Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Artificial Intelligence in Digital Forensics: A Review of Cyber-Attack Detection Models and Frameworks

Ms.Soni R.Ragho[1], Dr. Narendra Chaudhari[2]
Research Scholar, Mansarovar Global University, Bhopal (M.P), India[1]
Professor, Mansarovar Global University, Bhopal (M.P), India[2]

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

In the rapidly evolving landscape of cyber threats, traditional digital forensic methods often fall short in addressing the scale, speed, and complexity of modern attacks. This review explores the integration of Artificial Intelligence (AI) into digital forensics as a transformative approach for proactive cyber-attack detection and investigation. Drawing on over 30 peer-reviewed publications from 2016 to 2024, the study categorizes AI techniques into machine learning, symbolic AI, and hybrid systems, evaluating their applications in anomaly detection, forensic triage, behavioral profiling, and multimedia analysis. Comparative analysis highlights the strengths of AI—including automation, scalability, and predictive modeling—while also addressing key challenges such as explainability, adversarial robustness, and ethical concerns. Emphasis is placed on the need for explainable AI (XAI) frameworks, real-world validation, and legally admissible evidence generation. The review also examines notable AI-powered frameworks like D4I, Fronesis, and AIFIS, assessing their technical and legal efficacy. Finally, the paper outlines critical research gaps and future directions, including the development of open benchmarks, adversarially resilient models, and privacy-preserving forensic architectures. This synthesis aims to guide researchers and practitioners toward developing trustworthy, scalable, and legally sound AI-based digital forensic solutions.

Keywords: Artificial Intelligence, Digital Forensics, Cybersecurity, Intrusion Detection, Machine Learning, Threat Intelligence, Cyber-Attacks.

INTRODUCTION

Nowadays, with so many cyber-attacks, information systems, infrastructures and data worldwide are in major danger. These more advanced cyber-attacks are using new methods, so the existing, often slow, manual methods of digital forensics are not able to keep pace. Artificial Intelligence (AI), when introduced into digital forensics, has transformed the field by improving efficiency, precision and predictive strength when tackling cyber threats [1]. Digital forensics is a main area in cybersecurity that involves collecting, storing, examining and representing digital evidence. It is true, though, that traditional forensic approaches find it hard to handle massive and quick changes in data, meaning it falls to human analysts to analyze the logs and related artifacts once the incident has passed. Since AI can discover patterns and spot abnormalities, it allows these processes to be done automatically, hence making then faster and more accurate [2]. Using machine learning, it is possible to catch slight changes in the network that could show a breach is underway, allowing for prompt action [3].

New tools like Forensics have appeared to help detect cyber-attacks early, by combining digital forensic methods with advanced AI algorithms that do not rely solely on old intrusion detection measures [4]. Using AI, the D4I framework helps with forensics by giving flexible components that do tasks like reconstructing events and finding links between them [5]. They reveal that AI increases the capacity of digital forensics by reviewing more cases and working faster.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Thanks to advanced machine learning, AI systems like Cyberian study data from honeypots to help avoid attacks and get information systems ready for forensic investigation [6]. During forensic investigations, both capsule networks and deep learning architectures are used to find out if an image or code has been manipulated [7].

Since every piece of evidence matters in digital forensics, making sure AI systems are reliable and easy to explain is very important. As suggested by Puchalski et al., interpretability and being able to audit these models is necessary to validate that the evidence can be admitted and used in court [8].

Despite these advances, several challenges remain, including the scarcity of labeled forensic datasets, the threat of adversarial attacks on AI models, and the legal complexities surrounding AI-generated evidence. Nonetheless, ongoing research continues to explore AI applications in areas such as insider threat detection, automated threat classification, and behavior profiling [9][10].

Digital Forensics: Foundations and Developments

Digital forensics has become an indispensable discipline in the cybersecurity landscape, encompassing the recovery, investigation, and presentation of digital evidence derived from computing systems, mobile devices, cloud environments, and networks. Its primary goal is to ensure the integrity, admissibility, and reliability of data in both civil and criminal investigations. As cyber threats escalate in frequency and complexity, digital forensics has evolved from a reactive tool into a proactive and preventive science [11].

According to Anghel [11], digital forensics consists of the sequence's identification, preservation, analysis, documentation and presentation, so that evidence is unchanged and easy to verify. The process has great value to law enforcement; national security teams and response teams working to rebuild cyber crimes and find those responsible.

According to Kaur et al. [12], there are more tools available today for capturing data on disks, from mobile devices, in memory and from analyzing logs. Examples of these tools include Autopsy, Sleuth Kit which are open source and the commercial EnCase and FTK. Even though they are helpful, the authors point out that knowing what a tool cannot do, what systems work with it and if it meets legal standards is important when selecting them.

People are investigating the role of AI to help strengthen digital forensic operations. Ganesh [13] emphasizes that machine learning can help examine evidence quickly, locate unusual things in databases and automate routine tasks, making investigative processes more efficient and scalable. As AI's pattern recognition and predictive analysis become better, using it alongside forensic tools is more standardized.

Getting and managing evidence correctly in digital forensics is still a big problem because of both technological and legal standards. In their study, Kasper and Laurits [14] discuss how old laws often clash with the modern types of evidence found on computers. They emphasize making sure that forensic actions are legal and fit the requirements of data protection laws in different countries, especially when data is held in multiple countries using the cloud.

Reviewing and confirming capabilities of forensic tools is still a significant step in being forensically ready. Lovanshi and Bansal [15] compare different forensic tools, judging them on how easy they are to use, how accurate they are and how many kinds of file systems they work with. According to their conclusions, every approach may be suitable for some situations but not all and some tools work better in specific cases. Singh and Kumar [16] as well suggest a way to qualitatively judge the trustworthiness and dependability of forensic software used in real-life cases. It shows that deciding on the right tool calls for looking at the system environment, file arrangement and type of emergency.

REVIEW METHODOLOGY

To ensure a comprehensive and systematic understanding of current research on AI-based cyber-attack detection in digital forensics, this review followed a structured methodology grounded in established literature review principles. The process was divided into three key phases: literature identification, screening and eligibility, and thematic synthesis.

Literature Identification

Relevant literature was sourced from academic databases including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Taylor & Francis Online, and Google Scholar. Keywords such as "digital forensics," "AI

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

in cybersecurity," "cyber-attack detection," "machine learning for forensics," and "intrusion detection systems" were used in various combinations. The search targeted peer-reviewed journal articles, conference proceedings, technical reports, theses, and authoritative books published between 2016 to 2024 to capture recent advancements while maintaining historical context.

Inclusion and Exclusion Criteria

Inclusion criteria:

Papers explicitly focusing on AI or ML techniques applied to digital forensic tasks or cyber-attack detection.

Studies presenting frameworks, methodologies, or tools for forensic analysis enhanced by intelligent systems.

Publications in English, with accessible full-texts and valid metadata (e.g., DOI, volume, issue).

Exclusion criteria:

Studies solely focused on cryptography or non-AI-based traditional forensic techniques.

Duplicates, non-peer-reviewed web articles, and publications with insufficient technical depth.

DATA EXTRACTION AND SYNTHESIS

For each selected publication, metadata such as publication year, research domain (e.g., anomaly detection, network forensics, forensic frameworks), AI technique used (e.g., deep learning, CBR, clustering), and application context (e.g., malware, IoT, cloud) were recorded.

AI TECHNIQUES IN CYBER-ATTACK DETECTION

The combination of artificial intelligence (AI) and digital forensics has greatly improved how cyber-attacks are identified and probed. While traditional forensic methods usually look back and rely on people to do manual work, advanced systems now assist by detecting threats in real time, assessing situations and predicting future events.

The advance from classical digital forensics to intelligent forensics highlights that systems are needed to collect evidence, save it and also analyze, understand and link it automatically. Irons and Lallie [17] suggest using intelligent forensics which employs AI tools to make decisions in forensics by automating and using expert knowledge. As a result of this, complex threat patterns are easier to detect and fewer mistakes are made by analysts in busy environments.

The field of AI in forensic science relies mainly on machine learning (ML). As Qadir and Varol state [18], both supervised and unsupervised machine learning algorithms, among which are SVMs, decision tree, k-means clustering and neural networks, are effective in finding anomalies and inappropriate behaviors. The methods are best at spotting polymorphic malware, phishing attempts and attempts to break into systems, where other methods tend to fail.

Both symbolic and subsymbolic AI can be combined to handle reasoning by rule and abstract thinking. Costantini et al. [19] investigate such frameworks, so that intelligent agents can recognize context, conclude what the attacker aims to do and match data from various network and system sources. Such models greatly aid in deciding the primary people or nations behind a threat and in grouping incidents together.

Since IOT and edge devices are now frequently attacked, it is very important to use AI that does not require many resources. Dunsin and his colleagues [20] explain that it is important to create models that can function well in situations where there is limited access to bandwidth or computing power. As a result, people can quickly find out about issues on their systems, avoiding evidence being deleted or data being taken by attackers.

Automation plays a big role in how AI helps with digital forensics. According to Mitchell [21], AI technology allows data to be triaged fast, threats to be sorted and a detailed timeline to be assembled. But when it comes to forensic science, the difficulty of understanding these models can be a problem due to the emphasis on proving evidence and it being accepted in court. Jarrett and Choo [23] stress that explainable AI (XAI) techniques should be used to ensure the transparency of model results and reports in forensic sciences.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The application of AI in forensic investigations must also address ethical and legal dimensions. Mohsin [22] emphasizes the importance of algorithmic accountability, particularly in cases where AI findings contribute to legal outcomes. Ensuring compliance with forensic standards such as ISO/IEC 27037 and safeguarding against bias and error are critical to maintaining trust in AI-assisted investigations.

Table 1: Comparative Analysis of AI Techniques in Cyber-Attack Detection for Digital Forensics

AI Technique	Core Approach	Strengths	Limitations	Forensic Applications	Ref
Machine Learning (ML)	Data-driven statistical models (e.g., SVM, decision trees, neural networks)	- High detection accuracy- Scalable to large datasets- Fast classification	- Requires large labeled data- Limited interpretability- Vulnerable to adversarial input	- Malware detection- Intrusion detection- Log analysis	Qadir & Varol [18], Mitchell [21]
Symbolic AI	Rule-based reasoning, expert systems, logic programming	- Transparent logic paths- Easier to audit in legal contexts- Effective for known rule sets	- Poor adaptability to new threats- Cannot handle unstructured data- Slower in large-scale scenarios	- Policy violation detection- Static rule enforcement	Irons & Lallie [17], Costantini et al. [19]
Hybrid Models	Combines ML and symbolic reasoning (e.g., neuro-symbolic systems, case-based reasoning)	- Context-aware inference- Balances accuracy and explainability- Suitable for complex scenarios	- Computationally intensive- Integration complexity- Less standardized	- Threat attribution- Multi-source log correlation- Intelligent triage	Al-Mousa, Costantini et al. [19]

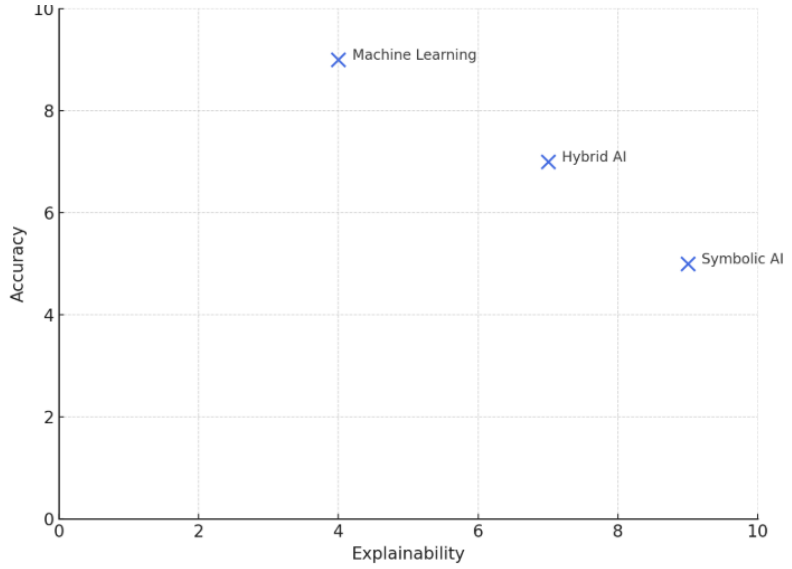

Figure 1. Accuracy vs Explainability of AI Techniques in Cyber Attack detection

DIGITAL FORENSIC FRAMEWORKS POWERED BY AI

The integration of artificial intelligence (AI) into digital forensic systems has fundamentally transformed how cyber-attacks are investigated. AI enables automation, intelligent inference, and real-time decision-making—enhancing traditional forensic methodologies that are often manual, reactive, and constrained by data volume and complexity.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Solanke [24] highlights a growing concern around the interpretability of AI systems in forensic investigations. He advocates for explainable AI (XAI) to bridge the trust gap between automated decisions and human experts, particularly in legally sensitive environments where decisions must be transparent and defensible. The paper emphasizes models like LIME (Local Interpretable Model-Agnostic Explanations) and SHAP for dissecting black-box outputs, underscoring their necessity in court-admissible digital evidence.

Building on this, Hall et al. [25] explore use cases for XAI in digital forensics, identifying model accountability as a cornerstone for forensic reliability. Their analysis indicates that integrating interpretable algorithms such as decision trees and rule-based classifiers enhances not only transparency but also user trust, especially among non-technical stakeholders like legal practitioners and investigators.

Earlier frameworks, such as that by Hoelz et al. [26], implemented expert systems and case-based reasoning for forensic triage, offering rule-based knowledge inference tailored to digital crime investigation. While foundational, their approach lacked the scalability and learning capacity of modern deep learning systems.

Rughani [27] proposed an intelligent-agent-based framework wherein AI modules perform modular tasks such as log analysis, evidence correlation, and anomaly detection. Although theoretically comprehensive, the absence of public benchmarks and quantitative validation hinders its adoption and reproducibility.

Zhang et al. [28] focused on the forensic challenges of video evidence tampering. They introduced a CNN-based model to detect missing frames in surveillance videos, leveraging temporal sequence modeling and frame transition consistency. Their model achieved over 94% detection accuracy, demonstrating the power of AI in multimedia forensics. However, it was tested on synthetic datasets, raising concerns about real-world robustness.

Maratsi et al. [29] examined ethical and legal compliance in AI-enhanced forensic systems. They warned against algorithmic bias and data privacy violations, advocating for embedded governance protocols in forensic tools to ensure chain-of-custody integrity and GDPR compliance.

A notable contribution to event reconstruction is by Ogundiran et al. [30], who proposed a goal-oriented modeling framework for inferring user intent and behavior. Unlike conventional timeline reconstructions, their approach integrates semantic modeling and probabilistic reasoning to understand the attacker's objectives—a critical advancement for motive attribution in forensic reporting.

Alnafrani and Wijesekera [31] developed AIFIS, a scalable AI-driven forensic system. It incorporates supervised learning classifiers (e.g., random forests) for evidence classification and ranking. AIFIS's modularity allows it to be adapted to diverse crime scenarios, but its performance under adversarial input manipulation remains unexplored.

Natural Language Processing (NLP) has also gained traction. Ukwen and Karabatak [32] reviewed systems that extract, summarize, and cross-reference forensic artifacts from unstructured data sources such as chat logs and e-mails. Despite their utility, these systems often struggle with semantic ambiguity and language obfuscation used by sophisticated attackers.

Jeong [33] proposed a taxonomy of AI threats and forensic responses, offering a comprehensive classification of AI-driven attack vectors and corresponding forensic strategies. Punjabi and Chaure [34], on the other hand, advanced the notion of forensic intelligence by combining predictive analytics with digital evidence extraction—moving toward a proactive forensic paradigm.

Table 2: Comparative Overview of AI-Based Digital Forensic Frameworks

Ref. No.	Framework / Study	AI Techniques Used	Application Area	Key Strength	Identified Limitation
[24]	Solanke (2022)	XAI (LIME, SHAP)	General forensic explainability	Enhances legal transparency	Lacks empirical performance metrics
[25]	Hall et al. (2022)	Decision Trees, Rule-based Models	Interpretability in forensic AI	Auditable and user-trusted AI outputs	Limited in handling high-dimensional data

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[26]	Hoelz et al. (2009)	Expert Systems, Case-Based Reasoning	Evidence triage	Early AI-forensics integration	No learning capability, lacks scalability
[27]	Rughani (n.d.)	Multi-agent AI, Pattern Matching	Modular digital forensic automation	Comprehensive process modeling	No performance benchmarking
[28]	Zhang et al. (2020)	CNN (Deep Learning)	Surveillance video forensics	High accuracy (94%) in frame tampering detection	Evaluated on synthetic datasets only
[29]	Maratsi et al. (2022)	Ethical Governance Layers	Evidence acquisition regulation	Regulatory compliance focus	Conceptual; lacks implementation prototype
[30]	Ogundiran et al. (2023)	Goal-Oriented Modeling, Probabilistic Logic	Event reconstruction	Behavioral intent inference	Needs large semantic datasets
[31]	Alnafrani & Wijesekera (2022)	Supervised Learning (Random Forests)	General forensic case handling	Scalable and modular	Unknown adversarial resilience
[32]	Ukwen & Karabatak (2021)	NLP, Text Mining	Chat/email forensic analysis	Efficient unstructured data parsing	Struggles with semantic ambiguity
[33]	Jeong (2020)	AI Taxonomy Modeling	Security threat categorization	Broad classification of AI forensics	High-level taxonomy, lacks algorithm design
[34]	Punjabi & Chaure (2022)	Predictive Analytics, Forensic Intelligence	Proactive digital forensics	Anticipates threat patterns	Not tested in operational environments

CHALLENGES

Lack of Standardization and Benchmarking

There is no universally accepted framework or dataset for evaluating AI-based digital forensic tools. Many models, such as those in [27], [28], are validated on synthetic or private datasets, making reproducibility and cross-comparison difficult. The absence of standardized benchmarks inhibits the ability to measure progress across approaches or verify claims of performance.

Explainability and Legal Admissibility

While explainable AI (XAI) techniques have been proposed [24], [25], they are not yet robust enough to consistently produce outputs that meet evidentiary standards in legal settings. Many forensic tools operate as black boxes, raising concerns about transparency, bias, and the right to contest automated decisions in judicial proceedings.

Adversarial Robustness

Most existing AI models are not tested against adversarial threats, such as input manipulation or poisoning attacks. Given that forensic systems may themselves be targeted by attackers, the lack of defensive mechanisms against adversarial AI threatens the integrity and trustworthiness of such systems [31].

Ethical and Privacy Concerns

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The use of AI in analyzing personal data (e.g., emails, chat logs, behavioral patterns) raises significant ethical and legal questions. As noted by [29], failure to ensure privacy-preserving analysis or respect data governance laws like GDPR can lead to the inadmissibility of evidence or institutional misuse.

Semantic Ambiguity in Unstructured Data

NLP-based forensic systems [32] often struggle to accurately interpret natural language communication, particularly when attackers use obfuscation, slang, or multilingual content. These semantic challenges can lead to misclassification or incomplete evidence extraction.

Limited Real-World Validation

Many proposed frameworks remain at the conceptual or prototype stage and have not been deployed in active forensic environments. Without operational validation, their scalability, adaptability, and integration potential with existing forensic workflows remain speculative.

FUTURE WORK

Development of Open Benchmarks and Shared Datasets

The creation of publicly available forensic datasets with diverse attack scenarios and modalities (e.g., text, video, logs) is essential. These benchmarks will enable fair evaluation, improve reproducibility, and foster collaborative model improvement.

Hybrid and Explainable Architectures

Merging deep learning with interpretable models (e.g., combining LSTM-based detectors with rule-based post-hoc explainers) can balance accuracy and explainability. Research should also focus on real-time explainability for live forensic analysis in incident response.

Adversarially-Aware Forensic AI

Future systems should incorporate adversarial training, robust optimization, and input validation layers to withstand attempts at model evasion and evidence tampering. This is particularly critical for forensics used in critical infrastructure and national security investigations.

Privacy-Preserving Forensic Models

Integrating federated learning and differential privacy into forensic pipelines can enable multi-agency collaboration without compromising sensitive data. These approaches allow distributed learning on decentralized data, supporting cross-border investigations.

CONCLUSION

The integration of AI into digital forensics represents a pivotal shift from reactive evidence processing to proactive and intelligent cyber-attack detection. As demonstrated in this review, AI models—ranging from traditional machine learning to complex hybrid architectures—have significantly enhanced forensic capabilities across diverse applications such as intrusion detection, multimedia forensics, and behavior analysis. However, these advancements are tempered by persistent challenges, including a lack of standardized evaluation benchmarks, limited explainability, vulnerability to adversarial manipulation, and ethical concerns regarding data privacy.

Notable frameworks like D4I, Fronesis, and AIFIS provide foundational insights into the modular and scalable design of AI-driven forensic systems. Nevertheless, most models still lack operational validation and fail to meet the stringent requirements of legal admissibility. To bridge these gaps, future research must prioritize explainable and auditable AI, develop adversarially robust alg3orithms, and ensure compliance with forensic and data protection standards. Furthermore, the creation of open datasets and cross-disciplinary collaboration between legal, technical, and policy domains is essential for the maturation of AI-based digital forensics. By addressing these gaps, the field can advance toward creating trustworthy, effective, and legally credible forensic systems fit for the complexity of modern cyber warfare.

Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFERENCES

[1] Rughani, P. H. (2017). Artificial intelligence-based digital forensics framework. Retrieved from https://www.researchgate.net/publication/320758716
[2] Jain, P., Verma, P., Debnath, T., & Heisnam, L. (n.d.). Cybersecurity forensics with AI: A comprehensive review. Taylor & Francis. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003499459-10
[3] Fakiha, B. (2023). Enhancing cyber forensics with AI and machine learning: A study on automated threat analysis and classification. https://search.ebscohost.com
[4] Dimitriadis, A., Lontzetidis, E., & Kulvatunyou, B. (2022). Fronesis: Digital forensics-based early detection of ongoing cyber-attacks. https://ieeexplore.ieee.org/document/10004506
[5] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks.
[6] https://www.sciencedirect.com/science/article/pii/S2590005619300153
[7] AbuOdeh, M., Adkins, C., & Setayeshfar, O. (2021). A novel AI-based methodology for identifying cyber attacks in honeypots.
[8] https://ojs.aaai.org/index.php/AAAI/article/view/17786
[9] Manasa, S., & Kumar, K. P. (2022). Digital forensics investigation for attacks on artificial intelligence. ECS Transactions, 107(1), 9639. https://doi.org/10.1149/10701.19639ecst
[10] Puchalski, D., Pawlicki, M., Kozik, R., Renk, R., & Choraś, M. (2024). Trustworthy AI-based cyber-attack detector for network cyber crime forensics. Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 39(1), Article No. 88. https://doi.org/10.1145/3664476.3670880
[11] Kolluri, V. (2016). A pioneering approach to forensic insights: Utilization AI for cybersecurity incident investigations. https://www.researchgate.net/publication/380729744
[12] Al-Mousa, M. R. (2021). Analyzing cyber-attack intention for digital forensics using case-based reasoning. https://arxiv.org/abs/2101.01395
[13] Anghel, C. (2019). Digital Forensics–A Literature Review. *The Annals of "Dunarea de Jos" University of Galati Fascicle III, Electrotechnics, Electronics, Automatic Control, Informatics*, 42, 23–27.
[14] Kaur, M., Kaur, N., & Khurana, S. (2016). A literature review on cyber forensic and its analysis tools. *International Journal of Advanced Research in Computer and Communication Engineering*, 5, 23–28.
[15] Ganesh, V. (n.d.). Artificial intelligence applied to computer forensics. *International Journal*, 5.
[16] Kasper, A., & Laurits, E. (2016). Challenges in collecting digital evidence: a legal perspective. In *The Future of Law and eTechnologies* (pp. 195–233).
[17] Lovanshi, M., & Bansal, P. (2019). Comparative study of digital forensic tools. In *Data, Engineering and Applications: Volume 2* (pp. 195–204).
[18] Singh, S., & Kumar, S. (2020). Qualitative Assessment of Digital Forensic Tools. *Asian Journal of Electrical Sciences*, 9, 25–32.
[19] Irons, A., & Lallie, H. S. (2014). Digital forensics to intelligent forensics. Future Internet, 6(3), 584–596. https://doi.org/10.3390/fi6030584
[20] Qadir, A. M., & Varol, A. (2020). The role of machine learning in digital forensics. In 2020 8th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1–5). IEEE. https://doi.org/10.1109/ISDFS49300.2020.9116386
[21] Costantini, S., De Gasperis, G., & Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. Annals of Mathematics and Artificial Intelligence, 86, 193–229. https://doi.org/10.1007/s10472-019-09644-2
[22] Dunsin, D., Ghanem, M., Ouazzane, K., et al. (n.d.). The use of artificial intelligence in digital forensics and incident response (DFIR) in a constrained environment. [Conference presentation or journal pending clarification].
[23] Mitchell, F. (2010). The use of artificial intelligence in digital forensics: An introduction. Digital Evidence and Electronic Signature Law Review, 7, 35–39. https://doi.org/10.14296/deeslr.v7i0.2242
[24] Mohsin, K. (2021). Artificial intelligence in forensic science. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3910244

[25] Jarrett, A., & Choo, K.-K. R. (2021). The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science, 3(4), e1418. https://doi.org/10.1002/wfs2.1418
[26] Solanke, A. A. (2022). Explainable digital forensics AI: Towards mitigating distrust in AI-based digital forensics analysis using interpretable models. Forensic Science International: Digital Investigation, 42, 301403. https://doi.org/10.1016/j.fsidi.2022.301403
[27] Hoelz, B. W. P., Ralha, C. G., & Geeverghese, R. (2009). Artificial intelligence applied to computer forensics. In Proceedings of the 2009 ACM Symposium on Applied Computing (pp. 883–888). ACM. https://doi.org/10.1145/1529282.1529479
[28] Rughani, P. H. (2017). Artificial intelligence-based digital forensics framework. *International Journal of Advanced Research in Computer Science, 8*(1). https://www.researchgate.net/publication/320758716
[29] Hall, S. W., Sakzad, A., & Choo, K.-K. R. (2022). Explainable artificial intelligence for digital forensics. *Wiley Interdisciplinary Reviews: Forensic Science, 4*(3), e1434. https://doi.org/10.1002/wfs2.1434
[30] Zhang, Z., Feng, H., Pan, S., et al. (2020). Missing frame detection of surveillance videos based on deep learning in forensic science. In *Proceedings of the 2020 6th International Conference on Computing and Artificial Intelligence* (pp. 298–304). ACM. https://doi.org/10.1145/3404555.3404627
[31] Maratsi, M. I., Popov, O., Alexopoulos, C., et al. (2022). Ethical and legal aspects of digital forensics algorithms: The case of digital evidence acquisition. In *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance* (pp. 32–40). ACM. https://doi.org/10.1145/3560107.3560331
[32] Ogundiran, A., Chi, H., Yan, J., et al. (2023). A framework to reconstruct digital forensics evidence via goal-oriented modeling. In *2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC)* (pp. 1–11). IEEE. https://doi.org/10.1109/ICAIC56717.2023.10176813
[33] Alnafrani, R., & Wijesekera, D. (2022). AIFIS: Artificial Intelligence (AI)-based forensic investigative system. In *2022 10th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–6). IEEE. https://doi.org/10.1109/ISDFS53851.2022.9765360
[34] Ukwen, D. O., & Karabatak, M. (2021). Review of NLP-based systems in digital forensics and cybersecurity. In *2021 9th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1–9). IEEE. https://doi.org/10.1109/ISDFS52856.2021.9486345
[35] Jeong, D. (2020). Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues. *IEEE Access, 8*, 184560–184574. https://doi.org/10.1109/ACCESS.2020.3029357
[36] Punjabi, S. K., & Chaure, S. (2022). Forensic intelligence—Combining artificial intelligence with digital forensics. In *2022 2nd International Conference on Intelligent Technologies (CONIT)* (pp. 1–5). IEEE. https://doi.org/10.1109/CONIT55038.2022.9848103