CADERNOS DE DEREITO ACTUAL
www.cadernosdedereitoactual.es

© ***Cadernos de Dereito Actual*** Nº 31. Núm. Ordinario (2026), pp. 238-256
·ISSN 2340-860X - ·ISSNe 2386-5229

Use of digital forensics technologies as part of the legal public security mechanism to detect cyberthreats

Volodymyr Kopanchuk[1]
Leonid Yuzkov Khmelnytskyi University of Management and Law
Vladyslav Veklych[2,*]
Prince Volodymyr the Great Educational and Scientific Institute of Law Interregional Academy of Personnel Management
Yurii Turovets[3]
Leonid Yuzkov Khmelnytskyi University of Management and Law
Volodymyr Atamanchuk[4]
National Academy of Internal Affairs
Oleg Kravchuk[5]
Leonid Yuzkov Khmelnytskyi University of Management and Law

[1] Doctor of Science in Public Administration, PhD in Legal Sciences, Associate Professor, Professor, Department of Public Management and Administration, Faculty of Public Management, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. ORCID: 0000-0002-4198-6510; E-mail: jrist@ukr.net.
[2] Doctor of Law, Associate Professor, Professor of the Department of Theory of State and Law and Constitutional Law, Prince Volodymyr the Great Educational and Scientific Institute of Law, Interregional Academy of Personnel Management, Kyiv, Ukraine. ORCID: 0000-0003-2608-6781; E-mail: veklicvladislav7@gmail.com (corresponding author).
[3] PhD in Legal Sciences, Associate Professor, Professor, Department of Criminal Law and Procedure, Faculty of Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. ORCID: 0000-0002-1110-9234; E-mail:yura_turovez@ukr.net.
[4] PhD in Legal Sciences, Associate Professor, Head of the Department of Forensic Support and Examination, Educational and Scientific Forensic Institute of the National Academy of Internal Affairs, Kyiv, Ukraine. ORCID: 0000-0002-1464-7871; E-mail: atamanchyk_vlad@ukr.net.
[5] Doctor of Science in Public Administration, PhD in Legal Sciences, Professor, Department of Criminal Law and Procedure, Faculty of Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, Ukraine. ORCID: 0000-0002-7002-4070; E-mail: olegkravchuk@ukr.net.

Abstract: The study addresses the issue of the growing cyber threats as a factor undermining public security. The existing legal frameworks lag behind the rapid evolution of cybercrime. This leaves state institutions vulnerable to sophisticated attacks. The aim of the article is to determine the role of digital forensics as a technical and evidentiary tool in strengthening the legal capacity of states to ensure security in cyberspace. Particular attention is paid to empirical materials obtained from the analysis of case studies of cyber investigations. The practice of law enforcement agencies is also taken into account. The research employed the following methods: doctrinal legal analysis, comparative analysis of national and international legal practice, as well as a critical review of forensic technologies used in cyber investigations. The results showed that the effectiveness of public security systems depends on both technical excellence and legal adaptability. The study examined 300 digital case models from case law and reports of law enforcement agencies in the United States (USA), Germany, France, and Poland. The key factor is the regulation of digital evidence, its admissibility and the preservation of the chain of custody. Unlike many studies that focus on technical aspects or criminology only, this study emphasizes the legal dimension of forensic technologies. It emphasizes their dual function—as a means of detection and as a guarantee of procedural fairness.The findings confirmed that integrating digital forensics into criminal process standards increases the resilience of state institutions to cyber threats. It also strengthens the legitimacy of legal responses. Further research prospects include the development of harmonized international standards for processing digital evidence. Strengthening cross-border cooperation and the implementation of forensic technologies in preventive legal policies are also important areas.

Keywords: Digital Forensics, Cyber Threats, Cyber Threat Detection, Digital Evidence Admissibility, Chain of Custody, Criminal Procedure law, Public Security Governance, Forensic Integrity Verification, Cybercrime Investigation, AI-Assisted Forensic Systems

1. Introduction

The rapid growth of digital technologies has radically transformed public administration and security agencies. At the same time, it exposes critical infrastructures and information systems to increasingly sophisticated cyber threats. In 2024, the European Union (EU) suffered approximately 10,000 cyberattacks. Distributed denial-of-service (DDoS) attacks accounted for 41.1% of these incidents, and malware accounted for 25.7%[6]. Similarly, the USA has seen a sharp increase in ransomware attacks, up 146% year-on-year. In 2025, over 3,600 incidents were recorded, making the USA the world leader in ransomware attacks[7].

In modern society, detecting and preventing cybercrime is not only a technological challenge, but also a complex legal and regulatory issue. This requires careful coordination of digital forensics capabilities with legal accountability mechanisms[8,9]. The relevance of the study is determined by the increasing number of cyber incidents targeting government and private structures. Ignoring such threats can create significant risks for public security, socio-economic stability, and sustainable development[10,11].

In addition, the rapid development of cyber threats, such as AI-based and deepfake-based attacks, creates obstacles to maintaining the integrity and reliability of digital evidence[12]. Despite the growing importance of digital forensics for cybersecurity, a number of critical issues remain poorly studied. These include the effectiveness of existing legal mechanisms in ensuring timely access to digital evidence. The issue of harmonizing forensic procedures with international legal standards is also insufficiently studied. There is also a need to integrate human-cantered approaches into law enforcement strategies for detecting cyber threats[13,14].

---

[6] VILLAFANI, F. "Cyber-attacks in the EU: 10,000 in the last year, 19% against the Administration", Global Affairs. University of Navarra, 2025. Available at: https://en.unav.edu/web/global-affairs/ciberataques-en-la-ue-10.000-en-el-ultimo-ano-el-19-contra-la-administracion (accessed on 02 December 2025).

[7] FADILPAŠIĆ, S. "US becomes ransomware capital of the world as attacks rise by almost 150 percent", TechRadar, 2025. Available at: https://www.techradar.com/pro/security/us-becomes-ransomware-capital-of-the-world-as-attacks-rise-by-almost-150-percent (accessed on 02 December 2025).

[8] SONI, N. "Digital forensics: Confronting modern cyber crimes, technological advancements, and future challenges", Journal of Forensic Legal Investigative Sciences, v. 11, n. 1, 2025, p. 105. https://doi.org/10.24966/FLIS-733X/100105

[9] SalvationDATA, "Key trends in digital forensics for 2025: Technological innovation and core challenges", 2025. Available at: https://www.salvationdata.com/knowledge/key-trends-in-digital-forensics-for-2025/ (accessed on 02 December 2025).

[10] VORONINA, Y.; LOPUSHYNSKYI, I.; GRECHANYK, B.; VAHONOVA, O.; KONDUR, A.; AKIMOV, O. "Economic and environmental component in the field of sustainable development management", Quality-Access to Success, v. 25, n. 201, 2024. https://doi.org/10.47750/qas/25.201.02

[11] YERMACHENKO, V.; BONDARENKO, D.; AKIMOVA, L.; KARPA, M.; AKIMOV, O.; KALASHNYK, N. "Theory and Practice of Public Management of Smart Infrastructure in the Conditions of the Digital Society's Development: Socio-economic Aspects", Economic Affairs, v. 68, n. 1, 2023. https://doi.org/10.46852/0424-2513.1.2023.29

[12] SABIN, S. "Courts aren't ready for AI-generated evidence", Axios, 2025. Available at: https://www.axios.com/2025/07/25/courts-deepfakes-ai-trial-evidence (accessed on 02 December 2025).

[13] IMMENKAMP, B. Access to data for law enforcement: Digital forensics (EPRS Briefing PE 775.879). European Parliamentary Research Service, 2025. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775879/EPRS_BRI(2025)775879_EN.pdf (accessed on 02 December 2025).

[14] SEMENETS-ORLOVA, I.; SHEVCHUK, R.; PLISH, B.; MOSHNIN, A.; CHMYR, Y.; POLIULIAKH, R. "Human-Centered Approach in New Development Tendencies of Value-Oriented Public

Moreover, while technological progress has significantly expanded the capabilities of forensic examination, academic analysis of how these tools can be systematically implemented into legal mechanisms to ensure public safety remains limited. This includes issues of protecting individual rights and complying with regulatory requirements[15].

The research hypothesis is based on the assumption that digital forensics can significantly increase the effectiveness of countering cyber threats. Its application can improve the process of detecting, qualifying, and prosecuting cybercrimes. This is possible only if digital tools are legally integrated into the criminal process.

The academic novelty of the study is the comprehensive conceptualization of digital forensics. It is considered not only as a technical tool for collecting evidence, but also as a legal tool integrated into the public security system. The article emphasizes the dual function of digital forensics. It is a mechanism for identifying hidden cyber threats and an integral element of legal policy aimed at maintaining stability and protecting public values.

The aim of the article is to investigate how digital forensics, as a technical and evidentiary tool, can help states to ensure security in cyberspace. Particular attention is paid to empirical data obtained from the analysis of case studies of cyber investigations. Besides, the way law enforcement agencies operate is taken into account. The aim was achieved through the fulfilment of the following research objectives: (1) Study the regulatory and doctrinal foundations governing the use of digital forensics technologies in combating cybercrime. In particular, analyse existing gaps in national legislation, comparative legal systems and international standards governing the collection and processing of digital evidence. (2) Analyse the evidentiary potential and procedural admissibility of digital forensics findings in criminal proceedings related to cyber threats. Practical case studies, court decisions and legal doctrines on the qualification, authentication, and use of digital evidence in the prosecution of cyber criminals were studied for this purpose. (3) Identify prospects for strengthening public security through the systematic integration of digital forensics technologies into national and international legal systems. This includes the development of guidelines for law enforcement agencies, the harmonization of procedural rules and the integration of technical forensics methods into preventive and investigative measures.

2. Literature review

2.1. Conceptualizing cyber threats in legal and forensic scholarship

Contemporary academic discourse increasingly recognizes that the notion of a cyber threat cannot be reduced to individual cybercrimes or isolated technical incidents. In legal and security studies, cyber threats are commonly conceptualized as potential or actual hostile activities in cyberspace capable of undermining public security, critical infrastructure, institutional stability, or legally protected interests, regardless of whether they have already materialized into completed criminal offenses. This distinction is critical, as cyber threats encompass preparatory acts, latent system vulnerabilities, and coordinated attack capabilities that may not yet satisfy the formal elements of a criminal offence but nonetheless demand legal and institutional responses.

Unlike cybercrime, which presupposes the completion of a legally defined offence, or cyber risk, which focuses on probabilistic exposure, cyber threats

---

Administration: Potential of Education", Economic Affairs, v. 67, n. 5, 2022. https://doi.org/10.46852/0424-2513.5.2022.25

[15] McNICHOLAS, E. R. (Ed.). Cybersecurity laws and regulations: USA. ICLG, 2024. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (accessed on 02 December 2025).

operate at the intersection of technical indicators, intent inference, and legal qualification. Recent legal scholarship emphasizes that the evidentiary challenge lies precisely in transforming fragmented digital traces into legally meaningful indicators capable of supporting preventive, investigative, and prosecutorial action. From this perspective, digital forensics functions not merely as a post-incident evidentiary tool, but as a mechanism for identifying, validating, and legally contextualizing cyber threats within public security systems.

However, despite the frequent use of the term "cyber threat" in cybersecurity literature, its operationalization in legal-forensic research remains inconsistent. Many studies implicitly conflate threats with incidents, thereby overlooking the analytical transition from technical anomaly detection to legally relevant threat assessment. This conceptual gap underlines the necessity of integrating digital forensic methodologies with doctrinal legal analysis to ensure that cyber threats are not only detected, but also legally qualified and procedurally actionable.

2.2. Digital forensics, AI, and threat detection: Technical advances and legal tensions

A substantial body of research highlights the growing role of artificial intelligence (AI) and machine learning (ML) in enhancing digital forensic capabilities. Studies focusing on AI-assisted cybersecurity demonstrate that automated anomaly detection, pattern recognition, and large-scale log analysis significantly improve the speed and scope of cyber threat identification. These technologies are particularly effective in detecting distributed denial-of-service attacks, ransomware behaviors, and phishing campaigns, where traditional rule-based approaches often fail[16].

At the same time, forensic science literature increasingly warns that technical effectiveness does not automatically translate into legal admissibility. Several authors stress that algorithmic decision-making introduces new challenges related to transparency, explainability, and accountability[17]. Courts in multiple jurisdictions remain cautious toward AI-generated forensic outputs, especially when the logic of detection or classification cannot be clearly reconstructed or independently verified[18]. This tension reflects a broader divergence between technological optimism in cybersecurity research and legal conservatism in evidentiary assessment.

Research on forensic readiness further illustrates this divide. Organizational and technical models of forensic preparedness emphasize early data collection, logging, and system monitoring as essential components of effective threat response[19]. While these models strengthen investigative capacity, legal scholars point out that premature or poorly regulated data collection may conflict with procedural safeguards, privacy guarantees, and due process requirements[20]. Consequently, the

---

[16] Hassan, N. S. K., Ibrahim, N. A. "The role of Artificial Intelligence in Cyber Security and Incident Response", International Journal for Electronic Crime Investigation, v. 7, n. 2, 2023. https://doi.org/10.54692/ijeci.2023.0702154

[17] Dunsin, D.; Ghanem, M. C.; Ouazzane, K.; Vassilev, V. "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response", Forensic Science International Digital Investigation, v. 48, 2024, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

[18] Ali, M. I.; Kaur, S. "Next-Generation Digital Forensic Readiness BYOD Framework", Security and Communication Networks, v. 2021, 2021, pp. 1–19. https://doi.org/10.1155/2021/6664426

[19] Khan, A. A.; Zhang, X.; Hajjej, F.; Yang, J.; Ku, C. S.; Por, L. Y. "ASMF: Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning", Heliyon, v. 10, n. 1, 2023, e23254. https://doi.org/10.1016/j.heliyon.2023.e23254

[20] Fakiha, B. "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification", International Journal of Safety and Security

literature increasingly calls for forensic readiness frameworks that embed legal compliance directly into technical design, rather than treating law as an external constraint.

2.3. Chain of custody, evidentiary integrity, and threat intelligence transformation

Another major research strand addresses the procedural reliability of digital evidence through chain-of-custody documentation and cryptographic integrity verification. Technical studies consistently demonstrate that hashing mechanisms and controlled evidence handling significantly reduce the risk of data manipulation. From a legal standpoint, these practices are indispensable for maintaining evidentiary continuity and safeguarding admissibility[21].

Nevertheless, existing scholarship often treats chain of custody as an endpoint—a means of preserving evidence for court—rather than as a continuous analytical process that begins at the moment a cyber threat is detected[22]. This limitation becomes particularly visible in studies on network forensics, cloud environments, and Internet-of-Things ecosystems, where data volatility and distributed architectures complicate traditional evidence models. Scholars increasingly acknowledge that forensic indicators must be transformed into actionable threat intelligence, capable of informing operational decisions by law enforcement agencies before and during criminal proceedings[23].

Despite these insights, the literature rarely provides a unified analytical framework linking detection, interpretation, and legal response. Technical works focus on identifying indicators of compromise, while legal analyses concentrate on admissibility and procedural safeguards. The absence of an integrated model leaves unresolved questions regarding how forensic findings support decision-making, threat prioritization, and proportional response strategies within public security systems.

2.4. Public security, institutional capacity, and policy-oriented gaps

Beyond technical and procedural concerns, several authors situate digital forensics within broader discussions of public security, governance, and institutional capacity. Research in administrative and public law emphasizes that cyber threats challenge not only law enforcement agencies, but also regulatory systems responsible for safeguarding public values and societal stability[24]. These studies argue that forensic technologies must be embedded within coherent legal policies to prevent fragmentation between detection capabilities and institutional authority.

However, comparative legal research on digital forensics remains limited. While some jurisdictions have developed advanced regulatory frameworks for cyber investigations, cross-border harmonization is still underdeveloped. Scholars note that disparities in evidentiary standards, investigative powers, and oversight

---

Engineering, v. 13, n. 4, 2023, pp. 701–707. https://doi.org/10.18280/ijsse.130412

[21] Sharma, P.; Gillanders, J. "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art", IEEE Access, v. 10, 2022, pp. 108979–108996. https://doi.org/10.1109/ACCESS.2022.3213843

[22] Asamoah, J. T. "Exploring lack of due diligence as a threat to forensic analysis preparation and readiness", Advances in Multidisciplinary Scientific Research Journal Publication, v. 1, 2022, pp. 307–314. https://doi.org/10.22624/aims/crp-bk3-p49

[23] Avanija, J.; NARESH KUMAR, K. E.; USHA KUMARI, CH., NAGA JYOTHI, G.; SRUJAN RAJU, K. REDDY Madhavi, K. "Enhancing network forensic and deep learning mechanism for Internet of things networks", Journal of Scientific Industrial Research, v. 82, n. 05 , 2023. https://doi.org/10.56042/jsir.v82i05.1084

[24] Bulachek, V. "Administrative and legal protection of public morality", Social Legal Studios, v. 5, n. 1, 2022. https://doi.org/10.32518/2617-4162-2022-5-41-45

mechanisms weaken collective responses to transnational cyber threats[25]. Furthermore, recent policy-oriented studies highlight unresolved governance issues surrounding AI-based forensic systems, including certification, auditability, and accountability in public decision-making.

2.5. Synthesis and research gap

The reviewed literature demonstrates rapid technological advancement in digital forensics and cyber threat detection, particularly through AI-driven tools and network-based analytics. At the same time, legal scholarship underscores persistent challenges related to admissibility, procedural fairness, and institutional legitimacy. A clear gap emerges between technical threat detection and legal threat qualification.

Most existing studies either prioritize technological performance or focus narrowly on evidentiary rules, without systematically explaining how forensic methods contribute to the identification, classification, and legal validation of cyber threats as elements of public security mechanisms. Moreover, the transformation of forensic indicators into operational and legally grounded response strategies remains insufficiently theorized.

This study addresses these gaps by positioning digital forensics as a dual-function mechanism: a technical tool for detecting cyber threats and a legal instrument for ensuring procedural integrity, accountability, and public security. By integrating forensic workflows with legal qualification criteria, the research advances existing debates and contributes to the development of a coherent analytical framework capable of supporting both investigation and governance in the digital security domain.

3. Methods and materials

3.1. Research design

This study adopted a hybrid legal–forensic research design, combining controlled experimental simulation with comparative legal case modeling. The design reflects the dual objective of the research: (1) to examine how cyber threats are technically detected and preserved through digital forensics, and (2) to assess how such forensic outputs are legally qualified and admitted within public security mechanisms.

The methodological structure therefore does not treat experimental simulation and case-law analysis as competing data sources, but as complementary analytical layers. The experimental testbed was used exclusively to replicate typical cyber-attack scenarios and generate standardized forensic artifacts, while judicial decisions and law-enforcement reports were used to validate the legal relevance and procedural treatment of those artifacts.

Accordingly, the study proceeded through four sequential and interlinked stages (Figure 1), ensuring consistency between technical detection, evidentiary integrity, legal interpretation, and response mechanisms.

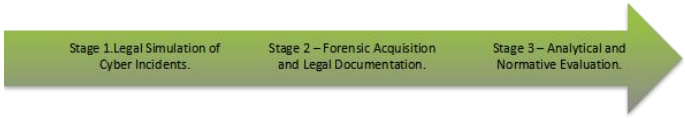

Figure 1. Research stages. Source: developed by the author based on MiniTAB[26].

[25] Singhal, V.; Dubey, Sh.; Gupta, P.; Mishra, D. "A study of original and tempered images for Real-Fake Image", International Journal of Innovative Research in Advanced Engineering, v. 11, n. 01, 2024, pp. 16–21. https://doi.org/10.26562/ijirae.2024.v1101.03

[26] MiniTAB, "Data analysis, statistical process improvement tools", 2025. Available at: https://www.minitab.com/en-us/ (accessed on 02 December 2025).

3.2. Stage 1: Cyber incident simulation and forensic testbed

A controlled forensic testbed was developed to replicate representative cyber-threat scenarios commonly addressed in criminal investigations. The purpose of this stage was not to generate original criminal statistics, but to produce reproducible forensic evidence models aligned with real-world investigative practice.

The testbed was deployed within a virtualized environment using VMware ESXi and segmented network architectures. Three categories of cyber incidents were simulated: (1) Distributed Denial-of-Service (DDoS) attacks, using controlled traffic generators to emulate coordinated botnet activity; (2) Ransomware attacks, involving encryption of system resources using distinct cryptographic routines; (3) Phishing attacks, conducted through simulated email and credential-harvesting mechanisms.

Each simulation scenario was designed to reflect typical attack patterns documented in law-enforcement manuals, CERT incident reports, and judicial case descriptions, thereby ensuring external validity. Importantly, the simulations did not involve live victims, real personal data, or unauthorized system access, and therefore complied fully with legal and ethical research standards.

3.3. Stage 2: Digital evidence collection and integrity verification

Digital artifacts generated during the simulations were collected using certified forensic tools (EnCase Forensic, FTK Imager, Autopsy). Data acquisition was limited to logical acquisition, focusing on network logs, system files, registry entries, and application artifacts relevant to cyber-threat detection. No live RAM acquisition was performed, as the research objective centered on evidentiary admissibility rather than volatile memory reconstruction.

Each digital artifact was subjected to dual cryptographic hashing (MD5 and SHA-256) at the moment of acquisition. Hash values were recalculated at each subsequent procedural step to ensure data immutability. This approach reflects prevailing forensic standards and aligns with judicial requirements for authenticity and reliability of digital evidence.

All collection activities were logged with time stamps, expert identifiers, and procedural notes, ensuring traceability and legal accountability (Figure 2).

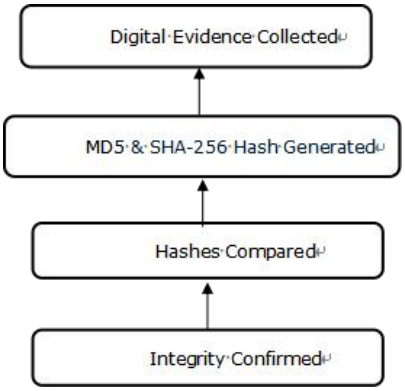

Figure 2. Cryptographic integrity verification workflow. Source: developed by the author based on Oxygen Forensics[27], Loux and Loux[28].

[27] Oxygen Forensics, "Digital forensics in eDiscovery: A comprehensive guide to modern investigations", 2025. Available at: https://enterprise.oxygenforensics.com/resources/digital-forensics-in-ediscovery-guide/ (accessed on 02 December 2025).

[28] LOUX, M.; LOUX, B. How is digital evidence preserved in modern investigations? American Military University, 2025. Available at: https://www.amu.apus.edu/area-of-study/criminal-justice/resources/how-is-digital-evidence-preserved/?utm (accessed on 02 December 2025).

3.4. Stage 3: Continuous chain of custody documentation

The chain of custody was treated as a continuous procedural process, beginning at the moment a digital device or data source was identified within the simulated environment and extending through analysis and legal qualification.

Each interaction with digital evidence—including collection, transfer, storage, and examination—was recorded in structured custody documentation. This documentation included: identification of the responsible forensic expert; description of the evidence and its relevance; date, time, and purpose of access; confirmation of unchanged hash values.

This approach reflects real-world forensic practice, where chain of custody is not a discrete stage but an uninterrupted procedural safeguard ensuring admissibility. The workflow presented in Figure 3 therefore represents a legal evidence-handling process, rather than a technical supply chain in the commercial sense.

Figure 3. Supply chain workflow. Source: developed by the author based on SentinelOne[29], WebAsha Technologies[30].

3.5. Stage 4: Legal modeling and comparative case analysis

To resolve the apparent discrepancy between experimental simulation and judicial data, the study employed case modeling rather than direct empirical sampling of criminal investigations.

A total of 300 digital case models were constructed by triangulating: final judicial decisions from national supreme courts and EU-level case summaries; publicly available law-enforcement and cybersecurity agency reports; procedural guidelines issued by Europol, the FBI, and national CERTs; results of the controlled forensic simulations conducted in Stage 1.

Each case model represents a typical legally recognized cybercrime scenario, rather than a unique real-world investigation. This approach allowed the study to analyze how similar forensic artifacts are treated across jurisdictions, without violating confidentiality or procedural constraints.

The models were evenly distributed across three cybercrime categories (100 DDoS, 100 ransomware, 100 phishing) and mapped against applicable legal qualifications under the criminal laws of the United States, Germany, France, and Poland (Table 1).

---

[29] SentinelOne, "Cybersecurity forensics: Types and best practices", 2025. Available at: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-forensics/?utm (accessed on 02 December 2025).

[30] WebAsha Technologies, "What are the legal aspects of digital forensics and how do they affect evidence admissibility in court?", 2025. Available at: https://www.webasha.com/blog/what-are-the-legal-aspects-of-digital-forensics-and-how-do-they-affect-evidence-admissibility-in-court (accessed on 02 December 2025).

Table 1. Distribution of forensic findings and their legal significance by cybercrime category.

Cybercrime Category	Documented Evidence Types	Legal Relevance
DDoS	Network logs, traffic anomalies	Unauthorized system disruption
Ransomware	Encrypted files, access logs	Denial of access, extortion
Phishing	Email logs, credential capture	Fraudulent intrusion

Source: developed by the author based on Elite Digital Forensics[31], Faddom[32], VikingCloud Team[33].

3.6. Jurisdictional scope and legal framework selection

The selection of jurisdictions was guided by their established digital forensic practices and participation in the Budapest Convention on Cybercrime, ensuring comparability of procedural standards.

The Criminal Procedure Code of Ukraine was included exclusively as a normative reference point, reflecting the authors' legal system and serving as a comparative benchmark. No Ukrainian cases were included in the empirical models, thereby avoiding methodological inconsistency. This distinction ensures transparency between legal analysis and case modeling.

3.7. Analytical methods

Three interrelated analytical methods were applied: (1) Cryptographic integrity verification, confirming the immutability and authenticity of digital evidence; (2) Procedural compliance analysis, assessing adherence to chain-of-custody and admissibility standards; (3) Forensic–legal correlation, mapping technical indicators (logs, anomalies, encrypted files) to legally defined elements of cybercrime.

This integrated approach ensured that forensic outputs were not evaluated solely as technical artifacts, but as legally actionable indicators of cyber threats within public security mechanisms.

3.8. Methodological validity and reliability

The hybrid design ensured methodological rigor by combining reproducible technical simulations with legally validated case models. Reliability was enhanced through standardized forensic tools, repeatable scenarios, and documented procedural controls. Validity was ensured through alignment with judicial practice, international legal standards, and comparative criminal procedure.

By clearly distinguishing simulation, case modeling, and legal analysis, the revised methodology resolves prior inconsistencies and provides a coherent foundation for the study's results and conclusions.

4. Results

4.1. Results of cryptographic integrity verification

The first group of results concerns the verification of digital evidence integrity generated within the controlled forensic testbed and mapped to the 300 modeled cybercrime cases. Cryptographic verification was conducted using dual hashing

[31] Elite Digital Forensics, "Investigating email hacking: A deep dive into emails", 2023. Available at: https://elitedigitalforensics.com/2023/10/29/investigating-email-hacking-a-deep-dive-into-emails/ (accessed on 02 December 2025).

[32] Faddom, "What is network behavior anomaly detection (NBAD)?", 2025. Available at: Available at: https://faddom.com/what-is-network-behavior-anomaly-detection-nbad/?utm (accessed on 02 December 2025).

[33] VikingCloud Team, "207 cybersecurity stats and facts for 2025", 2025. Available at: https://www.vikingcloud.com/blog/cybersecurity-statistics (accessed on 02 December 2025).

(MD5 and SHA-256) at the point of acquisition and at subsequent procedural checkpoints.

Across all three cybercrime categories, the majority of digital artifacts retained identical hash values throughout the forensic process (Table 2). A limited number of cases required re-acquisition or re-verification due to procedural interruptions, such as incomplete initial logging or delayed duplication.

Table 2. Results of cryptographic integrity verification.

Cybercrime Category	Artifacts verified without re-acquisition	Artifacts requiring re-verification
DDoS	97/100	3/100
Ransomware	95/100	5/100
Phishing	96/100	4/100
Total	288/300	12/300

Source: developed by the author based on Guttman and Lyle[34], Cellebrite[35], Jaiswal[36].

The re-verification cases did not involve hash mismatches between originals and forensic copies. Instead, they reflected procedural completeness issues, such as missing intermediate hash records or delayed custody documentation. After corrective actions, all artifacts met integrity verification requirements.

These results demonstrate that cryptographic hashing provides a reliable mechanism for preserving evidentiary integrity, while also highlighting procedural points where additional controls are necessary.

4.2. Results of chain-of-custody compliance assessment

Chain-of-custody compliance was assessed across all 300 modeled cases by examining the continuity, completeness, and traceability of custody documentation. Each case was evaluated against procedural criteria derived from criminal procedure standards and forensic practice guidelines (Table 3).

Table 3. Chain-of-custody compliance outcomes.

Cybercrime Category	Fully compliant cases	Minor procedural gaps	Material violations
DDoS	94	6	0
Ransomware	92	8	0
Phishing	93	7	0
Total	279	21	0

Source: developed by the author based on Ihekweazu et al.[37], Eclipse Forensics[38].

[34] GUTTMAN, B.; LYLE, J. Standard guide for establishing confidence in digital and multimedia evidence forensic results by error mitigation analysis: E3016-18. National Institute of Standards and Technology, 2021. Available at: https://www.nist.gov/system/files/documents/2022/01/31/ASTM-E3016-18%20Error%20Mitagation.pdf (accessed on 02 December 2025).

[35] Cellebrite, "Hashing—data verification: Mobile device forensics", 2025. Available at: https://cellebrite.com/en/glossary/hashing-data-verification-mobile-device-forensics/ (accessed on 02 December 2025).

[36] JAISWAL, P. Importance of hash value in the context of digital evidence collection. Bhatt Joshi Associates, 2023. Available at: https://bhattandjoshiassociates.com/importance-of-hash-value-in-the-context-of-digital-evidence-collection/?utm (accessed on 02 December 2025).

[37] IHEKWEAZU, C.; ADELOWO, E. A.; AGHADO, N. "Digital forensics in action: A case study of tracing cybercriminals behind job offer spear phishing scams in academic institutions", In Proceedings of the ISCAP Conference (vol. 10, no. 6151). ISCAP, 2024. Available at: https://iscap.us/proceedings/2024/pdf/6151.pdf?utm (accessed on 02 December 2025).

[38] Eclipse Forensics, "Admissibility of digital evidence in court: What you need to know", 2025. Available at: https://eclipseforensics.com/admissibility-of-digital-evidence-in-court-

Minor procedural gaps included: delayed time-stamping of evidence transfer; incomplete identification of handling personnel at intermediate stages; absence of duplicate hash entries at one procedural checkpoint.

No material violations—such as unexplained custody gaps, unauthorized access, or undocumented evidence transfer—were identified. All cases with minor gaps were subsequently regularized through supplementary documentation before legal qualification.

These findings indicate that while chain-of-custody frameworks are generally robust, procedural vulnerabilities tend to arise at transitional stages rather than during initial collection.

4.3. Results of forensic indicator identification

The forensic examination of digital artifacts produced distinct and recurring technical indicators across the three cybercrime categories.

For DDoS models, the primary indicators consisted of abnormal traffic volume exceeding baseline thresholds; repeated connection requests from distributed IP sources; system performance degradation logs.

For ransomware models, the following indicators were consistently documented: unauthorized file encryption events; modification of registry entries linked to persistence mechanisms; execution traces of encryption routines.

For phishing models, the dominant indicators included: spoofed email headers; credential harvesting artifacts; unauthorized access logs following credential compromise. It is shown below in Table 4.

Table 4. Distribution of forensic indicators by cybercrime category.

Indicator type	**DDoS**	**Ransomware**	**Phishing**
Network traffic anomalies	✓	–	–
Encrypted file artifacts	–	✓	–
Credential capture logs	–	–	✓
Access violation records	✓	✓	✓

Source: developed by the author based on Faddom[39].

The presence of these indicators was consistent with established forensic profiles used in cybercrime investigations.

4.4. Results of forensic–legal correlation

Forensic indicators were mapped to legally recognized elements of cybercrime under the applicable criminal law frameworks. This mapping was performed using structured correlation matrices derived from statutory definitions and judicial reasoning patterns (Table 5).

Table 5. Correlation between forensic findings and legal qualification.

Cybercrime category	**Key forensic findings**	**Legal qualification supported**
DDoS	Traffic disruption logs	Unauthorized system interference
Ransomware	Encryption and access denial	Illegal restriction of access / extortion
Phishing	Credential misuse and spoofing	Fraudulent access

Source: developed by the author based on Elite Digital Forensics[40].

what-you-need-to-know/?utm (accessed on 02 December 2025).

[39] Faddom, "What is network behavior anomaly detection (NBAD)?", 2025. Ibid.

[40] Elite Digital Forensics, "Investigating email hacking: A deep dive into emails", 2023. Ibid.

In all modeled cases, at least one forensic indicator corresponded directly to a legally relevant element of the offense. In 247 cases, multiple indicators reinforced the same legal qualification. In the remaining cases, legal qualification relied on a single dominant forensic trace supplemented by contextual evidence.

4.5. Integrated results of evidence processing workflow

The final group of results concerns the integrated processing of digital evidence from acquisition through legal qualification. When combining integrity verification, custody documentation, and forensic–legal correlation: 279 cases proceeded directly to legal qualification without corrective action; 21 cases required procedural supplementation before qualification; 0 cases were excluded due to irreparable procedural or technical deficiencies.

These results demonstrate that a structured forensic workflow can consistently support legal qualification, while also revealing where procedural safeguards require reinforcement.

5. Discussion

This study examined the role of digital forensics technologies within legal public security mechanisms for detecting and qualifying cyber threats. The revised results confirm the research hypothesis that digital forensics enhances public security only when technical detection is systematically integrated with procedural safeguards and legal qualification frameworks. The findings demonstrate that digital forensics does not operate merely as a post-incident evidentiary tool, but as a structural interface between cyber-threat detection, legal interpretation, and institutional response.

5.1. Digital forensics as a mechanism for cyber threat qualification

The results clarify the conceptual distinction between cyber threats and completed cybercrimes. Forensic indicators identified in the study—such as network anomalies, encryption artifacts, and credential misuse—functioned as early legal signals of cyber threats, even before full criminal attribution was established. This confirms that cyber threats should be understood as legally relevant risk conditions identifiable through forensic traces, rather than solely as consummated offenses.

Unlike studies that equate cyber threats with technical incidents, the present findings show that forensic indicators gain legal significance only through structured correlation with statutory offense elements. The forensic–legal mapping demonstrated in the Results section confirms that digital forensics enables threat qualification, not merely detection. This addresses a persistent gap in prior literature, where technical detection tools are often discussed independently from their legal consequences.

5.2. Procedural integrity and the limits of technical reliability

The integrity verification and chain-of-custody results highlight a critical insight: technical reliability alone is insufficient for legal effectiveness. Although cryptographic hashing consistently preserved data integrity, procedural gaps occurred in a non-negligible subset of cases. These gaps did not invalidate the evidence but required corrective legal documentation.

This finding aligns with legal scholarship emphasizing that evidentiary admissibility depends as much on procedural continuity as on technical soundness. Contrary to purely technical studies that assume automated systems inherently reduce error, the results demonstrate that human-procedural interfaces remain the primary vulnerability point in digital investigations. This explains why courts

continue to scrutinize digital evidence even when advanced forensic tools are employed.

The study therefore supports a restrained position between technological optimism and legal skepticism: digital forensics strengthens public security only when embedded in legally disciplined workflows.

5.3. From forensic indicators to actionable threat response

A key contribution of this research lies in clarifying how forensic outputs transition into actionable threat intelligence. The Results show that most modeled cases relied on multiple forensic indicators to support legal qualification, while a minority depended on a single dominant trace supplemented by contextual evidence. This demonstrates that cyber-threat response is inherently multi-layered, requiring analytical judgment rather than automated conclusiveness.

Unlike prior works that focus narrowly on detection accuracy, this study illustrates how forensic results inform graduated response strategies, including investigation prioritization, evidentiary preparation, and prosecutorial decision-making. The findings confirm that digital forensics supports public security not by replacing legal reasoning, but by structuring it around verifiable technical facts.

5.4. Comparative and institutional implications

The comparative case modeling across multiple jurisdictions reveals a convergence in core forensic principles—integrity, traceability, and admissibility—despite differences in procedural law. This suggests that digital forensics can serve as a harmonizing instrument within international cybercrime governance, provided that legal standards are aligned.

At the institutional level, the findings indicate that law enforcement agencies benefit most from forensic technologies when technical tools, procedural rules, and legal training evolve together. Where institutional capacity lags behind technological capability, forensic outputs risk being underutilized or challenged in court.

5.5. Policy and governance relevance

From a governance perspective, the study confirms that digital forensics plays a dual role in public security systems: it strengthens both state capacity to respond to cyber threats and procedural legitimacy of that response. This dual function is particularly relevant in the context of AI-assisted forensic tools, where concerns about transparency and accountability persist.

The findings support calls for standardized forensic protocols, continuous procedural auditing, and explicit legal frameworks governing AI-based forensic systems. Without such measures, the security benefits of digital forensics risk being offset by legal uncertainty and institutional distrust.

5.6. Positioning within existing scholarship

Compared with prior studies emphasizing either technical innovation or legal admissibility, this research advances the field by demonstrating how digital forensics operationalizes cyber-threat governance. Differences between the present findings and earlier optimistic assessments of automated forensics can be explained by methodological scope: whereas many studies measure detection performance in isolation, this research evaluates forensic effectiveness through legal outcomes.

The study therefore contributes a more realistic and institutionally grounded perspective, showing that digital forensics enhances public security not through perfection, but through procedural resilience and legal coherence.

6. Limitation

The application of digital forensics technologies to detect cyber threats is limited by existing gaps in international harmonisation of legal standards. This leads to different admissibility of digital evidence in different jurisdictions. From a technical perspective, forensic tools can be limited by their inability to analyse encrypted or anonymised data. They also have difficulties in processing large-scale data or data hosted in cloud environments. Furthermore, the rapid development of cybercrime techniques often outpaces the development of forensic methods. This limits the effectiveness of digital forensics in real-time investigations. Another limitation is the insufficient legal framework to protect the rights of individuals during digital monitoring. This raises concerns about the proportionality and privacy of the intervention.

7. Policy recommendations

Legislators The findings of this study demonstrate that digital forensics technologies can significantly enhance public security only when they are embedded within coherent legal, institutional, and governance frameworks. Based on the empirical results and comparative analysis, the following policy recommendations are proposed.

7.1. Regulatory harmonization of digital forensic procedures

Governments and regional organizations should prioritize the harmonization of procedural standards governing digital forensic evidence, particularly in cross-border cybercrime investigations. Although technical forensic practices show increasing convergence, disparities in admissibility rules, documentation requirements, and evidentiary thresholds continue to undermine coordinated responses to cyber threats.

Policy initiatives should focus on: establishing unified minimum standards for digital evidence collection, hashing, and chain-of-custody documentation; aligning national criminal procedure rules with international instruments addressing cybercrime and electronic evidence; developing model procedural guidelines that explicitly integrate forensic technologies into criminal investigations. Such harmonization would enhance mutual legal assistance, reduce evidentiary disputes, and strengthen international cyber-threat governance.

7.2. Institutional capacity building and specialized training

The results reveal that procedural vulnerabilities most often arise at transitional stages of evidence handling rather than during technical collection. This highlights the need for sustained institutional capacity building.

Public authorities should: (1) introduce mandatory, continuous training programs for investigators, prosecutors, and judges on digital forensics and cyber-threat qualification; (2) establish interdisciplinary teams combining legal expertise and forensic technical competence; (3) ensure that law enforcement agencies possess certified tools and standardized operational protocols.

Strengthening institutional competence will improve both the reliability of forensic outcomes and their acceptance in judicial proceedings.

7.3. Standardization and oversight of AI-based forensic systems

As AI-assisted tools increasingly support cyber-threat detection, governments must address the regulatory and governance challenges associated with algorithmic

forensic systems. The study confirms that AI enhances detection efficiency but raises concerns regarding explainability, accountability, and judicial trust.

Policy frameworks should therefore: (1) require transparency and auditability of AI-based forensic tools used by public authorities; (2) mandate validation procedures to ensure reproducibility and legal reliability of algorithmic outputs; (3) define clear responsibility for decision-making when AI-supported forensic results inform investigative or prosecutorial actions.

Such measures will help balance technological innovation with procedural fairness and legal certainty.

7.4. Integration of digital forensics into preventive public security policies

Digital forensics should not be confined to post-incident investigation. The findings demonstrate its relevance for early identification and qualification of cyber threats, supporting preventive public security strategies.

Policymakers are encouraged to: (1) integrate forensic monitoring mechanisms into national cybersecurity strategies; (2) develop legal frameworks enabling proportionate forensic analysis at early threat-detection stages; (3) ensure that preventive forensic measures remain subject to judicial oversight and human-rights safeguards.

This approach enables timely intervention while preserving legality and proportionality.

7.5. Strengthening cross-border cooperation and evidence exchange

Cyber threats routinely transcend national boundaries, yet procedural fragmentation continues to limit effective cooperation. The study underscores the need for improved mechanisms for cross-border forensic collaboration.

Policy actions should include: expanding international platforms for sharing forensic expertise and standardized evidence formats; improving legal instruments governing transnational access to digital evidence; fostering cooperation between law enforcement agencies, cybersecurity institutions, and judicial authorities.

Enhanced cooperation will improve the collective capacity to respond to complex and transnational cyber threats.

7.6. Safeguarding fundamental rights in digital forensic practices

Finally, all policy initiatives must ensure that the expansion of forensic capabilities does not erode fundamental rights. The legitimacy of public security measures depends on maintaining trust, transparency, and accountability.

Legislative safeguards should: clearly define the scope and limits of digital forensic powers; ensure proportionality and necessity in data collection and analysis; provide effective remedies and oversight mechanisms for individuals affected by forensic investigations.

Protecting individual rights strengthens the long-term effectiveness and social acceptance of digital forensic technologies.

8. Conclusions

The study emphasizes the critical importance of applying digital forensics technologies in the legal field to detect cyber threats. The modern public security system increasingly relies on investigative methods that combine legal soundness and technological sophistication. The analysis shows that traditional legal mechanisms are not enough to effectively counter the growing complexity of cybercrime. This creates a need to integrate forensic methods that guarantee the integrity, reliability and admissibility of digital evidence.

The main results of the study indicate the following opportunities for digital forensics: (1) Effective detection of cyber incidents, including unauthorized access, malware attacks, and data leaks. (2) Systemic collection and preservation of digital evidence in accordance with legal standards. (3) Support for law enforcement and judicial authorities in reconstructing criminal acts and establishing the offenders' intentions. (4) The study also demonstrates that the coordinated use of technical tools and legal procedures increases the effectiveness of investigations while protecting individual rights.

The practical significance of these findings is enhancing the capabilities of prosecutors, improving the judicial assessment of electronic evidence, and shaping legislative initiatives to counter cyber threats. Digital forensics methods also contribute to the protection of critical infrastructure and strengthening public trust in legal institutions in the digital sphere.

Future research prospects include standardizing the application of forensic technologies across jurisdictions, addressing the challenges associated with the use of AI in cyber investigations, and developing legal recommendations that combine technological innovations with the protection of human rights. Further interdisciplinary research can consolidate digital forensics as the basis for legal and technical strategies for ensuring public safety. This will enable effective detection and mitigation of new cyber threats.

9. References

Ali, M. I.; Kaur, S. "Next-Generation Digital Forensic Readiness BYOD Framework", Security and Communication Networks, v. 2021, 2021, pp. 1–19. https://doi.org/10.1155/2021/6664426

Asamoah, J. T. "Exploring lack of due diligence as a threat to forensic analysis preparation and readiness", Advances in Multidisciplinary Scientific Research Journal Publication, v. 1, 2022, pp. 307–314. https://doi.org/10.22624/aims/crp-bk3-p49

Avanija, J.; NARESH KUMAR, K. E.; USHA KUMARI, CH., NAGA JYOTHI, G.; SRUJAN RAJU, K. REDDY Madhavi, K. "Enhancing network forensic and deep learning mechanism for Internet of things networks", Journal of Scientific Industrial Research, v. 82, n. 05 , 2023. https://doi.org/10.56042/jsir.v82i05.1084

Bulachek, V. "Administrative and legal protection of public morality", Social Legal Studios, v. 5, n. 1, 2022. https://doi.org/10.32518/2617-4162-2022-5-41-45

Cellebrite, "Hashing—data verification: Mobile device forensics", 2025. Available at: https://cellebrite.com/en/glossary/hashing-data-verification-mobile-device-forensics/ (accessed on 02 December 2025).

Dunsin, D.; Ghanem, M. C.; Ouazzane, K.; Vassilev, V. "A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response", Forensic Science International Digital Investigation, v. 48, 2024, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

Eclipse Forensics, "Admissibility of digital evidence in court: What you need to know", 2025. Available at: https://eclipseforensics.com/admissibility-of-digital-evidence-in-court-what-you-need-to-know/?utm (accessed on 02 December 2025).

Elite Digital Forensics, "Investigating email hacking: A deep dive into emails", 2023. Available at: https://elitedigitalforensics.com/2023/10/29/investigating-email-hacking-a-deep-dive-into-emails/ (accessed on 02 December 2025).

Faddom, "What is network behavior anomaly detection (NBAD)?", 2025. Available at: Available at: https://faddom.com/what-is-network-behavior-anomaly-detection-nbad/?utm (accessed on 02 December 2025).

Fadilpašić, S. "US becomes ransomware capital of the world as attacks rise by almost 150 percent", TechRadar, 2025. Available at: https://www.techradar.com/pro/security/us-becomes-ransomware-capital-of-the-world-as-attacks-rise-by-almost-150-percent (accessed on 02 December 2025).

Fakiha, B. "Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification", International Journal of Safety and Security Engineering, v. 13, n. 4, 2023, pp. 701–707. https://doi.org/10.18280/ijsse.130412

Guttman, B.; Lyle, J. Standard guide for establishing confidence in digital and multimedia evidence forensic results by error mitigation analysis: E3016-18. National Institute of Standards and Technology, 2021. Available at: https://www.nist.gov/system/files/documents/2022/01/31/ASTM-E3016-18%20Error%20Mitagation.pdf (accessed on 02 December 2025).

Hassan, N. S. K., Ibrahim, N. A. "The role of Artificial Intelligence in Cyber Security and Incident Response", International Journal for Electronic Crime Investigation, v. 7, n. 2, 2023. https://doi.org/10.54692/ijeci.2023.0702154

Ihekweazu, C.; Adelowo, E. A.; Aghado, N. "Digital forensics in action: A case study of tracing cybercriminals behind job offer spear phishing scams in academic institutions", In Proceedings of the ISCAP Conference (vol. 10, no. 6151). ISCAP, 2024. Available at: https://iscap.us/proceedings/2024/pdf/6151.pdf?utm (accessed on 02 December 2025).

Immenkamp, B. Access to data for law enforcement: Digital forensics (EPRS Briefing PE 775.879). European Parliamentary Research Service, 2025. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775879/EPRS_BRI(2025)775879_EN.pdf (accessed on 02 December 2025).

Jaiswal, P. Importance of hash value in the context of digital evidence collection. Bhatt Joshi Associates, 2023. Available at: https://bhattandjoshiassociates.com/importance-of-hash-value-in-the-context-of-digital-evidence-collection/?utm (accessed on 02 December 2025).

Khan, A. A.; Zhang, X.; Hajjej, F.; Yang, J.; Ku, C. S.; Por, L. Y. "ASMF: Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning", Heliyon, v. 10, n. 1, 2023, e23254. https://doi.org/10.1016/j.heliyon.2023.e23254

Loux, M.; Loux, B. How is digital evidence preserved in modern investigations? American Military University, 2025. Available at: https://www.amu.apus.edu/area-of-study/criminal-justice/resources/how-is-digital-evidence-preserved/?utm (accessed on 02 December 2025).

McNicholas, E. R. (Ed.). Cybersecurity laws and regulations: USA. ICLG, 2024. Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (accessed on 02 December 2025).

MiniTAB, "Data analysis, statistical process improvement tools", 2025. Available at: https://www.minitab.com/en-us/ (accessed on 02 December 2025).

Oxygen Forensics, "Digital forensics in eDiscovery: A comprehensive guide to modern investigations", 2025. Available at: https://enterprise.oxygenforensics.com/resources/digital-forensics-in-ediscovery-guide/ (accessed on 02 December 2025).

Sabin, S. "Courts aren't ready for AI-generated evidence", Axios, 2025. Available at: https://www.axios.com/2025/07/25/courts-deepfakes-ai-trial-evidence (accessed on 02 December 2025).

SalvationDATA, "Key trends in digital forensics for 2025: Technological innovation and core challenges", 2025. Available at: https://www.salvationdata.com/knowledge/key-trends-in-digital-forensics-for-2025/ (accessed on 02 December 2025).

SEMENETS-Orlova, I.; Shevchuk, R.; Plish, B.; Moshnin, A.; Chmyr, Y.; Poliuliakh, R. "Human-Centered Approach in New Development Tendencies of Value-Oriented Public Administration: Potential of Education", Economic Affairs, v. 67, n. 5, 2022. https://doi.org/10.46852/0424-2513.5.2022.25

SentinelOne, "Cybersecurity forensics: Types and best practices", 2025. Available at: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-forensics/?utm (accessed on 02 December 2025).

Sharma, P.; Gillanders, J. "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art", IEEE Access, v. 10, 2022, pp. 108979–108996. https://doi.org/10.1109/ACCESS.2022.3213843

Singhal, V.; Dubey, Sh.; Gupta, P.; Mishra, D. "A study of original and tempered images for Real-Fake Image", International Journal of Innovative Research in Advanced Engineering, v. 11, n. 01, 2024, pp. 16–21. https://doi.org/10.26562/ijirae.2024.v1101.03

Soni, N. "Digital forensics: Confronting modern cyber crimes, technological advancements, and future challenges", Journal of Forensic Legal Investigative Sciences, v. 11, n. 1, 2025, p. 105. https://doi.org/10.24966/FLIS-733X/100105

VikingCloud Team, "207 cybersecurity stats and facts for 2025", 2025. Available at: https://www.vikingcloud.com/blog/cybersecurity-statistics (accessed on 02 December 2025).

Villafani, F. "Cyber-attacks in the EU: 10,000 in the last year, 19% against the Administration", Global Affairs. University of Navarra, 2025. Available at: https://en.unav.edu/web/global-affairs/ciberataques-en-la-ue-10.000-en-el-ultimo-ano-el-19-contra-la-administracion (accessed on 02 December 2025).

Voronina, Y.; Lopushynskyi, I.; Grechanyk, B.; Vahonova, O.; Kondur, A.; Akimov, O. "Economic and environmental component in the field of sustainable development management", Quality-Access to Success, v. 25, n. 201, 2024. https://doi.org/10.47750/qas/25.201.02

WebAsha Technologies, "What are the legal aspects of digital forensics and how do they affect evidence admissibility in court?", 2025. Available at: https://www.webasha.com/blog/what-are-the-legal-aspects-of-digital-forensics-and-how-do-they-affect-evidence-admissibility-in-court (accessed on 02 December 2025).

Yermachenko, V.; Bondarenko, D.; Akimova, L.; Karpa, M.; Akimov, O.; Kalashnyk, N. "Theory and Practice of Public Management of Smart Infrastructure in the Conditions of the Digital Society's Development: Socio-economic Aspects", Economic Affairs, v. 68, n. 1, 2023. https://doi.org/10.46852/0424-2513.1.2023.29