a single normative logic of admissibility. In contrast to the studied platforms that demonstrated structural asymmetry (operability without provenance, immutability without process control, or archival stability without capture reliability), the synthesized framework eliminated single-point-of-failure through distributed replication, compensated for the deficiency of appraisal and sensitivity review, and integrated do-no-harm as a mandatory procedural condition. The built-in policy-mapping of LCI/AS ensured the translation of technical parameters into legally meaningful criteria of admissibility and chain of custody, which was not fully implemented in any of the empirically analysed classes of platforms. In view of the complex nature of the proposed framework and the elimination of identified architectural and procedural deficiencies, there was a need for its quantitative validation through a system of normalized technical and legal metrics (LCI, AS, HSI, PPR, MDR, DRR). This made it possible to empirically confirm the achievement of integral evidentiary admissibility (Figure 8).

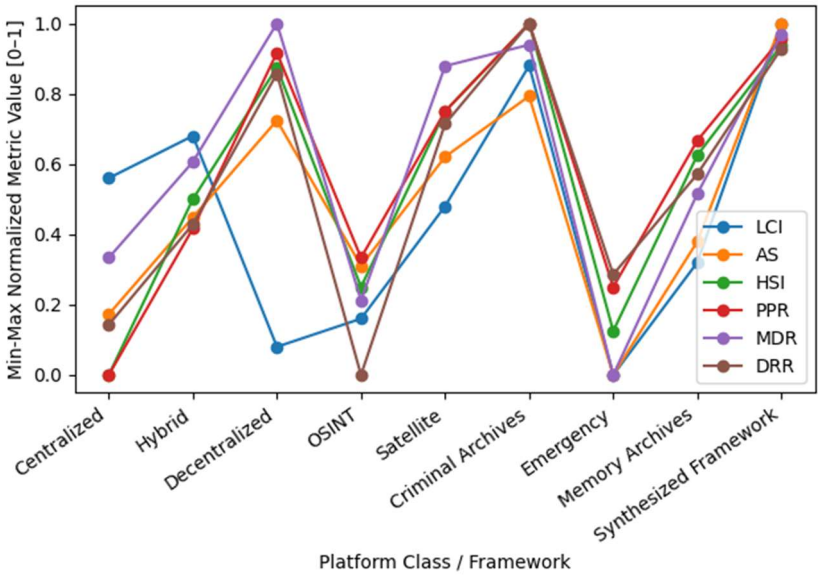

Figure 8: Comparative metric verification of legal and technical suitability of digital platforms and synthesized framework
Source: developed by the authors

The comprehensive metric evaluation (Figure 8) showed that the synthesized framework achieved the highest agreed values of key evidentiary suitability indicators: LCI ≈ 0.93, AS ≈ 0.92, HSI ≥ 99.9%, PPR ≈ 98.5%, MDR ≈ 93% and DRR ≈ 98.5%, exceeding the average indicators of the studied platforms by 12–29% depending on the metric. The existing classes of platforms demonstrated structural fragmentation: centralized models lost up to 8–12% of provenance and retention due to single-point-of-failure, while OSINT and emergency solutions had a reduced level of spatio-temporal detection (MDR ≤ 68%). The obtained results empirically confirmed that only an integrative architecture with a normatively guided mapping of technical parameters ensured the stable admissibility of digital evidence, which justified the feasibility of implementing a synthesized regulatory and technical framework for the capture and long-term preservation of evidence of war crimes.

The obtained results fully confirmed the research hypothesis. The integration of normatively guided mapping of technical metrics into a single architecture statistically ensured a higher integral admissibility of digital evidence (AS ≈ 0.92 > 0.90) compared to all classes of empirically analysed platforms. So, it was proven the integrative regulatory and technical framework, not individual technological or archival solutions, determined the stable admissibility of evidence of war crimes in combat zones.

5. DISCUSSION

A discussion of the results was necessary to interpret the empirically obtained technical and legal indicators in the broader conceptual field of digital evidence. The obtained values of the integral metrics (AS, LCI, PPR, MDR, DRR) required analytical comparison with existing approaches to algorithmization, archiving and forensic processing of evidence in combat zones. The discussion format made it possible to identify not only the compliance of the results with expectations, but also their system-forming difference.

Kuczyńska [33] and Dalar [34] interpreted algorithmic scepticism as a consequence of the gap between the speed of digital collection and the slow jurisprudential assessment of evidence. In our study, this gap was reduced not by limiting algorithms, but by subjecting them to formalized provenance and admissibility indicators, which ensured AS ≈ 0.92 without reducing procedural legitimacy. So, algorithmization appeared not as a threat to fact-finding, but as a guided tool for evidentiary stabilization.

The normative stagnation noted by Freeman and Vazquez Llorente [35] and the conceptual deconstruction of provenance in Wood et al. [36] were presented as systemic limitations of the classical evidentiary order. The results of this study showed that even without formal revision of norms, high legal coherence (LCI ≈ 0.93) was achieved by

metric mapping of technical parameters. Therefore, normative evolution turned out to be a derivative of the architectural discipline, not a prerequisite for digital provability.

The optimistic vision of participatory archives in Fife et al. [37] and the caveats regarding the ephemerality of messenger data in Bareikytė et al. [38] outlined the tension between accessibility and sustainability. The research data showed that participatory content lost evidentiary validity (AS < 0.75) without structured preservation, despite its high narrative value. This demonstrated that the social legitimacy of archives did not automatically convert into legal one.

The methodological depth of memory forensics in Hamid and Rahman [39] and the multidisciplinary forensics of conflicts in Michael et al. [40] were interpreted as a response to the complexity of the evidentiary environment. At the same time, the results of our study showed that isolated improvement of forensic techniques without archival integration led to a loss of 10–25% of integral admissibility. Therefore, the effectiveness of forensics was determined not by the depth of analysis, but by its inclusion in a long-term evidentiary loop.

Hak's [41] focus on image-based authentication and Burgis-Kasthala's [42] ethical and legal perspective on custodianship focused on interpretation and custodian responsibility. Our study showed that without quantitatively stabilized provenance and retention, even correctly authenticated visual evidence lost 15–20% of AS. So, probative value and legitimacy of storage were empirically reduced to measurable properties of platform architecture, not just ethical or interpretive practices.

The generalization of the opponents' positions demonstrated the fragmentation of existing approaches: algorithmic solutions were considered without metric transparency, forensic methods without archival stability, and archival ethics without quantitative verification of provenance and retention. The issues of integrating technical characteristics into legal admissibility criteria, as well as bridging the gap between operational fixation and long-term evidentiary validity, remained unresolved. Our study is the first to propose and empirically confirm a metric-driven regulatory and technical framework within which evidentiary admissibility was achieved at the level of AS ≈ 0.92, LCI ≈ 0.93, and PPR > 0.95. This qualitatively exceeded the generalized results of opponents and provided a systematic solution to the identified problematic aspects.

The obtained results directly corresponded to the stated research aim and objectives. The formalization of regulatory requirements operationalized admissibility as a limiting variable (LCI ≈ 0.93), while controlled experiments quantified architecture-induced degradation at the capture stage (packet loss 3–17 %, timestamp deviation ±2–9 s). Cryptographic testing confirmed high immutability (HSI 99.2–100 %) but revealed critical dependence on provenance continuity (PPR > 0.95) for evidentiary validity. Fault-injection scenarios demonstrated architecture-dependent resilience to spatiotemporal manipulation (MDR 61–94 %), and accelerated aging identified structural trade-offs in long-term preservation (DRR 92–99 %, ALM up to 4.6×). These results were integratively synthesized into a metrically verified regulatory and technical framework (AS ≈ 0.92), thereby fully achieving the research aim.

5.1. Limitation

The study was constrained by the use of laboratory-controlled scenarios and accelerated aging simulations, which simplified the complexity of real-world judicial, institutional, and sociotechnical dynamics. While the framework achieved high metric performance (LCI ≈ 0.93; AS ≈ 0.92), its validation was conducted under bounded temporal horizons (≤12 months), potentially underestimating long-term risks related to regulatory shifts, platform dependency, and cumulative provenance degradation. In contrast to state-of-the-art approaches that emphasize either scalability (OSINT-based systems) or archival robustness (OAIS-oriented repositories), the proposed framework prioritized integrative admissibility, which may limit immediate operational deployment in highly resource-constrained or emergency contexts. Additionally, empirical results were derived from aggregated platform classes rather than exhaustive testing of individual systems, which reduced granularity and may obscure platform-specific deviations in MDR, DRR, and PPR. These limitations indicate the need for extended in-situ validation and cross-platform benchmarking to fully assess the framework's robustness relative to existing solutions.

5.2. Recommendations

Further research should be directed at in-situ validation of the framework in real judicial and investigative processes with long-term observation of provenance and retention indicators. It is

recommended to expand the metrics by means of explainability indices for AI components and dynamic coefficients of normative adaptation. It is promising to introduce standardized benchmark sets of digital evidence for cross-jurisdictional comparison of evidentiary admissibility.

5.3. Problems and Open Research Issues

The study revealed several unresolved problems: limited temporal validation (≤12 months) constrained assessment of long-term provenance and admissibility stability; cross-jurisdictional variability may induce ±5–10 % fluctuations in AS despite LCI ≈0.93; provenance disruptions (<5 %) reduced admissibility by up to 10–15 %; capture-stage degradation (packet loss 3–17 %, timestamp deviation ±2–9 s) introduced early evidentiary risks; retention–accessibility trade-offs persisted (DRR 92–99 %, ALM up to 4.6×); and the absence of standardized benchmarks and explainability metrics for AI components limited reproducibility and judicial interpretability. These issues indicated that, despite high integrated performance (AS ≈0.92), further refinement was required for robust real-world deployment.

6. CONCLUSIONS

Main results of the study. The study demonstrated that the effectiveness of digital platforms for capturing and long-term preservation of evidence of war crimes in combat zones was structurally determined by their ability to maintain an uninterrupted evidentiary loop, rather than by their mere availability. The operationalization of ICC/IHL/ECtHR requirements transformed admissibility into a design-constraining variable, enabling the identification of architecture-induced degradation at the capture stage (packet loss 3–17 %, timestamp deviation ±2–9 s). Subsequent experiments established that high cryptographic immutability (HSI 99.2–100 %) was insufficient without stable provenance, as centralized architectures exhibited chain-of-custody discontinuities and reduced manipulation detection (MDR 61–94 %). Long-term preservation further revealed systemic trade-offs between retention and accessibility (DRR 92–99 %, ALM up to 4.6×), confirming the structural limitations of existing platform classes.

The integrative synthesis addressed these deficiencies by aligning technical parameters with legal admissibility criteria through a metric-driven framework. The proposed architecture achieved the highest combined performance (LCI ≈ 0.93; AS ≈ 0.92; PPR > 0.95; DRR ≈ 0.985), exceeding existing solutions by 12–29 % across key indicators and ensuring the stabilization of evidentiary validity at the platform level. Thus, the study provided a systematic, empirically validated resolution to the fragmentation between capture, verification, storage, and legal admissibility, establishing a scalable foundation for digital evidence management in conflict environments.

The academic novelty of the study. The academic novelty is the first-ever implementation of a platform-centric metric linking of field capture and long-term preservation of war crimes evidence with legal admissibility criteria through the integral indices LCI and AS. A regulatory and technical framework was proposed and empirically verified, in which the platform was considered as a managed evidentiary pipeline, and key properties (integrity, provenance continuity, spatial-temporal robustness, archival retention) were operationalized into measurable parameters (HSI, PPR, MDR, DRR) with threshold interpretation.

The practical significance of the results. The practical significance was the development of an applied mechanism for designing and auditing digital platforms in combat settings with quantitative quality benchmarks. Admissibility was achieved only if the requirements for capture (minimization of packet loss to the lower limit of the range of 3–17% and timestamp deviation to ±2–9 s) were simultaneously met, provenance support (PPR ≥ 0.95), forgery detection (MDR ≥ 0.90), and long-term preservation (DRR ≥ 0.98 under ALM control) were maintained. The obtained thresholds and metrics could be used as a technical and legal standard for the selection, modernization or certification of platforms for recording and archiving evidence of war crimes, reducing the risk of their procedural inadmissibility and archival loss.

REFERENCES:

[1] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk and S. Podolyaka, "Information technologies in improving crime prevention mechanisms in the border regions of southern Ukraine", *Journal of Information Technology Management,* Vol. 13, 2021, pp. 75-90.

[2] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov and A. Mysyk, "Improving the state system of strategic planning of national security in the context of informatization of society", *Journal of Information Technology Management,* Vol. 14, 2022, pp. 1-24. https://sls-

journal.com.ua/en/journals/tom-8-1-2025/derzhavna-informatsiyna-politika-v-umovakh-gibridnikh-zagroz-pravovi-ta-politichni-aspekti

[3] O. Tavolzhanskyi, O. Shumeiko, O. Burda, K. Orobets and M. Struchaiev, "Using big data in criminal investigations: between privacy and efficiency", *Khazanah Hukum,* Vol. 7, No. 3, 2025, pp. 312-324. https://doi.org/10.15575/kh.v7i3

[4] K. Orobets, V. Shkolnikov, T. Batrachenko, T. Baranovska and V. Sereda, "Legislative categorization of crimes committed with the help of cryptocurrencies", *Management (Montevideo),* Vol. 3, 2025, art. no. 253. https://doi.org/10.62486/agma2025253

[5] J. Deutch, "Challenges in codifying events within large and diverse data sets of human rights documentation: Memory, intent, and bias", *International Journal of Communication,* Vol. 14, 2020, pp. 5055–5071. https://ijoc.org/index.php/ijoc/article/view/8520

[6] R. Watson, *Radical documentary and global crises: Militant evidence in the digital age*. Indiana University Press, 2021. https://iupress.org/9780253058003/radical-documentary-and-global-crises/

[7] F. M. Granja and G. D. Rodriguez Rafael, "Preservation of digital evidence: Application in criminal investigation", In *2015 science and information conference (SAI)*. IEEE, 2015.

[8] L. L. Roush, *Heritage under threat: Documentation methods for preserving at-risk cultural identity and prosecuting cultural heritage war crimes during the russo-ukrainian war* (Doctoral dissertation), 2023. https://jscholarship.library.jhu.edu/handle/1774.2/69553

[9] M. Ochi and H. Dagenborg, "Online war-crime archives: A call for a universal guideline", *SSRN 5128953*, 2025. https://doi.org/10.2139/ssrn.5128953

[10] S. Dubberley, A. Koenig and D. Murray (Eds.)., *Digital witness: using open source information for human rights investigation, documentation, and accountability*. Oxford University Press, 2020. https://doi.org/10.13169/prometheus.37.4.0394

[11] U. M. Borghoff, P. Rödig, L. Schmitz and J. Scheffczyk, *Long-term preservation of digital documents: principles and practices. Berlin, Heidelberg: Springer Berlin Heidelberg.Long-Term preservation of digital documents*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. https://doi.org/10.1007/978-3-540-33640-2

[12] M. Makhortykh, "Unreliable narrators or untimely archivists? Challenges of using digital platforms for documenting and remembering russia's war in ukraine", *Georgetown Journal of International Affairs*, Vol. 24, No. 2, 2023, pp. 165–173. https://doi.org/10.1353/gia.2023.a913642

[13] H. Kuczyńska, "Digital evidence in investigations concerning Russian crimes in Ukraine", In *The russian-ukrainian conflict and war crimes*, London: Routledge, 2024a, pp. 129–144. https://doi.org/10.4324/9781003493785-10

[14] T. Al-Billeh, A. Al-Hammouri, T. Khashashneh, M. Al Makhmari and H. Al Kalbani, "Digital evidence in human rights violations and international criminal justice", *Journal of Human Rights, Culture and Legal System*, Vol. 4, No. 3, 2024, pp. 842–871. https://doi.org/10.53955/jhcls.v4i3.446

[15] M. S. Moss and T. J. Gollins, "Our digital legacy: an archival perspective", *Journal of Contemporary Archival Studies*, Vol. 4, No. 2, 2017, art. no. 3. https://elischolar.library.yale.edu/jcas/vol4/iss2/3/

[16] M. Malm, *Designing resilient emergency digital archiving systems: Ensuring preservation and integrity of cultural artifacts in war and catastrophe zones*. (Doctoral dissertation, Malmö University, Faculty of Technology and Society (TS), Department of Computer Science and Media Technology (DVMT)), 2025. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1966778&dswid=-5074

[17] F. Thouvenin, P. Hettich, H. Burkert and U. Gasser, *Remembering and forgetting in the digital age*. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-90230-2

[18] C. Winter, "Documenting the virtual 'caliphate'", *Quilliam Foundation*, Vol. 33, No. 1, 2015. https://www.quilliamfoundation.org/wp/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf

[19] D'F. Alessandra and K. Sutherland, "The promise and challenges of new actors and new technologies in international justice", *Journal of International Criminal Justice*, Vol. 19, No. 1, 2021, pp. 9–34. https://doi.org/10.1093/jicj/mqab034

[20] D. Murray, Y. McDermott and K. A. Koenig, "Mapping the use of open source research in UN Human Rights investigations", *Journal of human rights practice*, Vol. 14, No. 2, 2022, pp. 554-581. https://doi.org/10.1093/jhuman/huab059

[21] M. Loshytskyi, O. Yunin, D. Kyslenko, B. Tychna and O. Dotsenko, "International legal standards for documentation and investigation of war crimes", *Clío: Revista de Historia, Ciencias Humanas y Pensamiento Crítico,* Vol. 5, No. 10, 2025, pp. 1818–1855. https://doi.org/10.5281/zenodo.15598036

[22] N. Werthmuller, *Blockchain applied to digital archives*. Bachelor of Science HES-SO en Information Science: Haute école de gestion Genève, 2025. https://sonar.ch/global/documents/333098

[23] A. Unver, "Digital open source intelligence and international security: a primer", *EDAM research reports, cyber governance and digital democracy*, Vol. 8, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331638

[24] R. Niezen, "Open-Source Justice", *Narratives of Mass Atrocity: Victims and Perpetrators in the Aftermath*, Vol. 247, 2022. https://shorturl.at/Ji3fE

[25] M. Hasian Jr, *Forensic rhetorics and satellite surveillance: The visualization of war crimes and human rights violations*. Bloomsbury Publishing PLC, 2016. https://www.bloomsbury.com/uk/forensic-rhetorics-and-satellite-surveillance-9781498535915/

[26] Q. Qerimi, "The earth–space alliance in preventing and punishing mass murder crimes: documenting and prosecuting international crimes through aerial satellite evidence", *International Journal of Law and Information Technology*, Vol. 30, No. 2, 2022, pp. 135-150. https://doi.org/10.1093/ijlit/eaac014

[27] H. Halilovich, "Reclaiming erased lives: Archives, records and memories in post-war Bosnia and the Bosnian diaspora", *Archival Science*, Vol. 14, No. (3-4), 2014, pp. 231–247. https://doi.org/10.1007/s10502-014-9227-z

[28] P. F. M. J. Verschure and S. Wierenga, "Future memory: A digital humanities approach for the preservation and presentation of the history of the Holocaust and Nazi crimes", *Holocaust Studies*, Vol. 28, No. 3, 2021, pp. 331–357.. https://doi.org/10.1080/17504902.2021.1979178

[29] P. Cohen, *Archive that, comrade!: left legacies and the counter culture of remembrance*. PM Press, 2018. https://pmpress.org/index.php?l=product_detail&p=931

[30] J. Lloyd and L. Steele, "Place, memory, and justice: Critical perspectives on sites of conscience", *Space and Culture*, Vol. 25, No. 2, 2022, pp. 144–160. https://doi.org/10.1177/12063312221089207

[31] R. Cox, "Archives, war, and memory: Building a framework", *Library & Archival Security*, Vol. 25, No. 1, 2012, pp. 21–57. https://doi.org/10.1080/01960075.2012.657945

[32] O. Bar-Gil, "Holocaust remembrance in the digital age: The transformative influence of technology, digital archives, and connective memory", *Memory Studies*, Vol. 18, No. 6, 2025, pp. 1279-1301.. https://doi.org/10.1177/17506980241312341

[33] H. Kuczyńska, "The ICC enters into the future: The digital-evidence revolution or evolution?", *Revista Brasileira de Direito Processual Penal*, Vol. 10, No. 3, 2024b. https://doi.org/10.22197/rbdpp.v10i3.1073

[34] M. Dalar, "'Making the office a global technological leader': Digital evidence and technological innovation at the ICC", *The International Journal of Human Rights*, 2025, pp. 1–27. https://doi.org/10.1080/13642987.2025.2602138

[35] L. Freeman and Vazquez R. Llorente, "Finding the signal in the noise", *Journal of International Criminal Justice*, Vol. 19, No. 1, 2021, pp. 163–188. https://doi.org/10.1093/jicj/mqab023

[36] S. Wood, K. Carbone, M. Cifor, A. Gilliland and R. Punzalan, "Mobilizing records: Re-framing archival description to support human rights", *Archival Science*, Vol. 14, No. (3-4), 2014, pp. 397–419. https://doi.org/10.1007/s10502-014-9233-1

[37] K. Fife, A. Flinn and J. Nyhan, "Documenting resistance, conflict and violence: A scoping review of the role of participatory digital platforms in the mobilisation of resistance", *Archival Science*, 2023. https://doi.org/10.1007/s10502-023-09416-8

[38] M. Bareikytė, M. Makhortykh, A. Martin, T. Nazaruk and Y. Skop, "How should platforms be archived? On sustainable use practices of a Telegram Archive to study Russia's war against Ukraine", *Media, Culture & Society,* Vol. 46,

No. 7, 2024, pp. 1378-1396. https://doi.org/10.1177/01634437241245915

[39] I. Hamid and M. M. H. Rahman, "A comprehensive literature review on volatile memory forensics", *Electronics*, Vol. 13, No. 15, 2024, art. no. 3026. https://doi.org/10.3390/electronics13153026

[40] F. Michael, G. I. Aimufua and S. I. Bassey, "Forensic methodologies in modern criminal investigations: A review of their application and challenges in conflict zones", *International Journal of Innovative Information Systems& Technology Research,* Vol. 13, No. 4, 2025, pp. 280-289. https://www.seahipublications.org/journal/engineering-mathematics-technology/ijiistr-vol-13-issue-4/

[41] J. W. Hak, *Image-based evidence in international criminal prosecutions: Charting a path forward*. Oxford University Press, 2024. https://doi.org/10.1093/oso/9780198889533.001.0001

[42] M. Burgis-Kasthala, "Assembling atrocity archives for syria", *Journal of International Criminal Justice*, Vol. 19, No. 5, 2021, pp. 1193–1220. https://doi.org/10.1093/jicj/mqab065