International Journal of Innovative Computer Science and IT Research

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

# AI-Driven Digital Forensics for Automated Cybercrime Investigation

**Prof. Ville Heikkinen**

Professor, Tampere University, Finland

**Abstract**

The rapid expansion of digital technologies, cloud services, mobile platforms, Internet-connected devices, and online communication has significantly increased the complexity and volume of evidence generated during cybercrime investigations. Conventional digital forensic processes frequently depend on manual acquisition, examination, correlation, and interpretation of large heterogeneous datasets, creating challenges related to investigation time, evidence prioritization, scalability, and analyst workload. Artificial intelligence (AI) provides opportunities to automate several forensic activities through machine learning, deep learning, natural language processing, anomaly detection, pattern recognition, and intelligent evidence correlation. This paper examines an AI-driven digital forensics framework designed to support automated cybercrime investigation across heterogeneous digital environments. The proposed framework integrates evidence acquisition, preprocessing, feature extraction, intelligent classification, behavioral analysis, forensic correlation, and automated reporting within a unified investigation workflow. The methodology emphasizes the preservation of evidence integrity while applying computational intelligence to identify suspicious files, communication patterns, system activities, user behaviors, and potentially relevant forensic artifacts.

A conceptual analysis is conducted using two structured tables to examine AI techniques, forensic functions, investigation benefits, and operational limitations. The analysis indicates that AI can reduce repetitive forensic workloads, accelerate evidence triage, identify hidden relationships among artifacts, and support prioritization of high-value evidence. However, challenges involving adversarial manipulation, explainability, dataset quality, privacy, chain of custody, false positives, model drift, and legal admissibility remain significant. The study proposes that AI should operate as an intelligent forensic assistance layer rather than an uncontrolled replacement for professional investigators. Human validation, transparent decision mechanisms, secure evidence handling, and auditable model operations are therefore essential. The proposed approach contributes to the development of scalable and intelligent digital forensic environments capable of supporting faster, more consistent, and evidence-centered cybercrime investigations.

***Keywords:*** Artificial Intelligence, Digital Forensics, Cybercrime Investigation, Machine Learning, Deep Learning, Evidence Analysis, Automated Investigation, Cybersecurity, Digital Evidence, Forensic Intelligence

## 1. Introduction

The increasing dependence on digital infrastructure has transformed the nature of criminal activity. Cybercriminals exploit computers, mobile devices, cloud platforms, social networks, communication applications, and Internet-connected systems to conduct unauthorized access, financial fraud, identity theft, data breaches, ransomware attacks, and other forms of cybercrime. Each incident can generate extensive quantities of digital evidence distributed across multiple devices, applications, networks, and storage environments. Consequently, investigators must examine heterogeneous datasets while maintaining evidence integrity and establishing reliable relationships between events, users, devices, and activities.

Traditional digital forensics generally follows systematic procedures involving evidence identification, acquisition, preservation, examination, analysis, and reporting. Although these procedures provide important safeguards for forensic reliability, many activities remain resource-intensive. Investigators may need to manually examine thousands or millions of files, logs, messages, metadata records, browser artifacts, system events, and network traces. The increasing volume of evidence can therefore create substantial investigation delays. Automated computational techniques are increasingly relevant because they can assist investigators in filtering large datasets and identifying potentially significant evidence.

Artificial intelligence provides capabilities for processing complex datasets and recognizing patterns that may be difficult to identify through conventional manual examination. Machine learning can classify artifacts, detect anomalies, recognize behavioral patterns, and prioritize suspicious events. Deep learning can process complex representations derived from images, text, network traffic, and system activity. Natural language processing can assist with the examination of communications and documents, while graph-based methods can reveal relationships between entities and events. These capabilities create opportunities for developing more intelligent forensic investigation environments.

AI-driven digital forensics also introduces important concerns. Digital evidence must be preserved in a manner that maintains integrity and supports legal scrutiny. An AI model may generate incorrect classifications, overlook relevant evidence, or produce results that investigators cannot easily explain. Attackers may additionally manipulate data to evade automated detection or intentionally generate misleading artifacts. Therefore, AI cannot be treated simply as an automated decision-maker. Its outputs must be evaluated within established forensic procedures and subjected to appropriate human validation.

This research examines the role of AI in automated cybercrime investigation and proposes an integrated conceptual framework connecting evidence acquisition, preprocessing, intelligent analysis, correlation, prioritization, and reporting. The study focuses on how computational intelligence can improve investigation efficiency while maintaining forensic reliability, transparency, and evidentiary accountability.

## 2. Objectives

### Primary Objective

The primary objective of this research is to develop a conceptual AI-driven digital forensic framework capable of automating major stages of cybercrime investigation while maintaining evidence integrity, analytical transparency, and investigator oversight. The framework seeks to improve evidence

processing, accelerate forensic triage, identify complex relationships among digital artifacts, and support consistent investigation outcomes across heterogeneous computing environments.

### 2.1 Automated Evidence Identification and Prioritization

The first objective is to improve the identification and prioritization of potentially relevant digital evidence. AI-based classification and anomaly detection can evaluate large collections of files, logs, communication records, metadata, and system artifacts to identify information associated with suspicious activities.

Automated prioritization can enable investigators to focus their attention on high-value evidence before examining less relevant datasets. This objective is particularly important when investigations involve large storage systems, multiple devices, or extensive network records.

### 2.2 Intelligent Cybercrime Pattern Recognition

The second objective is to examine how machine learning and computational intelligence can identify behavioral and technical patterns associated with cybercrime. AI systems can analyze sequences of system events, communication activities, authentication records, network behavior, and file operations to identify deviations from expected behavior.

Correlating these patterns across multiple evidence sources can assist investigators in reconstructing attack sequences and identifying relationships among users, devices, accounts, and suspicious activities.

### 2.3 Evidence-Centered Investigation Support

The third objective is to establish an investigation model in which AI assists forensic professionals without eliminating human judgment. AI-generated findings should remain traceable to underlying evidence and should be accompanied by interpretable reasoning, confidence indicators, and audit records.

This objective emphasizes the importance of combining automated analysis with expert validation, legal requirements, evidence preservation, and transparent reporting.

## 3. Review of Literature

### 3.1 Artificial Intelligence in Digital Forensic Analysis

Artificial intelligence has increasingly been investigated as a mechanism for improving digital forensic examination. Machine learning techniques can classify digital artifacts according to predefined or learned patterns, enabling automated evidence triage. Supervised learning can be applied when labeled forensic datasets are available, whereas unsupervised learning can identify previously unknown behavioral patterns. Deep learning further expands analytical capabilities by learning complex representations from large-scale datasets. These techniques can reduce repetitive examination activities and assist investigators in identifying evidence requiring detailed human analysis.

The application of AI to digital forensics extends beyond simple classification. Intelligent systems can support event correlation, anomaly detection, malware identification, document analysis, and behavioral profiling. When evidence is distributed across multiple sources, AI can identify relationships between otherwise disconnected artifacts. However, the effectiveness of these approaches

depends heavily on training-data quality, feature representation, model robustness, and appropriate forensic validation.

### 3.2 Machine Learning for Cybercrime Detection

Machine learning has become an important analytical approach in cybersecurity because of its ability to detect deviations from established behavioral patterns. In forensic environments, machine learning can evaluate authentication logs, network events, file-system activities, application records, and communication patterns. Classification algorithms can distinguish potentially malicious artifacts from ordinary system activities, while clustering approaches can group related evidence without requiring predefined categories.

Nevertheless, forensic machine learning presents distinctive challenges. Cybercrime environments are dynamic, and attackers continually modify their techniques. Models trained on historical data may therefore experience performance degradation when confronted with new attack strategies. In addition, imbalanced forensic datasets may cause models to favor common benign activities over rare but important malicious events. These limitations demonstrate the need for continuous validation and adaptive analytical mechanisms.

### 3.3 Explainable and Trustworthy AI for Forensic Investigation

Explainability is particularly important in digital forensics because investigators must often justify how evidence contributed to an investigative conclusion. A highly accurate model that provides no understandable reasoning may be difficult to integrate into professional forensic workflows. Explainable AI techniques can provide feature importance, decision explanations, confidence values, and evidence relationships that allow investigators to assess automated findings.

Trustworthy forensic AI also requires secure data handling, reproducibility, model validation, and auditability. An AI system should not modify original evidence or obscure the distinction between source evidence and analytical inference. Maintaining this separation allows investigators to preserve evidentiary integrity while benefiting from computational automation.

## 4. Methodology

### 4.1 Research Design and Framework Development

This study adopts a conceptual and analytical research design for developing an AI-driven digital forensic framework. The framework is organized around sequential forensic activities beginning with evidence acquisition and preservation and continuing through preprocessing, feature extraction, intelligent analysis, evidence correlation, prioritization, and reporting. Each stage is designed to maintain a clear distinction between original evidence and computationally generated findings. The methodology emphasizes scalable processing because modern cybercrime investigations may involve heterogeneous evidence from endpoints, mobile devices, cloud systems, networks, and application environments.

The proposed methodology integrates conventional forensic principles with AI-based analytical mechanisms. Evidence is first preserved through controlled acquisition and integrity verification. Relevant artifacts are then normalized into analyzable representations while retaining source metadata. Machine learning, anomaly detection, natural language processing, and graph-based analysis are subsequently applied to identify suspicious patterns and relationships. The final stage produces

investigator-oriented findings containing evidence references, analytical confidence, and traceable reasoning. Human investigators remain responsible for validating significant conclusions.

### 4.2 Evidence Acquisition and Preprocessing

The evidence acquisition stage focuses on collecting relevant digital artifacts without compromising their original state. Evidence may include disk images, memory captures, network records, system logs, browser artifacts, application databases, emails, documents, metadata, and mobile-device information. Cryptographic integrity mechanisms can be used to verify that acquired evidence remains consistent during subsequent processing. Each evidence object is assigned an identifier and associated metadata describing its source, acquisition context, and processing history.

Preprocessing transforms heterogeneous forensic artifacts into standardized analytical representations. Duplicate records can be identified, corrupted or incomplete records can be flagged, timestamps can be normalized, and metadata can be extracted for subsequent analysis. Textual evidence may be processed using natural language techniques, while network and system events can be converted into structured sequences. Importantly, preprocessing should create analytical copies rather than modifying original evidence. This approach supports reproducibility and preserves the distinction between evidence and computational transformation.

### 4.3 AI-Based Evidence Analysis

The AI analysis stage combines multiple computational techniques according to the characteristics of the evidence. Supervised learning can classify known artifact categories, while unsupervised learning can identify unusual patterns. Deep learning can support complex feature extraction, and natural language processing can examine large quantities of textual material. Graph-based analysis can additionally represent relationships between users, devices, accounts, files, addresses, and events.

**Key analytical functions include:**

- Automated evidence classification.
- Anomaly and outlier detection.
- Suspicious file identification.
- Behavioral sequence analysis.
- Communication and document analysis.
- Entity and relationship extraction.
- Cross-source evidence correlation.
- Evidence prioritization.

The outputs generated by these techniques are treated as analytical indicators rather than automatically established facts. Each result should maintain links to its supporting evidence, model version, processing stage, and confidence information. This enables investigators to reproduce or independently verify important findings.

### 4.4 Validation, Correlation, and Reporting

Validation involves examining AI-generated findings against original evidence and independent forensic indicators. A suspicious classification, for example, should be evaluated using file metadata, execution records, system logs, network activity, and other relevant evidence. Cross-source correlation is

particularly important because isolated anomalies may not represent actual criminal activity. Combining multiple evidence sources can improve investigative reliability and reduce the risk of interpreting individual artifacts incorrectly.

The reporting stage converts validated analytical findings into structured investigative information. Reports should distinguish original evidence, derived features, AI predictions, investigator interpretations, and confirmed conclusions. Model information, confidence levels, processing timestamps, and evidence identifiers should be retained where appropriate. Such reporting supports auditability and facilitates subsequent review. The methodology therefore treats AI as a forensic decision-support layer rather than an autonomous authority capable of independently determining criminal responsibility.

## 5. Analysis

### 5.1 AI Techniques and Forensic Functions

AI-driven digital forensics can employ different computational methods according to the characteristics of the evidence and the investigation objective. No single algorithm is suitable for every forensic task. Classification techniques are useful when predefined artifact categories exist, whereas anomaly detection is valuable for identifying unusual behavior. Natural language processing is suitable for textual evidence, while graph-based approaches can reveal relationships between entities and events.

**Table 1: AI Techniques and Their Applications in Digital Forensic Investigation**

| AI Technique | Forensic Application | Primary Benefit | Major Limitation |
|---|---|---|---|
| Supervised Machine Learning | Artifact and malware classification | Rapid categorization | Requires quality labeled data |
| Unsupervised Learning | Unknown anomaly discovery | Detects previously unseen patterns | Difficult interpretation |
| Deep Learning | Complex behavioral and multimedia analysis | High representation capability | Computationally intensive |
| Natural Language Processing | Email, message, and document analysis | Processes large textual datasets | Contextual ambiguity |
| Graph Neural Networks | Relationship and event analysis | Reveals complex connections | Model complexity |
| Anomaly Detection | Suspicious system/network behavior | Identifies deviations | False-positive risk |

**Interpretation:** Table 1 demonstrates that AI provides complementary capabilities across digital forensic tasks. Supervised learning can accelerate routine classification, while unsupervised approaches can assist in discovering unfamiliar behaviors.

NLP can reduce the workload associated with textual evidence examination, and graph-oriented methods can support relationship analysis. However, each method introduces limitations involving data

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

requirements, computational complexity, interpretability, or false positives. Consequently, effective forensic systems should use multiple techniques within a controlled workflow rather than relying on one AI method.

### 5.2 Automated Investigation Workflow

An automated forensic workflow can significantly reduce the time required to process large evidence collections. After acquisition and integrity verification, AI can perform initial evidence filtering and prioritize artifacts based on predefined investigation criteria.

**Table 2: Stages of AI-Driven Automated Cybercrime Investigation**

| Investigation Stage | AI Capability | Expected Outcome | Human Oversight |
|---|---|---|---|
| Evidence Acquisition | Metadata extraction and integrity support | Organized evidence inventory | High |
| Preprocessing | Data normalization and duplicate detection | Clean analytical dataset | Moderate |
| Evidence Triage | Classification and ranking | Prioritized evidence | High |
| Behavioral Analysis | Anomaly and sequence detection | Suspicious activity identification | High |
| Correlation | Entity and event relationship analysis | Reconstructed activity patterns | High |
| Interpretation | Explainable AI and confidence analysis | Investigator-oriented findings | Very High |
| Reporting | Automated report generation | Structured forensic documentation | Very High |

**Interpretation:** Table 2 indicates that automation can be integrated throughout the forensic investigation lifecycle, but the required degree of human oversight varies by stage. Computational automation is particularly suitable for repetitive activities such as preprocessing, classification, ranking, and pattern discovery.

Conversely, interpretation and reporting require stronger human involvement because investigative conclusions may have legal and procedural consequences. The workflow therefore supports a hybrid model in which AI provides computational scale while forensic professionals retain responsibility for evidentiary interpretation and final conclusions.

### 5.3 Performance and Reliability Considerations

The effectiveness of an AI-driven forensic system should not be evaluated exclusively through classification accuracy. Important evaluation dimensions include precision, recall, false-positive rate,

false-negative rate, processing time, scalability, explainability, reproducibility, and evidence traceability. A model with high overall accuracy may still perform poorly when identifying rare cybercrime events. Therefore, forensic evaluation should emphasize the consequences of missed evidence as well as incorrect alerts.

Reliability also depends on the stability of the analytical pipeline. Changes in operating systems, applications, file formats, communication platforms, and attacker behavior can alter the distribution of forensic data. Continuous validation is therefore necessary to detect model degradation. Version-controlled models, documented preprocessing procedures, controlled testing datasets, and audit logs can improve reproducibility and provide investigators with greater confidence in AI-assisted findings.

## 6. Discussion

### 6.1 Contribution of AI to Automated Forensics

AI can transform digital forensics from predominantly manual evidence examination toward intelligent evidence prioritization and computationally assisted investigation. Large evidence collections can be screened rapidly, enabling investigators to focus their attention on artifacts with greater investigative relevance. Pattern-recognition mechanisms can additionally identify relationships that may be difficult to discover through isolated manual examination.

The major contribution of AI is therefore not simply faster processing but improved analytical capacity. By combining multiple evidence sources, intelligent systems can provide a broader representation of cybercrime activity. However, these advantages are meaningful only when AI outputs remain traceable to underlying evidence and are evaluated by qualified investigators.

### 6.2 Human-AI Collaboration in Cybercrime Investigation

A hybrid investigative model provides a practical balance between computational automation and professional judgment. AI can conduct repetitive screening, identify anomalies, rank evidence, and suggest relationships. Investigators can then evaluate whether these findings are consistent with the broader investigative context. This approach reduces workload while avoiding excessive dependence on automated predictions.

Human oversight is particularly important for ambiguous evidence. A communication pattern, unusual login, or file anomaly may have legitimate explanations. Investigators therefore need contextual information that automated models may not possess. Human-AI collaboration allows computational findings to be interpreted alongside investigative knowledge and procedural requirements.

### 6.3 Trust, Explainability, and Evidentiary Reliability

Forensic AI systems must provide sufficient transparency to allow investigators to understand why an artifact was prioritized or classified as suspicious. Explainable outputs can improve confidence and enable experts to identify incorrect model behavior. Evidence references and analytical reasoning should be retained so that significant findings can be independently examined.

Trust also requires strict separation between original evidence and AI-generated interpretations. AI should analyze verified copies and preserve a complete record of transformations. This architecture strengthens forensic accountability and supports repeatable investigations. Accordingly, explainability, integrity, and auditability should be treated as core design requirements rather than optional features.

## 7. Challenges

The first major challenge is the quality and diversity of forensic data. Digital evidence originates from numerous platforms and may contain incomplete records, inconsistent timestamps, proprietary formats, encrypted information, or irrelevant data. Machine learning models depend on representative datasets, yet realistic cybercrime datasets can be difficult to obtain because of privacy, security, and legal restrictions. Poorly represented training data can cause inaccurate classifications and increase both false-positive and false-negative outcomes.

A second challenge concerns adversarial manipulation. Cybercriminals may deliberately modify files, alter timestamps, encrypt communications, generate misleading activity, or exploit weaknesses in AI models to avoid detection. Adversarial machine learning can further threaten systems that rely heavily on automated classification. Robust models therefore require continuous testing against evolving attack strategies, unusual inputs, and manipulated evidence.

The third challenge involves legal, ethical, and operational accountability. Digital forensic evidence may influence criminal investigations and judicial proceedings, making transparency and reproducibility essential. Automated conclusions must not be treated as unquestionable facts. Privacy protection, controlled access, secure model deployment, chain-of-custody requirements, and investigator validation must remain integral components of AI-enabled forensic systems.

## 8. Future Research

Future research should investigate adaptive forensic AI models capable of responding to emerging cybercrime behaviors without requiring complete retraining after every environmental change. Continual learning, federated learning, and privacy-preserving analytical approaches may allow forensic systems to benefit from distributed knowledge while limiting unnecessary exposure of sensitive evidence. Research should also explore standardized benchmark datasets that represent diverse operating systems, devices, applications, and cybercrime scenarios.

Another important research direction is explainable forensic intelligence. Future systems should provide investigators with understandable explanations for classifications, anomaly scores, evidence rankings, and relationship predictions. Explainability mechanisms should be designed specifically for forensic workflows rather than simply transferred from general AI applications. Evidence-linked explanations could allow investigators to move directly from an AI-generated conclusion to the supporting artifacts.

Future studies should also evaluate AI-driven forensic frameworks in realistic multi-stage cybercrime scenarios. Research can examine how models perform when evidence is distributed across endpoints, cloud environments, mobile devices, and networks. Evaluation should include accuracy, processing efficiency, robustness, interpretability, reproducibility, and legal usability. Human-in-the-loop experiments can additionally determine how investigators interact with AI recommendations and whether automation genuinely improves decision quality.

## 9. Conclusion

AI-driven digital forensics represents an important advancement in the automation and scalability of cybercrime investigation. The growing quantity and diversity of digital evidence make purely manual examination increasingly difficult, particularly when investigations involve multiple devices, cloud

services, communication platforms, and extensive system records. Artificial intelligence can address several of these challenges by supporting automated evidence classification, anomaly detection, behavioral analysis, natural language processing, relationship discovery, and evidence prioritization. The conceptual framework presented in this study integrates these capabilities into a structured forensic workflow beginning with evidence acquisition and preservation and continuing through preprocessing, intelligent analysis, correlation, validation, and reporting. Such integration can reduce repetitive analytical workloads and allow investigators to concentrate on evidence with greater investigative relevance.

Despite these advantages, AI should not be considered a complete substitute for forensic expertise. Machine learning models can produce false positives, overlook relevant evidence, perform poorly on unfamiliar datasets, or become vulnerable to adversarial manipulation. The quality of AI-generated results also depends on data representation, preprocessing procedures, model selection, and continuous validation. More importantly, digital forensic investigations involve evidentiary and legal requirements that cannot be satisfied through predictive accuracy alone. Evidence integrity, chain of custody, explainability, auditability, privacy protection, and reproducibility must therefore remain central to system design. The proposed framework consequently adopts a human-centered model in which AI provides computational intelligence while trained investigators retain responsibility for interpretation and final conclusions.

Future development of AI-driven digital forensics should focus on trustworthy, adaptive, explainable, and evidence-centered intelligence. Continual learning, graph-based reasoning, multimodal analysis, privacy-preserving computation, adversarial robustness, and automated evidence correlation can further expand forensic capabilities. At the same time, standardized evaluation frameworks and realistic benchmark datasets are required to determine whether proposed systems perform reliably across different cybercrime environments. A carefully governed combination of artificial intelligence and forensic expertise can create investigation environments that are faster, more scalable, and analytically powerful without compromising evidentiary accountability. The long-term value of AI in digital forensics will therefore depend not only on technological sophistication but also on the ability to integrate intelligent automation with established forensic principles, professional judgment, and transparent investigative procedures.

## References

1. Abulaish, M., & Haldar, N. A. H. (2020). Advances in digital forensics frameworks and tools: A comparative insight and ranking. In *Digital forensics and forensic investigations* (pp. 374–401). IGI Global. https://doi.org/10.4018/978-1-7998-3025-2.ch027
2. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.
3. Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation, 48*, 301675. https://doi.org/10.1016/j.fsidi.2023.301675

4. Fähndrich, J., Honekamp, W., Povalej, R., Rittelmeier, H., Berner, S., & Labudde, D. (2023). Digital forensics and strong AI: A structured literature review. *Forensic Science International: Digital Investigation, 46*, 301617. https://doi.org/10.1016/j.fsidi.2023.301617
5. Garach, J., Singh, S. K., R. N., R., Reddy, A. P. C., & Khan, H. (2024). A comprehensive review on artificial intelligence in digital forensics with taxonomies, issues, and solutions: AI in digital forensics. In P. Goel (Ed.), *Strategies for e-commerce data security: Cloud, blockchain, AI, and machine learning* (pp. 1–28). IGI Global. https://doi.org/10.4018/979-8-3693-6557-1.ch001
6. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*, S64–S73. https://doi.org/10.1016/j.diin.2010.05.009
7. Garfinkel, S. L. (2013). Digital media triage with bulk data analysis. *Computers & Security, 32*, 56–72.
8. Jarrett, A., & Choo, K.-K. R. (2021). The impact of automation and artificial intelligence on digital forensics. *WIREs Forensic Science, 3*(6), e1418. https://doi.org/10.1002/wfs2.1418
9. Mar-Raave, J. R. D., Bahşi, H., Mršić, L., & Hausknecht, K. (2021). A machine learning-based forensic tool for image classification—A design science approach. *Forensic Science International: Digital Investigation, 38*, 301265. https://doi.org/10.1016/j.fsidi.2021.301265
10. Ngejane, C. H., Eloff, J. H. P., Sefara, T. J., & others. (2021). Digital forensics supported by machine learning for the detection of online sexual predatory chats. *Forensic Science International: Digital Investigation, 36*, 301109. https://doi.org/10.1016/j.fsidi.2021.301109
11. Nordvik, R., Stoykova, R., Franke, K., Axelsson, S., & Toolan, F. (2021). Reliability validation for file system interpretation. *Forensic Science International: Digital Investigation, 37*, 301174. https://doi.org/10.1016/j.fsidi.2021.301174
12. Scanlon, M., Breitinger, F., Hargreaves, C., Hilgert, J.-N., & Sheppard, J. (2023). ChatGPT for digital forensic investigation: The good, the bad, and the unknown. *Forensic Science International: Digital Investigation, 46*, 301609. https://doi.org/10.1016/j.fsidi.2023.301609
13. Serhal, C., & Le-Khac, N.-A. (2021). Machine learning based approach to analyze file metadata for smart phone file triage. *Forensic Science International: Digital Investigation, 37*, 301194. https://doi.org/10.1016/j.fsidi.2021.301194
14. Sikos, L. F. (2020). AI in digital forensics: Ontology engineering for cybercrime investigations. *WIREs Forensic Science, 3*(2), e1394. https://doi.org/10.1002/wfs2.1394
15. Silva, I., do Valle, J. M., Souza, G., Budke, J., Araújo, D., Carvalho, B., Cacho, N., Sales, H., Lopes, F., & Silva Júnior, R. (2021). Using micro-services and artificial intelligence to analyze images in criminal evidences. *Forensic Science International: Digital Investigation, 37*, 301197. https://doi.org/10.1016/j.fsidi.2021.301197
16. Solanke, A. A., & Biasiotti, M. A. (2022). Digital Forensics AI: Evaluating, standardizing and optimizing digital evidence mining techniques. *KI—Künstliche Intelligenz, 36*, 143–161. https://doi.org/10.1007/s13218-022-00763-9
17. Baryamureeba, V., & Tushabe, F. (2004). The enhanced digital investigation process model. In *Proceedings of the 2004 Digital Forensics Research Workshop*. Digital Forensics Research Workshop.

Volume 01, Issue 04 – Jul-Aug 2025 • E-ISSN: 3067-1108 | P-ISSN: 3067-1094

18. Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objective-based framework for the digital investigations process. *Digital Investigation, 2*(2), 147–167. https://doi.org/10.1016/j.diin.2005.04.002
19. Roussev, V. (2016). Digital forensic science: Issues and challenges. *Digital Investigation, 18,* 1–2. https://doi.org/10.1016/j.diin.2016.07.001
20. Quick, D., Choo, K.-K. R., & others. (2014). Digital forensic investigation of cloud computing environments. *Digital Investigation, 11*(2), 81–95.