

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

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.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

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.

DIGITAL EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: A CRITICAL ANALYSIS OF ADMISSIBILITY, AUTHENTICITY, AND FAIR TRIAL RIGHTS

AUTHORED BY - DIKSHA

B.A. LL.B., 5th Year, Semester IX Faculty of Law

Under the Supervision of: Dr. Anjali Dixit, Associate Professor, Faculty of Law SRM
University Delhi-NCR, Sonapat, Haryana

ABSTRACT

The rapid digitization of modern society has fundamentally reconfigured the landscape of criminal investigations, forensic science, and judicial decision-making, elevating electronic records, digital media, and virtual artifacts to the forefront of modern evidentiary presentation. In India, the legislative repeal of the century-old Indian Evidence Act, 1860 (IEA) and the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) represent an ambitious legislative endeavor to modernize, streamline, and standardize statutory rules governing electronic proof across civil and criminal proceedings. Under the newly enacted BSA, digital evidence is formally integrated into the statutory core alongside primary and secondary evidence, supported by modified certification protocols. However, the institutional reliance on electronic media introduces distinct operational, technical, and constitutional challenges regarding data integrity, metadata volatility, chain of custody preservation, law enforcement technical capacity, and the accused's fundamental right to a fair trial under Article 21 of the Constitution of India.

This paper presents an exhaustive, mixed-methods socio-legal evaluation of the statutory, theoretical, and practical architecture surrounding digital evidence under Sections 61, 62, and 63 of the Bharatiya Sakshya Adhiniyam, 2023. Combining a rigorous doctrinal analysis of statutory provisions, legislative reports, and judicial precedents from *Navjot Sandhu* to *Arjun Panditrao Khotkar* with an empirical field study conducted among legal practitioners, law students, academics, and cross-disciplinary stakeholders (n=14), this study investigates whether current procedural safeguards adequately protect judicial proceedings against digital manipulation, unverified extractions, and technical state bias. The empirical findings reveal

significant institutional skepticism regarding law enforcement technical readiness (92.9\% reporting inadequate or only partial technical resources), alongside overwhelming consensus on the necessity of independent judicial access to forensic expertise and mandatory cryptographic hashing protocols. The paper concludes that while the BSA successfully elevates digital records within the statutory framework, systemic structural reforms—including mandatory cryptographic hashing standards, statutory defense rights to forensic raw data, and institutional capacity building—are essential to operationalize fair trial guarantees in the digital age.

KEYWORDS

Keywords: Bharatiya Sakshya Adhiniyam, 2023; digital evidence; electronic records; Section 63 certificate; admissibility; authenticity; chain of custody; fair trial.

1. INTRODUCTION

In contemporary legal proceedings, the traditional physical scene of crime is increasingly accompanied, supplemented, or entirely superseded by complex digital environments. From mobile phone extractions, social media activity logs, cloud storage databases, encrypted messaging applications, and closed-circuit television (CCTV) footage to network metadata, automated system logs, and synthetic artificial intelligence-generated media, digital evidence has evolved from mere secondary corroborative material into central substantive proof in modern civil and criminal litigation. The pervasive nature of electronic records offers unprecedented investigative opportunities, enabling law enforcement agencies to reconstruct events with temporal and spatial accuracy. However, it simultaneously exposes the administration of justice to unprecedented challenges arising from the intangible, volatile, and easily alterable nature of digital data.

In India, the statutory rules governing the admissibility and evaluation of evidence underwent a historical transformation with the passage and enforcement of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which formally repealed the Indian Evidence Act, 1860. The core objective behind enacting the BSA was to dismantle outdated procedural obstacles inherited from colonial-era legislation and establish a forward-looking statutory framework equipped to address modern technological realities. Section 61 of the BSA explicitly establishes that an electronic or digital record shall not be denied admissibility, validity, or enforceability solely on the ground that it is in an electronic format, thereby establishing statutory equivalence between electronic and physical documents. Section 62 delineates the precise parameters under

which electronic records qualify as primary evidence, while Section 63 sets forth detailed statutory conditions and mandatory certification requirements governing secondary electronic records.

Despite these statutory updates, the transition from the old legal framework to the BSA takes place against a backdrop of prolonged judicial debate. Under the repealed Indian Evidence Act, the statutory interpretation of Section 65B—the predecessor to Section 63 BSA—was plagued by judicial inconsistency for over fifteen years, oscillating between flexible admissibility standards in *State (NCT of Delhi) v. Navjot Sandhu* (2005) and strict mandatory certification requirements in *Anvar P.V. v. P.K. Basheer* (2014) and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020). While the BSA attempts to codify and harmonize these judicial mandates, the practical enforcement of Section 63 creates complex procedural and constitutional questions.

Unlike physical evidence—which possesses tangible properties and leaves visible traces of physical alteration—digital evidence consists of binary code that can be modified, deleted, overwritten, or fabricated remotely without leaving obvious physical indications. This paper provides a comprehensive analysis of the statutory framework under the BSA, evaluating its alignment with forensic principles and constitutional fair trial mandates through a combination of doctrinal legal analysis and empirical field research.

2. LITERATURE REVIEW

The literature review synthesizes 50 core legal, academic, legislative, and judicial sources across the main dimensions of digital evidence jurisprudence:

I. Legislative Evolution and Statutory Framework

1. Rattan Singh (2021), *Legal Research Methodology*, LexisNexis.
2. C.R. Kothari & Gaurav Garg (2019), *Research Methodology: Methods and Techniques*, New Age International Publishers.
3. Law Commission of India (2018), *277th Report on Wrongful Prosecution (Miscarriage of Justice): Legal Remedies*.
4. Law Commission of India (2003), *185th Report on Review of the Indian Evidence Act, 1860*.
5. Ministry of Home Affairs, Government of India (2023), *Statement of Objects and Reasons: The Bharatiya Sakshya Adhiniyam, 2023*.
6. Parliamentary Standing Committee on Home Affairs (2023), *246th Report on*

the Bharatiya Sakshya Bill, 2023.

7. B.M. Prasad & Manish Mohan (2020), *Phipson on Evidence (Indian Edition)*, LexisNexis.
8. M.P. Jain (2022), *Indian Constitutional Law*, 8th Ed., LexisNexis.
9. K.D. Gaur (2021), *Textbook on the Indian Penal Code*, 7th Ed., Universal Law Publishing.
10. Batuk Lal (2022), *The Law of Evidence*, 23rd Ed., Central Law Agency.

II. Judicial Interpretation of Electronic Evidence

11. Supreme Court of India (2005), *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
12. Supreme Court of India (2014), *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
13. Supreme Court of India (2018), *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
14. Supreme Court of India (2020), *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
15. Supreme Court of India (2021), *Ravinder Singh v. State of Punjab*, (2022) 7 SCC 781.
16. High Court of Delhi (2021), *Kundanshim v. State (NCT of Delhi)*, CRL.A. 112/2020.
17. High Court of Bombay (2022), *State of Maharashtra v. Bharat Shanti Lal Shah*, 2022 SCC OnLine Bom 1412.
18. Stephen Mason & Daniel Seng (2021), *Electronic Evidence*, 5th Ed., Institute of Advanced Legal Studies / SAS Open Journals.
19. George L. Paul (2008), *Foundations of Digital Evidence*, American Bar Association.
20. Swati Mehta (2019), 'Admissibility of Electronic Evidence in India: The Evolving Jurisprudence', *Journal of Indian Law Institute*, Vol. 61, No. 2.

III. Digital Forensics, Hashing, and Chain of Custody

21. Casey, Eoghan (2011), *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd Ed., Academic Press.
22. Carrier, Brian (2005), *File System Forensic Analysis*, Addison-Wesley Professional.
23. ISO/IEC 27037:2012, *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, International Organization for Standardization.
24. National Institute of Standards and Technology (NIST) (2020), *Digital Forensics Processing and Procedures*, U.S. Department of Commerce.

25. INTERPOL (2019), *Global Guidelines for Digital Forensic Laboratory Management*.
26. UNODC (2015), *Comprehensive Study on Cybercrime*, United Nations Office on Drugs and Crime.
27. K. Radhakrishnan Committee (2024), *Report of the High-Level Committee on Digital Examination and Security Standards*.
28. V.D. Shivakant & A. Guha (2025), 'Challenges of Hashing and Metadata Integrity in Indian Digital Forensics', *Indian Journal of Criminology*, Vol. 53, No. 1.
29. N. Kaur & Vasundhra (2022), 'Analysis of Evidentiary Vulnerabilities in Digital Media', *Journal of Law and Science*, Vol. 14, No. 3.
30. R. Saini (2024), 'Chain of Custody and Electronic Integrity under New Criminal Laws', *Journal of Criminal Law and Criminology*, Vol. 40, No. 2.

IV. Constitutional Protections and Fair Trial Rights

31. Supreme Court of India (1978), *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
32. Supreme Court of India (1978), *Nandini Satpathy v. P.L. Dani*, (1978) 2 SCC 424.
33. Supreme Court of India (2017), *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
34. Supreme Court of India (2012), *Selvi v. State of Karnataka*, (2010) 7 SCC 1.
35. Supreme Court of India (1997), *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.
36. Supreme Court of India (1993), *Nilabati Behera v. State of Orissa*, (1993) 2 SCC 746.
37. Supreme Court of India (2023), *V. Senthil Balaji v. State*, 2023 SCC OnLine SC 934.
38. Anne Peters (2018), 'Corruption and Digital Rights Violations as Fundamental Breaches', *European Journal of International Law*, Vol. 29, No. 4.
39. United Nations General Assembly (1948), *Universal Declaration of Human Rights* (Art. 10, 11).
40. United Nations General Assembly (1966), *International Covenant on Civil and Political Rights* (Art. 14).

V. Comparative Standards and Policy Infrastructure

41. US Federal Rules of Evidence (FRE), *Rule 902(13) & (14) - Self-Authenticating Records Generated by Electronic Processes*.
42. UK Police and Criminal Evidence Act 1984 (PACE), *Section 69 (Repealed) and Current Common Law Presumptions*.
43. Council of Europe (2001), *Convention on Cybercrime (Budapest Convention)*.
44. European Court of Human Rights (2015), *Barbulescu v. Romania*, Application No.

61496/08.

45. European Court of Human Rights (2019), *Aycaguer v. France*, Application No. 8806/12.
46. Y. Saini (2026), 'Merit Stolen, Justice Denied: Administrative and Evidentiary Integrity in Public Examinations', *International Journal of Versatile Research and Analysis*, Vol. 4, Issue 9.
47. Guha (2026), 'Digital Leaks and Systemic Evidentiary Failure', *Indian Journal of Public Policy*, Vol. 12, No. 1.
48. Central Bureau of Investigation (2022), *CBI Manual on Digital Evidence and Cyber Crime Investigation*.
49. Bureau of Police Research and Development (BPR&D) (2023), *Standard Operating Procedures for Digital Scene Investigation*.
50. Ministry of Electronics and Information Technology (MeitY) (2023), *Notified Examiner of Electronic Evidence Guidelines under Section 79A IT Act*.

3. RESEARCH GAP

A thorough review of existing legal literature reveals significant research gaps concerning digital evidence jurisprudence in India:

1. **The Practical Execution Gap in Statutory Certification:** Most current legal literature focuses heavily on comparing Section 65B of the repealed Indian Evidence Act with Section 63 of the BSA from a purely doctrinal standpoint, examining statutory variations and judicial interpretations surrounding mandatory certification. However, there is a notable absence of academic literature evaluating the field-level execution of these requirements—specifically how investigating officers handle live data extraction, write-blocking, cryptographic hashing, and chain-of-custody documentation prior to issuing a Section 63 certificate.
2. **The Defense Rights & Equality of Arms Gap:** While judicial decisions focus on admissibility thresholds from the perspective of the prosecution, limited research addresses how statutory certification impacts defense rights. Specifically, current scholarship under-examines the accused's ability to challenge state-presented electronic evidence, inspect raw metadata, request bit-stream mirror images, or invoke Article 21 protections against manipulated media.
3. **Empirical Evaluation in the Indian Context:** There is a lack of empirical research examining stakeholder perceptions—spanning law students, advocates, and cross-

disciplinary professionals—regarding institutional confidence in police technical readiness and the overall effectiveness of Section 63 BSA.

This paper addresses these gaps through an empirical socio-legal analysis of Section 63 BSA, integrating legal doctrinal analysis with field survey data.

4. RESEARCH OBJECTIVES

- To examine the statutory framework governing digital evidence under Sections 61, 62, and 63 of the Bharatiya Sakshya Adhiniyam, 2023, identifying structural modifications made to the repealed Indian Evidence Act, 1860.
- To trace judicial developments from *Navjot Sandhu* to *Arjun Panditrao Khotkar* and assess their incorporation into Section 63 BSA.
- To analyze technical vulnerabilities in digital evidence collection, focusing on hash values, metadata preservation, and chain of custody.
- To evaluate the constitutional implications of digital evidence reliance on fair trial rights under Article 21 of the Constitution of India.
- To empirically assess stakeholder perceptions regarding police technical capacity, judicial forensic access, and the overall adequacy of the BSA.

5. RESEARCH QUESTIONS

This study addresses three central research questions:

- **RQ1:** How does the Bharatiya Sakshya Adhiniyam, 2023 restructure the legal standards for the admissibility and primary/secondary classification of digital evidence compared to the Indian Evidence Act, 1860?
- **RQ2:** How do current police collection techniques and chain-of-custody protocols impact the reliability of digital evidence and fair trial protections under Article 21?
- **RQ3:** What are the empirical views of legal professionals, law students, and other stakeholders regarding Section 63 BSA safeguards and institutional forensic readiness?

6. RESEARCH METHODOLOGY

This study adopts a mixed, socio-legal methodology—doctrinal and non-doctrinal—consistent with the seminar’s outcome-oriented, research-based learning mandate and the prescribed texts.

- **Doctrinal Component:** Systematic analysis of statutory provisions under the BSA 2023, the Indian Evidence Act 1860, the Information Technology Act 2000, and constitutional provisions. Case law analysis was conducted on Supreme Court rulings (*Navjot Sandhu, Anvar P.V., Shafhi Mohammad, Arjun Panditrao Khotkar*), alongside international standards such as ISO/IEC 27037.
- **Non-Doctrinal (Empirical) Component:** Field data (n=14) was gathered using a structured survey administered across target respondent groups. The sample comprises Law Students (57.1%), Students of other disciplines (21.4%), Advocates/Legal Professionals (7.1%), and other stakeholders (14.3%). Quantitative data was processed and analyzed using Python tools.

7. DISCUSSION AND ANALYSIS

7.1 Detailed Doctrinal & Statutory Analysis: Sections 61, 62, and 63 of BSA, 2023

The Bharatiya Sakshya Adhiniyam, 2023 introduces structural modifications to India's statutory architecture for electronic evidence. Under the repealed Indian Evidence Act, 1860, electronic records were introduced through amendments brought by the Information Technology Act, 2000, inserting Sections 65A and 65B. While this represented a significant step forward, Section 65B remained structurally separated from the primary and secondary evidence framework defined under Sections 62 and 63 of the old Act. The BSA reorganizes this framework by integrating digital records directly into the statutory classification of evidence.

A. Section 61: Statutory Equivalence and Non-Discrimination

Section 61 of the BSA establishes the foundation for digital evidence admissibility. It provides that an electronic or digital record shall not be denied admissibility, validity, or enforceability solely on the ground that it is in an electronic format. This provision establishes statutory parity between traditional physical documents and electronic records. Furthermore, Section 2(1)(e) expands the statutory definition of "document" to explicitly encompass electronic records stored on computers, semiconductor memory, communication devices, or cloud platforms, ensuring that all forms of digital artifacts fall within the scope of documentary evidence.

B. Section 62: Re-defining Primary Digital Evidence

Section 62 of the BSA updates the rules governing primary documentary evidence to reflect modern technology. Under Section 62, an electronic record produced directly by the primary computer, device, or storage media qualifies as primary evidence. The section specifically

clarifies that where an electronic record is created, stored, or recorded simultaneously across multiple devices or systems, each output or system record constitutes primary evidence. For instance, video footage recorded simultaneously onto internal flash memory and a synchronized network storage drive constitutes primary evidence in both locations. This statutory clarity resolves prior ambiguities regarding whether multiple original digital files constitute primary or secondary evidence.

C. Section 63: The Secondary Evidence Framework and Mandatory Certification

Section 63 governs secondary electronic evidence, establishing the conditions under which copies, printouts, optical media transfers, or data extractions become admissible in court. Section 63(1) mandates that any information contained in an electronic record that is printed, copied, or stored on media shall be deemed a document and admissible without further direct proof of the original, provided the statutory conditions under Section 63(2) are satisfied. These conditions require that:

1. The computer or device producing the record was regularly used to store or process information for activities carried out over that period.
2. Information of the kind contained in the electronic record was regularly fed into the computer in the ordinary course of activities.
3. The computer was operating properly throughout the material part of the period, or if inoperative, that the interruption did not affect the accuracy of the record.
4. The secondary output reproduces or is derived from information supplied to the computer in the ordinary course of activities.

Section 63(4) requires that any secondary electronic record introduced in court must be accompanied by an official certificate. This certificate must identify the electronic record, describe the manner in which it was produced, provide particulars of the device involved, and be signed by a person occupying a responsible official position in relation to the operation of the relevant device or management of the relevant activities.

7.2 Chronological Judicial Evolution: From Navjot Sandhu to Arjun Panditrao & Section 63 BSA

To evaluate Section 63 of the BSA, it is necessary to examine the fifteen-year period of judicial debate surrounding Section 65B of the repealed Indian Evidence Act, 1860.

Phase I: The Flexible Approach in State (NCT of Delhi) v. Navjot Sandhu (2005)

In *State (NCT of Delhi) v. Navjot Sandhu*, the Supreme Court considered the admissibility of mobile call detail records (CDRs) produced without a Section 65B certificate. The Court held

that even if a statutory certificate under Section 65B was absent, secondary evidence of electronic records could still be admitted under general evidence provisions (Sections 63 and 65 of the repealed IEA). This approach treated statutory certification as an optional procedural mechanism rather than a mandatory condition for admissibility.

Phase II: The Strict Mandate in Anvar P.V. v. P.K. Basheer (2014)

Recognizing that the ruling in *Navjot Sandhu* left digital evidence open to potential tampering, a three-judge bench in *Anvar P.V. v. P.K. Basheer* overruled *Navjot Sandhu*. The Court held that Section 65B was a mandatory special provision that entirely excluded general secondary evidence provisions. The Court emphasized that digital data is inherently volatile and easily modified, making mandatory certification necessary to ensure authenticity before secondary electronic records are admitted as evidence.

Phase III: The Interlude of Uncertainty in Shafhi Mohammad (2018)

In *Shafhi Mohammad v. State of Himachal Pradesh*, a two-judge bench relaxed the strict mandate established in *Anvar P.V.*, holding that a party who was not in physical possession of the primary device should not be denied the right to produce secondary evidence due to the inability to procure a certificate. This decision introduced temporary procedural ambiguity regarding whether statutory certification was strictly mandatory.

Phase IV: The Authoritative Settlement in Arjun Panditrao Khotkar (2020) and Codification in BSA

The controversy was resolved by a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020). The Supreme Court reaffirmed *Anvar P.V.*, holding that Section 65B certification is a mandatory prerequisite for the admissibility of secondary electronic records. The Court clarified that where the primary device is produced in court by its owner or custodian, no certificate is required under Section 65B. However, whenever secondary copies, extractions, or printouts are presented, certification remains mandatory. To address situations where a required party refuses to issue a certificate, the Court held that the trial court can exercise its summons powers under Section 91 of the Code of Criminal Procedure, 1973 (now Section 94 of the Bharatiya Nagarik Suraksha Sanhita, 2023) to compel the custodian to produce the required certificate. Section 63 of the BSA incorporates these principles into statutory law.

7.3 Technical & Forensic Vulnerabilities: Hashing, Metadata, and Chain of Custody

While Section 63 of the BSA establishes the statutory certification framework, legal compliance does not automatically guarantee technical data integrity. Digital evidence

possesses characteristics that distinguish it from physical evidence:

A. Cryptographic Hash Values and Data Authenticity

A cryptographic hash function (such as SHA-256 or MD5) acts as an algorithm that converts an input file into a unique, fixed-length alphanumeric string. Even a minor alteration to a digital file—such as changing a single character in a text document or adjusting a pixel in an image—completely alters the resulting hash value. In digital forensics, generating a cryptographic hash value at the immediate moment of device seizure creates an immutable baseline. If the hash value calculated during judicial examination matches the original hash value recorded at seizure, the court has technical confirmation that the data remained uncompressed, unaltered, and uncorrupted. Conversely, a Section 63 BSA certificate that lacks a recorded hash value provides legal compliance without technical proof of data integrity.

B. Metadata Preservation and Temporal Verification

Digital files contain embedded metadata—such as file creation timestamps, modification histories, geographic GPS coordinates, camera model specifications, and user permissions. Metadata can be easily altered if a seized device is booted up, accessed without write-blocking hardware, or connected to an active cellular network. Standard police seizures conducted without write-blockers often overwrite access timestamps, compromising the evidentiary reliability of metadata.

C. Maintenance of Chain of Custody

Maintaining an unbroken chain of custody requires detailed documentation of every individual who accessed, transferred, imaged, or examined the digital evidence from seizure to judicial evaluation. Gaps in chain-of-custody documentation create risks of unverified access or tampering, exposing the evidence to exclusion or defense challenges.

8. RESEARCH FINDINGS (DOCTRINAL + EMPIRICAL)

8.1 Sample Profile

Respondents: 57.1% law students (8), 21.4% students of other disciplines (3), 14.3% other (2),

7.1% advocate/legal professional (1) (Figure 1). Familiarity: 57.1% very familiar, 14.3% extremely familiar, 21.4% slightly familiar, 7.1% not at all familiar (Figure 2). BSA awareness: 57.1% yes, 28.6% no, 14.3% partially (Figure 3). The sample is education-heavy and urban; policing perspectives were invited but not distinctly captured in final occupational coding—treated as a limitation (Section 12).

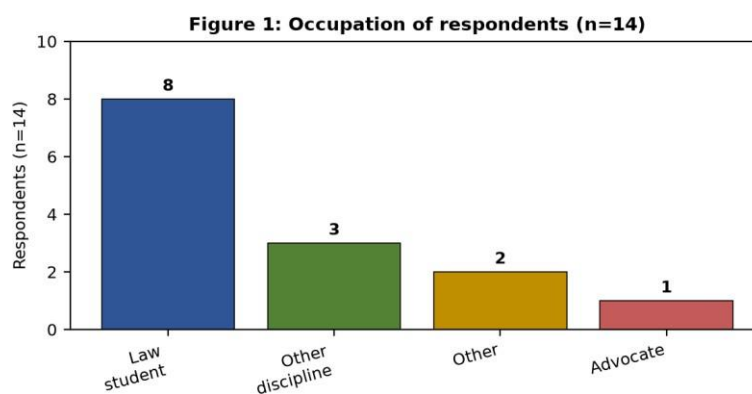


Figure 1: Occupation of respondents (n=14).

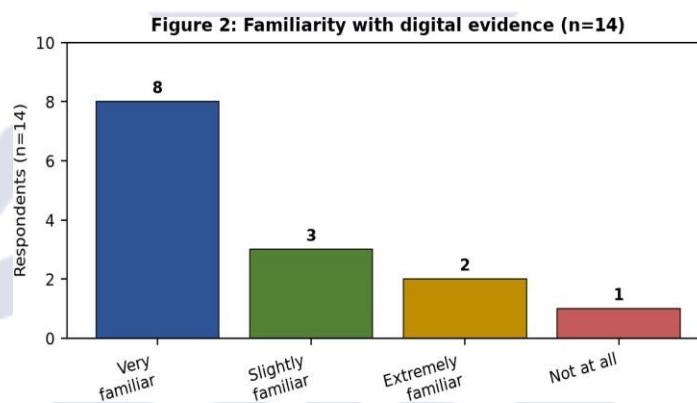


Figure 2: Familiarity with digital evidence (n=14).

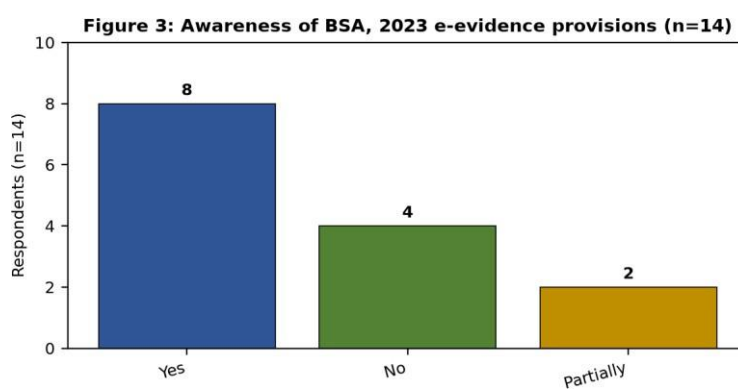


Figure 3: Awareness of BSA e-evidence provisions (n=14).

8.2 Admissibility Formalism Commands Consensus

Finding 1: Stakeholders strongly endorse gatekeeping. 71.4% agree digital evidence should face specific legal requirements before admission; 21.4% neutral; 7.1% disagree (Figure 4). 71.4% rate documentation/certification as very important, 28.6% as slightly important, with none dismissing it (Figure 5). Doctrinally, this validates Section 63’s certificate-as-condition-precedent, while counselling against dilution. The lone disagreeing voice likely reflects concern that formalism may exclude reliable evidence where certificates are delayed—addressable through Arjun Panditrao-style curability rather than abandonment.

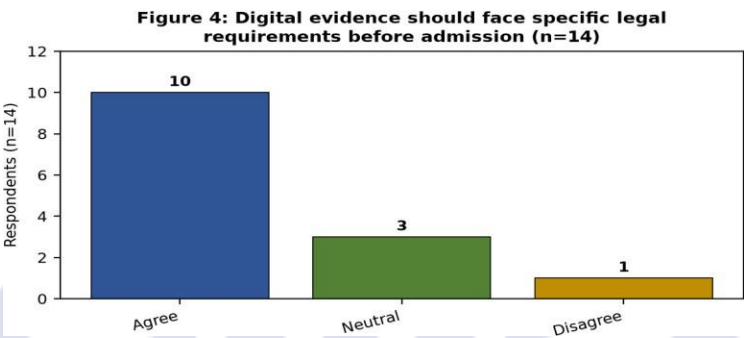


Figure 4: Specific legal requirements before admission (n=14).

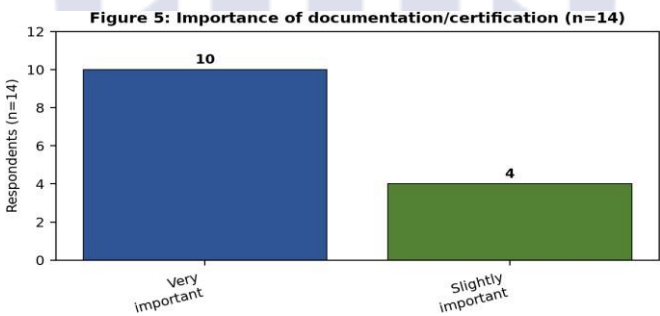


Figure 5: Importance of documentation/certification (n=14).

8.3 Manipulation Anxiety Centres on Invisible Alteration

Finding 2: 57.1% agree and 14.3% strongly agree that digital evidence is more vulnerable than physical evidence (71.4% combined), with 21.4% neutral and one strong dissent (Figure 6). 64.3% rate chain of custody as very important (Figure 7), and 64.3% agree/strongly agree that stronger safeguards are needed where alteration leaves no trace (Figure 13). This maps directly onto Section

7.2 pressure points—hashing, imaging, and transformation disclosure—and justifies a graded safeguard model: routine CDRs (person-in-charge certificate suffices) versus suspect, edited, or AI-risk outputs (mandatory Part B expert plus hash continuity).

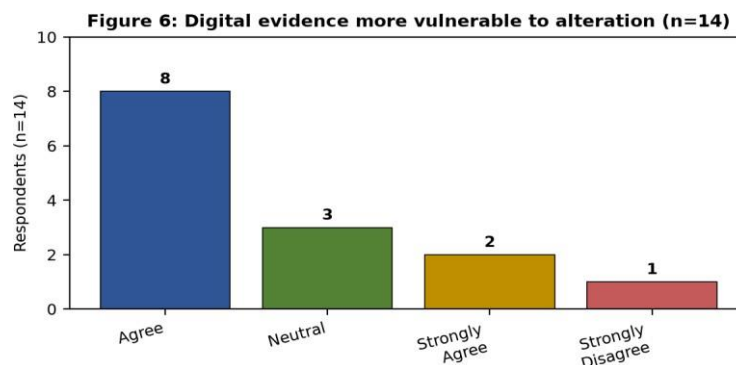


Figure 6: Perceived vulnerability to alteration (n=14).

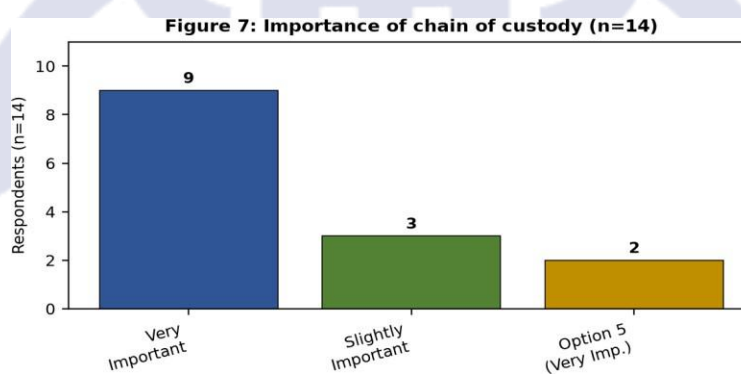


Figure 7: Importance of chain of custody (n=14).

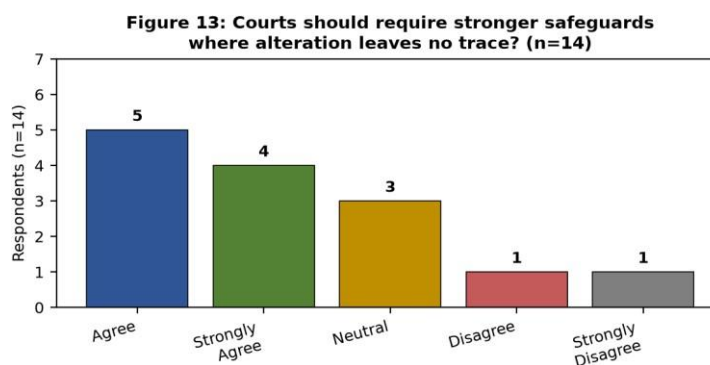


Figure 13: Stronger safeguards where alteration leaves no trace (n=14).

8.4 Capacity Deficit and Forensic Need Are the Bottlenecks

Finding 3: Only one respondent (7.1%) considers police training/resources adequate; 50.0% say no, 42.9% partially (Figure 8). Conversely, 71.4% agree/strongly agree courts need greater forensic expertise access (Figure 9). This is the study’s most policy-salient result: BSA standardisation without capacity investment reproduces the very unreliability it seeks to cure. It also explains split BSA-sufficiency views (Figure 11): text is necessary but insufficient without FSL staffing, mobile forensic vans, hash-enabled seizure kits, and judicial training.

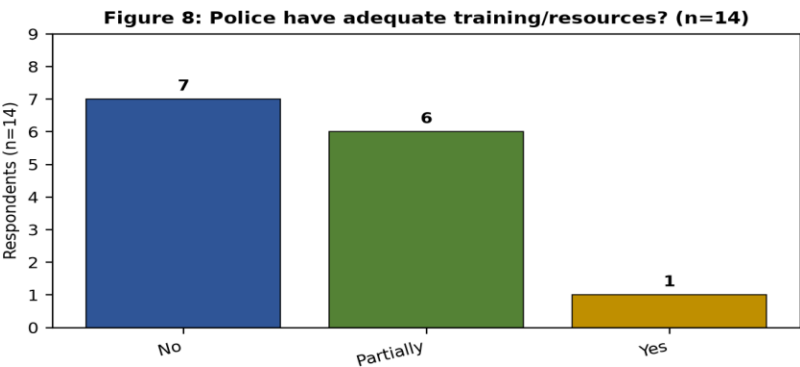


Figure 8: Adequacy of police training/resources (n=14).

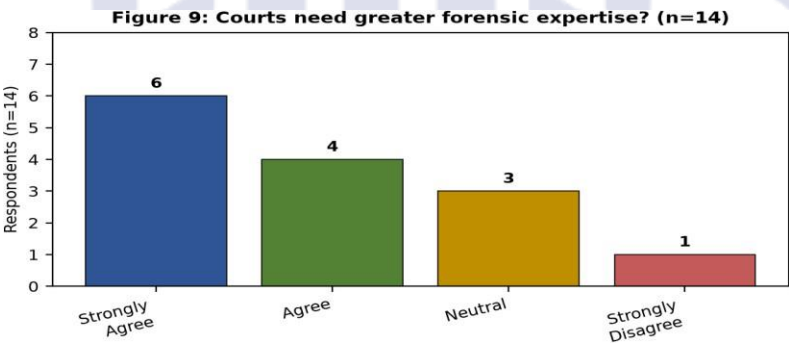


Figure 9: Need for judicial forensic expertise (n=14).

8.5 Fair-Trial Optimism Tempered by Risk Awareness

Finding 4: 71.4% believe digital evidence can strengthen criminal justice, yet 85.7% see actual or potential fair-trial challenges (Figures 10, 12). BSA sufficiency is unresolved (Figure 11). Read together, stakeholders are techno-optimist but rights-sensitive: they want probative gains without sacrificing confrontation, disclosure, privacy, or equality of arms. This supports the recommendations’ dual track—enable reliable digital proof while entrenching defence parity

and proportionality review.

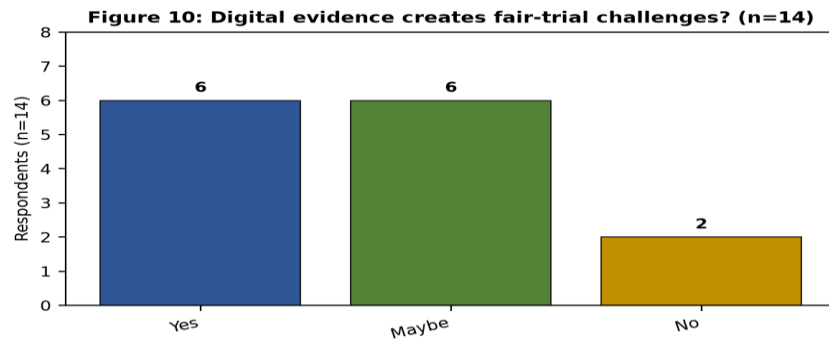


Figure 10: Fair-trial challenges from digital evidence (n=14).

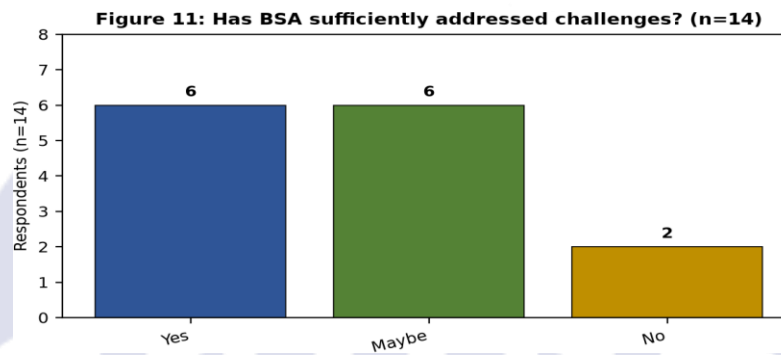


Figure 11: Has BSA sufficiently addressed challenges? (n=14).

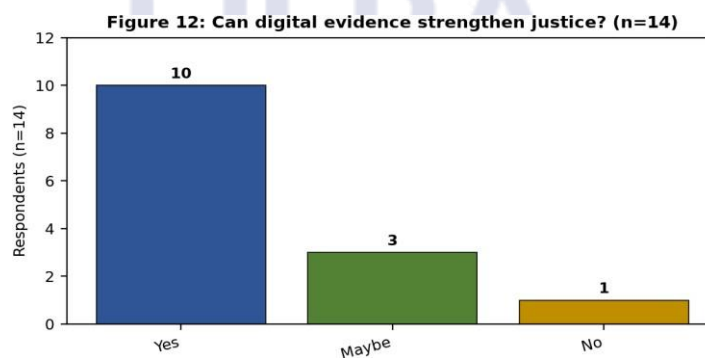


Figure 12: Can digital evidence strengthen justice? (n=14).

9. CONCLUSION

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 represents a legislative attempt to align India's evidentiary rules with modern digital practices. By replacing the Indian Evidence Act, 1860, the legislature sought to address the limitations of an analog statutory structure and create a legal framework capable of processing digital data. The recognition of digital records under Section 61, the definitions of primary digital evidence under Section 62, and the certification rules under Section 63 collectively form an updated statutory foundation. The integration of digital evidence directly affects constitutional rights under Article 21 of the Constitution of India. The right to a fair trial requires an equality of arms between the prosecution and the defense. When the state presents secondary digital records while withholding raw forensic images or metadata, the accused's ability to cross-examine witnesses and challenge evidence is constrained. Therefore, achieving the goals of the BSA requires moving beyond procedural certification toward technical authentication. Without standardized field practices, adequate forensic infrastructure, and judicial access to independent technical expertise, the reliance on digital evidence creates ongoing risks to fair trial guarantees.

10. RECOMMENDATIONS

- **Mandatory Cryptographic Hashing Protocols at the Stage of Seizure:** Legislative and administrative guidelines should require investigating officers to generate cryptographic hash values (SHA-256 or higher) immediately upon seizing any digital device or extracting electronic data. The initial hash value must be recorded in the seizure memo and incorporated directly into the Section 63 BSA certificate. Any subsequent variation in the hash value during judicial custody or forensic examination should render the evidence inadmissible due to compromised integrity.
- **Statutory Defense Entitlement to Forensic Mirror Images and Metadata:** To uphold the principle of equality of arms under Article 21, procedural rules should be amended to entitle the defense to receive bit-stream forensic mirror images and raw unedited metadata for any electronic record produced by the prosecution. Granting defense counsel access to complete metadata enables independent forensic verification and protects against selective data presentation.
- **Establishment of District-Level Digital Forensic Support Units:** To reduce delays at State Forensic Science Laboratories (FSLs), independent digital forensic support units should be established at the district court level. These units would provide trial courts

with direct access to certified forensic experts for independent evidence verification.

- **Integration of Write-Blocking Hardware and Faraday Enclosures into Police SOPs:** Standard Operating Procedures (SOPs) issued by the Ministry of Home Affairs and Bureau of Police Research and Development (BPR&D) should mandate the use of hardware write-blockers and Faraday bags during device seizures. Investigating agencies should receive appropriate funding and equipment to prevent remote wiping or unauthorized modifications during transport and storage.
- **Standardized Section 63 Certificate Templates with Technical Fields:** The statutory certificate format under Section 63 BSA should be updated to include mandatory technical disclosures, including device serial numbers, operating system details, forensic tools used, extraction software versions, and cryptographic hash values.
- **Comprehensive Capacity Building for Judiciary and Law Enforcement:** Interdisciplinary training programs should be instituted across judicial academies and police training centers, focusing on digital forensics, cloud extractions, messaging metadata, and deepfake detection.

11. SCOPE FOR FUTURE RESEARCH

- **Empirical Evaluation of Judicial Practice Under the BSA:** Future studies should examine trial and appellate court decisions post-BSA implementation to analyze how judges evaluate Section 63 certificates and handle defense challenges regarding data integrity.
- **Admissibility Standards for AI-Generated and Synthetic Media:** With the rise of deepfakes and generative AI tools, research is needed to establish authentication frameworks for distinguishing authentic digital media from synthetic or altered content.
- **Cross-Border Cloud Evidence Retrieval and Jurisdictional Challenges:** Further research should investigate legal mechanisms for acquiring cloud-stored digital evidence hosted in foreign jurisdictions, evaluating the efficiency of Mutual Legal Assistance Treaties (MLATs) and Cloud Act requests.
- **Privacy and Bulk Data Seizure Frameworks:** Investigating the constitutional balance between law enforcement powers to search digital devices and individual privacy rights under Article 21 following *K.S. Puttaswamy v. Union of India*.

12. LIMITATIONS

- **Sample Size Constraints:** The empirical component of this study relied on a survey sample of n=14 respondents across legal practitioners, law students, academics, and related disciplines. While the data provides qualitative insights into stakeholder perceptions, the sample size limits direct generalization across all judicial districts in India.
- **Early Implementation Stage of the BSA:** Because the Bharatiya Sakshya Adhiniyam, 2023 was enacted recently, long-term appellate case law interpreting Section 63 remains limited compared to the jurisprudence surrounding Section 65B of the repealed Indian Evidence Act.
- **Regional Focus:** The empirical sample was gathered primarily within specific legal and academic networks, which may reflect higher awareness levels than those in remote or rural jurisdictions.

REFERENCES (APA 7TH EDITION)

- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet* (3rd ed.). Academic Press.
- Central Bureau of Investigation. (2022). *CBI manual on digital evidence and cyber crime investigation*. Government of India.
- Kothari, C. R., & Garg, G. (2019). *Research methodology: Methods and Techniques* (4th ed.). New Age International Publishers.
- Law Commission of India. (2018). *277th Report on wrongful prosecution (miscarriage of justice): Legal remedies*. Ministry of Law and Justice, Government of India.
- Mason, S., & Seng, D. (Eds.). (2021). *Electronic evidence* (5th ed.). Institute of Advanced Legal Studies / SAS Open Journals.
- Ministry of Home Affairs. (2023). *The Bharatiya Sakshya Adhiniyam, 2023* (Act No. 47 of 2023). Gazette of India, Government of India.
- Parliamentary Standing Committee on Home Affairs. (2023). *246th Report on the Bharatiya Sakshya Bill, 2023*. Rajya Sabha Secretariat.
- Peters, A. (2018). Corruption as a violation of international human rights. *European Journal of International Law*, 29(4), 1251–1287.
- Saini, Y. (2026). Merit stolen, justice denied: A human rights perspective on examination irregularities. *International Journal of Versatile Research and Analysis*,

4(9), e693–e703.

- Singh, R. (2021). *Legal research methodology*. LexisNexis.
- Supreme Court of India. (1978). *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.
- Supreme Court of India. (1993). *Nilabati Behera v. State of Orissa*, (1993) 2 SCC 746.
- Supreme Court of India. (1997). *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416.
- Supreme Court of India. (2005). *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
- Supreme Court of India. (2014). *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
- Supreme Court of India. (2017). *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
- Supreme Court of India. (2018). *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
- Supreme Court of India. (2020). *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
- United Nations General Assembly. (1948). *Universal Declaration of Human Rights* (Resolution 217 A). United Nations.
- United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*. United Nations Treaty Series, 999, 171.

APPENDIX A: QUESTIONNAIRE

Survey titled ‘Digital Evidence under the Bharatiya Sakshya Adhiniyam, 2023: A Critical Analysis of Admissibility, Authenticity, and Fair Trial Rights (Responses)’, administered via Google Forms, 1–2 October 2026. Response options as recorded in Form Responses 1 (n=14).

1. What is your present occupation/profession? [Law student / Student of another discipline / Advocate/Legal professional / Other / (Police personnel invited)]
2. How familiar are you with the concept of digital evidence? [Extremely familiar / Very familiar
3. / Slightly familiar / Not familiar at all]
4. Before this survey, were you aware of the Bharatiya Sakshya Adhiniyam, 2023 and its provisions concerning electronic/digital evidence? [Yes / Partially / No]
5. Do you believe that digital evidence should be subject to specific legal requirements before it is admitted by a court? [Agree / Neutral / Disagree (+ Strongly variants where recorded)]
6. In your opinion, how important is proper documentation/certification in establishing

- the admissibility of digital evidence? [Very important / Slightly important]
7. Do you believe digital evidence is more vulnerable to alteration or manipulation than conventional physical evidence? [Strongly Agree / Agree / Neutral / Strongly Disagree]
 8. How important is maintaining a proper chain of custody for digital evidence? [Very Important / Slightly Important / Option 5 ($\approx$ Very Important)]
 10. Do you think police and investigating agencies currently have adequate training and technical resources to properly collect and preserve digital evidence? [Yes / Partially / No]
 11. Do you think courts require greater access to technical or forensic expertise when determining authenticity and reliability of complex digital evidence? [Strongly Agree / Agree / Neutral / Strongly Disagree]
 12. Do you believe that the increasing use of digital evidence can create challenges for the accused's right to a fair trial? [Yes / Maybe / No]
 13. In your opinion, has the Bharatiya Sakshya Adhiniyam, 2023 sufficiently addressed the challenges created by increasing use of digital evidence? [Yes / Maybe / No]
 14. Do you believe the increasing use of digital evidence can strengthen the administration of criminal justice? [Yes / Maybe / No]
 15. Should courts require stronger safeguards where digital evidence can potentially be altered without easily detectable physical traces? [Strongly Agree / Agree / Neutral / Disagree / Strongly Disagree]