



OPEN ACCESS

Volume: 5

Issue: 4

Month: October

Year: 2026

ISSN: 2583-7117

Published: 05.10.2026

Citation:

Sheena Razdan "Digital Evidences, Cyber Forencics & Admissibility In Criminal Trials" International Journal of Innovations in Science Engineering and Man-
agement, vol.5, no.4, 2026, pp. 39-43

DOI:

10.69968/ijisem.2026v5i439-43



This work is licensed under a Creative
Commons Attribution-Share Alike 4.0
International License

Digital Evidences, Cyber Forencics & Admissibility In Criminal Trials

Sheena Razdan¹

¹Assistant Professor of Law MKPM RV Institute of legal studies 22nd cross, 3rd block, Jayanagar, Ban-
galore, Karnataka, India

Abstract

In Today's Digitalization world cyberspace has become an important area without which our work is not completed in any domain. New tools and techniques for gathering, analysing, and preserving digital evidence have emerged as a result of the expansion of digital data. Digital evidence, privacy, and data protection are only a few of the many concerns that have arisen in the field of digital forensics. Another major difficulty is the complicated legal framework for gathering and evaluating digital evidence. Despite these difficulties, digital evidence has developed into a vital instrument for the legal system and law enforcement, offering vital proof in both criminal and civil proceedings. Cyber forensics, as a specialized branch of forensic science, plays a crucial role in identifying, collecting, preserving, analyzing, and presenting such digital evidence in a manner that maintains its integrity and evidentiary value. Because of the rapid advancement of digital technology, cybercrimes increasingly represent a serious threat to society. Digital evidence obtained from computer devices is a major component of cybercrime investigation. However, proving that digital evidence is admissible in Indian courts might be challenging. For the investigation of cybercrime in India, digital evidence is crucial. The admissibility of digital evidence is governed by both "the Information Technology Act of 2000 and the Bharatiya Sakshya Adhiniyam, 2023 (BSA)". The Indian Supreme Court has set specific guidelines for the admissibility of electronic evidence in court. In the fight against cybercrime, Indian courts have suddenly realised the importance of digital evidence. In conclusion, India's recognition of digital evidence as acceptable proof is a positive move in the fight against the growing worldwide problem of cybercrime. To effectively address cybercrime, India must continue to advance its legal system, technological capabilities, and professional understanding.

Keywords; Data Protection, Privacy, Forensics Evidence, Cybercrime, Digital Evidence.

INTRODUCTION

Traditional rules of evidence were designed for a world of paper, ink and eyewitnesses. The digital revolution has disrupted that world: financial fraud is committed through spoofed emails, harassment through social media, terrorism is planned over encrypted messaging apps, and even ordinary offences like murder or theft are frequently solved using call location data or CCTV footage. Digital evidence is now central — sometimes decisive — in criminal trials. It is a common feature of the current digital age that the very nature of criminal acts has changed. Digital devices and virtual networks have become a key tool in carrying out conspiracy crimes, financial scams, cyber warfare launched by nation-states, terror acts, and inter-personal crimes. Hence, digital evidences such as emails, social media communications, database hosted on cloud infrastructure, coordinates, metadata of instant messaging application, and server logs have gained prominence and form the base of today's criminal investigation. Any type of information kept on a device that may be used to demonstrate what transpired during a crime is considered "digital evidence". "Emails, texts, files, videos, and even postings on social media" might fall under this category. Digital evidence may assist identify who did what, when, and how, just like fingerprints or DNA can in routine investigations.

Investigating crimes that occur in the digital realm is known as cyber forensics. To ensure that everything is done correctly, professionals in this industry meticulously gather and examine digital evidence using specialised tools and adhere to legal regulations. Police and solicitors can better grasp how a cybercrime occurred and who is at fault thanks to their efforts.

Investigating crimes that occur in the digital realm is known as cyber forensics. In order to ensure that everything is done correctly, professionals in this sector meticulously gather and examine digital evidence using specialised tools and adhere to legal rules. Police and solicitors can better grasp how a cybercrime occurred and who is at fault thanks to their efforts. These are more crucial tools than ever. A single data breach or hack may result in significant harm since so much of our personal and corporate information is stored online.

BACKGROUND

From the mid-1970s onwards, personal computers became popular. In the late 1990s and early 2000s, the public availability of the internet was seen as an important step in digitizing information sharing and communication. The widespread use of smartphones and tablet devices allowed digitalization to be personalized and accessible from anywhere.

Digitalization started with the development and use of electronic computers in a historical process of humanity. The first digital computers started to be developed in the first half of the 20th century and continuously improved with technological advances. For example, Alan Turing's Turing machine theory laid the foundation for today's computers. Digitalization is a concept in which the advancement of technology and the impact of digital technologies on society, economy and culture differ from country to country. The levels of digitalization between countries vary depending on many factors.

The digitalization levels of countries are closely related to their technological infrastructure. Infrastructure elements such as internet access, mobile networks, fast data transmission and information technologies deeply affect digitalization. By committing greater resources for digitalisation, wealthy nations are investing more to raise their levels of digitalisation. Digitalization is a process where society needs to accept and embrace these changes. The society's approach to technology and its desire for digitalization affect the level of digitalization of the country. At the same time, the cultural values and norms of countries

affect the digitalization process. Some countries are more attached to traditional values and this increases the potential to influence the pace of digitalization.

STATEMENT OF THE PROBLEM

"Digital evidence" is central to modern criminal trials, yet it is inherently fragile, easily tampered with, and difficult to authenticate using standards designed for physical and documentary evidence. Legal systems, including India's, continue to grapple with unclear statutory language, inconsistent judicial interpretation, and a lack of standardized forensic protocols, all of which compromise "the reliability of digital evidence" presented in court. Compounding this is a shortage of technical expertise among judges, prosecutors, and defense counsel, and the cross-border nature of much digital data, which complicates lawful collection and admissibility. This creates uncertainty in outcomes and raises the risk that either unreliable evidence is admitted, or reliable evidence is wrongly excluded on technical grounds — both of which threaten the fairness and accuracy of criminal adjudication.

OBJECTIVES OF THE STUDY

- 1 To examine the concept and nature of "digital evidence" and understand how it differs from traditional forms of evidence in criminal investigations.
- 2 To analyze the process of cyber forensics — including "collection, preservation, and chain of custody" — and assess whether current forensic practices ensure "the integrity and reliability of digital evidence".
- 3 To study "the legal framework governing the admissibility of digital evidence in criminal trials" and evaluate its adequacy in addressing challenges posed by emerging technology.
- 4 To identify the challenges and gaps faced by courts, investigators, and prosecutors in authenticating and relying on digital evidence, including issues of tampering, technical expertise, and jurisdiction.
- 5 To suggest legal and procedural reforms for strengthening the framework governing digital evidence, ensuring its fair, accurate, and consistent admissibility in criminal proceedings.

RESEARCH METHODOLOGY

This study adopts a doctrinal, non-empirical method of legal research. It relies on the analysis of primary legal sources — including "the Indian Evidence Act, 1872, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023", and landmark judicial decisions — supplemented by secondary sources such as textbooks, law

journal articles, government and law commission reports, and reputed online legal databases. The research is descriptive, analytical, and comparative in nature: descriptive in explaining the concepts of digital evidence and cyber forensics, analytical in critically examining statutory provisions and case law, and comparative in briefly referencing foreign approaches such as “the United States' Federal Rules of Evidence and the United Kingdom's Police and Criminal Evidence Act, 1984”. The study is confined to legal and procedural analysis and does not involve independent forensic laboratory testing or empirical field data collection.

CONCEPT OF DIGITAL EVIDENCE

Any information that may be used as evidence in a court of law and is kept or communicated in binary form is referred to as digital evidence. It includes, but is not limited to, emails, text and instant messages, digital images and videos, browser history, metadata, GPS location data, server logs, social media content, and data stored on hard drives, mobile devices, or cloud servers. Under Indian law, such material generally falls within the definition of an “electronic record” under “Section 2(1)(t) of the Information Technology Act, 2000”, and is treated as a form of “documentary evidence under the Indian Evidence Act, 1872” (now the Bharatiya Sakshya Adhiniyam, 2023).

Digital evidence possesses certain distinctive characteristics that separate it from traditional evidence:

- Intangibility — it exists as data rather than a physical object, and can only be perceived through a device or software interface.
- Volatility — certain forms of data (e.g., RAM contents, live network traffic) exist only momentarily and can be lost if not captured immediately.
- Alterability — digital data can be modified, deleted, or fabricated without leaving visible signs, unless proper forensic safeguards are used.
- Duplicability — The dilemma of which copy qualifies as the “original” for evidential purposes is raised by the fact that digital evidence may be flawlessly replicated.
- Cross-jurisdictional storage — data may be stored on servers located outside the territorial jurisdiction of the investigating agency or trial court.

CYBER FORENSICS: PROCESS AND CHALLENGES

Cyber forensics (or digital forensics) is the scientific process of identifying, collecting, preserving, analyzing, and

presenting digital evidence in a manner that maintains its evidentiary integrity. The process broadly follows several stages:

- Identification — locating potential sources of digital evidence, such as computers, mobile phones, servers, or cloud accounts.
- Collection and Imaging — creating a bit-by-bit forensic image (clone) of the storage media, ensuring the original device is not altered during the process.
- Preservation — preserving the data's integrity by using cryptographic hashing (such as MD5 or SHA-256), which enables confirmation that the data hasn't been changed after it was collected.
- Analysis — examining the imaged data using forensic software to recover deleted files, trace user activity, or establish timelines.
- Documentation and Reporting — recording every step taken, including who handled the evidence and when, to establish an unbroken chain of custody.
- Presentation — producing the findings, along with the required certification, before the court in an admissible and comprehensible form.

Despite established international standards (such as those of the ISO/IEC 27037 guideline on identification, collection, and preservation of digital evidence), practical application varies widely between agencies. In many jurisdictions, including India, forensic laboratories are unevenly resourced, chain-of-custody documentation is inconsistent, and personnel may lack specialized training — all of which can be exploited by the defense to challenge “the reliability of the evidence” at trial.

LEGAL FRAMEWORK GOVERNING ADMISSIBILITY IN INDIA

Statutory Provisions

Before the Information Technology Act of 2000, Sections 65A and 65B of the Indian Evidence Act of 1872 controlled “the admissibility of electronic evidence in India”. Section 65B created a special procedure for “the admissibility of electronic records” as secondary evidence, requiring a certificate under Section 65B(4) identifying the electronic record, describing the manner of its production, and confirming the conditions under which it was produced. “Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023”, which went into effect with the other new criminal law codes, essentially re-enacted this clause.

“The Information Technology Act, 2000” further defines “electronic record” under Section 2(1)(t), and Section 79A empowers the Central Government to notify an “Examiner

of Electronic Evidence" for the purposes of providing expert opinion on electronic evidence under Section 79A. Procedural safeguards for search, seizure, and investigation involving electronic devices are found in "the Code of Criminal Procedure, 1973" (now the Bharatiya Nagarik Suraksha Sanhita, 2023).

Judicial Evolution

The judicial treatment of "electronic evidence in India" has evolved significantly over two decades:

- "State (NCT of Delhi) v. Navjot Sandhu (2005)" — The Supreme Court initially held that secondary electronic evidence could be admitted even without a Section 65B certificate, if its authenticity could otherwise be established, for instance through oral testimony.
- "Anvar P.V. v. P.K. Basheer (2014)" — Navjot Sandhu was overturned by a three-judge panel, which concluded that electronic records' admissibility as secondary evidence was dependent on conformity with Section 65B(4); without the certificate, such evidence could not be trusted, independent of other authentication evidence.
- "Shafhi Mohammad v. State of Himachal Pradesh (2018)" — A two-judge bench sought to relax this requirement, holding that the certificate requirement was procedural and could be waived where the device in question was not in the possession of the party seeking to rely on it, causing conflicting interpretations across courts.
- "Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)" — A three-judge bench resolved the conflict, reaffirming Anvar P.V. as the correct position and clarifying that Section 65B(4) certification is mandatory, though a court may, in appropriate cases, order the production of the certificate at a later stage or summon it from the person in control of the relevant device.

This trajectory illustrates how the judiciary has had to repeatedly recalibrate the balance between insisting on a rigorous procedural safeguard and ensuring that genuine evidence is not excluded merely due to practical difficulty in obtaining certification, particularly in cases where the device is in the custody of a third party or a foreign entity.

KEY CHALLENGES IN ADMISSIBILITY

Chain of Custody Failures — Gaps or inconsistencies in documenting who accessed, handled, or transferred digital evidence weaken its credibility and are a common ground for challenge by the defense.

Certification Hurdles — Practical difficulty in obtaining a Section 65B(4) certificate, particularly where the relevant device or server is controlled by a third party, service provider, or foreign entity, can delay or derail otherwise reliable evidence.

Lack of Forensic Standardization — The absence of uniform national protocols for imaging, hashing, and analysis across forensic laboratories affects the consistency and reproducibility of forensic findings.

Technical Capacity Gaps — Judges, prosecutors, and defense counsel often lack the technical background needed to critically assess forensic methodology, leading to either uncritical acceptance or unwarranted rejection of expert findings.

Cross-Border Data Access — Data hosted on servers outside India (as with many cloud and social media platforms) requires mutual legal assistance treaties (MLATs) or platform cooperation, both of which are often slow and unpredictable.

Privacy and Rights Concerns — Aggressive collection of digital evidence, including from personal devices and cloud accounts, raises constitutional concerns regarding the right to privacy recognized in Justice "K.S. Puttaswamy v. Union of India (2017)", requiring courts to balance probative value against invasiveness.

SUGGESTIONS AND RECOMMENDATIONS

Enact clearer statutory guidance on when and how the Section 61–63 (BSA) certification requirement may be relaxed, particularly in cases involving third-party or foreign-held data.

Develop and mandate a uniform national protocol for digital evidence collection, imaging, and hashing, applicable to all state and central forensic laboratories.

Establish specialized cyber forensic units and fast-track digital evidence certification mechanisms within investigating agencies.

Introduce mandatory training modules on digital evidence and forensic methodology for judges, public prosecutors, and defense counsel.

Strengthen international cooperation mechanisms, including faster MLAT processing and direct cooperation frameworks with major technology platforms, to address cross-border evidence challenges.

Encourage judicial guidelines or a practice manual, akin to those in other jurisdictions, to standardize how courts assess “the weight and reliability of digital evidence”.

CONCLUSION

The modern criminal justice system now relies heavily on digital evidence, but "the legal and forensic infrastructure" needed to manage it consistently is still being developed. India's judicial journey from Navjot Sandhu to Arjun Panditrao Khotkar reflects a continuing effort to strike the right balance between procedural rigor and practical accessibility. However, persistent gaps in forensic standardization, technical capacity, and cross-border cooperation mean that “the admissibility of digital evidence in criminal trials” remains inconsistent and, at times, uncertain. A coordinated approach — combining legislative clarity, forensic standardization, and capacity building among judicial and prosecutorial actors — is essential to ensure that digital evidence serves its intended purpose:

helping courts arrive at accurate and fair verdicts in an increasingly digital world.

REFERENCES

- [1] Indian Evidence Act, 1872.
- [2] Information Technology Act, 2000.
- [3] Bharatiya Sakshya Adhiniyam, 2023.
- [4] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600.
- [5] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- [6] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
- [7] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- [8] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- [9] Pavan Duggal, Cyberlaw: The Indian Perspective.
- [10] Ratanlal & Dhirajlal, The Law of Evidence.
- [11] Law Commission of India Reports (relevant reports on evidenc