 DOI: https://10.5281/zenodo.23533560

Admissibility of Electronic Evidence: A Doctrinal and Empirical Analysis of Statutory Frameworks and Digital Forensic Protocols

Tushar Rana[1]

© The Author(s), under exclusive licence to Oxford Law Review 2026.

Abstract

Modern society has undergone a significant digital transformation which has changed the way legal proceedings are undertaken and, in turn, the law that has to be updated to reflect this change. This research paper thoroughly examines the shift from the basic principles of Section 65B, Indian Evidence Act, 1872, to modern requirements of Section 63, Bharatiya Sakshya Adhiniyam, 2023. This analysis looks at the evolving judicial philosophies in key decisions and the critical need for mandatory electronic certification, strict chain of custody procedures and uncompromising forensic integrity. The research method is a scientific doctrinal analysis with a qualitative assessment of the effectiveness of the statutory certification mechanisms, and the empirical effect of verifying the cryptographic hash value on the reliability of the evidence. The results revealed that the new legislative framework, which includes both cryptographic hash requirements and dual-signatories, greatly reduces the risks of data manipulation and unauthorized tampering. In addition, state-of-the-art digital forensic techniques helps to preserve digital artifacts in adversarial processes. The paper concludes that efforts to ensure that the basic elements of admission of electronic records to court are well under way, but ongoing capacity development efforts in the judiciary and forensic enforcement agencies are necessary to meet technological justice's goals.

Keywords: Electronic Evidence, Section 65B, Bharatiya Sakshya Adhiniyam, Digital Forensics, Chain of Custody, Hash Value Verification, Admissibility.

1. Introduction

The digital revolution has touched every aspect of human interaction and electronic devices are now the primary means of committing and investigating today's offenses. Thus, the admissibility of electronic evidence has become a critical issue in today's legal doctrine with the potential to radically influence the course and eventual resolution of civil disputes and criminal trials (Dagar, n.d.). In contrast to paper-based evidence, digital data is extremely volatile, easily alterable and presents an additional challenge to the legal profession and forensic investigators. The difficulty of creating, altering or destroying electronic evidence is immense because anyone with basic computer skills can alter or delete anything on storage media, delete the hard disk memory, change electronic dates, or

[1] **CGC University, Mohali, Punjab, India;** ✉**tusharrana1108@gmail.com**

send an email that never actually existed. Statutory provisions throughout the world, including in the Indian context, have been forced to change to address these weaknesses and incorporate technological advances into the legal process, moving from a paper-based evidentiary system to more advanced systems of digital authentication (CDJ Law Journal, n.d.). This transformation has been formalised for the first time in the Indian context in the Information Technology Act, 2000, which modified the old Indian Evidence Act, 1872 with specific provisions to confer legal recognition on electronic records (Jyothi, 2024).

Definitions of the traditional evidence and standard documents were broadened to cover any information stored, recorded or transmitted digitally, such as emails, digital photographs, spreadsheet databases and system network logs (Shukla, 2023). The Indian Evidence Act was amended by Section 65A and 65B to address the admissibility of these newly-defined electronic records and introduced a specific procedural gatekeeper for digital data. Any information contained in an electronic record, whether transmitted in print on paper or electronically in magnetic or optical form, was expressly declared to be a document that met the requirements for admission of the paper copy, provided the following strict conditions of the statute were clearly met (CDJ Law Journal, n.d.). The statutory insertion introduced a non-obstante clause, in that it would retain overriding status with respect to other traditional provisions of the evidence act and provide that only those electronic records which are capable of being established following certain specified certification procedures in the subsections of the evidence act would be admissible as evidence (CMR University, 2022). This procedural rule was based on the underlying goal of elevating the status of the secondary evidence by providing a basis for authenticity, namely that the computer output was produced in the regular course of activity and that the computer was working as intended (CDJ Law Journal, n.d.).

The volume and complexity of digital data grew at an exponential rate, with legal systems realizing that a statutory certificate alone was not enough, and that it was necessary to prove that a digital forensic procedure had been followed with scientific rigor. Indian Courts increasingly required that the chain of custody, which is a documentary and procedural proof of who handled the digital item, when and how the item was handled, and when and how the digital item was extracted, be established. Such a requirement is consistent with the international standard, the Federal Rule of Evidence 902 in the United States, which sets out parameters for self-authenticating electronic records and stresses the need to adopt certified data extraction methodologies (Grimm et al., 2017). Incorporation of these best practices from around the world shed light on the shortcomings in the procedures under the existing Indian laws and regulations, particularly in respect of authentication of data seized from a cloud network and complicated server networks (Simou et al., 2014). When the process of forensically extracting the underlying integrity from a digital artifact was flawed, it became apparent that a certificate issued under Section 65B was often not enough to establish the integrity of the underlying digital artifact.

However, the Bharatiya Sakshya Adhiniyam, 2023 (Lex Scripta Magazine, n.d.-a) came into effect after the Indian legislature passed a comprehensive revision to the criminal justice statutes which were not adequate to deal with complex modern crimes. The new law, in particular under Section 63, attempts to clear up the ambiguity of evidence found in Section 65B by elevating certain

Copyright © Oxford Law Review. (editor@oxfordlr.com)

electronic records to become primary evidence and by making the certification process much more rigorous - requiring documentation of cryptographic hash values and introducing independent forensic experts (Lex Scripta Magazine, n.d.-a). The change is intended to provide a strong presumption of scientific reliability of digital forensic evidence seized from electronics, CCTV footage, GPS and call detail records when those items enter the courtroom. The shift from the Indian Evidence Act to the Bharatiya Sakshya Adhiniyam is a groundbreaking transformation that combines complex legal processes with cutting-edge digital forensics to ensure the integrity and authenticity of electronic evidence in today's courtrooms (Niyam.ai, n.d.).

2. Literature Survey

The debate around the admissibility of electronic evidence is a jurisprudential journey that has experienced a number of intense debates, conflicting interpretations and rolling legislative adjustments, all aimed at reconciling the search for truth and the requirements for evidentiary integrity. The legal literature and precedent shows a very dynamic jurisprudence, in which the judiciary was grappling with laws designed for the physical world of paper documents to the immaterial world of binary data (Digital Forensics Investigation Jurisprudence, n.d.). Before definitive use of strict electronic protocols, courts have been known to be tolerant of secondary electronic records. The Supreme Court of India in *State (N.C.T. of Delhi) v. Navjot Sandhu* (2005) also ruled that the secondary evidence of electronic records including CDR may be accepted under the general rules of evidence without the certificate required under Section 65B(4) of the Indian Evidence Act (Admissibility of Electronic Evidence under Indian Law, n.d.). In fact, this decision effectively superseded the specialized technological protections that were put in place by the legislature, and admitted oral testimony and traditional corroboration of digital evidence – a move that unintentionally paved the way for the judiciary to be exposed to the many weaknesses of unauthenticated and potentially tampered digital evidence (Admissibility of Electronic Evidence under Indian Law, n.d.).

The *Navjot Sandhu* ruling created a lot of fears among legal scholars and forensic experts that digital evidence needed specialized gatekeeping because of the possibility of invisible changes to the data (Digital Forensics Investigation Jurisprudence, n.d.). In 2014, the Supreme Court in a significant decision in *Anvar P.V. v. P.K. Basheer* (2014) (Lex Scripta Magazine, n.d.-a) finally addressed this significant legal lacuna. The court in *Anvar P.V.* expressly overruled the said part of the *Navjot Sandhu* judgment and gave an unambiguous pronouncement that any documentary evidence by way of an electronic record can only be established following the procedure laid down under Section 65B (CDJ Law Journal, n.d.). The Court's judgment set the precedent that, for secondary evidence to be admissible, a formal certificate of compliance with Section 65B(4) must be produced (Lex Scripta Magazine, n.d.-a). This changed the approach of law enforcement agencies and civil litigants across the country when seeking to admit secondary evidence. The decision noted that if an electronic record was the main evidence and the original device was made available to the court, then there was no need to provide any certification; but if a copy, printout, or transferred data

Copyright © Oxford Law Review. (editor@oxfordlr.com)
URN:OXF:UK:0000OXFLR:V1I2:307

presented to court was the primary evidence, and a certified copy of the original electronic record was presented, then the certification requirement must be met (CDJ Law Journal, n.d.).

The clarity that *Anvar P.V.* brought was later revealed through subsequent litigation of significant practical hurdles that exist for parties seeking the mandatory certificate, particularly when the electronic device is under the control of an adversarial party or a neutral third party service provider. This conundrum resulted in an adverse decision in *Shafhi Mohammad v. State of H.P.* (2018), where the Supreme Court, for the first time, relaxed the strict requirement of certification and had found that the requirement of Section 65B(4) can be relaxed, if the party on whose production of the document the original device is based was not in the possession or control of the original device. This relaxation, designed to prevent the denial of justice, brought back the discussion on the possibility of presenting fabricated digital data, which led to a quick reconsideration by the judiciary (Electronic Evidence: Admissibility and Authentication, n.d.). Finally, controversy was put to rest by a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) in which the strict legal rule of *Anvar P.V.* was reiterated and *Shafhi Mohammad* was completely overturned (IJLRA, 2026). The court in *Arjun Panditrao Khotkar* has held that under Section 65B(4) it was obligatory to present the certificate along with the electronic record for its production as a record in evidence, and, without the certificate, the secondary evidence was completely barred (IJLRA, 2026).

In addition to the domestic legal context, the literature points to the international trend of adopting strong cyber forensic regulations to guarantee the admissibility of technological evidence. International standards, like the ISO/IEC 27043 guidelines, focus on the desired models for incident response and digital investigation and propose systematic use of forensic processes to ensure that the maximum amount of potential digital evidence can be admitted and inter-jurisdictionally accepted (Digital Forensics Investigation Jurisprudence, n.d.). Advanced literature in the field of cyber forensics highlights the importance for the preservation of a verifiable chain of custody from the point of seizure to the point of presentation to court that the data should not be altered by any unauthorized parties (Vidhigyata, n.d.). Defence counsels can immediately identify possible mishandling or manipulation of evidence by looking at the chain of custody and obtaining the required technological grounds to argue against admissibility at trial, according to scholars. Technically speaking, the principle of completeness requires that digital data be made available in addition to its metadata, system logs, and means of transmission in order to have any probative value (Vidhigyata, n.d.).

Comparative law studies have pointed to the fact that jurisdictions like the United States utilize the Federal Rule of Evidence 902 to allow for self-authentication of electronic records through specific certification of technical reliability by the record custodians, which greatly facilitates the presentation of data with rigorous underlying technical reliability (Grimm et al., 2017). Federal Rule of Evidence 902(11) provides that "electronic evidence" that is "furnished by the custodian of the records in the form of a formal certificate that certifies the evidence to be accurate and authentic" is admissible without the need for parties to present witnesses to testify about the source of the evidence (Grimm et al., 2017). The current forensic models need to be adapted to meet the needs of modern investigations where the context is increasingly complex, including within the

Copyright © Oxford Law Review. (editor@oxfordlr.com)

framework of cloud computing architectures and IoT devices (Simou et al., 2014). The academic opinion indicates that, for these sophisticated networks, admissibility can only be achieved with the ongoing use of bit-stream imaging, hardware write-blockers and automated cryptographic hashing algorithms in order to meet the continuously increasing bar of the legal examination (Lex Scripta Magazine, n.d.-a).

3.Research Methodology

This research is organised in a systematic manner on an extensive doctrinal and analytical approach, which aims at critically analysing the changing legal requirements and procedural rules applicable to the admissibility of electronic evidence. The key method of investigation is an exhaustive statutory review of the transition from the Indian Evidence Act, 1872, and the Information Technology Act, 2000, to the Bharatiya Sakshya Adhiniyam, 2023. For the purpose of the present study the structural changes to the law to address the vulnerabilities of digital data will be examined, particularly those to the regulations concerning the reconstitution of secondary electronic evidence. In addition to the primary legislative analysis, the research draws heavily on secondary sources, such as a wealth of landmark judicial decisions, peer-reviewed legal journals and manuals from around the world that use digital forensics. The synthesis of the doctrines allows a complex understanding of the interpretation of the requirements of the technology by the appellate courts and their way of putting the theoretical principles of law into practice in highly conflictual circumstances in criminal and civil trials.

A well-structured analytical framework is applied to the study in a detailed manner to assess the implementation of digital evidence integration in practice on two parameters that are crucial. The first aspect that has been evaluated is the effectiveness of statutory certification mechanisms under the previous Section 65B of the Indian Evidence Act compared to the new multi-layered evidence authentication mechanisms in Section 63 of the Bharatiya Sakshya Adhiniyam. This parameter is one that examines the impact of the legal drafting on the burden of proof, and regulates the entry of unverified digital information into the judicial record. The research assesses the specific wording of these clauses to understand the extent to which they require objective technological safeguards and thus inexorably link the legal documentation with the real-world science. They are compared to the legislature of the previous era to identify those legal developments that are particularly effective at reducing the chances of evidence being fabricated.

The second parameter is the empirical result of the use of forensic integrity and cryptographic hash value verification on the overall admissibility rates of electronic evidence. This includes examination of the SOPs used by advanced investigation agencies like the Directorate of Forensic Science, Gujarat and assessment of the use of advanced forensic tools to ensure the integrity of the digital chain of custody (Sandeep Sharma v. State of Madhya Pradesh, n.d.). In order to measure this parameter properly, the methodology includes an evaluation of technical mechanisms that are a fundamental part of the preservation of digital evidence such as bit-stream imaging, the use of hardware write blockers, and the generation of MD5 and SHA-256 hash values. This research examines the abilities of standardized forensic suites, including EnCase Professional,

Copyright © Oxford Law Review. (editor@oxfordlr.com)

and how they meet the strict documentation requirements of judicial systems through their secure data acquisition processes and all-encompassing reporting capabilities (IJFMR, 2024). The study also examines the intersections between international legal standards, by drawing on the Federal Rules of Evidence adopted and applied in foreign jurisdictions to situate domestic developments in the larger global context (Grimm et al., 2017). This methodological approach, which combines statutory interpretation and also a technical evaluation of forensic acquisition tools, ensures that the complex mechanisms for the successful admission of electronic evidence in contemporary legal proceedings are analyzed in an exhaustive and multi-dimensional manner.

4. Results and Discussion

The in-depth examination of the statutory provisions and judicial case law along with the forensic approaches provides in-depth understanding of the evolving landscape of electronic evidence admissibility. As we are coming to an understanding of the fragility of these digital artefacts, it has become necessary to develop much more structured, scientifically-based protocols for legal systems. This investigation yields two main analytical parameters that together convey a good sense of the operational reality of digital evidence management in the adversarial litigation context. The results demonstrate a deliberate shift from reliance on documents to an absolute requirement for a digital forensics that is verifiable.

The first parameter of this analysis is based on the effectiveness of statutory certification processes, which is measured by the difference in the structure of Section 65B of the Indian Evidence Act and Section 63 of the Bharatiya Sakshya Adhiniyam. The former Section 65B had made the admission of secondary evidence solely on the basis of a certificate signed by one person in a responsible official capacity for the operation of the computer concerned. Although this was a major step over the documentary rules, it often led to the courts having to deal with incomplete certificates, third parties unwilling to provide services and a lack of technical detail in the certificate on how the data was to be extracted (Lex Scripta Magazine, n.d.-b). The certificate requirement of the previous regime posed enormous practical problems because it was not always available during the crucial stages of the investigation, or because it was not prepared by one with a high degree of technical expertise (Lex Scripta Magazine, n.d.-b). The analysis has shown that the Bharatiya Sakshya Adhiniyam is a step forward in addressing these historical ambiguities as it has raised the status of many kinds of electronic records as evidence, and it will completely change the way digital evidence is certified as secondary documents.

Section 63 of the new legislation establishes a new dual-signatory requirement by adding an independent, qualified digital expert (Niyam.ai, n.d.) to the requirement of the person in charge of the electronic device to validate the evidentiary certificate. This structural improvement now places the authentication of the evidence before the adjudicating authority on a new plane - one that is more scientific and reliable, rather than administrative. The statutory upgrade explicitly discusses the susceptibility of single-source verification, and that the operator of a computer system can have built-in biases, or may not have the expertise needed to ensure the forensically sound nature of a digital export (Lex Scripta Magazine, n.d.-a). The comparative data is organised in Table 1 to

Copyright © Oxford Law Review. (editor@oxfordlr.com)

systematically illustrate the developments of the statutory certification processes and their direct effect on the judicial proceedings.

Assessment Parameter	Section 65B (Indian Evidence Act, 1872)	Section 63 (Bharatiya Sakshya Adhiniyam, 2023)
Primary Signatory	Single signature from a responsible official managing the device.	Dual signatures required: Device manager and an independent expert.
Cryptographic Verification	Not explicitly mandated by the statutory text.	Mandatory inclusion of algorithmic Hash Values (e.g., SHA-256).
Documentary Format	Loosely defined; led to inconsistent submissions across jurisdictions.	Strict adherence to a prescribed legal Schedule and standardized format.
Evidentiary Status	Treated primarily as secondary evidence requiring strict gatekeeping.	Expands the scope of electronic records classified as primary evidence.
Judicial Exemption	Historically fluctuating exemptions (e.g., Shafhi Mohammad ruling).	Strict mandatory compliance; judicial waivers strictly curtailed.

Table 1: Statutory Evidentiary Certification Requirements

The data is clear that the changes in the law made under the Bharatiya Sakshya Adhiniyam are a revolutionary step towards the cause of integrity of evidence. The legislation specifically prescribes the use of hash values in the statute itself, thus filling the significant gap between legal procedure and forensic science. This requirement makes it possible to mathematically connect any digital artifact submitted to the court's attention to its state when it was extracted, allowing for easy verification by judicial officers of any later intentional alterations to the artifact (Lex Scripta Magazine, n.d.-a).

The second parameter examined is how crucial forensic integrity is and how immediate the impact of hash value verification rates are on the successful prosecution of cybercrime and digitally-dependent crime. The analysis shows that the legal notion of the chain of custody is inseparably intertwined with the technological notion of cryptographic hashing. Each dataset can be assigned a hash value, usually calculated using an advanced algorithm like the MD5 or SHA-256, which is a unique alphanumeric digital fingerprint for each set of data, even if the only difference is the most minor in the underlying binary data in the set, the hash will be vastly different. The study reveals that the courts in India are increasingly relying on major institutions such as the National Forensic Sciences University and the Directorate of Forensic Science, and require forensic scientists to routinely calculate and record these in real-time at the time of seizure and at every point of data transfer. If a hash value is not consistent throughout the chain of custody, it is a fatal problem that automatically leads to a legal presumption of evidence tampering, which is always exclusive of the digital artifact from the judicial record (Digital Forensics Investigation Jurisprudence, n.d.).

Copyright © Oxford Law Review. (editor@oxfordlr.com)
URN:OXF:UK:0000OXFLR:V1I2:307

The need for absolute precision has pushed law enforcement and private investigators towards advanced digital forensic tools that automatically implement these rigorous integrity practices. The analysis assesses the use of industry-standard software platforms capable of capturing digital evidence that are specifically designed to capture digital evidence in a forensically sound manner (IJFMR, 2024). These high-end tools produce exact binary copies of storage media and make sure that the original evidence is not altered at all, while strictly using hardware write-blockers. In addition, these platforms offer detailed timeline analysis, automatic hash generation and standardized reporting, which directly meet the requirements of the judicial chain of custody documentation (IJFMR, 2024). On the other hand, basic tools with no user authentication or automated hashing systems often create irremovable evidentiary issues that greatly diminish the likelihood of successful presentation to court (IJFMR, 2024). The power of these forensic techniques on the legal value of digital evidence is quantified systemically in Table 2.

Forensic Methodology Applied	Integrity Mechanism Utilized	Impact on Chain of Custody	Admissibility Probability
Live Device Analysis	Direct interaction without hardware write-blockers.	High risk of metadata alteration and unrecoverable data loss.	Extremely Low (Inadmissible)
Standard File Copy	Logical transfer via standard operating systems.	Modifies creation dates and fails to capture deleted space.	Low (Subject to intense challenge)
Bit-Stream Imaging	Exact binary sector-by-sector duplication.	Preserves all hidden data, system metadata, and unallocated space.	High
Write-Blocker Deployment	Hardware prevents data from being written to the source.	Guarantees the original device remains completely pristine.	Very High
Cryptographic Hashing	MD5 / SHA-256 algorithm generation and logging.	Provides mathematical proof of complete data immutability.	Absolute Prerequisite

Table 2: Forensic Acquisition Methodologies and Evidentiary Admissibility

The results are plain, and it is evident that mathematical proof by cryptographic hashing has now become a legal requirement, and not just a best practice, for the admissibility of electronic evidence (Lex Scripta Magazine, n.d.-a). The forensic community has established strict operating procedures to prevent unauthorized access to digital data and data manipulation from third parties. There is extensive scrutiny of digital devices like Digital Video Recorders (DVR) when they are confiscated

Copyright © Oxford Law Review. (editor@oxfordlr.com)
URN:OXF:UK:0000OXFLR:V1:I2:307

from a crime scene; if information from the seal and the information from the device's digital footprint is not the same, the entire forensic analysis is compromised (Sandeep Sharma v. State of Madhya Pradesh, n.d.). Courts expressly depend on the knowledge and experience of institutions such as the Directorate of Forensic Science to determine whether these systems have been accessed in an unauthorized way prior to the creation of the formal forensic image (Sandeep Sharma v. State of Madhya Pradesh, n.d.).

The extensive merging of these forensic processes with the new statutory requirements creates an almost impassable obstacle to the introduction of fabricated digital evidence. The findings suggest that courts are becoming tech-savvy, and are quick to throw out evidence that shows inconsistencies with the digital footprint or if the digital investigator didn't specify the versions of software used to investigate (Vidhigyata, n.d.). In addition, advanced forensic analyses techniques like Layered Voice Analysis are sometimes used by local forensic labs to assess psychological stress and deception in a deceptive voice during interrogation but have strong reliance on underlying compliance with the strict cryptographic and procedural standards that apply to all electronic records (IJIP, 2026). The raw data files produced by such experimental systems should be treated as though they are traditional electronic documents, and be bit-stream imaged and hashed according to the same procedures. Finally, the findings of this analysis validate the need for the seamless integration of accurate statutory language and rigorous digital forensic science in the proper functioning of justice in today's technologic age.

5. Conclusion

The detailed analysis in this research paper proves conclusively that the legal framework that regulates the admissibility of electronic evidence has evolved from a time of judicial uncertainty to a sophisticated, rigorously science-based system. The intangible and volatile character of digital data has been a historical problem that brought up fabricated or unauthenticated digital records into adversarial proceedings, and has been systematically extirpated by bold legislative measures and clearly-stated judicial rulings. Section 63 of Bharatiya Sakshya Adhiniyam marks a significant leap in the evolution of current jurisprudence, shifting the focus from relatively simplistic, one-signer, paper-based evidence requirements of Section 65B of the Indian Evidence Act. This legislative framework has been successful in bringing the legal aspects of digital forensics into line with the actual practice of digital forensics: by making digitally authenticated data the primary evidence, it is also requiring mathematical proof of integrity through the use of hash value verification.

But the results also reveal that, by itself, statutory advancement is not enough if the proper application of flawless forensic method at the field level is not followed. The core principles of hardware write-blockers, forensically sound bit-stream images, and an unbroken chain of custody, that began at the time of initial seizure, continue to be the final and most critical factors in determining courtroom admissibility. The embedding of standard operating procedures used by top forensic institutions is evidence that technological skills are integral to the exercise of legal representation and judicial management. Technologies will always change and as they do, with complex new features like non-centralized cloud storage and ever more complex and encrypted

Copyright © Oxford Law Review. (editor@oxfordlr.com)
URN:OXF:UK:0000OXFLR:V1Iz.307

communications, the judiciary and forensic enforcement agencies will need ongoing, targeted capacity building efforts to avoid being rendered obsolete. The proper administration of modern justice depends solely on this constant and fruitful cooperation between the living laws and the uncompromising scientific rectitude with which they are applied, so that whatever passes on the electronic highways of modern society may be fairly and accurately judged in the court of law.

References

Admissibility of Electronic Evidence under Indian Law. (n.d.). ResearchGate.

https://www.researchgate.net/publication/345233647_Admissibility_of_Electronic_Evidence_under_Indian_Law

CDJ Law Journal. (n.d.). Articles. https://www.cdjlawjournal.com/articles_home_main.php?id=92

CMR University School of Legal Studies. (2022). A need to amend Sec. 65B of the Indian Evidence Act, 1872.
https://cmr.edu.in/school-of-legal-studies/journal/wp-content/uploads/2022/11/Electronic-Evidence-A-need-to-amend-Sec.-65B-of-the-Indian-Evidence-Act-1872_CMR.pdf

Dagar, M. (n.d.). Admissibility of electronic records as evidence with special reference to the Indian Evidence Act, 1872. International Journal for Legal Research and Analysis.
https://www.ijlra.com/details/admissibility-of-electronic-records-as-evidence-with-special-reference-to-the-indian-evidence-act-1872-by-mayank-dagar

Digital Forensics Investigation Jurisprudence: Issues of admissibility of digital evidence. (n.d.). ResearchGate.
https://www.researchgate.net/publication/342706049_Digital_Forensics_Investigation_Jurisprudence_Issues_Of_Admissibility_Of_Digital_Evidence

Electronic Evidence: Admissibility and Authentication: A judicial perception of Apex Court of India. (n.d.). ResearchGate.
https://www.researchgate.net/publication/353581175_Electronic_Evidence-Admissibility_and_Authentication_A_Judicial_Perception_of_Apex_Court_of_India

Grimm, P. W., Capra, D. J., & Joseph, G. P. (2017). Authenticating digital evidence. Baylor Law Review. https://law.baylor.edu/sites/g/files/ecbvkj1546/files/2023-11/7_grimm_capra_joseph.pdf

International Journal for Legal Research and Analysis [IJLRA]. (2026). Volume 3, Issue 2 (May 2026), ISSN 2582-6433. https://www.ijlra.com/uploads/1293221868.pdf

International Journal of Indian Psychology [IJIP]. (2026). Revisiting 26/11: A forensic voice analysis of Ajmal Kasab's confession.
https://ijip.in/wp-content/uploads/2026/04/18.01.283.20261401.pdf

OXFORD LAW REVIEW
Copyright © Oxford Law Review. (editor@oxfordlr.com)

International Journal for Multidisciplinary Research [IJFMR]. (2024). Understanding digital forensic tools: Their features, applicability and key shortcomings. A compendium. https://www.ijfmr.com/papers/2024/6/30026.pdf

Jyothi, S. (2024). Electronic evidence: An overview. https://cdnbbsr.s3waas.gov.in/s3ec030b6ace9e8971cf36f1782aa982a7/uploads/2024/12/2024121034.pdf

Lex Scripta Magazine. (n.d.-a). Admissibility and evidentiary challenges of digital evidence in criminal trials in India: A critical legal study. https://lexscriptamagazine.com/admissibility-and-evidentiary-challenges-of-digital-evidence-in-criminal-trials-in-india-a-critical-legal-study/

Lex Scripta Magazine. (n.d.-b). Scientific investigation under the new criminal laws: A study of forensic science in India. https://lexscriptamagazine.com/scientific-investigation-under-the-new-criminal-laws-a-study-of-forensic-science-in-india/

Niyam.ai. (n.d.). Electronic evidence under BSA section 63 (vs old 65B). https://niyam.ai/blog/bsa-section-63-electronic-evidence/

Sandeep Sharma v. State of Madhya Pradesh. (n.d.). CaseMine. https://www.casemine.com/judgement/in/6750b4f7a7b6b96bf618134c

Shukla, V. (2023). The admissibility of digital evidence: Challenges and future implications. The Law Brigade Publishers. https://thelawbrigade.com/wp-content/uploads/2023/09/Vanshika-Shukla-CLRJ.pdf

Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014). Cloud forensics: Identifying the major issues and challenges. Lecture Notes in Computer Science, 8484. https://www.icsd.aegean.gr/publication_files/646452506.pdf

Vidhigyata. (n.d.). E-evidence in Indian courts: Admissibility, chain of custody & forensics. https://www.vidhigyata.in/post/e-evidence-in-indian-courts-admissibility-chain-of-custody-forensics

OXFORD LAW REVIEW
Copyright © Oxford Law Review. (editor@oxfordlr.com)

 DOI: https://10.5281/zenodo.23533560

Publisher's Note

Oxford Law Review maintains neutrality with respect to the opinions, interpretations, and conclusions expressed in published articles, as well as jurisdictional claims in published maps and institutional affiliations. The views and arguments presented in this article are solely those of the author(s) and do not necessarily reflect the views of Oxford Law Review, its editors, or its publisher. Responsibility for the accuracy, originality, and integrity of the content rests with the author(s). Publication of an article does not constitute an endorsement by Oxford Law Review of the views expressed therein. All rights relating to the article are governed by the applicable publishing agreement between the author(s) or other rightsholder(s) and the publisher, together with applicable law.

OXFORD LAW REVIEW
Copyright © Oxford Law Review. (editor@oxfordlr.com)

URN:OXF:UK:0000OXFLR:V1Iz.307