



## Cyber Crime and the Legal Challenges of Digital Evidence: Admissibility and Reliability

Dipender Chhikara<sup>1</sup>, Udit Narayan Mishra<sup>2</sup>, Dr Sumbul Fatima<sup>3</sup>, Dr. Shobha Yadav<sup>4</sup>, Divya<sup>5</sup>, Dr. Bharat B.Purohit<sup>6</sup>

<sup>1</sup>Assistant Professor, Department of Law, The NorthCap University, Gurugram, Haryana, India 122017, ORCID ID: 0009-0007-3277-0383. Email Id: deepschhikara@gmail.com

<sup>2</sup>Assistant Professor of Law, School of Law, Kalinga Institute of Industrial Technology Deemed to be University, ORCID ID: 0000-0001-9146-801X, Email Id: adv.uditmishra@gmail.com

<sup>3</sup>Research scholar, Jamia Millia Islamia, ORCID ID: 0009-0005-5482-4376, Email Id: ias.sumbul21@gmail.com

<sup>4</sup>Assistant Professor, Amity law school, Amity University Bengaluru, ORCID ID: 0009-0005-7063-7546, Email Id: adv.shobhayadav@gmail.com

<sup>5</sup>University of technology, jaipur, ORCID ID : 0009-0000-5066-4006, Email Id:- yadav15manisha@gmail.com

<sup>6</sup>Visiting faculty, Department of Law of Veer Narmad South Gujarat University, Surat, ORCID ID: 0009-0004-2768-7057, Email Id : adv.bharatpurohit@gmail.com

### Abstract

The rapid growth of cybercrime has significantly increased the importance of digital evidence in criminal investigations and judicial proceedings. However, ensuring the admissibility and reliability of electronic evidence remains a complex challenge due to technological advancements, evolving legal standards, cross-border investigations, and concerns regarding evidence integrity. This narrative review examines the legal and forensic dimensions of digital evidence by synthesizing contemporary literature on its sources, characteristics, governing legal frameworks, and the factors influencing its acceptance in court. The review discusses key issues related to authentication, chain of custody, expert testimony, procedural fairness, and evidence validation, while also evaluating the impact of emerging technologies, including artificial intelligence, blockchain, the Internet of Things, and deepfake detection on digital forensic practice. The findings indicate that reliable digital evidence requires standardized forensic procedures, scientifically validated investigative methods, and harmonized legal frameworks capable of addressing rapidly evolving cyber threats. Strengthening collaboration among forensic practitioners, legal professionals, researchers, and policymakers will be essential for improving evidence integrity, enhancing judicial confidence, and supporting effective cybercrime investigations. The review provides an integrated perspective that contributes to ongoing discussions on developing secure, transparent, and legally robust digital evidence management practices.

**Keywords:** cybercrime, digital evidence, digital forensics, admissibility, blockchain.

### 1. Introduction

Digital technologies have also advanced quickly and so has the variety of cybercrime utilizing increasingly complicated interrelated networks, cloud, mobile and online communications systems. Cyber offenses often share none of the hallmarks of traditional offenses with piles of electronic records that may be of benefit in the investigation and litigation of the case; rather, mountains of such records are often scattered across multiple national boundaries. The latest international reviews show the worldwide distribution of cybercrime, which is more organised, technologically advanced and demands new approaches and digital forensic skills on the part of law enforcement agencies (Reedy, 2020). Further, continued increase in cyber-enabled offences, such as ransomware, financial fraud, identity theft, and attacks on critical infrastructure further indicate the centrality of digital environments to criminal activity and criminal

investigations (Reedy, 2023).

Cybercrime is constantly changing and digital evidence is an integral part of the modern criminal justice system. The information gathered from the computers, smart phones, cloud-based services, social media sites, surveillance and Internet connected devices is now being routinely used to recreate events, to find perpetrators, to determine intent and to validate witness accounts. The use of electronic records has revolutionized the practice of forensic medicine and shifted the focus from traditional physical evidence to electronic evidence. Casey (2019) has stressed that digital forensics has matured into a multidisciplinary scientific process which is used to assist crime investigations by systematically acquiring, preserving, analyzing, and presenting evidence. This increasing dependence on digital evidence is also accentuated by the fact that digital evidence can offer insights into criminal

behaviour that would otherwise be difficult to uncover in traditional forensic analyses (Klasén et al., 2024).

Although digital evidence is clearly evidentiary, it poses a multitude of legal and forensic challenges that are unique to it and make it different from traditional forms of evidence. Electronic data is easily modifiable, deletable, encryptable and manipulable, and it will always be a concern that the data is authentic and that its integrity has not been compromised. The proliferation of digital forensic capabilities across a myriad of organizations, private entities and cloud service providers has made the acquisition of evidence more complicated and introduced inconsistencies in the investigative practices, which pose risks to the reliability of evidence (Casey et al., 2019). Judicial concerns about authentication, chain of custody, scientific validity, and due process remain key factors in determining the admissibility of e-discovery. These concerns are exacerbated in cross-border investigations where there are often conflicting legal frameworks, jurisdictional limitations, and international cooperation mechanisms, which delay or otherwise may limit lawful access to electronically stored information (Casino et al., 2022). Additionally, the lack of proper protection measures for digital evidence can impact the transparency, reliability, and credibility of the results of digital forensic evidence that is presented in court for a fair trial (Stoykova, 2021).

This legal and technical complexity is increasingly being recognised, as demonstrated by the growing body of scholarship. Recent reviews have focused on the advancements of digital forensic approaches, evidence acquisition techniques, forensic validation, artificial intelligence, blockchain applications and new investigative technologies. Much of the literature, however, is in bits and pieces, and legal analysis, forensic methodology and technology innovations are often treated separately, and not in an integrated perspective. A synthesis of these interwoven areas is therefore needed to gain insight into the impact technological advances are having on evidentiary standards and how legal systems are reacting to the new modes of digital evidence. In this respect, the review by Casino et al. (2022) not only gives a good overview of the large body of existing digital forensic research, but also indicates the need for digital forensic standardization, interoperability, and legal harmonization to be effective in combating cybercrime.

The current review, addresses issues of admissibility and reliability of digital evidence and critically discusses the legal issues associated with the use of digital evidence in cybercrime investigation. The review will incorporate the latest legal research, forensic science and technology to give a comprehensive overview of the concepts and use of

digital evidence in court, and emerging challenges that will impact the future of cybercrime investigations.

## **2. Foundations of Cyber Crime and Digital Evidence**

### **2.1 Evolution and Classification of Cyber Crime**

Cybercrime has grown in scope and sophistication as a result of the rapid digitization of communication, commerce and of public services. Today's cybercrime is defined as unauthorized use of systems, malware, ransomware attacks, online financial fraud, cyber espionage, identity theft and crimes committed by connected smart devices. Cybercrimes frequently leave lots of electronic evidence that requires advanced cybercrime forensic analysis to discover and understand. New challenges in the area of evidence also have come with the advent of digital platforms, such as the documentation of crimes that span across multiple jurisdictions and digital ecosystems. Lessons learned from international criminal investigations show that evolving technology is increasingly used for collecting and interpreting digital evidence and poses new complexities for the law and technology (D'Alessandra & Sutherland, 2021).

### **2.2 Concept and Characteristics of Digital Evidence**

Digital evidence is any data, information or computer-generated records that can be used to prove facts in a legal context. It's characteristics are volatility, reproducibility, digital storage media, and it can be easily corrupted if not handled properly. To ensure that digital evidence is considered acceptable to courts during criminal trials therefore, authenticity, integrity, and traceability must be established. Standardized forensic examination procedures are crucial in maintaining evidentiary credibility and confidence in judicial outcomes (Onwubiko & Eboibi, 2020). Likewise, in the field of law, scholars have highlighted that in order to be admissible, electronic evidence must not only be technically correct but also adhere to the necessary procedural safeguards (Moussa, 2021).

### **2.3 Sources and Categories of Digital Evidence**

Digital evidence can be found on computers, smartphones, the 'Internet of Things' (IoT), cloud services, surveillance systems, mobile apps, voice assistants, and online communications. Acquisition and preservation of evidence in IoT environments are much more challenging as evidence may be spread across heterogeneous devices, communication protocols, and cloud environments (Servida & Casey, 2019). Similarly, systematic

assessment of information integrity, completeness, and reliability is needed throughout the forensic process to ensure the evidentiary quality of information gathered from interconnected devices (Costantini et al., 2020). With the increase in use of intelligent voice assistants, the scope of digital artifacts that could be useful in criminal

investigations is further extended (Akinbi & Berry, 2020). Table 1 summarizes the principal sources of digital evidence, the types of electronic artifacts commonly recovered, associated forensic considerations, and their legal relevance in criminal investigations.

**Table 1. Major Sources of Digital Evidence and Associated Forensic Considerations**

| Source of digital evidence     | Common evidentiary artifacts        | Primary forensic consideration      | Legal significance                       | References                                       |
|--------------------------------|-------------------------------------|-------------------------------------|------------------------------------------|--------------------------------------------------|
| Computers and laptops          | Documents, logs, browsing history   | Data integrity and recovery         | Authentication of electronic records     | Onwubiko & Eboibi (2020)                         |
| Smartphones and mobile devices | Messages, call logs, location data  | Secure acquisition and preservation | Establishing user activity               | Moussa (2021)                                    |
| IoT devices                    | Sensor data, device logs            | Distributed evidence collection     | Reliability of connected-device evidence | Servida & Casey (2019); Costantini et al. (2020) |
| Voice assistants               | Voice commands, interaction history | Metadata preservation               | Reconstruction of user actions           | Akinbi & Berry (2020)                            |
| Open-source and digital media  | Images, videos, online posts        | Verification of authenticity        | Corroboration of investigative findings  | McDermott et al. (2021); Radeva (2021)           |

## 2.4 Digital Forensic Investigation Lifecycle

A structured forensic investigation typically includes evidence identification, acquisition, preservation, examination, analysis, interpretation and presentation to the judicial authorities. Evidentiary integrity and compliance with forensic standards and legal requirements must be maintained for each phase. The use of mobile technologies, computer

vision and open-source intelligence has extended the possible types of digital evidence that can be used, especially in investigations of international and cyber-enabled crimes (Gabriele et al., 2021). However, investigators should be mindful of human and machine bias when assessing open-source information as the wrong interpretation can cause a

loss of evidentiary truth and fairness in court (McDermott et al., 2021). In addition, computer vision technologies have shown great promise in the context of digital image and multimedia evidence verification and accountability, in complex investigations (Radeva, 2021). All of these

developments indicate that a multi-faceted approach is needed for digital forensic investigations, with both parties implementing technological innovations and adhering to the digital forensic procedure and evidence management that meets legal requirements (Matijašević et al., 2024).

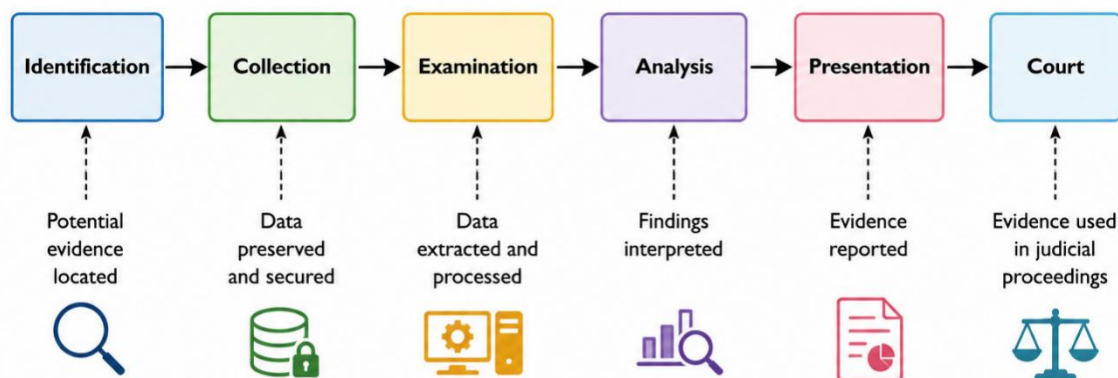


Figure 1: Digital Evidence Lifecycle

Figure 1 illustrates the digital evidence lifecycle from evidence identification and acquisition through forensic examination, legal evaluation, and courtroom presentation, highlighting the sequential stages necessary to preserve evidentiary integrity and admissibility.

### 3. Legal Framework Governing Digital Evidence

#### 3.1 Principles of Electronic Evidence Law

Digital evidence collected and used under the procedures of law have the same evidentiary value as traditional evidence under the criteria for legal

admissibility. These principles demand that evidence must be relevant, authentic, reliable and lawfully obtained before it can be considered by the court. As changing or copying electronic data is so easy, courts are looking for scientifically valid forensic methods that can verify that the electronic evidence is true and that it reflects the original data. So, the credibility of expert testimony has become a major issue to ensure that digital evidence meets acceptable legal standards to be admissible (Ward, 2020). At the same time, laws are still under development to strike a better balance between the efficiency of investigations and the protection of the right of individuals in criminal investigations (Stoykova, 2022).

#### 3.2 Authentication and Admissibility Requirements

Authentication confirms that the electronic evidence is authentic and has not been altered since being acquired and when it is introduced into evidence.

This typically includes forensic imaging, metadata validation, cryptographic hashing, documentation of acquisition process, and validation of analysis techniques. Studies have highlighted the need for structured legal frameworks that can assess the evidence produced using open-source forensic tools, which would increase judicial consistency and transparency in admissibility rulings (Ismail & Ariffin, 2025). Likewise, courts are increasingly faced with digital evidence that comes from leaked or hacked sources and must judiciously evaluate the lawfulness, authenticity, and evidentiary credibility of such evidence, before its admissibility in legal proceedings can be determined (Ferreira & Gromova, 2024).

#### 3.3 Chain of Custody and Evidence Integrity

Ensuring a seamless chain of custody is essential to the integrity and credibility of digital evidence through the investigative process. All steps of collecting, storing, examining, transferring, and presenting the evidence should be documented to show that the evidence has not been changed or contaminated. As more and more of our communications are dependent on communications metadata and electronic records, it is critical to have standardized evidence retention and documentation practices that are effective regardless of the rapidly changing communication technology (Robinson, 2023). Similarly, the introduction of new European legal procedures for the processing of cross-border electronic evidence has increased the accountability of the procedures and added more compliance obligations for investigators and judicial authorities (Sachoulidou, 2024). Table 2 provides an overview of the key legal considerations related to the

admissibility of digital evidence and their practical implications for ensuring the integrity and acceptance of the evidence in court.

Table 2. Core Legal Requirements for the Admissibility of Digital Evidence

| Legal principle          | Primary legal requirement                       | Importance for admissibility         | Practical implication                  | References              |
|--------------------------|-------------------------------------------------|--------------------------------------|----------------------------------------|-------------------------|
| Scientific reliability   | Validated forensic methodology                  | Demonstrates evidentiary credibility | Supports expert testimony              | Ward (2020)             |
| Authentication           | Verification of originality and integrity       | Confirms evidence authenticity       | Metadata, hashing, forensic validation | Ismail & Ariffin (2025) |
| Chain of custody         | Complete documentation of evidence handling     | Prevents tampering allegations       | Continuous evidence tracking           | Robinson (2023)         |
| Cross-border cooperation | Compliance with jurisdictional procedures       | Enables lawful evidence transfer     | International judicial coordination    | Sachoulidou (2024)      |
| Procedural fairness      | Protection of legal rights during investigation | Ensures judicial legitimacy          | Fair and transparent proceedings       | Stoykova (2022)         |

3.4 Expert Testimony and Scientific Reliability

In cases where specialized acquisition techniques or complex analytic processes are employed with electronic evidence, expert witnesses may be invaluable in assisting a judge and/or a jury to understand the technical results of the analysis. The use of the expert testimony should be accompanied by scientifically sound methodologies that can be independently verified to support the forensic conclusions. Thus, the evaluation of admissibility is now more heavily reliant upon the ability of experts to demonstrate methodological transparency, methodological reproducibility and compliance with accepted forensic practices than on their practical expertise (Ward, 2020). This emphasis on precision in method has given rise to governance models, ensuring accountability at all phases of digital evidence processing and evaluation in the courtroom

(Stoykova, 2024).

3.5 Comparative Legal Approaches

The national and international laws that regulate digital evidence are still evolving to keep pace with the development of technology, and the transnational nature of cybercrime. The complications of differences in the laws of data protection, privacy laws and the criminal process are often exacerbated by issues regarding the access to electronic evidence. Studies in comparative law show that there are a number of initiatives being pursued for the harmonization of these regulatory gaps including through international cooperation, legislative instruments and uniformity of evidentiary processes (Shurson, 2020). Recent developments,

such as the European Union's electronic evidence framework, have further reduced the uncertainty surrounding the law and provided clarity on the ways in which evidence will be secured beyond

national borders, but legal uncertainty and implementation challenges remain (Abraha, 2021; Tosza, 2024).

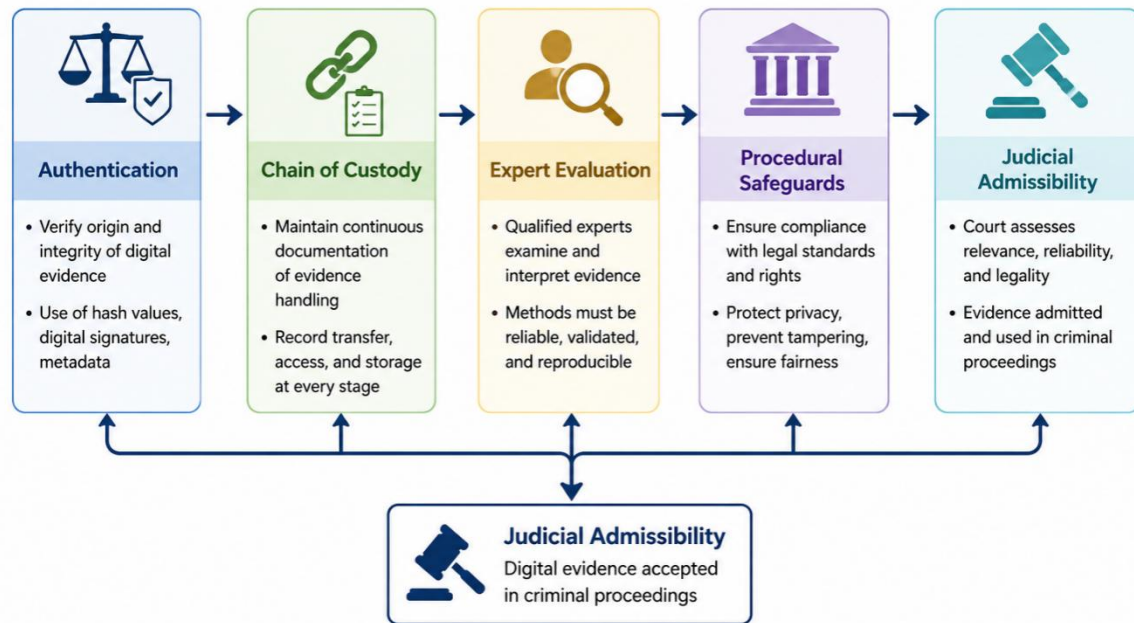


Figure 2: Legal Framework Governing Digital Evidence

Figure 2 illustrates the legal framework governing digital evidence, demonstrating the relationship between authentication, chain of custody, expert evaluation, procedural safeguards, and judicial admissibility within criminal proceedings.

#### 4. Reliability and Admissibility Challenges of Digital Evidence

##### 4.1 Technical Reliability and Evidence Integrity

The trust in electronic evidence is critical because it must be established that the electronic data are the true representation of the original data and have not been altered during the forensic process. Digital artifacts can be altered during the acquisition, transmission, storage, or analysis process, whereas integrity verification is an important step before a judicial determination, unlike physical evidence. Thus, more and more, the focus of forensic practice is on structured validation approaches that can assess the validity, reliability, and defensibility of forensic techniques prior to trial. One of such initiatives is the Reliability Validation Enabling Framework (RVEF), which aims to enhance trust in forensic results by providing standard procedures for validation (Stoykova & Franke, 2023). Similarly, blockchain chain-of-custody systems offer a way to create a verifiable history that is independent of the seller and makes it harder to tamper with evidence and improves the transparency of the procedures (Burri

et al., 2020).

##### 4.2 Human Factors and Cognitive Bias in Digital Forensics

While technical methodologies play an important role in digital forensic investigations, human judgement is still essential to evidence interpretation and reporting. Investigators can be influenced by cognitive bias, contextual information, confirmation bias, or preconceived investigative expectations that can potentially influence the objectivity of forensic conclusions. Such risks are especially relevant when analysts are examining dubious digital artifacts, or when reviewing a large amount of disparate data. Standardisation of analytical procedures, independent verification and structured decision-making are important aspects of forensic examinations, as cognitive and human factors studies demonstrate that these approaches can reduce the subjective influence of the examiner (Sunde & Dror, 2019). There have also been similar concerns about disparate access to technological resources and institutional expertise that can impact the collection and interpretation of digital evidence in various investigative environments (Koenig & Egan, 2021).

##### 4.3 Open-Source and Cloud-Based Digital Evidence

Open-source intelligence (OSINT), cloud platforms

and online repositories are sources of digital evidence that have proven useful during cybercrime investigations. But evidence collected from publicly available electronic spaces is vulnerable to a range of threats such as manipulation, changes to metadata, impersonation of the source, and inadequate documentation of provenance. For digital integrity, it is thus necessary to have systematic integrity verification procedures that can certify the authenticity of the digital data prior to its evidentiary use. Vulnerability assessments reveal that open-source investigations should involve standardised

mitigation strategies, to maintain the evidentiary integrity and minimise the risks of digital manipulation (Fiorella et al., 2021). In addition, expert interpretation is also becoming increasingly relevant in the presentation of complex online evidence to judicial bodies, especially if there is any doubt about technical authenticity in the context of legal proceedings (Gillett & Fan, 2023). Table 3 provides an overview of the key technical and legal considerations that affect the reliability and admissibility of digital evidence, along with some suggested mitigation strategies.

Table 3. Major Challenges Affecting the Reliability and Admissibility of Digital Evidence

| Challenge                   | Primary concern                           | Potential impact                    | Recommended mitigation                             | References                                             |
|-----------------------------|-------------------------------------------|-------------------------------------|----------------------------------------------------|--------------------------------------------------------|
| Evidence integrity          | Unauthorized alteration of digital data   | Reduced evidentiary credibility     | Validation frameworks and integrity verification   | Stoykova & Franke (2023)                               |
| Chain of custody            | Incomplete documentation                  | Challenges to admissibility         | Blockchain-based audit trails                      | Burri et al. (2020)                                    |
| Cognitive bias              | Subjective forensic interpretation        | Inconsistent investigative outcomes | Independent review and standardized protocols      | Sunde & Dror (2019)                                    |
| Open-source evidence        | Manipulated or unverifiable content       | Reduced evidentiary reliability     | Source authentication and digital integrity checks | Fiorella et al. (2021); Gillett & Fan (2023)           |
| Cross-border investigations | Jurisdictional and procedural differences | Delayed or restricted evidence use  | International legal coordination                   | Freeman & Vazquez Llorente (2021); Aksamitowska (2021) |

4.4 Cross-Border Collection and Jurisdictional Challenges

Often, investigators need to secure electronic evidence located in other legal jurisdictions because of the transnational nature of cybercrime. Investigations and cooperation between the courts are often hindered by disparities in procedural rules,

as well as in standards for gathering evidence and requirements for data protection and mutual legal assistance. Harmonized evidentiary procedures which allow for a timely exchange of evidence while preserving legal safeguards is therefore key to effective prosecution. International criminal

investigations have shown that effective digital evidence collection must be accompanied by a coordinated set of procedural standards that can help ensure that relevant information is preserved and collected from vast amounts of digital information without altering the evidentiary integrity of the information (Freeman & Vazquez Llorente, 2021). Comparative experiences from a number of European jurisdictions also suggest that a standard approach to investigations enhances the admissibility and consistency of digital evidence in domestic prosecutions for international crimes (Aksamitowska, 2021).

#### 4.5 Privacy, Due Process, and Procedural Fairness

The emerging opportunities with advanced

visualization technologies, digital reconstruction and automated evidence analysis have raised significant legal and ethical issues of procedural fairness. While these technologies can aid in the interpretation of evidence, if underlying assumptions and limitations are not properly disclosed, there may be an unintended effect on the perception of the judiciary when too much reliance is placed on digitally reconstructed material. In light of this, courts need to assess the reliability, transparency, and evidentiary value of technologically enhanced material before they can be admitted into criminal proceedings (Zarmsky, 2021). The ongoing technological advancements also show that combining blockchain, distributed storage, and smart contracts can enhance the long-term preservation of evidence collected from IoT devices and enable secure, transparent, and legally defensible evidence management practices (Rani et al., 2025).

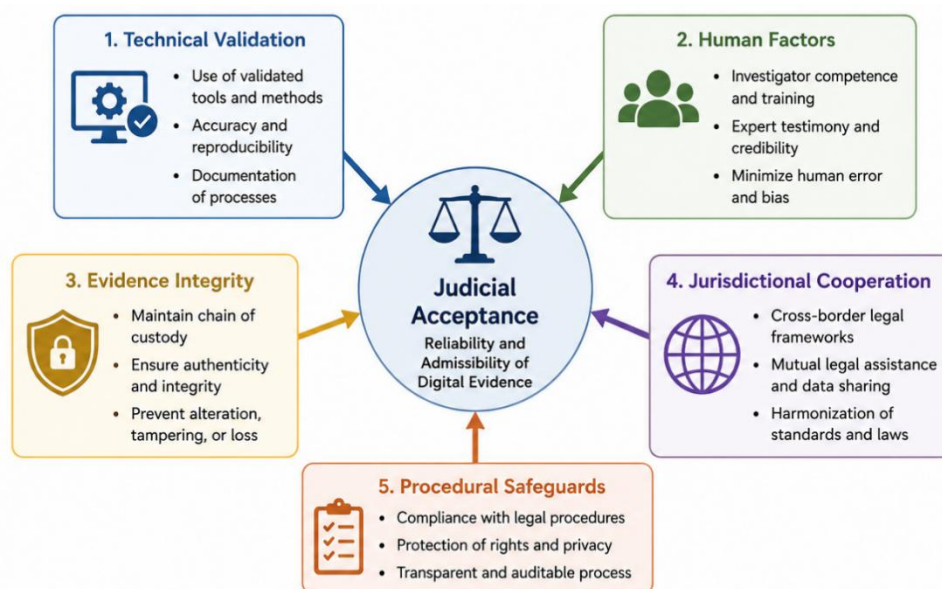


**Figure 3: Factors Influencing Reliability and Admissibility of Digital Evidence**

Figure 3 illustrates the major factors influencing the reliability and admissibility of digital evidence, demonstrating how technical validation, human factors, evidence integrity, jurisdictional cooperation, and procedural safeguards collectively determine judicial acceptance of electronic evidence.

#### 5. Emerging Technologies and Future Challenges

##### 5.1 Artificial Intelligence in Digital Forensic Investigations

The incorporation of artificial intelligence (AI) and machine learning has revolutionised digital forensic investigations, making the process faster, more efficient, and more accurate in identifying, categorizing, and analyzing digital evidence. Automated algorithms can reduce the number of

digital files that need to be manually processed and automate the identification of artifacts that may not be obvious to the human eye and prioritize them for analysis, helping to streamline the investigative workflow and achieve greater consistency across analysis. In this regard, these technologies are especially relevant in the context of cybercrime investigations, where they can help tackle the increasing complexity of the various data sources and attack techniques (Dunsin et al., 2024). In addition to traditional forensic uses, AI has proven to be highly promising in international crime investigations via automated image analysis, object recognition, and evidence correlation, allowing investigators to more efficiently process vast amounts of digital data (Freeman, 2021).

5.2 Blockchain for Evidence Preservation and Chain of Custody

Preservation, integrity and traceability are important properties of digital evidence that can be supported by blockchain technology. Blockchain offers a way to document each step of the evidence lifecycle in a transparent manner, as the records are immutable and time-stamped, minimizing the possibility of tampering and boosting courts' trust in electronic evidence. Some of the initial blockchain-based forensic models have showcased how blockchain technology can be used to manage digital evidence securely, using decentralized verification systems (Tian et al., 2019). Further studies have expanded these to the Internet of Things (IoT) space, where blockchain and forensic processes can be used to acquire, bind, and secure evidence in a distributed digital environment (Kumar et al., 2021). Recent research also suggests that blockchain could be used to improve the preservation of multimedia evidence and support forensic case management, providing a way to ensure accountability and long-term integrity of the evidence (Malik & Sharma, 2023; Patil et al., 2024).

5.3 Internet of Things (IoT) and Smart Device Evidence

With the proliferation of IoT devices, investigators have access to more and a wider variety of digital evidence. Electronic records are constantly created in smart homes, wearable technologies, connected cars, industrial sensors, and health care technologies that could help criminal investigations. The distributed nature of IoT ecosystems, however, brings with it a significant number of challenges with respect to forensics, such as heterogeneous device architectures, limited storage capacity, volatile data, and complex acquisition procedures. To make efficient the forensic processes, selective techniques for evidence acquisition and data reduction that preserve relevant information without jeopardizing the evidentiary reliability are thus needed (Montasari et al., 2020). The recent development of preservation frameworks that incorporate blockchain, distributed storage, and smart contracts further underscores the potential for securing IoT-generated evidence while ensuring authenticity and transparency across the entire forensic lifecycle (Rani et al., 2025). Table 4 provides a summary of some of the key emerging technologies that impact digital evidence, their uses in forensics, challenges, legal relevance, and literature.

Table 4. Emerging Technologies and Their Implications for Digital Evidence

| Emerging technology     | Primary forensic application               | Key challenge                     | Potential legal benefit                   | References                                                                          |
|-------------------------|--------------------------------------------|-----------------------------------|-------------------------------------------|-------------------------------------------------------------------------------------|
| Artificial intelligence | Automated evidence analysis                | Algorithm transparency            | Faster and more consistent investigations | Dunsin et al. (2024); Freeman (2021)                                                |
| Blockchain              | Evidence preservation and chain of custody | Integration with existing systems | Enhanced integrity and traceability       | Tian et al. (2019); Kumar et al. (2021); Malik & Sharma (2023); Patil et al. (2024) |
| Internet of Things      | Smart device evidence collection           | Distributed data environments     | Broader evidentiary coverage              | Montasari et al. (2020); Rani et al. (2025)                                         |

|                    |                               |                                         |                                                 |                                                                |
|--------------------|-------------------------------|-----------------------------------------|-------------------------------------------------|----------------------------------------------------------------|
| Deepfake detection | Verification of digital media | Increasing realism of synthetic content | Improved assessment of evidentiary authenticity | Chesney & Citron (2019); Verdoliva (2020); Mirsky & Lee (2021) |
|--------------------|-------------------------------|-----------------------------------------|-------------------------------------------------|----------------------------------------------------------------|

#### 5.4 Deepfakes and Synthetic Digital Evidence

Among the latest concerns in the realm of digital evidence, deepfake technology stands out as a key threat. The ability to create artificially designed images, audio recordings and videos to simulate real people with increasing realism gives it significant potential for criminal investigations and judicial proceedings. The growing prevalence of deepfake creation has led to worries about misinformation, the manipulation of identities, and the ability to create fabricated digital evidence that could deceive investigators and courtrooms (Chesney & Citron, 2019). Media forensics has thus evolved to detect synthetic content in an automated fashion by looking for inconsistencies in the visual, acoustic, and metadata properties (Verdoliva, 2020). In addition, extensive surveys have shown that machine-learning algorithms and forensic analysis methods have been proposed one after another, which is increasingly being proven to be effective for deepfake detection (Mirsky & Lee, 2021). Evidence further suggests that using a combination of human and machine-based detection is more effective than either one alone, which could be a helpful strategy in future litigations (Groh et al., 2022). The ongoing advancement of

deepfake technology thus highlights the importance of flexible approaches to forensic analysis and stronger regulations that can ensure trust in digital evidence (Westerlund, 2019).

#### 5.5 Future Policy Directions and Research Opportunities

The rapid pace of growth of AI, blockchain, IoT and synthetic media highlights the need for future digital forensic systems to be technologically innovative with harmonized legal frameworks and internationally recognised standards in the field. A greater emphasis needs to be placed on interoperable evidence management systems, open validation of new technologies, uniform training for investigators, and better working relationships among all forensic practitioners, legal practitioners, technology developers and policy makers. Further studies should also focus on developing explainable forensic algorithms, robust evidence preservation methods, and flexible legal frameworks that can effectively cope with the dynamic nature of cybercrime while ensuring procedural justice and trust in digital legal systems.

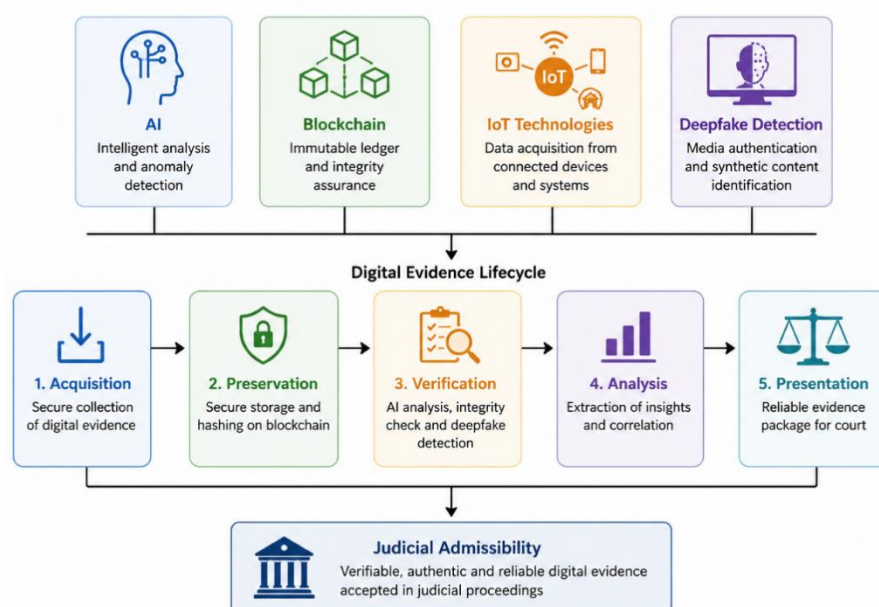


**Figure 4: Integrated Framework of Emerging Technologies in Digital Forensic Ecosystem**

Figure 4 presents an integrated framework illustrating how artificial intelligence, blockchain, IoT technologies, and deepfake detection collectively contribute to secure evidence acquisition, preservation, verification, and judicial admissibility within future digital forensic ecosystems.

## 6. Conclusion

Digital evidence is an invaluable tool in the digital landscape and is used widely in cybercrime investigations for the identification of offenders, crime scene reconstruction and supporting judicial decision making. But the value of evidence depends on not only the ability to utilize the technology but also to establish authenticity, integrity, reliability, and

procedural compliance during the forensic process. In this review, the growing sophistication of cybercrime, the growth of cloud computing, the Internet of Things (IoT) and cross-border cyber environments are identified as creating legal and technical challenges which are often out of the scope of traditional law enforcement and investigative structures. As well, the review shows that strong chain-of-custody protocols, scientifically sound forensic analysis methods, consistent evidence handling practices and qualified expert testimony continue to be the foundation for the admissibility of digital evidence in court. Significant opportunities exist to enhance evidence acquisition, preservation, verification, and analysis through emerging technologies, such as artificial intelligence, blockchain, and advanced media forensic techniques. However, they should be done under clear and transparent law and ethical principles that protect and ensure procedure, confidentiality and public trust in the judicial process. Finally, the evolving needs and challenges of digital evidence call for continued collaboration and cooperation among legal practitioners, forensic experts, researchers, technology suppliers, and policymakers. In a rapidly digitalizing society, harmonization of standards with international partners, enhanced forensic validation, and technological innovation in a responsible manner will be crucial to ensure that digital evidence is reliable, legally valid and can contribute to effective cybercrime investigations.

## References

1. Abraha, H. H. (2021). Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. *International Journal of Law and Information Technology*, 29(2), 118-153.
2. Akinbi, A., & Berry, T. (2020). Forensic investigation of google assistant. *SN Computer Science*, 1(5), 272.
3. Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: Lessons learned from germany, sweden, finland and the netherlands. *Journal of International Criminal Justice*, 19(1), 189-211.
4. Burri, X., Casey, E., Bolle, T., & Jaquet-Chiffelle, D. O. (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation*, 33, 300976.
5. Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian journal of forensic sciences*, 51(6), 649-664.
6. Casey, E., Ribaux, O., & Roux, C. (2019). The Kodak syndrome: risks and opportunities created by decentralization of forensic capabilities. *Journal of forensic sciences*, 64(1), 127-136.
7. Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *Ieee Access*, 10, 25464-25493.
8. Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014.
9. Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.*, 107, 1753.
10. Costantini, F., Galvan, F., De Stefani, M. A., & Battiato, S. (2020). Assessing information quality in IoT forensics: Theoretical framework and model implementation. *arXiv preprint arXiv:2012.14663*.
11. D'Alessandra, F., & Sutherland, K. (2021). The promise and challenges of new actors and new technologies in international justice. *Journal of International Criminal Justice*, 19(1), 9-34.
12. 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), 1-22.
13. Ferreira, D. B., & Gromova, E. A. (2024). Digital Evidence: The Admissibility of Leaked and Hacked Evidence in Arbitration Proceedings. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, 37(3), 903-922.
14. Fiorella, G., Godart, C., & Waters, N. (2021). Digital integrity: Exploring digital evidence vulnerabilities and mitigation strategies for open source researchers. *Journal of International Criminal Justice*, 19(1), 147-161.
15. Freeman, L. (2021). Weapons of war, tools of justice: using artificial intelligence to investigate international crimes. *Journal of International Criminal Justice*, 19(1), 35-53.
16. Freeman, L., & Vazquez Llorente, R. (2021). Finding the signal in the noise: International criminal evidence and procedure in the digital age. *Journal of International Criminal*

- Justice, 19(1), 163-188.
17. Gabriele, C., Matheson, K., & Llorente, R. V. (2021). The role of mobile technology in documenting international crimes: The affaire Castro et Kizito in the Democratic Republic of Congo. *Journal of International Criminal Justice*, 19(1), 107-130.
18. Gillett, M., & Fan, W. (2023). Expert evidence and digital open source information: Bringing online evidence to the courtroom. *Journal of International Criminal Justice*, 21(4), 661-693.
19. Groh, M., Epstein, Z., Firestone, C., & Picard, R. (2022). Deepfake detection by human crowds, machines, and machine-informed crowds. *Proceedings of the National Academy of Sciences*, 119(1), e2110013119.
20. Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, 20(9), e0331683.
21. Klasén, L., Fock, N., & Forchheimer, R. (2024). The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic science international*, 362, 112133.
22. Koenig, A., & EGAN, U. (2021). Power and privilege. *Journal of International Criminal Justice*.
23. Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Generation Computer Systems*, 120, 13-25.
24. Malik, A., & Sharma, A. K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *Journal of Information Security and Applications*, 77, 103579.
25. Matijašević, J., Bingulac, N., & Marinković, D. (2024). DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS-CHALLENGES AND SOLUTIONS. *Law-Theory and Practice*, 41(4), 18-33.
26. McDermott, Y., Koenig, A., & Murray, D. (2021). Open source information's blind spot: human and machine bias in international criminal investigations. *Journal of International Criminal Justice*, 19(1), 85-105.
27. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM computing surveys (CSUR)*, 54(1), 1-41.
28. Montasari, R., Hill, R., Montaseri, F., Jahankhani, H., & Hosseinian-Far, A. (2020). Internet of things devices: digital forensic process and data reduction. *International Journal of Electronic Security and Digital Forensics*, 12(4), 424-436.
29. Moussa, A. F. (2021). Electronic evidence and its authenticity in forensic evidence. *Egyptian Journal of Forensic Sciences*, 11(1), 20.
30. Onwubiko, D. C., & Eboibi, F. E. (2020). The application of forensics examination in crime-related prosecution: The need for standardization and a recognized model in Nigeria. *Digital Evidence & Elec. Signature L. Rev.*, 17, 83.
31. Patil, H., Kohli, R. K., Puri, S., & Puri, P. (2024). Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences*, 14(1), 12.
32. Radeva, E. (2021). The potential for computer vision to advance accountability in the Syrian crisis. *Journal of International Criminal Justice*, 19(1), 131-146.
33. Rani, D., Gill, N. S., Gulia, P., Yahya, M., Ahanger, T. A., Hassan, M. M., ... & Shukla, P. K. (2025). A secure digital evidence preservation system for an iot-enabled smart environment using ipfs, blockchain, and smart contracts. *Peer-to-Peer Networking and Applications*, 18(2), 5.
34. Reedy, P. (2020). Interpol review of digital evidence 2016-2019. *Forensic Science International: Synergy*, 2, 489-520.
35. Reedy, P. (2023). Interpol review of digital evidence for 2019-2022. *Forensic Science International: Synergy*, 6, 100313.
36. Robinson, G. (2023). Targeted Retention of Communications Metadata: Future-proofing the Fight Against Serious Crime in Europe?. *European Papers-A Journal on Law and Integration*, 2023(2), 713-740.
37. Sachoulidou, A. (2024). Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial'cooperation. *New Journal of European Criminal Law*, 15(3), 256-274.
38. Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, 28, S22-S29.
39. Shurson, J. (2020). Data protection and law enforcement access to digital evidence: Resolving the reciprocal conflicts between EU and US law. *International Journal of Law and Information Technology*, 28(2), 167-184.
40. Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, 105575.
41. Stoykova, R. (2022). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *University of Groningen Faculty of Law Research Paper*, (31).
42. Stoykova, R. A. (2024). A new right to procedural accuracy: A governance model for digital evidence in criminal proceedings. *Computer Law & Security Review*, 55, 106040.
43. Stoykova, R., & Franke, K. (2023). Reliability validation enabling framework (RVEF) for digital forensics in criminal investigations. *Forensic Science International: Digital Investigation*, 45, 301554.
44. Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital*

- investigation, 29, 101-108.
45. Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. *Information Sciences*, 491, 151-165.
  46. Tosza, S. (2024). Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems. *Studia Iuridica Lublinensia*, 33(5), 237-260.
  47. Verdoliva, L. (2020). Media forensics and deepfakes: an overview. *IEEE journal of selected topics in signal processing*, 14(5), 910-932.
  48. Ward, T. (2020). Explaining and trusting expert evidence: What is a 'sufficiently reliable scientific basis'?. *The International Journal of Evidence & Proof*, 24(3), 233-254.
  49. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology innovation management review*, 9(11).
  50. Zarnsky, S. (2021). Why seeing should not always be believing: Considerations regarding the use of Digital reconstruction Technology in International Law. *Journal of International Criminal Justice*, 19(1), 213-225.