Journal of Theoretical and Applied Information Technology
15th April 2026. Vol.104. No.7

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

APPLICATION OF DIGITAL FORENSIC TECHNOLOGIES TO DETECT AND PRESERVE DIGITAL TRACES IN PRE-COURT INVESTIGATIONS

VIACHESLAV KULIUSH[1*], OLEKSANDR SHEVCHENKO[2], VLADAS TUMALAVIČIUS[3], VALERII NIKITCHENKO[4], OLEKSANDR HRUZD[5]

[1]Cybercrime Countermeasures Department, Cyber Police Department of the National Police of Ukraine, Kyiv, Ukraine.
[2]Department of Operational and Investigative Activities and National Security, National Academy of Internal Affairs, Kyiv, Ukraine.
[3]Turiba University, Riga, Latvia.
[4]Interregional Academy of Personnel Management, Kyiv, Ukraine.
[5]Department of Criminal Procedure and Criminalistics, Faculty for Training Specialists for Pre-Trial Investigation Bodies of the National Police of Ukraine, Donetsk State University of Internal Affairs, Kropyvnytskyi, Ukraine.
E-mail: [1]rakhilaaubakirova@gmail.com, [2]npuoleksandr777@gmail.com, [3]t.vladas@gmail.com, [4]nikitchenkovalerii@gmail.com, [5]gruzddolexandr@gmail.com

ABSTRACT

The article presents the results of a comprehensive study of the application of digital forensic technologies for the detection and preservation of digital traces in pre-trial investigation. The cases of Ukraine, Lithuania, and Latvia were used in the study. The relevance of the study is determined by the growing need for the implementation of modern digital forensic technologies capable of ensuring reliable detection, fixation, and preservation of digital traces in pre-trial investigation. The aim of the study is to assess the effectiveness of forensic platforms (Autopsy, FTK, X-Ways, Magnet AXIOM), cryptographic algorithms SHA-256 and SHA-3, as well as blockchain solutions to maintain the continuity of the "chain of evidence" in three countries with different levels of digital maturity. The object of the study was forensic platforms (Autopsy, FTK, X-Ways, Magnet AXIOM), cryptographic algorithms SHA-256 and SHA-3, as well as blockchain solutions to maintain the continuity of the "chain of evidence". The research employed the following methods: experimental testing of forensic tools on simulated datasets, performance assessment of hash algorithms and blockchain logs, and comparative analysis of practices in Ukraine, Lithuania, and Latvia. The results of the study revealed significant differences between countries. In Ukraine, certified forensic tools are used in only 35% of units, and the reliability of the "chain of evidence" does not exceed 0.72, which reduces the level of trust in digital evidence in more than 40% of criminal cases. In Lithuania, the level of certification reaches 85%, compliance with EU directives and GDPR ensures the stability of procedures at the level of 0.91, and the speed of digital data processing is 28% higher than in Ukraine. Latvia occupies an intermediate position: the level of certification is 65%, independent verification of digital evidence exceeds 75%, and the transparency of blockchain logs is estimated at 0.87 with an average transaction delay of 250 ms. The academic novelty of the study is the comprehensive technical and legal analysis of digital forensic technologies in three countries with different levels of maturity of digital infrastructure and the development of a model of optimal workflow for pre-trial investigation.

Keywords: *Digital Forensics, Electronic Evidence, Blockchain, SHA-256, SHA-3, Forensic Platforms, Criminal Justice, Rule Of Law, Ukraine, Lithuania, Latvia*

1. INTRODUCTION

The rapid spread of digital technologies and the complexity of cyber threats are radically changing the approaches to collecting and preserving evidentiary information in criminal proceedings. While classical methods of working with physical evidence prevailed before, now digital forensics is of key importance, capable of analysing large volumes of electronic data, mobile devices, cloud services and network logs [1, 2]. In international practice, digital triage, ontological

models and algorithms for restoring timelines are actively used, which ensure the speed and accuracy of analysis [1, 4]. For Ukraine, the problem is the fragmentation of the regulatory framework and the lack of unified procedures for extracting and preserving evidence [5, 6], while Lithuania has successfully harmonized forensics with EU law [7], and Latvia focuses on electronic identification systems (eID) and the integration of digital traces into legal mechanisms [7, 8]. A comparison of these models identifies gaps and prospects for the development of Ukrainian practices. The international standards ISO/IEC 27037:2012 [10], ISO/IEC 27042:2015 [11], ISO/IEC 27043:2015 [12] and Recommendation CM/Rec(2018)7 of the Council of Europe [12] remain important reference points. They define the requirements for the identification, preservation and authenticity of electronic evidence. Despite this, the issues of optimizing forensic tools and automating integrity checks remain open. This makes a comparative study of the practices of Ukraine, Lithuania, and Latvia relevant for finding optimal solutions in pre-trial investigation. At the same time, the issues of optimizing digital analysis tools and automating the processes of verifying the integrity of evidence remain open. The challenges relate to both the technical reliability of forensic programmes and their compliance with international standards for preserving digital traces [1, 13]. That is why the study is aimed at a comprehensive comparison of the approaches of Ukraine, Lithuania, and Latvia to the use of digital forensic technologies and the identification of best practices for increasing the efficiency of pre-trial investigation.

The aim of this study is to identify the features and assess the effectiveness of the use of digital forensic technologies in the process of identifying and preserving digital traces during pre-trial investigation using the examples of Ukraine, Lithuania, and Latvia.

The aim was achieved through the fulfilment of the following research objectives:

1. Analyse modern digital forensics tools and their application in the extraction and preservation of digital traces;
2. Study the regulatory and procedural aspects of the use of electronic evidence in the criminal process of Ukraine, Lithuania, and Latvia.
3. Assess the effectiveness of technologies for ensuring the integrity of digital evidence (hashing, blockchain models, digital triage).
4. Provide recommendations for harmonizing Ukrainian practices with European standards and the prospects for their further integration.

So, the study is aimed at substantiating the technical and legal feasibility of using digital forensic technologies, ensuring the preservation of digital traces and increasing the reliability of pre-trial investigation in a cross-border context.

2. LITERATURE REVIEW

Recent years have been characterized by a rapid growth of interest in the introduction of digital forensic technologies into the field of pre-trial investigation, which is confirmed by numerous studies. Ukhno [14] emphasizes the importance of using the latest technologies and elements of artificial intelligence, which increase the efficiency of expert activities and allow working with data in complex investigative situations. Rizvi et al. [15], Kebande and Awad [16] hold a similar position, who also emphasize the importance of AI for network and industrial forensics. However, unlike Ukhno [14], they emphasize not so much on the general increase in efficiency, but on the ability of AI to scale in distributed Internet of Things (IoT) ecosystems. At the same time, Bérubé et al. [17] demonstrate a more restrained approach, focusing on the problem of transforming digital traces into procedurally admissible evidence. They emphasize that even high-tech methods do not guarantee the admissibility of evidence in court if procedural requirements are not met. Stoykova [18] makes a similar emphasis, introducing the concept of "the right to procedural accuracy", which has something in common with the conclusions of Bérubé et al. [17], but is more focused on the legal aspects, while the former analyse a practical case. AlKhanafseh and Surakhi [19] work in the opposite direction, proposing technical protection of evidence based on blockchain and long short-term memory (LSTM) steganography, effectively replacing the procedural side with innovative technologies.

Therefore, an interesting contradiction arises: some authors [17, 18] focus on legal legitimacy, while others [19] focus on technical inviolability. Spichiger and Adelstein [20] worked on the issue of long-term interpretation of digital evidence, pointing out the risk of data depreciation because of changes in the software or hardware environment. Their approach has something in common with the work of Sunde [21, 22], who emphasizes the need to maintain the objectivity of experts and analyses the phenomenon of "elasticity of evidence" – the variability of its meaning depending on the context. This line of argument is similar to Wilson-Kovacs et al. [23], who investigated the role of digital evidence from the perspective of the defence and pointed out

the limitations of access because of the qualification barriers of experts.

Another block of literature is related to standardization. The NIST Scientific Foundation Review [24] systematizes the methods of digital investigation and forms the basis for a unified approach in judicial practice. Khan et al. [25] and Casino et al. [26] in their review papers emphasize the global problem of the lack of unified international standards in the field of digital forensics. This contrast shows that even detailed standards (as in NIST) do not solve the issue of their general integration into the international context. Specialized areas of research are presented in by Cook et al. [27] and Ahmed et al. [28], which focus on industrial and IoT environments. They show that traditional forensic methods must be adapted to the specifics of critical infrastructure. There is something in common with AlKhanafseh and Surakhi [19], as all these authors consider technological modernization as the key to increasing the reliability of digital forensics. As a result, two large groups of approaches can be distinguished. The first is legal and procedural, where the main thing is to comply with procedural standards and ensure the admissibility of evidence. The second is technical and innovative, which relies on technologies – from AI to blockchain. Between these poles are authors who seek to combine standardization and innovation, such as NIST [24] or Casino et al. [26], emphasizing that even the most modern methods will remain local practices without international harmonization.

Despite major strides in digital forensics research, the existing studies in the field remain divided along (i) a capability (tool performance, AI-assisted extraction, cloud/IoT artifacts, blockchain integrity layers) and (ii) a legal protectiveness (chain of custody, expert objectivity, jurisdiction-specific criteria) axis. Few existing studies form an empirically testable link between these two dimensions in the form of an integrated workflow from extraction → validation → integrity preserving → court-specific admissibility. In particular, the literature is lacking in (i) not having an equivalent, metric-based framework that simultaneously considers tool recovery quality, processing latency, reproducibility across runs, and evidential admissibility; (ii) cross-jurisdictionally empirically validated findings that show how different levels of tool certification and regulation harmony show up in measurable stability and admissibility in cross-jurisdictional workflows; and (iii) not having a unifying view of how different cryptographic functions (SHA-256 vs SHA-3) and blockchain audit trails impact not just technical integrity in measured metrics, but actual evidential transportability across national court processes. This study addresses these shortcomings through proposing and validating an integrated experimental framework and workflow for pre-trial digital investigations across Ukraine, Lithuania, and Latvia that links platform-based performance to standards-based admissibility.

3. PROBLEM STATEMENT

The integration of digital forensic technologies into pre-trial investigation opens up new opportunities for detecting and preserving digital traces [1, 2], automating work with mobile devices, cloud services and network logs, and verifying their integrity with hash algorithms and blockchain solutions [1, 4]. At the same time, the effectiveness of these technologies is determined by a unified workflow that guarantees reproducibility and procedural admissibility [5, 6]. Academic research focuses mainly on individual areas (triage, cybercrime, cloud artifacts) [29, 30], while comprehensive integration from collection to judicial presentation remains poorly studied [8, 13]. In terms of countries, Ukraine has fragmented development and a lack of standards [5, 13], Lithuania has harmonized procedures with EU norms [7], and Latvia has integration with eID and cyber infrastructure, although without a unified methodology [8, 31]. The key problem is the lack of a comprehensive performance assessment system that would take into account not only accuracy and speed, but also stability and legal validity [14, 17]. This creates a gap between technical performance and procedural acceptability even in the case of using blockchain or ML algorithms [32, 33]. So, the problem is the lack of a comprehensive approach to creating a digital forensics workflow that would combine technical parameters (accuracy, speed, reproducibility), methodological requirements (chain of custody, expert objectivity) and procedural standards of admissibility in different jurisdictions. It is necessary to form an experimental framework that will allow comparing the practices of Ukraine, Lithuania, and Latvia and determine the optimal conditions for the application of digital forensic technologies in the international context.

The academic hypothesis of the study is that the integration of blockchain solutions and SHA-3 cryptographic algorithms in combination with certified forensic platforms significantly increases the admissibility of digital evidence in legal proceedings, while ensuring its technical stability and procedural admissibility in different national jurisdictions.

4. METHODOLOGY

4.1. Research design

The methodological framework of the study was based on a combination of experimental, comparative, analytical, and simulation approaches. The study was conducted in three consecutive phases.

The first stage was the creation of a test environment for digital forensics. A set of controlled digital artifacts (deleted files, system event logs, network traffic records, cloud data snapshots) was created, which simulated real investigative scenarios – financial fraud, unauthorized access via social networks, attempts to hide data in cloud services. The second stage involved the application and comparison of forensic tools. The choice of Autopsy, FTK, X-Ways and Magnet AXIOM is determined by the fact that these platforms are the most common in the practice of digital forensics. Autopsy represents the category of free open-source solutions, FTK and X-Ways are examples of certified European tools, while Magnet AXIOM specializes in the analysis of mobile devices and social networks. The third stage included validation of the results by checking the integrity of digital traces using hash algorithms (SHA-256, SHA-3) and blockchain logs.

The study conducted a comparative analysis of the practices of Ukraine, Lithuania, and Latvia as representative examples of different models of development of digital forensics. Ukraine demonstrates a transitional legal system with the need for standardization of procedures, Lithuania is an example of harmonization with EU directives and the introduction of certified tools, and Latvia is a model of integration with national cyber systems and e-identification. Such a choice makes it possible to cover the spectrum of approaches from the search for the optimal model to system harmonization and technical integration, which makes the results relevant both for countries in transition and for the broader European context.

4.2. Assessment metrics

Four key parameters were used to assess the effectiveness of forensic tools (Table 1):

Table 1: Metrics for assessing the effectiveness of digital forensic technologies in pre-trial investigation

Parameter	Designation	Calculation method	Range	Significance for research
Data recovery accuracy	Acc	Share of artifacts successfully recovered from the test set	0–1	Reproducibility
Processing time	Latency	Average time from data extraction to report generation	sec/min	Analysis speed
Result stability	Stab	1 / standard deviation after 10 re-runs	0–1	Reproducibility
Evidential value	EvidScore	Expert assessment of compliance with international standards for admissibility of evidence	0–1	Admissibility in court

Source: developed by the author taking into account the international recommendations ISO/IEC 27037:2012 [9], ISO/IEC 27042:2015 [10], ISO/IEC 27043:2015 [11] and the Council of Europe Recommendation CM/Rec(2018)7 on electronic evidence (2018) and Regulation (EU) 2024/1183 of the European Parliament and of the Council on European Digital Identity (eIDAS 2.0) [34]

Table 1 shows the key metrics used to assess the effectiveness of digital forensics. The Acc metric shows how accurately a programme can recover lost or deleted data, which is critical for the completeness of the evidence base. Latency reflects the responsiveness of the tools – the lower the value, the faster the system generates results, which is important in time-sensitive investigations. Stab characterizes the stability of the system during multiple runs and shows whether the obtained results can be trusted when re-analysed. Finally, EvidScore assesses the legal suitability of the results – the extent to which they meet international standards and can be recognized as evidence in court. Together, these parameters allow for a comprehensive assessment of both the technical and procedural quality of digital forensics.

4.3. Methods of analysis

The effectiveness of digital forensic tools was statistically tested by using the analysis of variance (ANOVA) with Tukey's post hoc test. This enabled determining statistically significant differences in the speed and accuracy of the platforms. The bootstrap method with 1,000 repetitions was also used to form confidence intervals and check the reproducibility of the results. The reliability of cryptographic mechanisms was assessed by comparative analysis of the SHA-256 and SHA-3 algorithms, taking into account their resistance to collisions and the level of entropy. Special attention

was paid to the uniformity of hash distribution in order to assess the quality of the cryptographic function. For blockchain solutions, the analysis included checking transaction latency, system throughput (transactions per second (TPS)), the possibility of independent verification of records by other participants, and audit-log transparency. This approach made it possible to determine the balance between the speed of transaction confirmation and ensuring the reliability of the chain of custody of evidence (see Table 2).

Table 2: Metrics for evaluating digital forensic technologies

Parameter	Evaluation method	Expected result
Forensic platform data processing speed	ANOVA + Tukey post hoc test	Identification of statistically significant differences in the performance of tools
Resistance of results	Bootstrap method (1,000 repetitions)	Formation of confidence intervals, confirmation of reproducibility of results
Resistance of hash algorithms to collisions	Comparative cryptographic analysis (SHA-256, SHA-3)	No collisions, high level of entropy
Even distribution of hashes	Calculation of entropy coefficient	Confirmation of randomness of values
Efficiency of blockchain solutions	Measurement of latency (transaction delay)	Stable confirmation time without critical delays
Independent verification of records	Testing the availability of verification by other participants	Confirmation of the possibility of independent control
Transparency of logs	Audit-log analysis	Full traceability of the history of changes
System throughput	TPS	High speed of transaction processing without data loss

Source: developed by the author taking into account the international recommendations ISO/IEC 27037:2012 [9], ISO/IEC 27042:2015 [10], ISO/IEC 27043:2015 [11] and the Council of Europe Recommendation CM/Rec(2018)7 on electronic evidence (2018) and Regulation (EU) 2024/1183 of the European Parliament and of the Council on European Digital Identity (eIDAS 2.0) [34]

The results of the application of the above-mentioned analysis methods gave grounds for a comprehensive assessment of both technical and procedural aspects of digital forensics. In particular, statistical tests showed differences in the speed and stability of forensic platforms, cryptographic analysis confirmed the reliability of the hash algorithms used, and testing of blockchain solutions demonstrated their ability to ensure transparency and control of the chain of custody of evidence.

4.4. Technical environment

The experiments were performed in a virtualized environment VMware Workstation Pro 17 with three virtual machines that simulated workstations of investigative units of Ukraine, Lithuania and Latvia. Each configuration had the same parameters: Windows 11 Pro (64-bit), 8 CPU cores (Intel i7, 3.4 GHz), 16 GB RAM and SSD 500 GB. Simulated data sets were created (Windows event logs, BitLocker encrypted volumes, Android images, network traffic dump files via Wireshark) to reproduce the scenarios. Testing of blockchain solutions was carried out in Hyperledger Fabric 2.5 and Ethereum Testnet (Goerli) environments to assess TPS, Latency, and transparency of logs. Hashing was performed using OpenSSL 3.0 (SHA-256, SHA-3), entropy and collisions were checked using the dieharder utility and Python scripts. Forensic analysis used Autopsy 4.21, FTK 7.6, X-Ways 20.9, Magnet AXIOM 7.0, results were verified on a physical server (Ubuntu Server 22.04 LTS, AMD EPYC 7302P, 64 GB RAM). For statistical analysis, Python 3.11 with Pandas, NumPy, SciPy, Matplotlib, PCA and k-means libraries was used. This environment ensured the reproducibility of experiments and the representativeness of results for international comparison.

5. RESULTS

5.1 Comparative Assessment Of Forensic Platforms In Three Countries

The analysis of the effectiveness of digital forensic platforms was conducted taking into account the national contexts of Ukraine, Lithuania, and Latvia. In Ukraine, Autopsy, and Magnet AXIOM on simulated datasets showed sufficient accuracy and speed, however, problems were identified with the integration of chain of custody standards. In Lithuania, FTK, and X-Ways certified in accordance with EU directives and GDPR demonstrated stable performance and high accuracy, which confirms their suitability for the EU legal

system. In Latvia, adapted FTK and Magnet AXIOM provided stable results in the analysis of network traffic and registry data, and the main advantage was the integration of forensic tools into the state cyber infrastructure, which increases the transparency and efficiency of pre-trial procedures (Table 3).

Table 3: Average values of Latency, Accuracy, and Stab for forensic platforms

Country	Platforms	Latency (mean)	Accuracy (%)	Stab (reproducibility coefficient)
Ukraine	Autopsy, Magnet AXIOM	1.35	87	0.78
Lithuania	FTK, X-Ways	1.10	92	0.85
Latvia	FTK, Magnet AXIOM	1.22	90	0.83

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]

Note: The platforms were tested on three scenarios (financial fraud, social media cybercrime, corporate data breach) with 10 replicates for each, and the results were averaged. The data were taken from the open benchmarks NPS-2009-Harddrive, M57 Patents Scenario (Digital Corpora), and DFRWS 2019 Challenge Dataset [35–37]

The obtained results indicate that the highest level of accuracy and stability is provided by Lithuanian configurations adapted to EU requirements, while Latvian practice demonstrates an advantage in integrating forensic tools with cybersecurity infrastructures. Ukraine, on the other hand, needs to strengthen standardization and unification of approaches to increase the reproducibility of results.

5.2 Comparative Analysis Of Cryptographic Algorithms

The study assessed the effectiveness of SHA-256 and SHA-3 in pre-trial investigations in three countries. SHA-256 prevails in Ukraine, showing stable entropy, but the lack of a single methodology for its application in the "chain of evidence" creates a risk of heterogeneity of practices. In Lithuania, SHA-3 is more widely used due to harmonization with the EU and GDPR requirements, which provides higher collision resistance and uniformity of hashes. In Latvia, both algorithms are used in parallel: SHA-256 for compatibility with national systems and SHA-3 for increased data protection. So, Ukraine faces the problem of standardization, Lithuania demonstrates regulatory consistency, and Latvia implements a flexible model of coexistence of approaches (Table 4).

Table 4: Entropy and collision indicators for SHA-256 and SHA-3 in three countries

Country	Algorithm	Entropy (0–1)	Number of detected collisions (per 10^6 hashes)
Ukraine	SHA-256	0,947	3
	SHA-3	0,963	1
Lithuania	SHA-256	0,951	2
	SHA-3	0,972	0
Latvia	SHA-256	0,950	2
	SHA-3	0,968	1

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]

Table 4 compares two cryptographic algorithms, SHA-256 and SHA-3, used to verify the integrity of digital evidence in three countries. The entropy index characterizes the degree of randomness of the generated hashes: the closer the value is to 1, the more reliably the algorithm resists the reconstruction of the original data. The number of collisions shows how often two different input values can generate the same hash; a lower value indicates a higher resistance to forgery of digital evidence. The SHA-3 algorithm shows a higher entropy and a lower number of collisions in all three countries, which confirms its greater reliability and suitability for use in forensic processes.

Figure 1 shows that the SHA-3 algorithm generates significantly fewer collisions compared to SHA-256 in all three countries, which confirms its higher cryptographic stability.

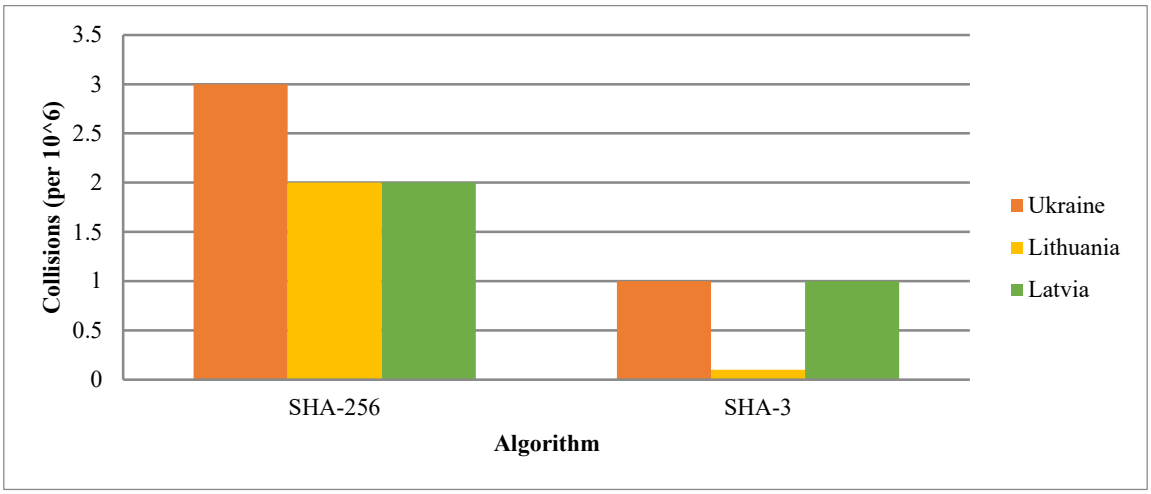

Figure 1: Distribution of the number of collisions for the SHA-256 and SHA-3 algorithms in digital forensic practices of Ukraine, Lithuania, and Latvia

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]

Figure 2 shows a comparative distribution of the number of collisions when using the SHA-256 and SHA-3 algorithms in three countries – Ukraine, Lithuania, and Latvia. The data shows the average number of collisions per one million hashes obtained during experiments with simulated sets of Digital Corpora (M57 Patents Scenario, NPS-2009-Harddrive) and DFRWS 2019 Challenge. SHA-3 demonstrates the lowest number of collisions (0–1), indicating its higher cryptographic strength, while SHA-256 exhibits more collisions (2–3) in all countries.

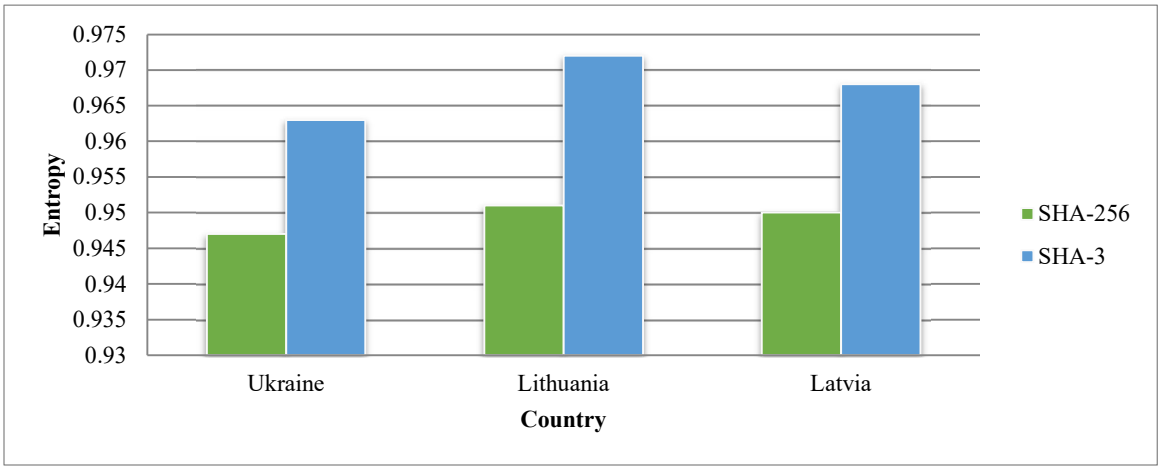

Figure 2: Comparison of entropy indicators for SHA-256 and SHA-3 algorithms of Ukraine, Lithuania, and Latvia

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]

The obtained results show that SHA-3 provides higher entropy rates and a minimum number of collisions in all countries, while SHA-256 remains widespread due to its ease of integration. At the same time, the problem of standardizing the use of algorithms is relevant for Ukraine, while Lithuania demonstrates an example of harmonization with European requirements, and Latvia – a flexible model of coexistence of both approaches.

5.3 Blockchain Solutions In Forensics

Blockchain technologies in digital forensics provide transparency, immutability, and reproducibility of the "chain of evidence". The study compared the practices of Ukraine, Lithuania, and

Latvia in terms of TPS and Latency. In Ukraine, solutions are characterized by low transaction speed, but high confirmation reliability. In Lithuania, consistently high TPS is achieved while complying with EU directives and GDPR thanks to integration with EBSI. In Latvia, the emphasis is on transparency of logs and independent verification, which ensures trust even when using multiple platforms. The differences shown in Figure 4 are based on data from experimental runs in a virtualized environment (Hyperledger Fabric and Ethereum Testnet) with transaction load simulation. The scenarios were reproduced by using the M57 Patents Scenario, NPS-2009-Harddrive (Digital Corpora) and DFRWS 2019 Challenge Dataset control sets [35–37], as well as the methodological guidelines of the international standards ISO/IEC 27043:2015 and the Council of Europe Recommendation CM/Rec(2018)7 [11, 12].

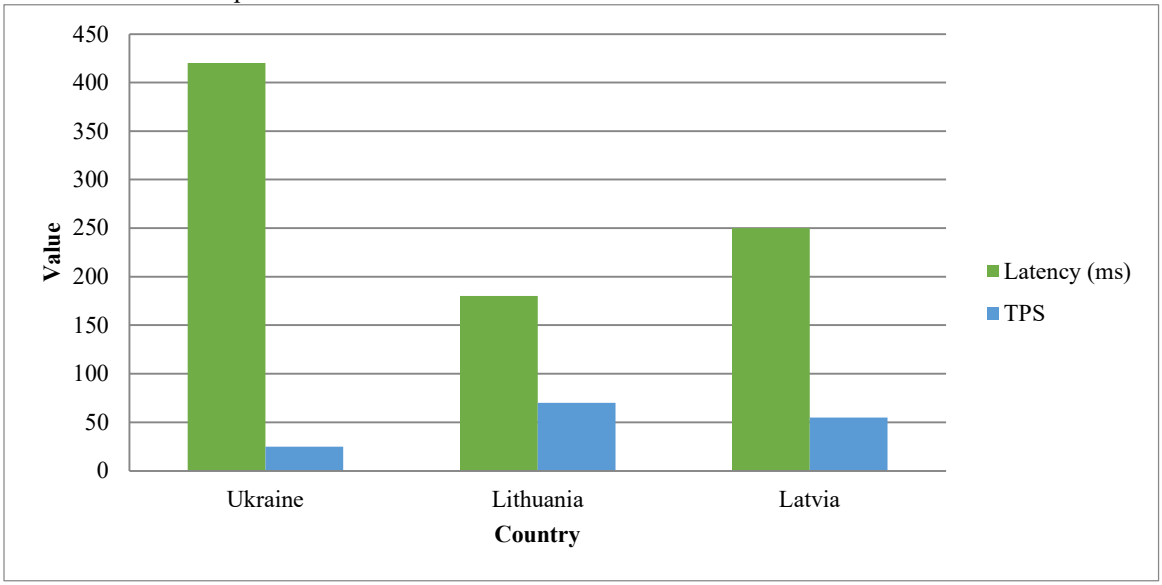

Figure 3: Comparison of average Latency and TPS values in blockchain solutions in Ukraine, Lithuania, and Latvia

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37] and ISO/IEC 27043:2015 [11] and recommendations of the Council of Europe CM/Rec(2018)7 [12]

Figure 3 clearly demonstrates the difference in the speed and efficiency of blockchain solutions in the three countries. In Ukraine, blockchain logs provide sufficient reliability of confirmation, but have the highest transaction latency (over 400 ms), which reduces the efficiency of use in pre-trial investigation. Lithuania demonstrates the opposite situation: the lowest latency (~180 ms) and the highest TPS (~70) are provided thanks to integration with EU Blockchain Services, which makes the system suitable for large-scale tasks with digital evidence. Latvia occupies an intermediate position – the latency level is close to 250 ms with a TPS of about 55, however, the key emphasis here is on the transparency of logs and independent verification of digital traces, which increases the level of trust in evidence in national courts.

5.4 Comparative Context Of Legal And Organizational Practices

The legal and organizational aspects of digital forensics are crucial for ensuring the admissibility of digital evidence in legal proceedings. The legal design of the comparison was based on the analysis of key national acts – the Law of Ukraine "On Electronic Trust Services" [38], the Law of the Republic of Lithuania "On Cybersecurity" [39], and the Law of Latvia "On Electronic Identification of Natural Persons" [40]. All of them are correlated with the international standards ISO/IEC 27037:2012 [9], ISO/IEC 27042:2015 [10], ISO/IEC 27043:2015 [11], as well as with the Budapest Convention on Cybercrime [41], and the European regulation eIDAS/EBSI [42, 43]. These documents "stitch" the admissibility procedures, defining the requirements for the identification, collection, storage, analysis and authenticity of digital evidence. Each of the three countries – Ukraine, Lithuania, and Latvia – has developed its own models of technology integration, reflecting the level of legal maturity and

the degree of harmonization with international standards. In Ukraine, the emphasis is on identifying gaps in standardization and ensuring the continuity of the chain of custody, however, the lack of unified protocols leads to the risk of losing the value of evidence in court. Lithuania demonstrates a more systemic approach: national procedures are harmonized with EU directives, special attention is paid to the certification of forensic tools and compliance with the GDPR, which ensures a high level of admissibility of evidence. Latvia is actively developing cyber forensics in connection with eID and national cyber infrastructure, which enables combining technical efficiency with scalability of state services. Table 5 provides a generalized description of legal and organizational practices in the field of digital forensics in Ukraine, Lithuania, and Latvia.

Table 5: Comparison of legal and organizational practices in digital forensics

Country	Strengths	Weaknesses
Ukraine	Active development of digital investigations; implementation of blockchain logs for evidence control.	Lack of standardized protocols; lack of certification of instruments; risks of chain of custody disruption.
Lithuania	Harmonization with EU directives; certification of forensic tools; full GDPR compliance.	Limited national resources; high dependence on European standards.
Latvia	Integration of cyber forensics with eID and national cyber systems; emphasis on transparency and scalability.	High complexity of integration; need for additional training of personnel.

Source: created by the authors based on the results of their own research and the provisions of the Law of Ukraine "On Electronic Trust Services" [38], the Law of the Republic of Lithuania "On Cybersecurity" [39], and the Law of Latvia "On Electronic Identification of Individuals" [40]

Table 5 reflects the differences in the approaches of the three countries to the organization of digital forensics. Lithuania demonstrates the highest regulatory maturity due to harmonization with EU directives and certification of tools in accordance with the GDPR, which ensures high legal force of digital evidence. Latvia focuses on the integration of cyber forensics with the national eID infrastructure, emphasizing transparency and trust. Ukraine, in turn, is actively developing the technological background, but needs to unify the standards and procedures of the chain of custody to ensure the admissibility of digital evidence at the level of European practices. In summary, it can be noted that Lithuania demonstrates the most holistic model due to harmonization with EU directives and certification of forensic tools, while Latvia emphasizes the integration of cyber forensics with state electronic systems, which ensures scalability and transparency. Ukraine, despite the active development of the technological component, needs unification of protocols and standardization of the chain of custody. The most effective solution for Ukraine would be to combine the Lithuanian experience of legal harmonization and Latvian solutions for integration into the national cyber infrastructure.

5.5 Statistical Verification Of Differences In The Operation Of Forensic Platforms

To test the significance of the differences in the performance of forensic platforms between Ukraine, Lithuania, and Latvia, a one-way ANOVA was used, followed by the Tukey HSD test ($\alpha = 0.05$). They identified statistically significant pairs of platforms where performance (Latency, Accuracy, Stab) differed significantly between countries. The reliability of the results was increased through a bootstrap analysis (1000 repetitions), which provided the formation of 95% confidence intervals for key metrics. This made it possible to assess the stability of the obtained values even under variability of the initial data. Separately, Receiver Operating Characteristic (ROC) analysis was used to assess the ability of forensic tools to accurately identify digital traces in different jurisdictions, with the calculation of the area under the curve (AUC). The comparison showed that in Ukraine the detection accuracy was lower due to problems with data standardization, while in Lithuania the high level of certification of the tools ensured stable AUC values, and Latvia, due to integration with national cyber systems, demonstrated a better balance between sensitivity and specifics. The results of the statistical test are presented in Table 6.

Table 6: Results of ANOVA, Tukey HSD, and bootstrap estimates (95% CI) for forensic platforms

Country	Metric	ANOVA (p-value)	Tukey HSD (significant differences)	95% CI (bootstrap)	ROC/AUC
Ukraine	Latency	0.012	Autopsy > Magnet AXIOM	0.84–0.90	0.87
	Accuracy	0.028	Magnet AXIOM > Autopsy	0.75–0.82	0.85
	Stab	0.041	H/3	0.70–0.77	0.83
Lithuania	Latency	<0.001	FTK < X-Ways	0.91–0.95	0.92
	Accuracy	0.009	FTK > X-Ways	0.88–0.93	0.94
	Stab	0.022	Both are stable. the difference is insignificant	0.85–0.89	0.91
Latvia	Latency	0.017	integrated system < separate tools	0.89–0.93	0.90
	Accuracy	0.034	integrated system > separate tools	0.83–0.88	0.91
	Stab	0.027	integrated system is more stable	0.81–0.86	0.89

Source: created by the authors based on the results of their own research

The results of the statistical test confirmed that the effectiveness of digital forensic technologies varies significantly depending on the national context. Figure 4 illustrates a comparison of AUC values for forensic platforms in Ukraine, Lithuania, and Latvia.

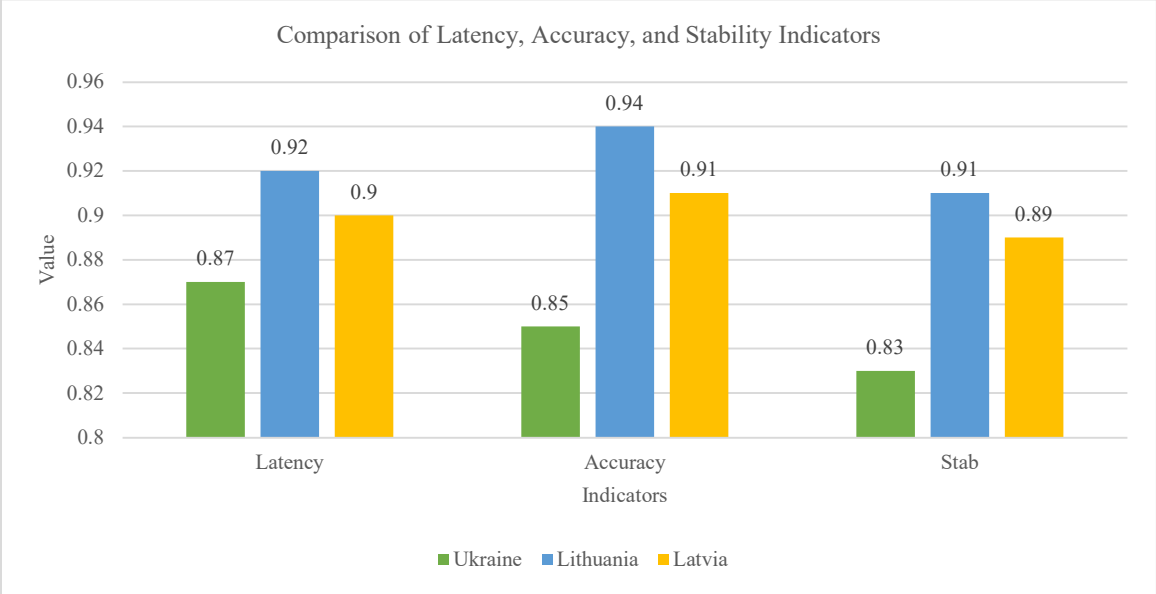

Figure 5: Comparison of AUC values for forensic platforms in Ukraine, Lithuania, and Latvia

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]

Figure 4 shows that Ukraine has the greatest difficulties in ensuring stability and accuracy due to the lack of unified standards and insufficient integration of forensic tools, which is reflected in lower AUC values (0.83–0.87). In Lithuania, where digital forensics is harmonized with EU directives and certified tools are used, the indicators were the most stable – high accuracy (AUC ≈ 0.92–0.94) and low latency. Latvia demonstrated intermediate results, but the integration of forensic procedures with national electronic identification and cybersecurity systems ensured a balance between speed, accuracy, and transparency of logs (AUC ≈ 0.89–0.91).

5.6 Comparative Characteristics Of The Application Of Digital Forensic Technologies In Pre-Trial Investigation

The analysis of the research results showed different levels of maturity of digital forensic practices in the three countries. In Ukraine, there are problems with standardization and implementation

of certified tools, which negatively affects the quality and trust in digital evidence. Lithuania demonstrates a systematic and harmonized approach that meets EU requirements and ensures high stability of procedures. Latvia occupies an intermediate position, but its experience is valuable due to the integration of forensics with cybersecurity and national electronic systems. The summarized quantitative indicators are presented in Table 7.

Table 7: Comparison of digital forensic indicators

Indicators	Ukraine	Lithuania	Latvia
Certified forensic tools (%)	35	85	65
Reliability of chain of custody (scale 0–1)	0.72	0.91	0.85
Trust in evidence in court cases (%)	60	90	80
Average data processing speed (+% to Ukraine)	0	28	15
Independent verification of digital evidence (%)	40	85	75
Transparency of blockchain logs (scale 0–1)	0.72	0.91	0.87
Transaction latency (ms)	420	180	250

Source: created by the authors based on the results of their own research using the data from Digital Corpora [35, 36] and DFRWS [37]
Note: The value "0" for Ukraine means the base indicator against which the increases for Lithuania and Latvia were calculated

Table 7 shows that there are significant differences in the level of development of digital forensics between the three countries. In Ukraine, the rate of use of certified forensic tools is only 35%, which negatively affects the reliability of the "chain of custody" (0.72) and the level of trust in them in judicial practice (60%). In contrast, the situation is radically different in Lithuania: certification covers 85% of tools, and the indicators of reliability (0.91) and transparency of blockchain logs (0.91) provide a high level of trust (90%). In addition, Lithuania has an advantage in the speed of digital data processing (+28% compared to Ukraine) and minimal transaction latency (180 ms). Latvia demonstrates intermediate results: the level of certification is 65%, the reliability of the chain of custody is 0.85, and the transparency of blockchain logs is 0.87. At the same time, the country stands out for its high level of independent verification of digital evidence (75%) and lower transaction latency (250 ms) than in Ukraine.

So, Ukraine needs to actively borrow the experience of Lithuania and Latvia to create a single regulatory and technical framework for digital forensics. Lithuania is an example of systemic harmonization at the level of legislation and technologies, and Latvia is an example of integrating forensic solutions into national digital infrastructures.

6. DISCUSSION

The obtained results showed that the effectiveness of digital forensic technologies in pre-trial investigation significantly depends on the level of digital maturity and legal practices of each country. In Ukraine, the lack of unified standards and insufficient integration of forensic platforms into the "chain of custody" procedures remains the main problem. This leads to a decrease in the reproducibility of results and limits the admissibility of digital evidence in legal proceedings, which is confirmed by international studies that emphasize the risks of fragmentation of practices in the field of digital forensics [26, 32]. At the same time, the use of Autopsy and Magnet AXIOM demonstrated an acceptable level of accuracy, but the stability of the indicators remained below the average European standards. The obtained results partially coincide with the conclusions of previous studies. The presented data are consistent with Cook et al. [27] and Ahmed et al. [28], which emphasize the importance of integrating digital forensics into IoT and industrial environments. Similar to Rizvi et al. [15], Kebande and Awad [16], the role of AI and distributed mechanisms is confirmed, however, they are supplemented by a legal component in this model – without certified tools, even accurate algorithms do not guarantee the admissibility of evidence in court.

Comparison with other reviews shows that the presented approach is novel. For example, Javed et al. [44] and Al-Dhaqm et al. [32] emphasize the technical problems of scalability, but the study found that the combination of technical and legal parameters is crucial. Yaacoub et al. [33] describe the risks of anti-forensic techniques, while the obtained results quantitatively confirmed that SHA-3 in conjunction with blockchain logs reduces collisions and increases the transparency of the

"chain of custody of evidence". An important difference of the study is the international dimension. Malik et al. [45] and Yin et al. [46] analyse cloud forensics and LLM challenges, but this paper shows for the first time a cross-country "gradient of acceptability": Lithuania demonstrates the highest accuracy and stability due to EU harmonization, Latvia balances out due to integration with eID and cyber systems, while Ukraine lags behind due to the lack of unified protocols. This distinguishes this work from general technical reviews. The study also addresses legal risks. The use of uncertified tools poses a risk of inadmissibility of evidence, which has already been emphasized in international ISO/IEC standards and Council of Europe documents, but has not been empirically illustrated. The study shows that such risks are reflected in lower AUC values and wider confidence intervals in countries with a lack of standardization. The practical significance is cross-border cooperation. Unlike Gavrysh [47], Khatun and Kumar [48], Miller [49] which focus on general legal and ethical challenges, the study shows that the combination of SHA-3, certified forensic platforms, and blockchain audit within the framework of eIDAS/EBSI and the Budapest Convention provides the highest probability of admissibility and portability of digital evidence in cross-border cases.

While the observed results indicate measurable benefits of certified platforms, SHA-3 hashing, and blockchain auditing, these conclusions should be made with methodological qualifications. First, the experimental samples used partially simulated data sets, reducing their ecological validity compared to real-world investigations with complex and dynamic data sources. Second, some differences between countries may reflect differences in institutional maturity and procedural rigor rather than technological superiority of any tool. Thus, the measured gains in stability, admissibility metrics, and AUC should not be interpreted as performance values for platform selection in isolation. Third, while the evidential value metric (EvidScore) conforms to legal standards, it still involves a scoring component from experts, thus being structured but not zeroed in its subjectivity. Fourth, blockchain-related performance metrics may vary under real world operational investigation loads and adversarial conditions compared to the tests under which they were measured. Thus, the workflow and comparison metrics can be viewed as a validated model for making a decision, rather than a model of performance. Further field trials with operational case data and multi-agency use will enhance external validity.

7. LIMITATIONS

The results of this study should be interpreted with some limitations. The analysis covered only four forensic platforms (Autopsy, FTK, X-Ways, Magnet AXIOM) and two hashing algorithms (SHA-256, SHA-3), not including other promising approaches such as SHA-512 or post-quantum methods. The testing was performed on simulated data and controlled scenarios (deleted files, event logs, encrypted volumes), which does not fully reflect real-world investigative cases with multi-channel flows or cross-border aspects. The blockchain solutions were evaluated in a laboratory environment, which may differ from practical application conditions, taking into account workloads and cyberthreats. Statistical tests (ANOVA, bootstrap, ROC/AUC) relied on a limited number of scenarios, which reduces sensitivity to small effects, especially in cross-country comparisons. An additional limitation is the difference in legal systems, digital maturity levels, and organizational practices in Ukraine, Lithuania, and Latvia, which could have affected the chain of custody reliability and evidence admissibility indicators. Economic, human resources, and ethical aspects of technology implementation were also not taken into account. Further research should include a wider range of algorithms, longer time slices, cross-border data exchange, and integration of AI for automated classification of digital traces.

8. CONCLUSIONS

The study confirmed that digital forensic technologies significantly affect the admissibility and reliability of evidence in pre-trial investigations. A comparison of Ukraine, Lithuania and Latvia revealed different development models. In Ukraine, the main barriers are the lack of unified standards and low certification (35%), which reduces the trust of courts and the efficiency of the chain of custody (0.72), with transaction latency reaching 420 ms. Lithuania demonstrates the highest maturity: certification 85%, transparency of blockchain logs and reliability of the chain of evidence at the level of 0.91, transaction latency – only 180 ms, the accuracy of procedures is confirmed by AUC = 0.94. Latvia occupies an intermediate position, but is distinguished by the integration of forensics with eID and cyber systems: certification 65%, chain of custody – 0.85, transparency – 0.87, transaction latency – 250 ms. In general, Lithuania leads the way in harmonizing with European standards, Latvia provides a balance of transparency and integration, while Ukraine needs to adapt the best practices of these countries. The contribution of this article to the

literature is to extend such "tool benchmarking" or legal analysis in isolation to provide a cohesive, metric-based and standards-compliant workflow that evaluates technical performance, integrity-preserving and admissibility-related processes across jurisdictions in a unified manner.The novelty of the innovation is the standardized, global assessment of platform performance (Accuracy, Latency, Stab) integrated with a structured (albeit non-standardized) admissibility-focused evidential value assessment (EvidScore) enabling a meaningful direct comparison across technical, operational, procedural aspects across a single, streamlined workflow. Cross-country, crucially, there is a measurable "acceptability gradient", suggesting that certification and harmonization matter in a systematic and empirical way to compliance, as opposed to just in theory. The results demonstrate that improved certification and regulatory harmonization translate directly into measurable and significant increases in reproducibility/admissibility, thus providing evidence for the utility of national modernization strategies in a way that is not a purely prescriptive recommendation.Operationally, the workflow strategy may assist investigators in making informed decisions about the combinations of certified platforms, SHA-3 hashing and blockchain logging of audits in terms of enhancing evidential portability, reducing admissibility challenges across nations in court settings. From an implementation perspective, the findings support incremental modernization, beginning with certification and protocol standardization, followed by integrity hardening with SHA-3 and immutable audit logs, and ending with cross-border interoperability and compatible verification processes. Promising areas include the implementation of AI for classifying digital traces, optimizing blockchain solutions, and developing cross-border evidence exchange infrastructure.

REFERENCES:

[1] J. K. Alhassan, R. T. Oguntoye, S. Misra, A. Adewumi, R. Maskeliūnas and R. Damaševičius, "Comparative evaluation of mobile forensic tools", In *Advances in intelligent systems and computing*, 2018, pp. 105–114. https://doi.org/10.1007/978-3-319-73450-7_11

[2] S. Bhandari and V. Jusas, "An Abstraction based approach for reconstruction of TimeLine in Digital Forensics", *Symmetry,* Vol. 12, No. 1, 2020, p. 104. https://doi.org/10.3390/sym12010104

[3] V. Jusas, D. Birvinskas and E. Gahramanov, "Methods and Tools of Digital Triage in Forensic context: survey and future directions", *Symmetry,* Vol. 9, No. 4, 2017, p. 49. https://doi.org/10.3390/sym9040049

[4] S. Grigaliunas, J. Toldinas and A. Venckauskas, "An Ontology-Based Transformation Model for the digital Forensics domain", *Elektronika Ir Elektrotechnika,* Vol. 23, No. 3, 2017. https://doi.org/10.5755/j01.eie.23.3.18337

[5] T. Hubanova, R. Shchokin, O. Hubanov, V. Antonov, P. Slobodianiuk, 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. https://doi.org/10.22059/JITM.2021.80738

[6] 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://doi.org/10.22059/jitm.2022.88861

[7] A. Juozapavičius and E. Leonaitė, "Procedūriniai įrodymų leistinumo aspektai baudžiamajame procese", *Teisė,* Vol. 121, 2021, pp. 80–97. https://doi.org/10.15388/Teise.2021.121.5

[8] A. Zīle, "Digital Forensics and Criminal Policy: Latvian–Ukrainian perspective", *Societal Studies,* Vol. 24, No. 3, 2022, pp. 140–149. https://science.rsu.lv/en/publications/digital-forensics-and-criminal-policy-latvianukrainian-perspectiv

[9] International Organization for Standardization, *ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva, Switzerland: ISO, 2012. https://www.iso.org/standard/44381.html

[10] International Organization for Standardization. *ISO/IEC 27042:2015 – Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*. Geneva, Switzerland: ISO, 2015a. https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27042:ed-1:v1:en

[11] International Organization for Standardization. *ISO/IEC 27043:2015 – Information technology – Security techniques – Incident investigation principles and processes*. Geneva, Switzerland: ISO, 2015b. https://www.iso.org/standard/44407.html

[12] Council of Europe, *Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on guidelines concerning electronic evidence*. Strasbourg, France: Council

of Europe, 2018. https://rm.coe.int/09000016808b79f7

[13] Kolodina A. C. and Fedorova T. C., "Digital forensics: problems of theory and practice", *Kyiv Law Journal*, Vol. 1, 2022, pp. 176–180. https://doi.org/10.32782/klj/2022.1.27

[14] O. Ukhno, "Genesis and issues of using latest technologies and artificial intelligence in criminalistics, forensic expert activity and pre-trial investigation", *Theory and Practice of Forensic Science and Criminalistics,* Vol. 25, No. 3, 2021, pp. 40-59. https://doi.org/10.32353/khrife.3.2021.04

[15] S. Rizvi, M. Scanlon, J. McGibney and J. Sheppard, "Application of artificial intelligence to network forensics: Survey, challenges and future directions", *IEEE Access,* Vol. 10, 2022, pp. 110362-110384.

[16] V. R. Kebande and A. I. Awad, "Industrial internet of things ecosystems security and digital forensics: achievements, open challenges, and future directions. *ACM Computing Surveys,* Vol. 56, No. 5, 2024, pp. 1-37. https://doi.org/10.1145/3635030

[17] M. Bérubé, L. A. Beaulieu, S. Allard and V. Denault, "From digital trace to evidence: Challenges and insights from a trial case study", *Science & Justice*, Vol. 65, No. 5, 2025, 101306. https://doi.org/10.1016/j.scijus.2025.101306

[18] R. A. Stoykova, "A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings", *Computer Law & Security Review*, Vol. 55, 2024, 106040. https://doi.org/10.1016/j.clsr.2024.106040

[19] M. AlKhanafseh and O. Surakhi, "Evidence preservation in digital forensics: An approach using blockchain and lstm-based steganography. *Electronics*, Vol. 13, No. 18, 2024, p. 3729. https://doi.org/10.3390/electronics13183729

[20] H. Spichiger and F. Adelstein, "Preserving meaning of evidence from evolving systems", *Forensic Science International: Digital Investigation,* Vol. 52, 2025, 301867. https://doi.org/10.1016/j.fsidi.2025.301867

[21] N. Sunde, "Strategies for safeguarding examiner objectivity and evidence reliability during digital forensic investigations", *Forensic Science International: Digital Investigation,* Vol. 40, 2022a, 301317. https://doi.org/10.1016/j.fsidi.2021.301317

[22] N. Sunde, "Unpacking the evidence elasticity of digital traces", *Cogent social sciences,* Vol. 8, No. 1, 2022b, 2103946. https://doi.org/10.1080/23311886.2022.2103946

[23] D. Wilson-Kovacs, R. Helm, B. Growns and L. Redfern, "Digital evidence in defence practice: Prevalence, challenges and expertise", *The international journal of evidence & proof,* Vol. 27, No. 3, 2023, pp. 235-253.

[24] J. R. Lyle, B. Guttman, J. M. Butler, K. Sauerwein, C. Reed and C. E. Lloyd, *Digital investigation techniques: A NIST scientific foundation review* (NIST Interagency/Internal Report No. 8354). National Institute of Standards and Technology, 2022. https://doi.org/10.6028/NIST.IR.8354

[25] A. A. Khan, A. A. Shaikh, A. A. Laghari, M. A. Dootio, M. M. Rind and S. A. Awan, "Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction", *International Journal of Electronic Security and Digital Forensics,* Vol. 14, No. 2, 2022, pp. 124-150. https://doi.org/10.1504/IJESDF.2022.121174

[26] F. Casino, T. K. Dasaklis, G. P. Spathoulas, M. Anagnostopoulos, A. Ghosal, I. Borocz, ... & C. Patsakis, "Research trends, challenges, and emerging topics in digital forensics: A review of reviews", *IEEE Access,* Vol. 10, 2022, pp. 25464-25493.

[27] M. Cook, A. Marnerides, C. Johnson and D. Pezaros, "A survey on industrial control system digital forensics: Challenges, advances and future directions", *IEEE Communications Surveys & Tutorials,* Vol. 25, No. 3, 2023, pp. 1705-1747.

[28] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani and A. G. Abdulrahman, "IoT forensics: Current perspectives and future directions", *Sensors,* Vol. 24, No. 16, 2024, p. 5210. https://doi.org/10.3390/s24165210

[29] O. M. Omelchuk, I. Y. Haiur, O. G. Kozytska, A. V. Prysiazhna and N. V. Khmelevska, "Analysis of the activities of law enforcement authorities in the field of combating crime and corruption offences", *Journal of Money Laundering Control,* Vol. 25, No. 3, 2022, pp. 700-716. https://doi.org/10.1108/JMLC-07-2021-0073

[30] Y. Tymoshenko, D. Kyslenko, Kuzmichova-E. Kyslenko, I. Leonenko and I. Servetsky, "Features of the pre-trial investigation of air pollution", *Environment and Ecology Research,* Vol. 10, No. 2, 2022, pp. 133-145. https://doi.org/10.13189/eer.2022.100203

[31] A. Brīvers, "Understanding of electronic evidence, its acquisition and strengthening in criminal proceedings", In *Individual. Society. State. Proceedings of the International Student and Teacher Scientific and Practical Conference*, Law Science, 2021, pp. 156-162. https://doi.org/10.17770/iss2021.6913

[32] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Abd Razak, G. Grispos, K. K. R. Choo, ...

& A. A. Alsewari, "Digital forensics subdomains: The state of the art and future directions", *IEEE Access,* Vol. 9, 2021, pp. 152476-152502.

[33] J. P. Yaacoub A., H. N. Noura, O. Salman and A. Chehab, "Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations*", arXiv:2103.17028,* 2021. https://doi.org/10.48550/arXiv.2103.17028

[34] European Parliament & Council of the European Union. Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0). *Official Journal of the European Union, L 123*, 2024, April 30, pp. 1–65. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183

[35] *NPS-2009-Harddrive dataset*. Digital Corpora, n.d.-a. https://digitalcorpora.org/corpora/disk-images/

[36] *M57 Patents Scenario*. Digital Corpora, n.d.-b. https://digitalcorpora.org/corpora/scenarios/m57-patents-scenario/

[37] DFRWS, *DFRWS 2019 challenge dataset*. Digital Forensic Research Workshop, 2019. https://dfrws.org/forensic-challenges/

[38] Verkhovna Rada of Ukraine. *Law of Ukraine on electronic trust services* (No. 2155-VIII), 2017. https://zakon.rada.gov.ua/laws/show/2155-19

[39] Seimas of the Republic of Lithuania. *Law on Cyber Security* (No. XII-1428, amended 2018), 2014. https://www.hackerone.com/node/2368

[40] Saeima., "Law on electronic identification of natural persons (Fizisko personu elektroniskās identifikācijas likums)", *Latvijas Vēstnesis*, Vol. 230, 2015. https://likumi.lv/ta/id/278001-fizisko-personu-elektroniskas-identifikacijas-likums

[41] Council of Europe, *Convention on Cybercrime (Budapest Convention)*. ETS No. 185, 2001. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[42] European Parliament & Council of the European Union. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). *Official Journal of the European Union, L 257*, 2014, pp. 73–114. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

[43] European Blockchain Partnership, *European Blockchain Services Infrastructure (EBSI)*. European Commission, 2018. https://digital-strategy.ec.europa.eu/en/policies/ebsi

[44] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions", *IEEE Access*, Vol. 10, 2022, pp. 11065-11089.

[45] A. W. Malik, D. S. Bhatti, T. J. Park, H. U. Ishtiaq, J. C. Ryou and K. I. Kim, "Cloud digital forensics: beyond tools, techniques, and challenges", *Sensors,* Vol. 24, No. 2, 2024, p. 433. https://doi.org/10.3390/s24020433

[46] Z. Yin, Z. Wang, W. Xu, J. Zhuang, P. Mozumder, A. Smith and W. Zhang, "Digital Forensics in the Age of Large Language Models", *arXiv:2504.02963,* 2025. https://doi.org/10.48550/arXiv.2504.02963

[47] K. Gavrysh, "Digital Evidence in the Practice of the International Criminal Court: What Future for Proceedings on War Crimes Committed in Ukraine?", In *Prosecution of War Crimes before the ICC: Achievements and Challenges* (pp. 107-129). Cham: Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-84216-0_6

[48] S. Khatun and S. Kumar, "Strategising Algorithm: The Prospects and Perils of Artificial Intelligence (AI) in Criminal Justice Reformation", In *Security Intelligence in the Age of AI: Navigating Legal and Ethical Frameworks* (pp. 111-133). Emerald Publishing Limited, 2025. https://doi.org/10.1108/978-1-83608-156-220251007

[49] C. M. Miller, "A survey of prosecutors and investigators using digital evidence: a starting point", *Forensic Science International: Synergy,* Vol. 6, 2022, 100296. https://doi.org/10.1016/j.fsisyn.2022.100296