INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL EVIDENCE AND CYBER CRIME INVESTIGATION IN INDIA: ISSUES OF ADMISSIBILITY, AUTHENTICATION AND RELIABILITY

AUTHORED BY - SAHIL SEHRAWAT

ABSTRACT

Digital evidence — mobile-device data, CCTV footage, call-detail records, banking transaction logs, cloud-hosted communications and server metadata — has become the evidentiary backbone of contemporary cybercrime investigation and prosecution in India, yet the legal architecture governing its admissibility, authentication and reliability continues to generate significant doctrinal uncertainty and practical difficulty. This paper undertakes a critical, doctrinal examination of digital evidence law in India following the replacement of the Indian Evidence Act, 1872 by the Bharatiya Sakshya Adhiniyam, 2023 ("BSA"), which came into force on 1 July 2024. It traces the jurisprudential evolution of the electronic-evidence certificate requirement from Section 65B of the erstwhile Evidence Act — through the Supreme Court's oscillating rulings in Anvar P.V. v. P.K. Basheer, Shafhi Mohammad v. State of Himachal Pradesh and Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal — to Section 63 of the BSA, which introduces a materially stricter, statutorily prescribed dual-part certificate architecture requiring hash-value disclosure and separate declarations from the device custodian and a technical expert. The paper critically analyses recent 2025-2026 jurisprudence, including Kailash Pawar v. State of Maharashtra and Chandrabhan Sudam Sanap, which reaffirm and refine the mandatory character of the Section 63 certificate while clarifying its inapplicability where electronic evidence is proved through oral witness testimony rather than the special statutory mode. Beyond the certification framework, the paper examines the practical realities of cyber forensic investigation in India — chain-of-custody documentation, hash-based integrity verification, the institutional divide between government forensic science laboratories and MeitY-empanelled private laboratories, and the persistent shortage of trained forensic personnel and standardised forensic tooling across India's twenty-seven state forensic science laboratories and seven central forensic science laboratories. Drawing on National Crime Records Bureau data indicating cybercrime conviction rates below eighteen percent, attributable substantially to deficient digital evidence handling, the paper identifies systemic reliability concerns including the absence of certified

ISSN: 2582-6433

indigenous blockchain-forensic capability, jurisdictional obstacles in obtaining evidence from foreign-headquartered platforms, and inconsistent judicial application of the certification requirement across trial courts. The paper concludes that closing the gap between digital evidence law's doctrinal sophistication and its practical enforcement will require standardised forensic protocols, expanded institutional forensic capacity, judicial training, and legislative attention to emerging evidentiary categories such as artificial-intelligence-generated content.

Keywords: *Digital evidence; Bharatiya Sakshya Adhiniyam; Section 65B; electronic evidence admissibility; cyber forensics; chain of custody; India.*

1. INTRODUCTION

The overwhelming majority of contemporary criminal investigation in India, and particularly cybercrime investigation, now turns decisively on electronic and digital evidence — WhatsApp chat exports, call-detail records, UPI transaction logs, CCTV footage, cloud-stored documents, and server-side metadata. Digital forensics scholarship describes this evidentiary category as encompassing any data "stored, created or transmitted electronically" capable of supporting or challenging a fact in issue, extracted and preserved through a scientific process combining computer science, cybersecurity and criminal investigation methodology.[1] Yet electronic evidence is, by its nature, distinctively vulnerable to alteration, incomplete capture and loss of contextual integrity, a vulnerability that has driven Indian evidentiary law towards an increasingly formalised, technically detailed certification regime governing its admission in judicial proceedings.[2]

With effect from 1 July 2024, the Bharatiya Sakshya Adhiniyam, 2023 ("BSA") replaced the Indian Evidence Act, 1872 ("IEA"), and with it, Section 65B's certificate regime for electronic records gave way to Section 63 of the BSA — a provision that substantially reproduces, but does not identically replicate, its predecessor, introducing a materially stricter, dual-part statutory certificate architecture.[3] This transition occurs against a backdrop of persistently low cybercrime conviction rates — National Crime Records Bureau data placing the figure below eighteen percent — substantially attributable, according to secondary literature, to deficient

[1]Munira M. Rampurawala & Anjali R. Vairagar, "Role of Cyber Forensic in Crime Investigation," 14(2) International Journal of Engineering Research & Technology (2026).
[2]"Electronic Evidence in Indian Law: Admissibility, Authentication and Evidentiary Value," Indian Journal of Law (2026).
[3]"Section 65B vs. Section 63 BSA: Electronic Evidence Admissibility in India," Legal Service India (2026).

ISSN: 2582-6433

evidentiary handling and inadequate digital chain-of-custody documentation.[4] This paper critically examines whether India's evolving digital evidence framework — doctrinal, statutory and institutional — adequately addresses the twin imperatives of admissibility (the threshold question of whether evidence may be considered at all) and reliability (the substantive question of whether admitted evidence deserves evidentiary weight), and identifies the practical obstacles that continue to undermine effective cybercrime prosecution notwithstanding two decades of statutory refinement.

1.1 Statement of the Problem

Indian courts and investigating agencies confront a persistent gap between the increasingly detailed statutory architecture governing digital evidence admissibility and the practical, institutional capacity to satisfy its requirements consistently across the country's cybercrime investigation apparatus. The BSA's stricter, dual-certificate regime addresses some doctrinal uncertainties inherited from Section 65B jurisprudence, but introduces new practical burdens — hash-value disclosure, expert certification — that presuppose a level of technical forensic capacity not uniformly available across India's investigating agencies and forensic laboratories.

1.2 Objectives of the Study

- To trace the jurisprudential evolution of electronic evidence admissibility in India from Section 65B of the Indian Evidence Act to Section 63 of the Bharatiya Sakshya Adhiniyam.
- To critically analyse the Section 63 BSA dual-certificate architecture and its 2025-2026 judicial interpretation.
- To examine the practical realities of cyber forensic investigation in India, including chain-of-custody protocols, hash-based verification, and institutional forensic infrastructure.
- To identify systemic reliability and authentication challenges affecting cybercrime prosecution outcomes.
- To recommend legislative, institutional and procedural reforms to strengthen the admissibility, authentication and reliability of digital evidence in India.

[4] "Cyber Forensics and the Law: Addressing Digital Crimes," International Journal of Creative Research Thoughts (2025), citing National Crime Records Bureau data (2022).

ISSN: 2582-6433

1.3 Research Questions

- How has the jurisprudential treatment of electronic evidence certification evolved from Anvar P.V. through Arjun Panditrao Khotkar to the Section 63 BSA regime, and does this evolution resolve or merely relocate prior doctrinal uncertainty?
- Does the Section 63 BSA dual-certificate architecture adequately balance evidentiary rigour against the practical forensic capacity available to Indian investigating agencies?
- What institutional and infrastructural constraints most significantly undermine the reliability and courtroom defensibility of digital evidence in Indian cybercrime prosecutions?
- What reforms would most effectively close the gap between digital evidence law's doctrinal sophistication and its practical enforcement?

1.4 Research Methodology

This study adopts a doctrinal legal research methodology, involving critical analysis of the BSA, the erstwhile Indian Evidence Act, the Information Technology Act, 2000, and judicial precedent, supplemented by secondary literature drawn from cyber forensic practice sources and National Crime Records Bureau data. The analysis integrates doctrinal statutory interpretation with practice-oriented forensic and institutional literature to ground the legal analysis in operational reality.

1.5 Scope and Limitations

The paper is confined to the admissibility, authentication and reliability of digital evidence within Indian criminal proceedings, with particular reference to cybercrime investigation. It does not address the use of electronic evidence in civil or matrimonial proceedings save where illustrative, nor does it undertake comparative analysis of foreign digital evidence regimes in detail. Data and case law are current as of August 2026.

2. LITERATURE REVIEW

2.1 The Section 65B Jurisprudential Trilogy

The doctrinal foundation for this paper's analysis rests on a well-documented trilogy of Supreme Court decisions interpreting Section 65B of the erstwhile Indian Evidence Act. In Anvar P.V. v. P.K. Basheer, the Supreme Court held that any documentary evidence by way of an electronic record, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B, and that a certificate under Section 65B(4) is a

ISSN: 2582-6433

mandatory precondition to the admissibility of secondary electronic evidence.[5] Subsequent practice revealed a significant practical difficulty: parties unable to obtain a certificate from a non-cooperating party in control of the relevant device found themselves unable to adduce otherwise probative electronic evidence, prompting the Supreme Court in Shafhi Mohammad v. State of Himachal Pradesh to hold that the certificate requirement could be relaxed where a party was not in possession of the device and thus unable to secure the necessary certification.[6] This relaxation itself generated fresh uncertainty, resolved by a three-judge bench in Arjun Panditrao Khotkar v. Kailash Kishanrao Gorantyal, which held that Shafhi Mohammad's relaxation was incorrect, reaffirming the certificate's mandatory character even where the original device is produced, while clarifying that a party unable to obtain a certificate from a recalcitrant custodian may seek a judicial direction compelling production.[7]

2.2 Section 63 BSA: Statutory Codification and Early Interpretation

A substantial and rapidly developing body of 2025-2026 commentary addresses Section 63 of the BSA, which came into force on 1 July 2024 and governs proceedings initiated on or after that date, while Section 65B continues to apply, by virtue of the BSA's savings clause, to matters already pending at commencement.[8] Shodhsagar's peer-reviewed review of the BSA's electronic-evidence framework observes that Sections 61, 62 and 63 together establish a modernised statutory pathway addressing admissibility, the mode of proof, and evidentiary value respectively — Section 61 providing that an electronic record shall not be denied admissibility merely because it is electronic, Section 62 stipulating that its contents are to be proved in accordance with Section 63, and Section 63 setting out the detailed certification mechanics.[9] A significant 2026 development, noted across multiple practitioner sources, is the introduction of a standardised, statutorily prescribed Schedule certificate format divided into two parts: Part A, completed by the person in charge of the relevant computer or communication device, and Part B, completed by a technical expert, who must additionally disclose the hash value computed for the electronic record and a corresponding hash report.[10] Commentary emphasises that courts are increasingly scrutinising the technical competence of the Part B expert signatory, treating an inadequately qualified or unsubstantiated expert

[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 Kishanrao Gorantyal, (2020) 7 SCC 1, at paras 55-72.
[8]"Section 65B and Section 63 BSA Certificate: Format, Rules and Complete Legal Guide 2026," Shonee Kapoor (2026).
[9]"Electronic Evidence in Indian Law," supra note 2.
[10]"BSA 63 Electronic Record Certificate: A 2026 Guide for Advocates," Nyaya Yantra (2026); "Section 65B and Section 63 BSA Certificate," supra note 4.

ISSN: 2582-6433

certification as a ground for challenging the certificate's sufficiency.[11]

2.3 Recent Supreme Court Interpretation of Section 63 BSA

Early appellate engagement with Section 63 confirms both continuity with, and material departure from, the Section 65B jurisprudential trilogy. One of the first significant Supreme Court judgments interpreting Section 63 held that a compact disc constitutes an electronic record admissible once Section 63's requirements are satisfied, and that where electronic evidence is proved through the special statutory certification mode, the certificate is mandatory — but where instead proved through oral witness examination, the certificate requirement may be treated as directory rather than mandatory, a clarification of practical significance for cases in which the device custodian or examining expert is available to testify directly.[12] The same body of commentary identifies Chandrabhan Sudam Sanap as a further 2025 reaffirmation of the Anvar/Arjun Panditrao line of authority as applied under the new BSA framework, alongside continuing application of the Anvar principles to matters straddling the 1 July 2024 transition date, as illustrated by the Andhra Pradesh High Court's July 2024 ruling applying the Section 65B framework while noting the BSA's prospective governance of matters initiated thereafter.[13] Further commentary references a 2026 ruling in which the Supreme Court is reported to have upheld the rationality of the Section 63 Schedule, including its hash-value and expert-certification requirements, while leaving certain questions concerning the permissible category of qualifying experts open for further clarification.[14]

2.4 Cyber Forensic Investigation Literature

A distinct strand of literature addresses the practical forensic methodology underlying digital evidence generation, emphasising the centrality of chain-of-custody documentation, forensic imaging, write-blocking tools, and cryptographic hash verification (typically SHA-256 or MD5) to preserving evidentiary integrity from seizure through courtroom presentation.[15] A peer-reviewed study specifically addressing cybercrime investigation and electronic evidence admissibility in India identifies persistent structural challenges — imbalanced forensic infrastructure across states, stringent and sometimes inconsistently applied procedural

[11]Nyaya Yantra, supra note 5.
[12]Kailash S/o Bajirao Pawar v. State of Maharashtra (2025), as discussed in "Section 63 of BSA Certificate: Latest Judgment and Legal Position (2024-2026)," Lawful Legal (2026).
[13]Legal Service India, supra note 3 (referencing Rahil and Chandrabhan Sudam Sanap, 2025); Lawful Legal, supra note 6 (referencing Andhra Pradesh High Court, CRLP/4885/2024).
[14]"Section 65B and Section 63 BSA Certificate," supra note 4, discussing Pune Bar Association v. Union of India (2026).
[15]Rampurawala & Vairagar, supra note 1.

ISSN: 2582-6433

regulations, and a shortage of well-qualified forensic experts — as undermining the practical efficacy of the BSA's otherwise strengthened legal framework, citing illustrative case law including Neha Rafiq Chachadi v. State of Karnataka and Vijesh v. State of Kerala on search-and-seizure and evidentiary procedure.[16]

2.5 Institutional Forensic Infrastructure

Comparative institutional literature on India's forensic laboratory ecosystem documents a two-tier structure: government Forensic Science Laboratories (FSLs) and Central Forensic Science Laboratories (CFSLs) — spanning twenty-seven state FSLs and seven CFSLs — offering the highest institutional credibility but subject to typical turnaround times of forty-five to one hundred eighty days due to case backlog, alongside MeitY Section 79A-empanelled private laboratories offering substantially faster turnaround (five to thirty days) with high, though not always equivalent, admissibility credibility.[17] The same literature identifies a significant capability gap in blockchain and cryptocurrency forensic analysis, noting the absence of any domestic forensic laboratory with certified, institutional-grade blockchain-analytics capability comparable to internationally established providers, a gap of particular significance given the increasing use of cryptocurrency in cross-border cybercrime proceeds.[18] Government initiatives such as NCRB-Abhigyan, the Crime and Criminal Tracking Network and Systems-integrated e-Prosecution 2.0, and e-Forensics 2.0, launched to strengthen chain-of-custody documentation and inter-agency coordination between forensic laboratories and law enforcement, represent institutional responses to these documented capacity gaps.[19]

2.6 Research Gap

Existing literature tends either to provide doctrinal commentary on the Section 65B-to-Section 63 transition in isolation, or to address cyber forensic institutional capacity as a separate, largely technical concern. This paper integrates both strands within a single critical analysis, examining how the BSA's stricter statutory certification requirements interact with, and are constrained by, the practical forensic infrastructure available to Indian investigating agencies, and what this interaction means for the ultimate reliability of digital evidence in Indian criminal proceedings.

[16]"Cybercrime Investigations and Admissibility of Electronic Evidence in India: Addressing Paradigm Shift with Digital Forensics Integration," NFSU Journal of Forensic Justice (2026).
[17]"Cyber Forensic Labs in India 2026: Complete Guide," Nahar Blogs (2026).
[18]Id.
[19]"NCRB-Abhigyan, CrPI, e-Prosecution 2.0 and e-Forensics 2.0: A Digital Leap in India's Criminal Justice System," Sanskriti IAS (2026).

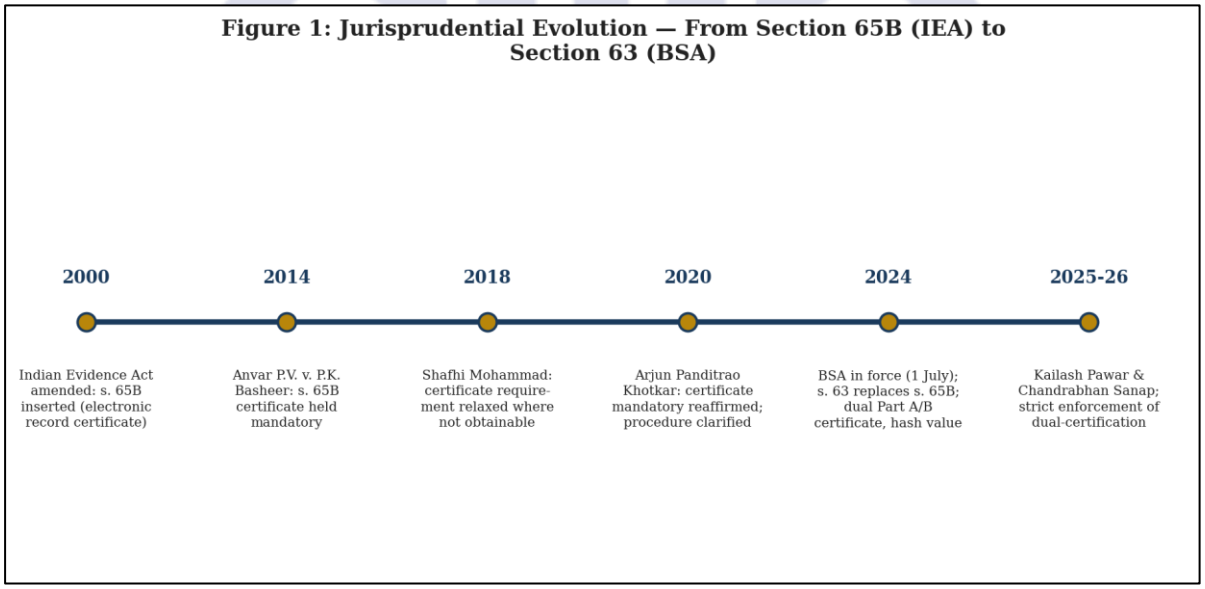
ISSN: 2582-6433

3. ANALYSIS AND DISCUSSION

3.1 From Section 65B to Section 63: A Jurisprudential Map

The two-decade evolution traced in Figure 1 reveals a doctrinal trajectory oscillating between strict formalism and practical flexibility, before converging, under the BSA, on a codified but substantially more technically demanding certification standard. Section 65B, inserted into the Indian Evidence Act by the Information Technology Act, 2000, required a certificate identifying the electronic record, describing the manner of its production, and detailing the device used, signed by a person occupying a responsible official position in relation to the device.[20] Anvar P.V. established this certificate as mandatory; Shafhi Mohammad introduced a practical relaxation for cases of genuine unavailability; and Arjun Panditrao Khotkar restored strict mandatoriness while clarifying the availability of judicial directions to compel a recalcitrant custodian's production of the certificate.[21] Section 63 of the BSA now codifies this settled position while adding materially new technical requirements — most significantly, the dual Part A/Part B certificate structure and mandatory hash-value disclosure, discussed in Part 3.2 below.

Figure 1: Jurisprudential Evolution — From Section 65B (IEA) to Section 63 (BSA)



3.2 The Section 63 BSA Dual-Certificate Architecture

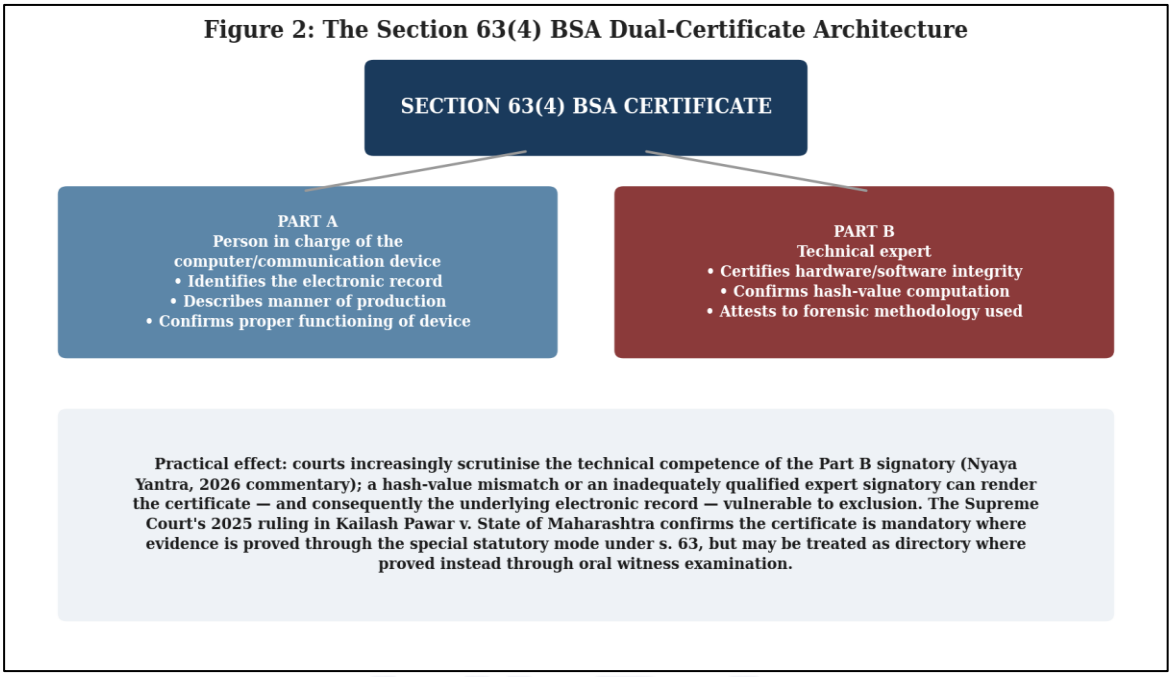
Section 63(1) of the BSA deems a "computer output" — information contained in an electronic record printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory, or otherwise stored, recorded or copied in electronic form — to be a document, admissible without further proof or production of the original, provided the

[20]Indian Evidence Act, 1872, s. 65B(4) (as inserted by the Information Technology Act, 2000) (repealed).
[21]Supra notes 8-10.

ISSN: 2582-6433

conditions specified in the section are satisfied.[22] Section 63(4) sets out the certificate requirements in materially greater technical detail than its predecessor, mandating a certificate that identifies the electronic record and describes its manner of production, particularises the device involved, addresses the conditions specified in Section 63(2), and is signed by a person in charge of the device or the management of the relevant activities, together with an expert.[23] As illustrated in Figure 2, practitioner commentary describes the resulting document as a standardised, statutorily prescribed Schedule divided into two parts — Part A completed by the device custodian and Part B completed by a technical expert, who must additionally disclose the hash value computed for the record and a supporting hash report.[24]

Figure 2: The Section 63(4) BSA Dual-Certificate Architecture



This dual-certificate architecture represents a deliberate legislative response to a recognised weakness of the erstwhile Section 65B regime: a single custodian's certificate could attest to a device's proper functioning without any independent verification of the electronic record's technical integrity, leaving courts reliant on essentially unverified assertions regarding data authenticity. The addition of a mandatory hash-value disclosure — a cryptographic fingerprint capable of demonstrating, with extremely high probability, whether a file has been altered since acquisition — introduces an objectively verifiable technical safeguard largely absent from the Section 65B framework.[25] Early judicial engagement confirms that courts are treating this technical rigour seriously: commentary notes increasing scrutiny of the Part B expert

[22]Bharatiya Sakshya Adhiniyam, 2023, s. 63(1).
[23]Id., s. 63(4).
[24]Nyaya Yantra, supra note 5.
[25]Rampurawala & Vairagar, supra note 1 (on hash-based integrity verification).

ISSN: 2582-6433

signatory's demonstrated technical competence, with an inadequately substantiated expert certification identified as a specific and growing ground for admissibility challenge.[26] At the same time, the Supreme Court's ruling in Kailash Pawar v. State of Maharashtra confirms an important practical safety valve carried over in substance from the Section 65B jurisprudence: the certificate requirement is mandatory only where electronic evidence is proved through the special statutory mode under Section 63; where instead proved through oral testimony from a witness with direct knowledge of the record's provenance, the certificate may be treated as directory rather than mandatory — preserving a route to admissibility for cases where rigid certificate compliance is not achievable but reliable alternative proof exists.[27]

3.3 Chain of Custody and Forensic Integrity in Practice

Beyond the certificate's formal requirements, the substantive reliability of digital evidence depends critically on unbroken chain-of-custody documentation from the point of seizure to courtroom presentation. Practice literature describes the chain of custody as a meticulous, unbroken record of every person who has handled a given item of evidence, ensuring no unauthorised access or tampering has occurred, typically involving secure evidence-locker storage and a complete handling log pending transmission to a forensic science laboratory or empanelled cyber forensic expert.[28] Sound forensic methodology requires that original data be preserved unaltered, with all analytical work conducted exclusively on verified forensic copies ("images") created using write-blocking hardware to prevent inadvertent modification of the source device, with cryptographic hash values computed both at seizure and at each subsequent point of analysis to demonstrate continued data integrity.[29] Peer-reviewed Indian scholarship confirms this methodology is well understood in principle but inconsistently applied in practice, citing persistent infrastructure imbalance and a shortage of adequately trained forensic personnel as recurring sources of chain-of-custody failure.[30]

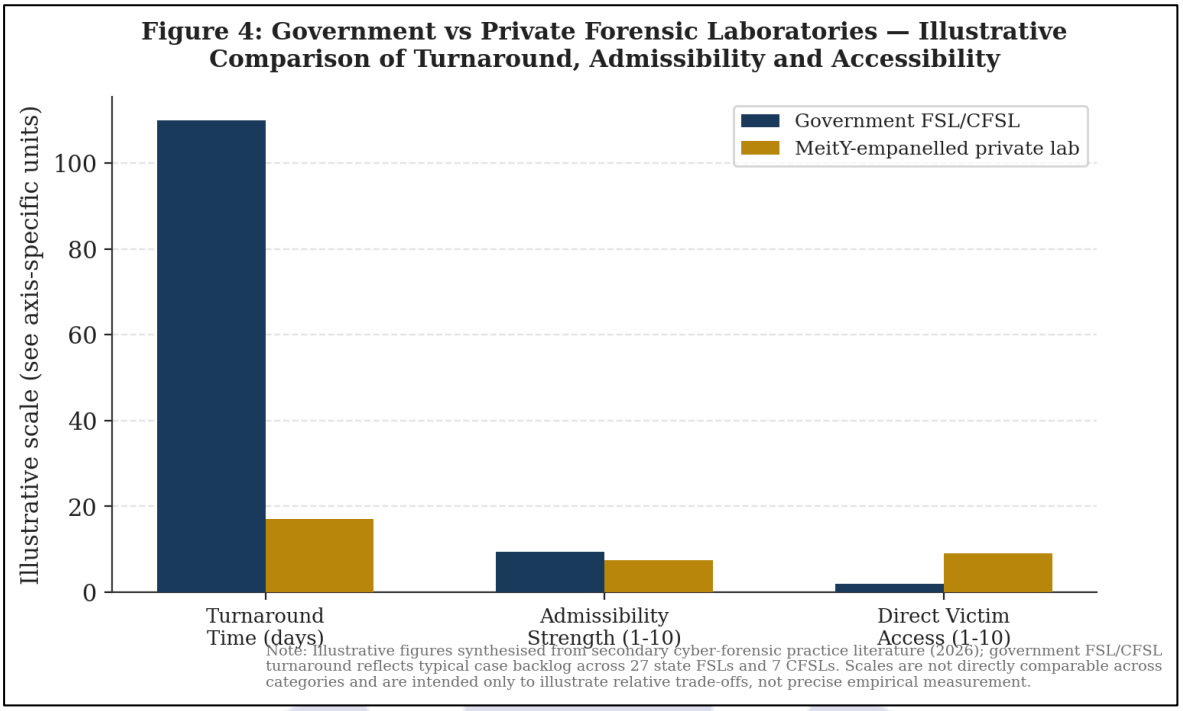
3.4 Institutional Forensic Infrastructure: Capacity and Constraint

Figure 4 presents an illustrative comparison of the two principal institutional pathways for digital forensic examination available to Indian investigators and litigants: government Forensic Science Laboratories and Central Forensic Science Laboratories, and MeitY Section

[26]Nyaya Yantra, supra note 5.
[27]Kailash Pawar v. State of Maharashtra, supra note 11.
[28]"The Digital Forensic Investigation Process: Chain of Custody and Evidence Preservation," Legal Service India (2026).
[29]Rampurawala & Vairagar, supra note 1.
[30]NFSU Journal of Forensic Justice, supra note 13.

ISSN: 2582-6433

79A-empanelled private laboratories.



As the comparison illustrates, government FSLs and CFSLs offer the highest institutional credibility — their reports are, in practitioner experience, almost never challenged on institutional grounds — but are subject to substantial case backlog across the twenty-seven state FSLs and seven CFSLs, producing typical turnaround times ranging from forty-five to one hundred eighty days, a delay with direct implications for pre-trial detention, investigative momentum, and, ultimately, conviction rates in time-sensitive cybercrime matters.[31] MeitY-empanelled private laboratories offer substantially faster turnaround and, where properly empanelled, high (if not always institutionally equivalent) admissibility credibility, but victims typically lack direct access to government forensic examination absent a formally registered FIR and a corresponding investigating officer's request, creating a further practical bottleneck for victims seeking expedited private examination as a complement to, or in advance of, formal government forensic processing.[32] A distinctly under-addressed capability gap concerns cryptocurrency and blockchain forensic analysis: the absence of certified, institutional-grade domestic blockchain-analytics capability means that, in cases involving cryptocurrency-denominated fraud proceeds — an increasingly common feature of cross-border cybercrime — the traceable evidentiary chain frequently terminates at the point of conversion to decentralised or foreign-exchange-held cryptocurrency, precisely where the most legally significant cross-

[31]Nahar Blogs, supra note 14.
[32]Id.

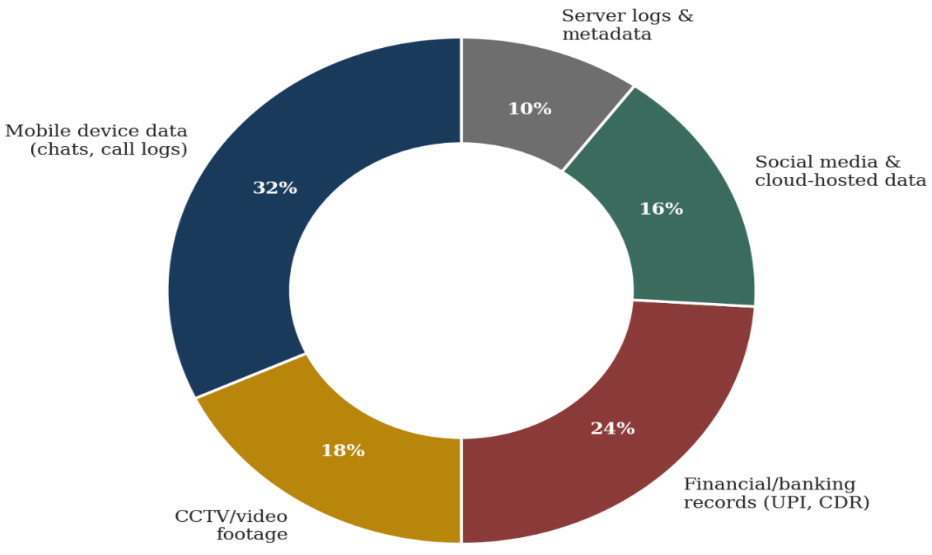
 ISSN: 2582-6433

border criminal network activity begins.[33]

3.5 Systemic Reliability Concerns and Conviction Outcomes

The cumulative effect of certification complexity, forensic capacity constraints and institutional bottlenecks is reflected in persistently low cybercrime conviction rates: secondary literature places India's cybercrime conviction rate below eighteen percent, attributing this substantially to a lack of prosecutable evidence and poor digital chain-of-custody practice.[34] The same literature identifies compounding structural obstacles beyond forensic capacity alone — low digital literacy among victims (particularly in rural areas) impeding effective initial evidence preservation, jurisdictional compliance requirements imposed by foreign-headquartered platforms (Meta, Google) that delay information exchange, and India's continued non-membership of the Council of Europe's Budapest Convention on Cybercrime, which constrains the speed and reliability of cross-border evidentiary cooperation.[35] Figure 3 illustrates the composition of digital evidence sources typically relied upon in Indian cybercrime prosecutions, underscoring the practical centrality of mobile-device and financial-transaction records — categories for which the Section 63 certification burden falls particularly heavily on investigating officers given the volume and diversity of devices and platforms involved in a typical cybercrime investigation.

Figure 3: Illustrative Distribution of Digital Evidence Sources in Indian Cybercrime Investigations



Note: Illustrative distribution synthesised from cyber forensic practice literature and NCRB cybercrime case-category data; mobile-device and financial-transaction records dominate evidentiary reliance.

[33]Id.
[34]International Journal of Creative Research Thoughts, supra note 3.
[35]Id.

ISSN: 2582-6433

3.6 Emerging Authentication Challenges: AI-Generated Content

A frontier challenge, not directly addressed by either the Section 65B jurisprudential trilogy or the codified Section 63 framework, concerns the authentication of artificial-intelligence-generated or synthetically manipulated digital content — deepfake audio, video and images capable of near-indistinguishable visual and auditory fidelity to genuine recordings. Neither the certificate's technical requirements nor its hash-value verification mechanism, designed to confirm that a file has not been altered since acquisition, addresses the logically prior question of whether the content itself, however unaltered since its creation, is an authentic record of a real event or an entirely fabricated synthetic artefact. Practitioner commentary notes that Indian courts are only beginning to grapple with this authentication challenge, and that the Section 63 framework's silence on AI-generated content authentication represents a significant and growing gap given the increasing accessibility of consumer-grade generative AI tools.

3.7 The Transition Period: Section 65B and Section 63 in Parallel

A further practical complexity arises from the BSA's savings clause, which preserves the application of the Indian Evidence Act, including Section 65B, to proceedings, applications, trials, inquiries, investigations and appeals pending immediately before the BSA's 1 July 2024 commencement.[36] Investigating officers, prosecutors and courts must consequently maintain dual procedural competence — correctly identifying which statutory certificate regime governs a given matter based on its commencement date — a transitional burden that practitioner literature identifies as a continuing, if diminishing, source of procedural confusion into 2026, more than two years after the BSA's commencement.[37]

3.8 Comparative Snapshot: Section 65B (IEA) and Section 63 (BSA)

Table 1 summarises the principal doctrinal and procedural differences between the two certification regimes.

Feature	Section 65B, Indian Evidence Act, 1872 (repealed)	Section 63, Bharatiya Sakshya Adhiniyam, 2023
Certificate structure	Single certificate by person in responsible official position	Dual-part certificate: Part A (device custodian) and Part B (technical expert)

[36]Shonee Kapoor, supra note 4.
[37]Lawful Legal, supra note 6.

ISSN: 2582-6433

Feature	Section 65B, Indian Evidence Act, 1872 (repealed)	Section 63, Bharatiya Sakshya Adhiniyam, 2023
Hash-value disclosure	Not statutorily mandated	Mandatory hash-value computation and hash report
Mandatory character	Mandatory (Anvar); relaxed (Shafhi Mohammad); reaffirmed mandatory (Arjun Panditrao)	Mandatory where proved via special statutory mode; directory where proved via oral testimony (Kailash Pawar)
Applicability	Continues to apply to matters pending before 1 July 2024 (savings clause)	Applies to proceedings initiated on or after 1 July 2024
Judicial direction for recalcitrant custodian	Available per Arjun Panditrao Khotkar	Continued availability, consistent with pre-BSA position
Expert certification standard	No express statutory expert-competence requirement	Part B requires demonstrated technical expert competence, increasingly scrutinised by courts

Table 1: Comparative snapshot of the Section 65B (IEA) and Section 63 (BSA) electronic evidence certification regimes.

4. FINDINGS

- The jurisprudential trajectory from Anvar P.V. through Shafhi Mohammad to Arjun Panditrao Khotkar reflects a search for the appropriate balance between certification rigour and practical accessibility, a balance the Section 63 BSA regime now attempts to codify more precisely but does not resolve definitively, given continuing judicial elaboration of its scope in 2025-2026 rulings.
- Section 63's dual-part certificate architecture, incorporating mandatory hash-value disclosure and expert Part-B certification, introduces a meaningful, objectively verifiable technical safeguard against evidentiary tampering absent from the Section 65B regime, but correspondingly raises the technical competency threshold investigating officers and forensic examiners must satisfy to secure admissibility.

ISSN: 2582-6433

- The Supreme Court's clarification in Kailash Pawar v. State of Maharashtra that the certificate requirement is directory rather than mandatory where proved through oral testimony preserves an important practical safety valve, though its precise contours remain subject to ongoing judicial elaboration.
- India's institutional forensic infrastructure — divided between high-credibility but slow government FSLs/CFSLs and faster but institutionally variable private empanelled laboratories — creates a persistent practical bottleneck disproportionately affecting time-sensitive cybercrime investigation and victim access to timely forensic examination.
- A significant capability gap in domestic blockchain and cryptocurrency forensic analysis leaves the evidentiary trail in cryptocurrency-facilitated cybercrime frequently terminating at the point of currency conversion, precisely where cross-border criminal network activity is most legally significant.
- Cybercrime conviction rates below eighteen percent are substantially attributable to deficient digital evidence handling and chain-of-custody practice, compounded by low victim digital literacy, jurisdictional friction with foreign-headquartered platforms, and India's non-membership of the Budapest Convention framework.
- Neither the Section 65B jurisprudential trilogy nor the codified Section 63 framework directly addresses the authentication of artificial-intelligence-generated or synthetically manipulated digital content, a significant and growing gap given the increasing accessibility of generative AI tools.
- The BSA's savings clause, preserving Section 65B's application to pre-1 July 2024 matters, continues to generate transitional procedural complexity for investigating officers, prosecutors and courts required to correctly identify the governing certification regime for a given matter.

5. RECOMMENDATIONS

5.1 Legislative and Doctrinal Reforms

- Issue authoritative judicial or Law Commission guidance clarifying the precise scope of the directory/mandatory distinction articulated in Kailash Pawar, to reduce inconsistent trial-court application of the Section 63 certificate requirement.
- Introduce specific statutory or subordinate-rule guidance on the authentication of artificial-intelligence-generated and synthetically manipulated digital content, addressing the authentication gap distinct from, and prior to, the hash-based integrity verification the current framework provides.

ISSN: 2582-6433

- Clarify, through amendment or authoritative guidance, the minimum technical qualification standard required for a Part B expert signatory under Section 63(4), to reduce present uncertainty and inconsistent judicial scrutiny.

5.2 Institutional and Capacity-Building Reforms

- Expand government FSL and CFSL capacity, staffing and case-management systems to reduce the current forty-five-to-one-hundred-eighty-day turnaround backlog, prioritising time-sensitive cybercrime matters.
- Invest in the development of certified, institutional-grade domestic blockchain and cryptocurrency forensic analysis capability, to close the presently identified evidentiary gap in cryptocurrency-facilitated cybercrime investigation.
- Expand and standardise MeitY Section 79A empanelment criteria for private forensic laboratories, with periodic institutional audit, to improve the consistency of admissibility credibility across empanelled laboratories.
- Institute mandatory, periodically refreshed training for investigating officers and forensic examiners on chain-of-custody documentation, hash-based verification methodology, and the Section 63(4) dual-certificate requirements.

5.3 Procedural and Access Reforms

- Consider a limited direct-victim-access pathway to government forensic examination for time-sensitive cybercrime matters, reducing present reliance on investigating-officer-mediated referral alone.
- Develop standardised, judicially endorsed chain-of-custody documentation templates for digital evidence, to promote consistency across investigating agencies and reduce admissibility disputes arising from documentation gaps.

5.4 Judicial Training and Coordination

- Expand specialised judicial training on the technical substance of hash-based verification, forensic imaging methodology, and the distinction between admissibility (certificate compliance) and evidentiary weight (substantive reliability), to support more consistent and technically informed trial-court decision-making.
- Strengthen coordination mechanisms, building on initiatives such as NCRB-Abhigyan and e-Forensics 2.0, between forensic laboratories, investigating agencies and

ISSN: 2582-6433

prosecuting authorities to reduce chain-of-custody documentation failures arising from inter-agency handoff.

6. CONCLUSION

India's digital evidence framework has undergone substantial doctrinal refinement over the past decade, culminating in the Bharatiya Sakshya Adhiniyam's codified, technically detailed Section 63 certification regime — a regime that resolves much of the interpretive uncertainty generated by the Section 65B jurisprudential trilogy while introducing meaningful new safeguards, most notably mandatory hash-value disclosure and dual custodian-expert certification. Yet this analysis demonstrates that legal codification alone cannot resolve the practical, institutional gap between the BSA's technically sophisticated evidentiary requirements and the forensic capacity available to investigate and prosecute cybercrime across India's diverse institutional landscape. Persistently low cybercrime conviction rates, institutional bottlenecks in government forensic laboratories, a significant capability gap in cryptocurrency forensic analysis, and the emerging, as-yet-unaddressed challenge of authenticating artificial-intelligence-generated content together constitute a substantial and continuing reliability deficit in Indian cybercrime evidence. Closing this deficit will require sustained institutional investment in forensic capacity and personnel training, clearer judicial and legislative guidance on the technical standards the Section 63 framework demands, targeted legislative attention to emerging authentication challenges, and continued procedural refinement informed by the practical realities of digital evidence handling at the investigative front line. Only through such integrated doctrinal and institutional development can India's digital evidence framework fulfil its stated aspiration of ensuring that electronic records, properly authenticated, serve as a reliable and trustworthy foundation for criminal justice in the digital age.

REFERENCES

A. Statutes and Legislative Instruments

1. *Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).*
2. *Indian Evidence Act, 1872 (repealed), s. 65B (as inserted by the Information Technology Act, 2000).*
3. *Information Technology Act, 2000 (Act No. 21 of 2000).*
4. *Bharatiya Nyaya Sanhita, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023.*

ISSN: 2582-6433

B. Cases

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 Kishanrao Gorantyal, (2020) 7 SCC 1.*
8. *Kailash S/o Bajirao Pawar v. State of Maharashtra (2025).*
9. *Chandrabhan Sudam Sanap v. State of Maharashtra (2025).*
10. *Pune Bar Association v. Union of India (2026).*
11. *Neha Rafiq Chachadi v. State of Karnataka.*
12. *Vijesh v. State of Kerala.*

C. Journal Articles and Reports

13. *Munira M. Rampurawala & Anjali R. Vairagar, "Role of Cyber Forensic in Crime Investigation," 14(2) International Journal of Engineering Research & Technology (2026).*
14. *"Electronic Evidence in Indian Law: Admissibility, Authentication and Evidentiary Value," Indian Journal of Law (2026).*
15. *"Cybercrime Investigations and Admissibility of Electronic Evidence in India: Addressing Paradigm Shift with Digital Forensics Integration," NFSU Journal of Forensic Justice (2026).*
16. *"Cyber Forensics and the Law: Addressing Digital Crimes," International Journal of Creative Research Thoughts (2025).*
17. *"Developments in Cyber Forensics in India: Combining Legal Frameworks with Technological Innovations," ResearchGate (2025).*

D. Web and Institutional Sources

18. *"Section 65B vs. Section 63 BSA: Electronic Evidence Admissibility in India," Legal Service India (2026), https://www.legalserviceindia.com.*
19. *"Section 65B and Section 63 BSA Certificate: Format, Rules and Complete Legal Guide 2026," Shonee Kapoor (2026), https://www.shoneekapoor.com.*
20. *"BSA 63 Electronic Record Certificate: A 2026 Guide for Advocates," Nyaya Yantra (2026), https://www.nyayayantra.in.*
21. *"Section 63 of BSA Certificate: Latest Judgment and Legal Position (2024-2026)," Lawful Legal (2026), https://lawfullegal.in.*

ISSN: 2582-6433

22. *"High Court Protocols 2026: Section 63 BSA & Technical Standards for Digital Evidence," Lawsathi (2026), https://lawsathi.in.*
23. *"Digital Forensics: Data Recovery, Electronic Triage, and Courtroom Admissibility," Legal Service India (2026).*
24. *"The Digital Forensic Investigation Process: Chain of Custody and Evidence Preservation," Legal Service India (2026).*
25. *"Cyber Forensic Labs in India 2026: Complete Guide," Nahar Blogs (2026), https://blogs.nahar.om.*
26. *"NCRB-Abhigyan, CrPI, e-Prosecution 2.0 and e-Forensics 2.0: A Digital Leap in India's Criminal Justice System," Sanskriti IAS (2026).*
27. *"The Future of Forensic and Cyber Law Trials Under New Criminal Codes in India," Legal Blur (2026).*