JOURNAL OF INTERNATIONAL LAW, POLITICS AND SOCIETY
An International Open Access Double Blind Peer Reviewed
ISSN No.: 3108-0464

Volume 2 | Issue 1 (Jan.-Mar.) | 2026 Art. 14

Electronic Evidence in Criminal Trials: Understanding Admissibility Standards and Authentication Requirements

Shivyanshu Gupta
Law Student,
B.A.LL.B. (Hons), 5th Year
Amity Law School, Amity University, Lucknow

Dr. Jyotsna Singh
Assistant Professor,
Amity Law School, Amity University, Lucknow

Recommended Citation
Shivyanshu Gupta and Dr. Jyotsna Singh, *Electronic Evidence in Criminal Trials: Understanding Admissibility Standards and Authentication Requirements*, 2 JILPS 250-262 (2026).
Available at www.jilps.in/archives/.

Electronic Evidence in Criminal Trials: Understanding Admissibility Standards and Authentication Requirements

Shivyanshu Gupta
Law Student,
B.A.LL.B. (Hons), 5th Year
Amity Law School, Amity University, Lucknow

Dr. Jyotsna Singh
Assistant Professor,
Amity Law School, Amity University, Lucknow

Manuscript Received	Manuscript Accepted	Manuscript Published
02 Mar. 2026	04 Mar. 2026	05 Mar. 2026

ABSTRACT

Electronic evidence has emerged as a cornerstone of modern criminal adjudication in India. The enactment of the Bharatiya Sakshya Adhiniyam (BSA), 2023, replacing the Indian Evidence Act of 1872, marks a transformative shift by elevating electronic records from secondary to primary evidence. This paper examines the evolving legal framework governing the admissibility and authentication of electronic evidence in Indian criminal proceedings. It analyses the Section 65B certification mechanism, the landmark judicial precedents in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, and the dual certification requirement introduced under BSA 2023. The paper further interrogates the practical challenges that impede the effective deployment of digital proof in courtrooms — including the legal-technical expertise divide, cross-border jurisdictional complexity, inadequate forensic infrastructure, and concerns regarding fair trial rights. The paper concludes that while the legislative reforms are commendable, their implementation requires urgent investment in judicial training, standardized forensic protocols, and international cooperation frameworks.

KEYWORDS

Electronic Evidence, Bharatiya Sakshya Adhiniyam 2023, Section 65B, Digital Forensics, Authentication, Chain of Custody, Criminal Trials, Cybercrime, Fair Trial

I. INTRODUCTION

Electronic evidence has fundamentally reshaped the manner in which crimes are proved in modern courtrooms. The surge in cybercrime across

India—Karnataka alone registers over sixteen percent of all reported cases nationally[1] underscores the urgency of a coherent legal framework for digital proof. The Bharatiya Sakshya Adhiniyam (BSA), 2023, enacted to replace the 150-year-old Indian Evidence Act of 1872, represents the most significant legislative milestone in this domain. By formally recognizing electronic records as primary evidence, it resolves long-standing judicial uncertainty that had for decades complicated the prosecution of digital crimes.

Despite this legislative advance, the operationalization of digital evidence in criminal trials remains fraught with difficulty. Courts, lawyers, and investigating agencies confront a spectrum of challenges: from authenticating evidence extracted from inaccessible or encrypted devices, to managing cross-border data requests from multinational technology companies. A study of eighty-seven court rulings found substantial confusion across Indian courts regarding the admissibility standards for digital evidence[2] a finding that reflects the persistent gap between legislative intent and courtroom reality.

This paper proceeds in four substantive parts. Part II maps the landscape of electronic evidence, cataloguing its principal categories and forensic significance. Part III analyzes the admissibility framework, tracing the evolution from Section 65B of the Indian Evidence Act to the BSA 2023 regime. Part IV examines authentication requirements and forensic validation standards. Part V identifies the practical challenges that persist in criminal trial proceedings, before the paper concludes with reform recommendations.

II. UNDERSTANDING ELECTRONIC EVIDENCE: TYPES AND SCOPE

Any probative information stored or transmitted in digital form constitutes electronic evidence.[3] Courts recognize numerous categories of digital material, each leaving distinct and analyzable traces. Understanding the taxonomy of electronic evidence is a prerequisite to evaluating the legal standards that govern its admissibility.

[1] Karnataka accounts for over 16% of all cybercrime cases registered nationally. See Press Trust of India, Karnataka Tops Cyber Crime List, The Hindu (2023); Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India) [hereinafter BSA 2023].

[2] Vintage Legal, Digital Evidence Admissibility in Indian Courts: Bridging Legal Gaps in the Age of Cybercrime (2024), https://www.vintagelegalvl.com/post/digital-evidence-admissibility-in-indian-courts-bridging-legal-gaps-in-the-age-of-cybercrime.

[3] Eclipse Forensics, Types and Sources of Digital Evidence (2024), https://eclipseforensics.com/types-and-sources-of-digital-evidence/.

A. Digital Documents and Computer Data

Document files—including word processing files, spreadsheets, presentations, and PDFs—constitute a primary category of electronic evidence. These files carry embedded metadata providing timestamps, authorship, and revision history that can be critical to establishing authenticity.[4] Data stored on computers, smartphones, tablets, printers, and internet-connected devices all constitute potential evidence. Digital footprints may be active or passive: an active digital footprint encompasses deliberately shared content such as social media posts and uploaded images, while a passive footprint consists of data generated incidentally, such as browsing history and location logs.[5]

B. Electronic Communications

Electronic mail reveals communication patterns, transactional records, and attachments that frequently prove pivotal in criminal investigations. Messaging platforms such as WhatsApp, Telegram, Facebook Messenger, and Viber contain timestamped texts, media files, and hyperlinks that have featured centrally in a growing body of criminal case law.[6] Cloud-based backup systems provide forensic investigators access to an average of one thousand to fifteen hundred or more of the last text messages transmitted from a particular device[7], a volume that greatly expands the evidentiary horizon available to investigators.

C. Multimedia Evidence

Digital photographs and videos serve as powerful forms of proof. Metadata embedded in image files—including timestamps and GPS geolocation coordinates—establishes the authenticity and contextual circumstances of media files.[8] Video footage sourced from private businesses, residential cameras, and law enforcement surveillance systems, together with audio recordings from telephone calls and voicemail, constitutes the principal forms of multimedia evidence in

[4] Forensic Science Simplified, How Digital Evidence Works (2024), https://www.forensicsciencesimplified.org/digital/how.html.
[5] United Nations Office on Drugs and Crime, Digital Evidence, in Cybercrime Module 4: Introduction to Digital Forensics (2023), https://www.unodc.org/cld/zh/education/tertiary/cybercrime/module-4/key-issues/digital-evidence.html.
[6] Indian Journal of Legal Research and Analysis, Digital Evidence in Indian Criminal Law: Admissibility and Authenticity Under the BSA 2023 (2024), https://www.ijllr.com/post/digital-evidence-in-indian-criminal-law-admissibility-and-authenticity-under-the-bsa-2023 [hereinafter IJLLR 2024].
[7] Forensic Science Simplified, supra note 4.
[8] Id.

contemporary criminal proceedings.

D. Network Data and Mobile Device Records

Network traffic logs, IP addresses, server logs, application logs, database logs, and firewall records are instrumental in cybersecurity investigations and cybercrime prosecutions.[9] Mobile devices additionally record GPS and cell tower location data; investigators can typically access the last two hundred cell tower locations accessed by a device.[10] Call logs, browsing history, and system-level operations may all be extracted using specialized forensic collection tools, making the modern smartphone a near-comprehensive record of its user's activity.

III. ELECTRONIC RULES ON EVIDENCE: THE ADMISSIBILITY FRAMEWORK

The admissibility of electronic evidence in India operates through a structured legal framework that has undergone significant evolution, culminating in the transformative reforms of the BSA 2023.

A. Section 65B and the Certification Mechanism

Section 65B of the Indian Evidence Act, 1872 established the foundational certification mechanism for electronic records. Any information contained in an electronic record is admissible without production of the original device, provided four specific cumulative conditions are satisfied: (i) the computer was regularly used during the relevant period; (ii) information was fed in the ordinary course of activities; (iii) the computer operated properly throughout the material period; and (iv) the information reproduced derives from data ordinarily fed into the system.[11]

A certificate under Section 65B(4) must identify the electronic record, describe the manner of its production, provide particulars of the device involved, and be signed by a person occupying a responsible official position in relation to the device. The Supreme Court of India authoritatively clarified this framework in *Anvar P.V. v. P.K. Basheer*, holding that Section 65B certification is a mandatory condition precedent to the admissibility of electronic evidence—not merely a procedural formality.[12]

This position was reaffirmed and elaborated in *Arjun Panditrao*

[9] NBF Tools, The Important Role of Timestamps in Forensic Science (2024), https://www.nbftools.com/important-role-of-timestamps-in-forensic-science/.
[10] Forensic Science Simplified, supra note 4.
[11] Indian Evidence Act, No. 1 of 1872, § 65B(2) (India).
[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

Khotkar v. Kailash Kushanrao Gorantyal, where the Supreme Court further held that the certificate must emanate from the person who originally operated or recorded the relevant device, not merely from an officer to whom the data was subsequently transferred[13].This requirement prevents the laundering of unverified digital copies through institutional intermediaries, thereby preserving the evidentiary integrity that the certification mechanism is designed to guarantee.

B. BSA 2023: Electronic Records as Primary Evidence

The BSA 2023 introduces a landmark reform by recognizing electronic records as primary evidence. Section 61 provides that electronic or digital records shall have the same legal effect, validity, and enforceability as paper documents[14].This departure from their prior classification as secondary evidence resolves the inferential disadvantage that digital proof historically suffered in adversarial proceedings. The reform reflects the contemporary reality that much of modern human communication, commercial activity, and personal record-keeping occurs in digital form, making it anomalous to treat the digital record as inherently less reliable than its paper counterpart.

Section 65B(2) of the BSA retains the four cumulative conditions for admitting computer output, ensuring continuity with prior judicial precedent while modernizing the terminological framework[15].Significantly, the BSA has reduced the scope for purely technical objections that had previously been invoked to exclude otherwise reliable electronic evidence on formalistic grounds, thereby advancing the substantive purpose of the evidence law.

C. The Dual Certification Requirement

BSA Section 63(4) introduces a notable innovation by requiring certificates to be signed by both the person in charge of the relevant device and an independent technical expert, following the format prescribed in the Schedule[16]. This dual certification requirement builds an additional layer of accountability into the authentication process, ensuring that both the custodial chain and the technical integrity of the evidence are independently attested by persons with relevant expertise[17].

---

[13] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[14] BSA 2023 § 61.
[15] BSA 2023 § 65B(2); see also Nitesh Kumar Upadhyay, Admissibility of Electronic Evidence: An Indian Perspective, 12 Forensic Res. & Criminology Int'l J. 102, 108 (2024).
[16] BSA 2023 § 63(4).
[17] LexisNexis, Decoding Bharatiya Sakshya Adhiniyam 2023: Comparative Insights with Indian Evidence Act 1872 (2024), https://www.lexisnexis.com/blogs/in-legal/b/law/posts/decoding-bharatiya-sakshya-adhiniyam-2023-comparative-insights-study-with-indian-evidence-act-1872.

The reform reflects the legislature's recognition that electronic evidence is susceptible to manipulation in ways that physical evidence is not, and that institutional checks are essential to preserve its forensic integrity and to withstand adversarial challenge in court.

IV. AUTHENTICATION REQUIREMENTS AND FORENSIC VALIDATION

Authentication of electronic evidence raises distinct and complex challenges that have no precise analogue in the law governing physical evidence. The volatility, replicability, and remote accessibility of digital data create authentication problems that demand specialized legal and forensic responses.

A. Proving Authenticity Without the Original Device

When the original device is damaged, encrypted, or otherwise inaccessible, authentication cannot proceed through direct forensic examination. In such circumstances, third-party data becomes indispensable[18].Cell tower records, cloud backup logs, and communications metadata can collectively authenticate a digital record by placing a suspect in proximity to the device at the material time, or by corroborating the content of a message through independent sources. The applicable legal standard requires only that sufficient evidence be adduced to permit a reasonable person to find that the electronic record is more probably than not what the proponent claims; the mere possibility of alteration affects the weight of the evidence rather than its admissibility threshold[19].

B. Forensic Analysis: Timestamps and Digital Footprints

Timestamps function as temporal fingerprints enabling analysts to reconstruct timelines, validate user activity, and detect tampering. In a representative forensic scenario, log examination may reveal that a confidential file was accessed and transmitted at a precise time, directly contradicting a suspect's exculpatory claim[20].[20] However, timestamps can be manipulated through third-party software or altered system settings, necessitating cross-verification across multiple independent sources—such as network logs, cloud server records, and device system clocks—and rigorous maintenance of the chain of custody from seizure

[18] See Mateusz Bialas et al., Chain of Custody and Digital Evidence, 10 J. Digital Forensics Security & L. 45, 49 (2023).
[19] Commonwealth v. Meola, 95 Mass. App. Ct. 303 (2019); see also Mass. Guide to Evidence § 1119 (2024).
[20] NBF Tools, supra note 9.

to courtroom presentation.

C. Hash Values, Encryption, and Tamper Detection

Cryptographic hash values serve as unique digital fingerprints for file content. When a file is submitted as evidence, its hash value is computed and stored. Any subsequent modification—however minor—produces an entirely different hash value, providing a reliable and mathematically rigorous mechanism for detecting tampering[21]. Algorithms such as the Secure Hash Algorithm (SHA-256) are deployed in forensic practice precisely because even a single-bit alteration generates a completely different output. Encryption techniques further protect digital evidence from unauthorized access during the period between seizure and courtroom presentation, maintaining evidentiary integrity throughout the chain of custody[22].

D. Cross-Examination and Reliability Standards

The adversarial examination of electronic evidence remains problematic. Whether defendants and their counsel possess the technical competence or financial resources to meaningfully contest complex digital evidence is frequently questionable[23].Expert testimony is often the only viable mechanism for translating technical forensic findings into comprehensible language for judges and lay adjudicators. Furthermore, digital forensics validation standards remain underdeveloped in India: there is no universally accepted reliability standard analogous to the framework established in Daubert-line jurisprudence in the United States, and forensic results must be independently repeatable and reproducible to carry genuine epistemic weight.

V. PRACTICAL CHALLENGES IN CRIMINAL TRIAL PROCEEDINGS

While the legislative framework provides the structural architecture for the admissibility of electronic evidence, the actual deployment of digital proof in Indian criminal courts reveals significant operational deficits that impair the effective delivery of criminal justice.

A. The Legal-Technical Expertise Divide

A substantial proportion of investigating officers, prosecutors, defense lawyers, and judges lack the technical knowledge required to

[21] Digital Evidence AI, How to Prevent Digital Evidence Tampering (2024), https://digitalevidence.ai/blog/prevent-digital-evidence-tampering.
[22] Id.; see also Scientia et Praxis, Encryption and Digital Evidence Integrity, 8 J. Digital Security 112 (2024).
[23] See Bialas et al., supra note 18, at 52.

properly evaluate electronic evidence[24]. A study of eighty-seven court rulings documented pervasive confusion in the application of digital evidence standards across Indian courts. This knowledge deficit leads to the systematic misinterpretation or undervaluation of digital proof, distorting trial outcomes in both directions—credible electronic evidence may be wrongly discounted, while manipulated or fabricated digital material may pass unchallenged[25].The consequences are particularly severe in cybercrime prosecutions, where the entire evidentiary edifice typically rests on digital proof.

B. Data Privacy and Search and Seizure Concerns

The collection of electronic evidence necessarily involves incursions into sensitive personal or proprietary information. The existing statutory framework under Indian penal and procedural law does not adequately constrain the scope of digital device searches, permitting investigating agencies to collect information beyond what is necessary and proportionate[26]. The constitutional right to privacy recognized in *K.S. Puttaswamy v. Union of India* demands that evidence collection procedures incorporate robust proportionality safeguards, yet the absence of detailed statutory guidelines for the search and seizure of digital devices creates a rights gap that is ripe for exploitation and judicial challenge.

C. Cross-Border Evidence Collection

More than half of all criminal investigations today involve a cross-border request to access electronic evidence[27].[27] Technology companies such as Google and Meta store data in foreign jurisdictions, placing substantial volumes of potentially critical evidence beyond the immediate reach of domestic law. Access to data was the predominant factor by which digital evidence was disputed in sixty-two percent of analyzed cybercrime cases, reflecting the systemic nature of the cross-border challenge[28]. The absence of streamlined mutual legal assistance

[24] International Journal of Research and Trends in Innovation, Challenges of Electronic Evidence in Indian Courts 4 (2024), https://www.ijrti.org/papers/IJRTI2511101.pdf [hereinafter IJRTI 2024].
[25] Vintage Legal, supra note 2.
[26] International Journal of Law and Research Analysis, Scope, Admissibility and Challenges of Electronic Evidence (2024), https://www.ijlra.com/public/details/scope-admissibility-and-challenges-of-electronic-evidence-by-pallamreddy-lasya-sri.
[27] European Commission, E-Evidence: Cross-Border Access to Electronic Evidence (2024), https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.
[28] Vintage Legal, supra note 2.

mechanisms and the inadequacy of existing bilateral treaty networks cause protracted delays that can fatally compromise time-sensitive investigations.

D. Inadequate Forensic Infrastructure

Few forensic laboratories are formally notified under Section 79A of the Information Technology Act, 2000, causing substantial delays in the generation of admissible forensic reports[29].Many district courts and local police agencies operate without digital forensics facilities or trained personnel whatsoever. Studies indicate that evidence collection procedures were found to be deficient in nearly half of analyzed cases[30].In jurisdictions as large as Greater Manchester Police in the United Kingdom, over 1,349 seized devices were awaiting forensic analysis at a single point in time—a figure that illustrates the global scale of the digital forensics backlog problem and its capacity to delay justice[31].

E. Fair Trial Rights and Prosecution-Defense Asymmetry

The expertise and resource asymmetry between prosecution and defense in digital evidence matters poses a systemic threat to fair trial rights. Digital forensic tools are predominantly designed to serve law enforcement needs, creating a structural bias in the architecture of evidence collection[32].Courts require equality between opposing parties in their opportunity to present and challenge evidence, yet defendants without access to independent forensic expertise are practically unable to mount effective adversarial challenge to digital proof.[33] This asymmetry is particularly acute in cases involving algorithmic or automated evidence—such as outputs of network traffic analysis tools or digital forensic platforms—where the underlying methodologies are frequently opaque, proprietary, or both.

VI. CONCLUSION

[29] LawVs, Digital Evidence in Criminal Trials: Challenges and the Way Forward (2024), https://lawvs.com/articles/digital-evidence-in-criminal-trials-challenges-and-the-way-forward.

[30] IJRTI 2024, supra note 24, at 5

[31] Caroline Morgan, The Digital Forensics Crisis in Policing: What's Going Wrong, Computer Weekly (Nov. 14, 2024), https://www.computerweekly.com/news/366630535/The-digital-forensics-crisis-in-policing-Whats-going-wrong.

[32] Yvonne McDermott, Digital Evidence and Fair Trial Rights at the International Criminal Court, 36 Leiden J. Int'l L. 581, 595 (2023).

[33] Fair Trials, Digital or Not, Fair Trial Principles Apply: Challenges of E-Evidence and the Right to a Fair Trial (2023), https://www.fairtrials.org/articles/publications/digital-or-not-fair-trial-principles-apply-challenges-of-e-evidence-and-the-right-to-a-fair-trial/.

The Bharatiya Sakshya Adhiniyam, 2023 represents a significant and commendable legislative achievement in the governance of electronic evidence in India. By elevating digital records to the status of primary evidence, mandating dual certification, and modernizing the conceptual vocabulary of evidence law, it lays a sound doctrinal foundation for the digital age. The judicial precedents established in Anvar P.V. and Arjun Panditrao Khotkar remain integral to this framework, embedding robust authentication norms into the structure of Indian evidence law.

Yet legislative reform is necessary but not sufficient. The efficacy of the BSA 2023 framework depends critically on its implementation environment: the quality of judicial and prosecutorial training, the capacity of forensic institutions, the availability of legal aid for digital defense, and the robustness of international cooperation mechanisms. A legal framework that is technically sophisticated on paper but operationally hollow in practice will serve neither justice nor the rights of the accused.

Three priority reforms emerge from the foregoing analysis. First, a national program of judicial, prosecutorial, and investigative training in digital evidence should be established, drawing on accredited forensic institutions and incorporating competency assessments. Second, the network of Section 79A-notified forensic laboratories should be substantially expanded, with dedicated funding for equipment, staffing, and quality assurance. Third, India should negotiate and ratify comprehensive cybercrime-specific mutual legal assistance treaties with its principal technology-hosting treaty partners, establishing expedited data request procedures calibrated to the time-sensitive character of electronic evidence.

Electronic evidence will only deepen its centrality to criminal adjudication as digital life expands. The challenge before Indian courts, legislators, and legal practitioners is not merely to accommodate this reality within existing frameworks, but to actively shape it in ways that simultaneously advance the interests of criminal justice and protect the constitutional rights of every person who stands before the court.

REFERENCES

Cases

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

- K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

Statutes

- Bharatiya Sakshya Adhiniyam, No. 47 of 2023 (India).
- Indian Evidence Act, No. 1 of 1872 (India).
- Information Technology Act, No. 21 of 2000 (India).

Journal Articles and Books

- Mateusz Bialas et al., Chain of Custody and Digital Evidence, 10 J. Digital Forensics Security & L. 45 (2023).
- Yvonne McDermott, Digital Evidence and Fair Trial Rights at the International Criminal Court, 36 Leiden J. Int'l L. 581 (2023).
- Nitesh Kumar Upadhyay, Admissibility of Electronic Evidence: An Indian Perspective, 12 Forensic Res. & Criminology Int'l J. 102 (2024).

Internet Sources

- Digital Evidence AI, How to Prevent Digital Evidence Tampering (2024), https://digitalevidence.ai/blog/prevent-digital-evidence-tampering.
- Drishti Judiciary, Electronic Evidence Under Bharatiya Sakshya Adhiniyam 2023 (2024), https://www.drishtijudiciary.com/bharatiya-sakshya-adhiniyam-&-indian-evidence-act/electronic-evidence-under-bhartiya-sakshya-adhiniyam-2023.
- Eclipse Forensics, Types and Sources of Digital Evidence (2024), https://eclipseforensics.com/types-and-sources-of-digital-evidence/.
- European Commission, E-Evidence: Cross-Border Access to Electronic Evidence (2024), https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.
- Fair Trials, Digital or Not, Fair Trial Principles Apply: Challenges of E-Evidence and the Right to a Fair Trial (2023), https://www.fairtrials.org/articles/publications/digital-or-not-

fair-trial-principles-apply-challenges-of-e-evidence-and-the-right-to-a-fair-trial/.

- Forensic Science Simplified, How Digital Evidence Works (2024), https://www.forensicsciencesimplified.org/digital/how.html.

- Indian Journal of Legal Research and Analysis, Digital Evidence in Indian Criminal Law: Admissibility and Authenticity Under the BSA 2023 (2024), https://www.ijllr.com/post/digital-evidence-in-indian-criminal-law-admissibility-and-authenticity-under-the-bsa-2023.

- International Journal of Research and Trends in Innovation, Challenges of Electronic Evidence in Indian Courts (2024), https://www.ijrti.org/papers/IJRTI2511101.pdf.

- LawVs, Digital Evidence in Criminal Trials: Challenges and the Way Forward (2024), https://lawvs.com/articles/digital-evidence-in-criminal-trials-challenges-and-the-way-forward.

- LexisNexis, Decoding Bharatiya Sakshya Adhiniyam 2023: Comparative Insights with Indian Evidence Act 1872 (2024), https://www.lexisnexis.com/blogs/in-legal/b/law/posts/decoding-bharatiya-sakshya-adhiniyam-2023-comparative-insights-study-with-indian-evidence-act-1872.

- Caroline Morgan, The Digital Forensics Crisis in Policing: What's Going Wrong, Computer Weekly (Nov. 14, 2024), https://www.computerweekly.com/news/366630535/The-digital-forensics-crisis-in-policing-Whats-going-wrong.

- NBF Tools, The Important Role of Timestamps in Forensic Science (2024), https://www.nbftools.com/important-role-of-timestamps-in-forensic-science/.

- UNODC, Digital Evidence (Cybercrime Module 4) (2023), https://www.unodc.org/cld/zh/education/tertiary/cybercrime/module-4/key-issues/digital-evidence.html.

- Vintage Legal, Digital Evidence Admissibility in Indian Courts: Bridging Legal Gaps in the Age of Cybercrime (2024), https://www.vintagelegalvl.com/post/digital-evidence-admissibility-in-indian-courts-bridging-legal-gaps-in-the-age-of-cybercrime.