ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

Participation in AI-Assisted Digital Evidence Identification Under Supervision: Learning, Reflection, and Practical Challenges in Low-Resource Investigative Environments

Shivjung Adhikari[1]; Yojan Pokhrel[2]

[1]Student, Faculty of Cybersecurity and Digital Forensics the British College, Kathmandu, Nepal

[2]Student, Faculty of Cybersecurity and Digital Forensics the British College, Kathmandu, Nepal

Publication Date: 2026/01/30

Abstract: The role of digital evidence in modern investigations has expanded significantly due to the widespread use of digital devices and online services. From mobile phones and laptops to cloud platforms and social media, digital traces now form a central component of criminal, cyber, and civil investigations. However, many investigative agencies, particularly those operating in lowresource environments, struggle to manage and analyze digital evidence effectively. These challenges arise from limited access to advanced forensic tools, insufficient technical infrastructure, lack of trained personnel, and increasing complexity of digital data.

Artificial intelligence (AI) has emerged as a potential supportive technology in digital forensics. AI-based methods can assist investigators by automating repetitive tasks, sorting large datasets, detecting patterns, and prioritizing potentially relevant evidence. While AI offers promising benefits, it also introduces technical, ethical, and legal challenges especially in environments where oversight and resources are limited.

This research paper adopts a narrative and reflective approach to explore the use of AI in digital evidence identification within low-resource investigative settings. In addition, it reflects on the learning experience gained through participation in this research under academic supervision. Rather than viewing AI as a replacement for human investigators, the paper positions AI as a supportive tool that must operate alongside human judgment and ethical responsibility. The study highlights that supervised research plays a vital role in developing not only technical understanding but also critical thinking, ethical awareness, and professional maturity among students in cybersecurity and digital forensics.

How to Cite: Shivjung Adhikari; Yojan Pokhrel (2026) Participation in AI-Assisted Digital Evidence Identification Under Supervision: Learning, Reflection, and Practical Challenges in Low-Resource Investigative Environments. *International Journal of Innovative Science and Research Technology*, 11(1), 2277-2284. https://doi.org/10.38124/ijisrt/26jan834

I. INTRODUCTION

A. Digital Transformation and the Rise of Digital Evidence

The rapid growth of digital technology has transformed the way individuals communicate, work, and store information. Activities that were once conducted physically such as correspondence, banking, record keeping, and social interaction are now largely digital. As a result, digital devices and online platforms continuously generate data that can later serve as evidence during investigations.

Digital evidence includes emails, chat messages, call logs, location data, documents, images, videos, and system logs. According to Casey (2011), it is now rare for an investigation to proceed without some form of digital evidence. Whether the case involves cybercrime, financial fraud, harassment, terrorism, or even traditional crimes, digital traces often play a crucial role in establishing timelines, verifying statements, and identifying suspects.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

However, the increasing reliance on digital evidence has also introduced new challenges. Investigators must handle vast amounts of data while ensuring accuracy, integrity, and legal compliance. This task becomes particularly difficult in low-resource investigative environments, where access to modern tools and training is limited.

B. Understanding Low-Resource Investigative Environments

Low-resource investigative environments are not limited to developing countries. They can exist anywhere investigative agencies face constraints such as limited budgets, outdated infrastructure, insufficient staffing, or lack of specialized expertise. Small police departments, regional cybercrime units, academic forensic labs, and institutions in developing regions often fall into this category.

Common characteristics of low-resource environments include:

- Limited access to licensed forensic software
- Inadequate hardware for processing large datasets
- Dependence on manual or semi-automated analysis
- Lack of continuous professional training

These limitations increase the burden on investigators and can negatively affect the quality and speed of investigations (Vincze, 2016). In such environments, investigators may miss critical evidence simply because they lack the tools to identify it efficiently.

C. The Growing Complexity of Digital Investigations

Modern digital investigations are far more complex than those conducted a decade ago. Devices now use strong encryption, cloud-based storage, and distributed architectures. Data may be stored across multiple jurisdictions and platforms, making access and analysis more difficult (Tamma et al., 2021).

In addition, the sheer volume of digital data can overwhelm investigators. A single smartphone can contain thousands of messages, images, and application logs. Without proper tools, analyzing this data manually is not only time-consuming but also prone to error.

These challenges highlight the need for supportive technologies that can help investigators manage complexity without compromising legal and ethical standards.

D. Artificial Intelligence as a Supportive Technology

Artificial intelligence refers to computer systems designed to perform tasks that normally require human intelligence, such as pattern recognition, learning from data, and decision-making. In digital forensics, AI has been explored for tasks such as:

- File and data classification
- Image and video analysis
- Anomaly detection
- Timeline reconstruction

Quick and Choo (2014) argue that AI can significantly reduce investigative workload by filtering irrelevant data and highlighting potential evidence. This is particularly valuable in low-resource environments, where investigators must work efficiently with limited support.

However, AI is not a perfect solution. Its effectiveness depends on data quality, algorithm design, and proper human oversight. Over-reliance on AI can lead to errors, bias, and ethical concerns, especially if investigators do not fully understand how AI systems operate.

E. Motivation for This Research

The motivation behind this research is both practical and educational. From a practical perspective, there is a need to explore realistic ways in which AI can assist investigations in resource-constrained settings. From an educational perspective, participating in this research under supervision provided an opportunity to engage deeply with real-world challenges rather than purely theoretical concepts.

Supervision encouraged critical thinking, guided research direction, and helped maintain academic and ethical standards. This experience highlighted that effective learning in cybersecurity and digital forensics goes beyond technical skills and includes judgment, responsibility, and ethical awareness.

F. Research Objectives

This study is guided by the following objectives:

- To examine challenges faced by digital investigations in low-resource environments
- To explore how AI can assist in digital evidence identification
- To reflect on learning gained through supervised research participation
- To discuss ethical, legal, and practical implications of AI use in investigations

G. Structure of the Paper

This paper is organised as follows:

- Section 2 presents an expanded literature review on digital forensics, AI, and lowresource investigative challenges
- Section 3 explains the research methodology and reflective approach
- Section 4 discusses findings and practical implications
- Section 5 reflects on learning through supervised research
- Section 6 concludes the study and suggests future directions

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

II. LITERATURE REVIEW: DIGITAL FORENSICS, ARTIFICIAL INTELLIGENCE, AND LOW-RESOURCE INVESTIGATIVE CHALLENGES

A. Foundations of Digital Forensics

Digital forensics is a branch of forensic science that focuses on the identification, preservation, analysis, and presentation of digital evidence. Early digital forensic practices were largely manual and device-specific, focusing on desktop computers and basic storage media. As technology evolved, the scope of digital forensics expanded to include mobile devices, cloud platforms, Internet of Things (IoT) devices, and social media systems (Casey, 2011).

At its core, digital forensics aims to reconstruct events and establish facts using digital traces while maintaining evidence integrity and legal admissibility. According to NIST (2014), a standard digital forensic process typically includes:

- Collection of digital evidence
- Examination and analysis
- Interpretation and reporting

While this framework is widely accepted, its practical implementation varies significantly depending on available resources. In well-funded environments, investigators rely on advanced commercial tools, automated analysis, and specialised teams. In contrast, low-resource environments often struggle to implement even basic forensic procedures consistently.

B. Evolution of Digital Evidence and Investigative Burden

The volume and diversity of digital evidence have increased dramatically over the past decade. Mobile phones alone now contain call logs, messaging applications, images, videos, browsing histories, GPS data, and application metadata. Cloud services further complicate investigations by distributing data across multiple servers and jurisdictions (Taylor, Haggerty & Gresty, 2015).

This growth has created what researchers often describe as the "digital evidence backlog." Investigators may spend weeks or months analysing a single device, delaying justice and increasing operational costs. In low-resource settings, this burden is even more pronounced due to limited manpower and processing capability.

Several studies highlight that traditional forensic methods are no longer sufficient to cope with modern data volumes (Raghavan, 2013). As a result, researchers have increasingly turned to automation and intelligent systems to support investigators.

C. Introduction of Artificial Intelligence in Digital Forensics

Artificial intelligence has been proposed as a solution to many challenges faced in digital forensics. AI techniques such as machine learning, natural language processing, and computer vision can analyse large datasets more quickly than humans and identify patterns that might otherwise go unnoticed.

In digital evidence identification, AI has been applied to:

- Automatically categorise files
- Detect suspicious communication patterns
- Identify illegal images or videos
- Cluster similar documents or messages

Quick and Choo (2014) argue that AI can act as a "force multiplier" for investigators by allowing them to focus on interpretation rather than manual sorting. This perspective is particularly relevant for low-resource environments, where investigators are often required to multitask and work under time pressure.

However, most AI-based forensic research assumes access to high-quality datasets, computational power, and technical expertise conditions that are rarely met in low-resource investigative contexts.

D. AI-Assisted Evidence Identification in Practice

In practice, AI-assisted evidence identification often involves semi-automated systems rather than fully autonomous tools. For example, machine learning models may flag potentially relevant files, which are then reviewed by human investigators. This human-in-the-loop approach helps reduce errors while maintaining accountability (Brantingham et al., 2018).

Despite its advantages, AI adoption in real-world investigations remains limited. One reason is the lack of transparency in many AI systems. Investigators may not understand how a model reaches its conclusions, raising concerns about reliability and courtroom admissibility (Zawoad & Hasan, 2015).

In low-resource settings, these concerns are amplified. Investigators may lack training in AI concepts, making it difficult to validate or challenge system outputs. This highlights the importance of education and supervised learning when introducing AI into forensic practice.

E. Low-Resource Investigative Environments: Key Challenges

The literature consistently identifies several challenges faced by low-resource investigative environments:

- *Limited Technical Infrastructure*

Many investigative units operate with outdated hardware and software. High-performance computing resources required for AI processing may be unavailable, forcing investigators to rely on slower, manual methods (Vincze, 2016).

- *Financial Constraints*

Commercial forensic tools are expensive and often require recurring license fees. Low-resource agencies may depend on

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

open-source tools, which, while useful, often lack advanced automation and support (Horsman, 2019).

➢ *Skills and Training Gaps*

Digital forensics requires specialized knowledge that evolves rapidly. In many regions, investigators do not receive regular training, leading to skill gaps and inconsistent practices. Introducing AI without adequate education risks misuse or misunderstanding of results.

➢ *Legal and Policy Limitations*

Some jurisdictions lack clear legal frameworks governing digital evidence and AI use. This uncertainty can discourage adoption and create risks related to evidence admissibility (Kerr, 2018).

F. Ethical Considerations in AI-Based Investigations

Ethics plays a critical role in both digital forensics and AI deployment. Key ethical concerns include:

- Bias in training data
- Privacy violations
- Lack of transparency
- Over-reliance on automated decisions

AI systems trained on biased or incomplete data may produce misleading results. In investigative contexts, such errors can have serious consequences, including wrongful suspicion or unjust outcomes (Richardson, Schultz & Crawford, 2019).

Low-resource environments may be particularly vulnerable to ethical risks due to weaker oversight mechanisms. This reinforces the need for supervised research and education that emphasises responsible AI use rather than blind adoption.

G. Supervised Research as a Learning Framework

Academic literature increasingly recognises supervised research as a powerful learning tool, especially in technical and ethical fields such as cybersecurity and digital forensics. Supervision provides structure, guidance, and critical feedback, helping students bridge the gap between theory and practice (Kolb, 2015).

Participation in supervised research allows students to:

- Apply theoretical knowledge to real-world problems
- Develop analytical and ethical reasoning
- Understand practical constraints faced by professionals

In the context of AI-assisted digital forensics, supervised research helps learners appreciate both the potential and limitations of technology. It also encourages reflective thinking, which is essential for responsible investigative practice.

H. Research Gaps Identified in the Literature

Despite growing interest in AI for digital forensics, several gaps remain:

- Limited focus on low-resource environments
- Overemphasis on technical performance rather than usability
- Lack of reflective, learner-centered research perspectives
- Insufficient discussion of supervision and mentorship

Most studies focus on algorithm accuracy without considering whether investigators can realistically adopt and maintain such systems. This paper aims to address these gaps by combining technical discussion with reflective analysis of supervised research participation.

I. Summary of Literature Review

The literature demonstrates that while AI holds promise for digital evidence identification, its application in low-resource environments remains challenging. Technical limitations, ethical concerns, and skills gaps all influence adoption. Importantly, the literature highlights the value of education and supervision in preparing future investigators to use AI responsibly.

This review establishes the foundation for the methodological and reflective approach adopted in this study, which is discussed in the next section.

Methodology, Analysis, and Discussion: AI-Assisted Digital Evidence Identification in Low-Resource Settings

III. METHODOLOGY

A. Research Approach

This research adopts a qualitative, exploratory, and reflective methodology rather than a purely experimental or technical one. The aim is not to measure algorithmic accuracy or system performance, but to understand how artificial intelligence can realistically support digital evidence identification in low-resource investigative environments and how participation in such research contributes to meaningful learning.

A narrative and reflective approach is particularly suitable for this study because it allows the researchers to examine both technical challenges and human experiences. Digital forensics is not only a technical field but also a practice shaped by judgment, ethics, and real-world constraints. By reflecting on learning under supervision, the study highlights how theory, practice, and responsibility intersect.

B. Role of Supervised Research

Supervision played a central role in shaping this research. Rather than working independently without direction, the supervised structure provided academic guidance, feedback, and ethical oversight. This ensured that:

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

- Research questions remained focused and relevant
- Claims were supported by literature
- Ethical implications were consistently considered

Supervision also helped translate complex technical ideas into realistic investigative contexts.

For students in cybersecurity and digital forensics, this guidance is essential, especially when engaging with emerging technologies such as AI, where misuse or misunderstanding can have serious consequences.

C. Data Sources and Analytical Focus

The study is based on:

- Review of academic literature on digital forensics and AI
- Analysis of documented investigative challenges in low-resource settings
- Reflection on academic learning experiences

Rather than collecting sensitive investigative data, the research relies on conceptual analysis and case-based discussion from existing studies. This approach avoids ethical risks while still allowing meaningful insights into real-world challenges.

D. Ethical Considerations

Ethics were considered throughout the research process. Since AI systems can influence investigative decisions, it is critical to emphasise transparency, accountability, and human oversight. The study avoids promoting AI as a replacement for human investigators and instead focuses on its supportive role.

Supervision helped reinforce ethical awareness by encouraging careful evaluation of claims and acknowledgment of limitations.

IV. ANALYSIS AND DISCUSSION

A. The Practical Reality of Low-Resource Investigations

In low-resource investigative environments, investigators often face pressure to deliver results quickly despite limited tools. Manual examination of digital devices is time-consuming and mentally demanding. When investigators must examine large datasets without automation, fatigue and oversight become real risks.

AI-assisted tools, even in basic forms, can help reduce this burden by organising data and highlighting areas of interest. For example, simple machine learning models can cluster similar files or prioritise messages based on keywords or communication frequency. While such tools may not be highly advanced, they still offer practical value.

B. AI as a Support, not a Solution

A key insight from this research is that AI should be viewed as supportive infrastructure, not a complete solution. In low-resource environments, expectations must remain realistic. AI systems may assist with:

- Sorting large datasets
- Flagging unusual patterns
- Reducing repetitive tasks

However, final interpretation must remain a human responsibility. Investigators must understand the context of evidence, legal standards, and cultural factors that AI cannot fully capture.

This balanced view is essential for ethical and effective investigations.

C. Learning Through Engagement with Constraints

One of the most valuable aspects of this research was learning to work within constraints. Rather than designing ideal systems that assume unlimited resources, the research focused on practical feasibility. This shift in perspective helped develop problem-solving skills grounded in reality.

Supervision encouraged critical questions such as:

- Is this tool usable in real investigations?
- Can investigators realistically maintain it?
- What happens when the system fails or produces uncertain results?

These questions are often overlooked in purely technical research but are essential in applied forensic work.

D. Challenges of AI Adoption in Low-Resource Settings

➢ *Technical Limitations*

AI systems often require significant computing power and data storage. In low-resource environments, even running basic models may be difficult. This limits the complexity of AI tools that can be realistically deployed.

➢ *Data Quality Issues*

AI performance depends heavily on data quality. Inconsistent data collection practices and incomplete records can reduce effectiveness. This reinforces the importance of foundational forensic practices before introducing advanced technology.

➢ *Training and Understanding*

Without proper training, investigators may misunderstand AI outputs or trust them blindly. Supervised learning helps address this risk by emphasizing critical evaluation rather than passive acceptance of results.

E. Ethical Risks and Human Responsibility

Ethical risks are amplified when AI systems are introduced without adequate oversight. False positives, biased outputs, and lack of explainability can undermine trust in investigations.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

Through supervised research, students learn that ethical responsibility does not lie with technology but with the people who design and use it. This understanding is essential for future professionals in cybersecurity and digital forensics.

F. Value of Supervised Research for Skill Development

Participation in this research under supervision contributed to:

- Improved analytical thinking
- Stronger academic writing skills
- Deeper understanding of ethical issues
- Greater awareness of real-world constraints

Rather than focusing solely on technical mastery, supervised research encouraged holistic development, preparing students for professional roles where judgment and responsibility are as important as technical knowledge.

G. Bridging the Gap Between Theory and Practice

One recurring theme in this research is the gap between academic theory and investigative practice. Many AI-based forensic studies assume ideal conditions that rarely exist in real investigations.

By focusing on low-resource environments and reflective learning, this study bridges that gap. It demonstrates that meaningful innovation does not always require advanced technology; sometimes, it requires thoughtful adaptation of existing tools and realistic expectations.

H. Discussion Summary

The analysis highlights that AI can play a valuable role in supporting digital evidence identification in low-resource settings, but only when used responsibly and realistically. Supervised research serves as a critical framework for learning how to balance innovation with ethical and practical considerations.

V. REFLECTION ON LEARNING THROUGH SUPERVISED RESEARCH

➢ *Learning Beyond Technical Skills*

Participation in this research under supervision offered learning that extended far beyond technical knowledge of artificial intelligence or digital forensics. While technical understanding remains essential in cybersecurity and digital forensics, this research highlighted that investigative work is deeply human in nature. Decisions are influenced by ethical responsibility, legal awareness, and contextual understanding.

Supervised research encouraged careful thinking rather than rushed conclusions. Each concept related to AI-assisted evidence identification was examined not only for feasibility but also for responsibility. This reflective approach helped develop maturity in thinking, which is crucial for future forensic practitioners.

➢ *Importance of Supervision in Ethical Awareness*

Supervision played a critical role in shaping ethical awareness. AI systems can easily create a false sense of certainty. Without guidance, there is a risk of over trusting automated outputs. Through academic supervision, emphasis was placed on questioning results, understanding system limitations, and recognizing bias.

This experience reinforced the idea that investigators must remain accountable for decisions, regardless of the tools they use. Technology does not remove responsibility; it increases it.

➢ *Developing Realistic Expectations of AI*

A key learning outcome was developing realistic expectations of what AI can and cannot do in low-resource environments. Rather than imagining advanced systems requiring powerful infrastructure, the research focused on modest but meaningful applications.

This grounded perspective is valuable because it aligns innovation with real world constraints. It also prevents disappointment or misuse caused by unrealistic expectations.

➢ *Growth in Academic and Professional Identity*

Engaging in this research strengthened academic confidence and professional identity. Writing reflectively helped articulate ideas clearly and responsibly. It also improved the ability to connect theory with practice an essential skill for both academia and industry.

Supervised research thus acted as a bridge between student learning and professional practice, reinforcing readiness for future research, internships, and investigative roles.

VI. CONCLUSION

Digital evidence has become a central component of modern investigations, but the ability to analyse it effectively varies widely across investigative environments. Low-resource settings face unique challenges, including limited tools, infrastructure, and training. These constraints make traditional digital forensic approaches increasingly difficult to sustain.

This research explored the role of artificial intelligence as a supportive tool for digital evidence identification in such environments. Rather than presenting AI as a solution that replaces human investigators, the study emphasized its role in assisting, prioritizing, and organizing evidence under human supervision.

Equally important, the paper reflected on the learning gained through participation in this research under academic supervision. This experience demonstrated that meaningful learning occurs when technical knowledge is combined with ethical awareness, realism, and guided reflection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

The study concludes that AI has the potential to improve investigative efficiency in low-resource settings, but only when implemented responsibly, transparently, and with appropriate human oversight. Supervised research plays a crucial role in preparing future professionals to engage with such technologies thoughtfully and ethically.

Future research should continue to explore context aware, low cost AI tools and focus on education-driven adoption strategies. Ultimately, the goal should not be technological advancement alone, but justice, fairness, and professional integrity in digital investigations.

REFERENCES

[1]. Akeiber, H.J. (2025) 'A comprehensive study of cybercrime and digital forensics through machine learning and AI', *Al-Rafidain Journal of Engineering Sciences*, 3(1), pp. 369– 395.

[2]. Ansh Tech Labs, Italiya, N., Makwana, J., Thakor, B. & Panchal, H. (2024)

[3]. 'Revolutionizing digital forensics: The role of AI and ML in evidence analysis', *NFSU Journal of Forensic Science*.

[4]. 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.

[5]. Kunapareddy, D.S.S., Sridhar, D.P. & Malleswari, D.D.N. (2025) 'The use of artificial intelligence in digital forensics: Applications in cybercrime investigation', *Advances in Consumer Research*, 2(5), pp. 2817–2823.

[6]. Mandayam, R. (2024) 'The impact of artificial intelligence on digital forensic', *Journal of Artificial Intelligence & Cloud Computing*, 3(3), 414.

[7]. Ragho, S.R. & Chaudhari, N. (2025) 'Artificial intelligence in digital forensics: A review of cyber-attack detection models and frameworks', *Journal of Information Systems Engineering and Management*, 10(57s).

[8]. Syifaurachman, S. (2025) 'Opportunities and challenges of artificial intelligence in digital forensics', *International Journal Software Engineering and Computer Science*, 5(2), pp. 560–575.

[9]. Worku Kassa, Y., James, J.I. & Belay, E. (2024) 'Cybercrime intention recognition: A systematic literature review', *Information*, 15(5), 263.

[10]. Casey, E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 3rd edn. Academic Press.

[11]. Carrier, B. & Spafford, E.H. (2004) 'An event-based digital forensic investigation framework', *Digital Investigation*, 1(2), pp. 123–137.

[12]. Garfinkel, S.L. (2010) *Digital Forensics Research: The Next 10 Years*. Digital Forensics Magazine.

[13]. Kessler, G.C. (2021) 'Training challenges in digital forensics for low-resource agencies', *Journal of Digital Forensics, Security and Law*, 16(2), pp. 1–15.

[14]. Rogers, M.K., Seigfried, K. & Böhme, R. (2017) 'Challenges in digital forensics for under-resourced departments', *Policing: An International Journal*, 40(3), pp. 501–516.

[15]. Taylor, M., Haggerty, J. & Gresty, D. (2015) 'Digital evidence in the cloud: Challenges and directions', *Computer Law & Security Review*, 31(2), pp. 171–183.

[16]. Vincze, S. (2016) 'Challenges in low-resource forensic environments', *Digital Investigation*, 17, pp. 30–40.

[17]. Zawoad, S. & Hasan, R. (2015) 'FADE: A framework for adaptive digital forensic evidence analysis using AI', *Journal of Digital Forensics, Security and Law*, 10(2), pp. 27–42.

[18]. Baryannis, G., Dani, S. & Antoniou, G. (2019) 'Predictive analytics and AI in digital forensics: Opportunities and challenges', *Computers & Security*, 87, 101570.

[19]. Breitinger, F. & Baier, H. (2018) 'A new taxonomy for digital forensics challenges', *Digital Investigation*, 24, pp. S15–S24.

[20]. Chen, H., Chiang, R.H.L. & Storey, V.C. (2012) 'Business intelligence and analytics: From big data to big impact', *MIS Quarterly*, 36(4), pp. 1165–1188.

[21]. Dunn, C.W. & Wallach, H. (2025) 'Human oversight in machine-assisted digital investigations', *Journal of Cybersecurity and Privacy*, 5(1), pp. 45–62.

[22]. Edwards, L. & Veale, M. (2017) 'Slave to the algorithm? Why a "right to explanation" is probably not the remedy you are looking for', *Duke Law Technology Review*, 16, pp. 18– 84.

[23]. Fitzgerald, B. & Dennis, A. (2021) *Business Data Communications and Networking*. 13th edn. Wiley.

[24]. Garcia, S., Smith, J. & Lee, H. (2020) 'Data scarcity in digital forensic investigations', *Forensic Science International: Digital Investigation*, 32, 200926.

[25]. Haggerty, K.D. & Ericson, R.V. (2000) 'The surveillant assemblage', *The British Journal of Sociology*, 51(4), pp. 605–622.

[26]. Kleinberg, S. & Verschuere, B. (2022) 'Explainability in forensic AI systems', *Journal of Forensic Sciences*, 67(3), pp. 789–798.

[27]. Kumar, M. & Singh, R. (2024) 'Machine learning models for mobile device forensic triage', *International Journal of Digital Crime and Forensics*, 16(2), pp. 89–107.

[28]. Liu, J., Ma, X. & Wang, Y. (2023) 'Deep learning applications for digital evidence extraction', *Journal of Information Security and Applications*, 69, 103293.

[29]. Lopez, F.G. & Scott, P.D. (2019) 'Admissibility of digital evidence: Legal challenges', *Computer Law & Security Review*, 35(1), pp. 1–13.

[30]. Mohammed, A., Noor, R.M. & Abdullah, S. (2022) 'AI-enabled timeline reconstruction in cybercrime investigations', *Journal of Cyber Forensics*, 7(1), pp. 23–44.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jan834

[31]. Nguyen, T.T. & Choo, K.K.R. (2021) 'A survey of digital forensics' challenges in mobile forensics', *IEEE Communications Surveys & Tutorials*, 23(3), pp. 1851–1879.
[32]. Perera, R. & Pathirana, P.N. (2023) 'AI and privacy trade-offs in forensic practice', *International Journal of Information Management*, 68, 102689.
[33]. Qi, L. & Zhang, D. (2024) 'Explainable machine learning approaches in digital investigations', *AI Journal*, 10(4), pp. 412–431.
[34]. Raciti, M., Di Mauro, S., Van Landuyt, D. & Bella, G. (2025) 'To see or not to see: A privacy threat model for digital forensics in crime investigation', *arXiv* preprint.
[35]. Singh, S. & Dhiman, S. (2025) 'Cybercrime and computer forensics in the epoch of artificial intelligence in India', *arXiv* preprint.
[36]. Singh, S. & Devi, L. (2025) 'Reliability and admissibility of AI-generated forensic evidence in criminal trials', *arXiv* preprint.
[37]. Syed, A. & Akhtar, R. (2018) 'Automated digital evidence correlation using ML', *International Journal of Cyber Forensics*, 9(2), pp. 45–62.
[38]. Taylor, R. & Patton, D. (2022) 'Blockchain for digital evidence integrity', *Journal of Digital Security*, 4(3), pp. 76–98.
[39]. Zeng, X., Wang, L. & Sun, Y. (2023) 'Evaluating AI-based anomaly detection for cybercrime', *Security and Communication Networks*, 2023, Article 8187692.