The Academic
International Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 4 | Issue 4 | April 2026
ISSN: 2583-973X (Online), SJIF IF: 5.6
Website: www.theacademic.in

Bridging Law and Technology: Strengthening Digital Forensic Evidence in Criminal Trials in India

Mr. Saket Saurav

Assistant Professor, Lloyd Law College

DOI : https://doi.org/10.5281/zenodo.20213056

ARTICLE DETAILS

Research Paper

Accepted: 29-04-2026

Published: 10-05-2026

Keywords:

Digital Forensics; Electronic Evidence; Criminal Trials; Judicial Trust; Chain of Custody; Admissibility

ABSTRACT

The rapid digitisation of society has profoundly transformed criminal investigations, placing digital forensic evidence at the centre of modern trials. This study examines the role, reliability, and admissibility of digital forensic evidence within India's criminal justice system, with special reference to Delhi-NCR under the Bharatiya Sakshya Adhiniyam, 2023 and allied legislations. Despite legislative recognition, challenges persist in forensic readiness, chain-of-custody compliance, technical competence, and judicial evaluation. The research adopts a quantitative approach using structured questionnaires administered to key stakeholders — investigating officers, forensic experts, prosecutors, defence lawyers, and judicial officers. Partial Least Squares Structural Equation Modelling (PLS-SEM) is used to analyse relationships between forensic readiness, evidence handling, perceived reliability, judicial trust, admissibility, and trial effectiveness. The study addresses a critical gap by empirically examining how institutional capacity and procedural compliance influence judicial reliance on digital evidence, and aims to provide insights for strengthening forensic infrastructure, improving evidentiary standards, and enhancing the fairness and efficiency of criminal trials.

1. Introduction

The term 'forensics' traces its roots to the Latin forensis, meaning 'of a forum or place of assembly.' In Roman times, judicial proceedings were conducted before public forums, and this practice gave rise to

the modern use of forensic evidence as a form of legal proof. Combined with 'science' (from the Latin for 'knowledge'), forensic science may be understood as a scientific methodology for solving crimes.

This research addresses the intersection of law and forensic science, which has emerged as a pivotal element in contemporary criminal justice worldwide. As scientific methods increasingly shape legal decision-making, forensic evidence has assumed a crucial role in investigation and adjudication. Rooted in disciplines such as pathology, psychiatry, and anatomy, forensic science serves a critical function in resolving crimes and disputes. However, the field continues to face challenges including flawed laboratory practices, lack of standardised protocols, funding constraints, and questions surrounding the admissibility and reliability of expert testimony.

The intersection of forensic science with legal systems across nations has significantly transformed the evidentiary landscape in criminal trials, particularly through increased reliance on digital evidence. The admissibility, reliability, and interpretation of such evidence have come under intense judicial and academic scrutiny. This research critically explores key judgments that have shaped digital forensic jurisprudence in India — focusing on admissibility, evidentiary value, and judicial reliance — through doctrinal analysis and case studies. It evaluates the application of the Bharatiya Sakshya Adhiniyam, 2023; Bharatiya Nagrik Suraksha Sanhita, 2023; the Information Technology Act, 2000; the Digital Personal Data Protection Act, 2023; and the Criminal Procedure (Identification) Act, 2022, revealing the strengths and limitations of the current legal framework.

Digital forensics has become a cornerstone of modern criminal investigations, particularly as cybercrime continues to escalate in frequency and complexity. Crimes now routinely leave electronic footprints, and this research examines current practices, policies, laws, infrastructure, and training in India's digital forensic ecosystem. It highlights existing gaps through practitioner analysis, emphasising the urgent need for a robust and standardised digital forensic framework.

The central objective of this paper is to examine the constitutional guarantee of a fair trial in India alongside the complexities of handling digital forensic evidence in courts. The focus is on admissibility and the obstacles to a fair trial, while offering perspectives to assist policymakers, judicial officers, and legal practitioners in developing balanced approaches that account for both legal and technological dimensions.

PS: Section 65 B of the Indian Evidence Act corresponds to Section 63 (4) (c) of the Bharatiya Sakshya Adhiniyam.

1.1 Origin of the Problem

The problem addressed in this research stems from India's rapid digitisation, which has fundamentally altered the nature of criminal evidence. Mobile phones, CCTV footage, call detail records, social media communications, cloud storage, GPS data, and digital transaction trails now form the backbone of investigation and prosecution across a wide spectrum of offences — from cybercrime and financial fraud to organised crime and violent offences. However, the criminal justice system historically evolved around physical and oral evidence, leaving investigative agencies and courts ill-prepared to handle the technical, procedural, and interpretative complexities of digital forensic evidence. Judicial inconsistencies, frequent exclusion of digital material due to procedural lapses, and difficulties in evaluating authenticity and chain of custody exposed systemic weaknesses under the earlier legal framework. In response, the Indian legislature introduced the Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, and Bharatiya Sakshya Adhiniyam, 2023, to formally integrate digital investigation and electronic evidence into criminal proceedings. Despite this legislative overhaul, practical concerns persist regarding institutional readiness, forensic capacity, stakeholder competence, and judicial confidence — particularly in high-pressure jurisdictions such as Delhi NCR, where technology-driven cases dominate court dockets.

2. Status of Research at the National Level

Digital forensics has gained significance alongside rising cybercrime and digital litigation. According to Steve Hailey of the Digital Forensics Certification Board (DFCB), computer forensics involves the preservation, identification, extraction, interpretation, and documentation of digital evidence, encompassing rules of evidence, legal processes, integrity standards, factual reporting, and expert testimony. The discipline developed progressively: in 1984, the FBI established the Computer Analysis and Response Team (CART); in 1993, it hosted the first International Law Enforcement Conference on Computer Evidence with delegates from twenty-six countries; the International Organization on Computer Evidence (IOCE) was formed in 1995; and by 2000, the FBI's first Regional Computer Forensic Laboratory (RCFL) was operational. In India, the Information Technology Act, 2000 provided legal recognition to electronic records and established the foundation for digital forensic investigations.

Since 2020, India has meaningfully advanced its cyber forensic ecosystem. The Indian Cyber Crime Coordination Centre (I4C), operational under the Ministry of Home Affairs from January 2020, serves as the national nodal agency for cybercrime response. Under I4C, the National Cyber Forensic Laboratory (NCFL) operates through two divisions: NCFL (Investigation) in New Delhi, which has supported over 11,800 cases with real-time forensic assistance; and NCFL (Evidence) in Hyderabad, established in 2022,

which has reduced forensic turnaround times by nearly 50% through advanced imaging, malware analysis, and decryption capabilities. Concurrently, the Central Forensic Science Laboratories (CFSLs) have been modernised to include mobile forensics, cryptocurrency tracking, and cloud data analysis. These labs are integrated through a national e-Forensics IT platform linking over 117 state and central forensic labs, enabling encrypted data transfer and real-time inter-agency collaboration.

The Cyber Crime Prevention against Women and Children (CCPWC) scheme has funded cyber forensic and training labs across 33 States and Union Territories. By 2025, over 24,600 officials — including police personnel, cyber response teams, and judicial functionaries — have been trained under associated schemes. In April 2022, CERT-In mandated service providers to retain user activity records for 180 days, and VPN and cloud providers to store subscriber data for five years, improving evidence traceability. The Sahyog portal has streamlined legal coordination among law enforcement, service providers, and digital platforms. Additionally, over 550 mobile forensic vans now operate across Indian districts, enabling on-site data extraction and digital triage, particularly in rural or remote areas.

Despite national-level investments, a 2024 review of forensic practices noted uneven development across states. Some regions, particularly at the district level, lack basic equipment and access to updated forensic software. Report generation delays, case backlogs, and limited technical staffing remain persistent concerns. Even when digital evidence is successfully gathered, it must meet stringent legal criteria for admissibility. The Section 65B certification requirement under the former Indian Evidence Act (now corresponding to Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam) continues to generate procedural challenges in courts, often resulting in acquittals or prolonged trials. The Supreme Court's 2020 ruling in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal provided important guidance on the handling of digital records, though compliance at the district court level remains inconsistent.

3. Status of Research at the International Level

As digital technology becomes ubiquitous, the volume of digital evidence in criminal and civil proceedings continues to grow rapidly. According to the International Telecommunication Union (ITU, 2024), global internet usage reached 5.4 billion people in 2023 — approximately 67% of the world's population. Cisco's Annual Internet Report projected over 29.3 billion network-connected devices by the end of 2023. The data per case at the FBI's fifteen Regional Computer Forensic Laboratories grew from 84GB to 559GB between 2003 and 2011 — a 6.65-fold increase — illustrating the escalating data challenge.

Digital traces are increasingly heterogeneous, scattered across multiple platforms, devices, and cloud services, often appearing in multiple versions with different timestamps. They may be encrypted, fragmented, or embedded within vast datasets, creating significant challenges for identification, acquisition, storage, and analysis. Advanced mobile and wearable technologies — now approaching the functional capabilities of desktop computers — further expand the variety of devices subject to forensic investigation. As the risks associated with cybercrime grow, so does the emphasis on cybersecurity breaches and the investigation of digital perpetrators. Significant ethical and legal challenges around privacy, data protection, and civil rights accompany the expanding access to personal data.

International frameworks are evolving in response. The ISO/IEC 21043 standard incorporates forensic evaluation as part of the digital forensics process. Sweden's Digital Forensics Sweden (DFS) network exemplifies an integrated approach, developing agile and proactive methodologies that include visualisation tools, predictive analysis, and early-stage crime detection. The Sydney Declaration further defines forensic science as a research-oriented, science-based endeavour to study traces through detection, recognition, recovery, examination, and interpretation — providing a foundation for reforming digital forensic science in the digitisation era.

4. Research Questions

1. How does digital forensic readiness influence the handling and presentation of digital evidence in criminal trials under the new criminal law regime?
2. What is the effect of chain-of-custody compliance on the perceived reliability and validity of digital forensic evidence?
3. How does perceived reliability of digital forensic evidence influence judicial trust and admissibility decisions?
4. Do stakeholder roles — police, forensic experts, prosecutors, defence lawyers, and judges — differ in their perceptions of digital forensic effectiveness?
5. How does judicial trust in digital forensic evidence influence perceptions of its impact on trial efficiency and evidentiary strength?

5. Research Gap

The application of forensic standards to digital evidence in India dates back to the early 1990s, when computers entered public life, and was given legislative shape by the Information Technology Act, 2000. Despite subsequent efforts to create institutional support for investigation and resolution of crimes, significant gaps in law enforcement procedure and infrastructure remain. While specialised forensic labs such as the Forensic Science Laboratory in West Bengal (later incorporating cyber units) have existed for decades, recent legislative changes — including the Bharatiya Nagarik Suraksha Sanhita — have modernised procedures for admissibility of electronic records as primary evidence. Nevertheless, practical implementation of digital forensics within the Indian criminal justice system continues to face challenges, particularly in establishing individual guilt through digital evidence while upholding the presumption of innocence.

Judicial reliance on digital forensic evidence has grown steadily, as reflected in landmark Supreme Court decisions. In Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1, the Court established strict procedural requirements for the admission of electronic records. The Bharatiya Sakshya Adhiniyam, 2023, together with the Bharatiya Nagarik Suraksha Sanhita and Bharatiya Nyaya Sanhita, represents a structural shift by formally embedding digital investigation and electronically mediated proof into the criminal process. However, existing scholarship largely focuses on statutory interpretation and case-law evolution, offering limited insight into how these reforms are operationalised at the levels of investigation, forensic analysis, prosecution, and judicial evaluation.

Institutional reports — including those of the Malimath Committee on Criminal Justice Reforms and NCRB publications — acknowledge persistent gaps in forensic capacity, training, and infrastructure, yet they do not empirically examine how these factors influence judicial trust, perceived reliability, and admissibility of digital forensic evidence in actual trials. There is a notable absence of integrated empirical models that explain how digital forensic readiness, chain-of-custody compliance, and technical competence interact to shape judicial approaches and trial outcomes, particularly in high-volume jurisdictions such as Delhi NCR.

The review of literature identifies the following research gaps:

1. No independent empirical study has examined the effectiveness and efficiency of digital forensics in criminal trials in India.

2. The influence of forensic readiness, chain of custody, and technical competence on judicial evaluation of digital evidence remains empirically untested.
3. No coherent multi-stakeholder framework exists for examining forensic reliability and admissibility.
4. The practical impact of BNS, BNSS, and BSA 2023 on courtroom use of digital forensics has not been examined in high-burden regions such as Delhi NCR.
5. Existing research lacks causal and mediational analysis linking digital forensic practices to perceived trial effectiveness and judicial decision-making.

6. Research Objectives

1. To assess the level of digital forensic readiness among criminal justice stakeholders in Delhi NCR under the new criminal law regime.
2. To examine the effect of chain-of-custody compliance and technical competence on perceived reliability of digital forensic evidence.
3. To analyse the relationship between perceived reliability of digital forensic evidence and judicial trust in such evidence.
4. To evaluate the influence of judicial trust on admissibility perceptions and perceived effectiveness of digital forensic evidence in criminal trials.
5. To develop and test a structural equation model explaining the role of digital forensics in shaping judicial approaches and perceived trial outcomes under BNS, BNSS, and BSA 2023.

7. Data and Methodology

The study is based on primary data collected through a structured questionnaire administered to evidence-collecting and evidence-analysing stakeholders involved in criminal trials in Delhi NCR. A five-point Likert scale is used to measure perceptions related to digital forensic readiness, procedural compliance, reliability, judicial trust, admissibility, and trial effectiveness. The research adopts a quantitative, cross-sectional design, and data will be analysed using descriptive statistics and Partial Least Squares Structural Equation Modelling (PLS-SEM). Reliability and validity of the measurement model will be established prior to testing the hypothesised structural relationships.

7.1 Research Hypotheses

H_{a1}: Digital forensic readiness has a significant positive effect on digital evidence handling competence and consequently enhances the perceived reliability and validity of digital forensic evidence in criminal trials.

H_{a2}: Chain-of-custody compliance has a significant positive effect on perceived reliability and validity of digital forensic evidence, and consequently strengthens judicial trust in such evidence.

H_{a3}: Digital evidence handling competence has a significant effect on perceived reliability and validity of digital forensic evidence.

H_{a4}: Perceived reliability and validity of digital forensic evidence has a significant positive effect on judicial trust in such evidence and consequently enhances its perceived admissibility.

H_{a5}: Judicial trust in digital forensic evidence has a significant positive effect on perceived admissibility and its perceived impact on trial effectiveness.

H_{a6}: Perceived admissibility of digital forensic evidence has a significant effect on perceived impact on trial effectiveness.

7.2 Research Design

This study employs a quantitative research design using a structured questionnaire administered to criminal justice stakeholders in Delhi NCR. Delhi NCR has been selected as the study area because it is one of India's most active and complex criminal justice jurisdictions, characterised by a high volume of cyber-enabled offences, extensive reliance on electronic evidence, and the presence of specialised investigative units, forensic laboratories, and multi-tier criminal courts. The concentration of forensic infrastructure and legal institutions makes it a particularly information-rich setting for empirically examining stakeholder perceptions and judicial approaches, while offering insights relevant to other metropolitan regions.

Population and Sampling: The study population includes investigating officers, digital forensic experts, public prosecutors, defence lawyers, and judicial officers in Delhi NCR. Stratified purposive sampling is employed to ensure adequate representation across evidence-collecting and evidence-analysing stakeholder groups.

Sample Size: The target sample is 320 respondents (minimum acceptable N ≈ 250), allocated as follows: Investigating Officers (110), Digital Forensic Experts (50), Public Prosecutors (50), Defence Lawyers

(90), and Judicial Officers (20, subject to feasibility). If judicial officers prove difficult to access, their allocation will be redistributed among other groups.

Justification for SEM and Sample Adequacy: Structural Equation Modelling requires an adequate sample to ensure stable parameter estimation across multiple latent constructs and mediating/moderating relationships. The proposed model comprises approximately 6-9 latent constructs, each measured with 3-5 indicators. For variance-based PLS-SEM, a sample of 200-300 respondents is generally sufficient for reliable estimation and acceptable statistical power (Hair et al., 2019; 2021). Multi-group analysis to compare evidence-producing and evidence-evaluating stakeholders requires a minimum of approximately 50 cases per group (Hair et al., 2018; Kline, 2016). By targeting 300-320 respondents, the study accommodates expected attrition while retaining a final usable sample of approximately 260-280 cases, well within recommended SEM thresholds.

Data Collection and Analysis: Data will be collected through online and offline surveys using a five-point Likert scale. Analysis will employ descriptive statistics to summarise respondent profiles and key perceptions, and PLS-SEM to test direct, mediating, and moderating hypotheses.

8. Expected Outcomes

1. The study's expected outcomes extend beyond academic contribution to generate practical, institutional, and policy-level value. Specifically:
2. Investigating agencies and forensic institutions will be assisted in identifying critical gaps in digital forensic readiness, evidence handling competence, and chain-of-custody practices, thereby contributing to improved reliability and courtroom acceptance of digital evidence.
3. Prosecutors, defence lawyers, and judicial officers will benefit from clearer understanding of the factors that influence judicial trust and admissibility of digital forensic evidence under the Bharatiya Sakshya Adhiniyam, 2023, leading to more consistent and informed evidentiary decision-making.
4. Policymakers, judicial academies, and police training institutions will be supported in formulating targeted training modules and standard operating procedures for digital forensics aligned with the requirements of the new criminal law regime.
5. Broader societal benefits will accrue through strengthened credibility and effectiveness of criminal trials involving digital evidence, enhancing public confidence in the criminal justice system in an increasingly digital environment.

- **References**

- Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 (Supreme Court of India).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (Supreme Court of India).
- Carrier, B. and Spafford, E.H. (2004) An event-based digital forensic investigation framework. West Lafayette, IN: CERIAS, Purdue University.
- Casey, E. (2011) Digital evidence and computer crime: Forensic science, computers and the internet. 3rd edn. London: Academic Press.
- Eisenhardt, K.M. (1989) 'Building theories from case study research', Academy of Management Review, 14(4), pp. 532-550.
- Gross, S.R. (2018) 'Expert evidence', Wisconsin Law Review, 2018(6), pp. 1139-1188.
- Goswami, D.P. (2025) Forensic evidence in India: A critical analysis of legal and practical challenges. SSRN eLibrary.
- Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2018) A primer on partial least squares structural equation modeling (PLS-SEM). 2nd edn. Thousand Oaks, CA: Sage Publications.
- Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2021) A primer on partial least squares structural equation modeling (PLS-SEM). 3rd edn. Thousand Oaks, CA: Sage Publications.
- Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019) 'When to use and how to report the results of PLS-SEM', European Business Review, 31(1), pp. 2-24.
- Imwinkelried, E.J. (2015) The methods of attacking scientific evidence. 5th edn. New York: LexisNexis.
- Kline, R.B. (2016) Principles and practice of structural equation modeling. 4th edn. New York: Guilford Press.
- Law Commission of India (2014) Report No. 245: Arrears and backlog — creating additional judicial (wo)manpower. New Delhi: Government of India.
- Malimath Committee (2003) Report of the committee on reforms of criminal justice system. New Delhi: Ministry of Home Affairs, Government of India.
- Mason, S. and Seng, D. (2017) Electronic evidence. 4th edn. London: Institute of Advanced Legal Studies, University of London.
- National Crime Records Bureau (NCRB) (2022) Crime in India 2021. New Delhi: Ministry of Home Affairs, Government of India.

- National Crime Records Bureau (NCRB) (2023) Crime in India 2022. New Delhi: Ministry of Home Affairs, Government of India.
- National Institute of Standards and Technology (NIST) (2006) Special Publication 800-86: Guide to integrating forensic techniques into incident response. Gaithersburg, MD: U.S. Department of Commerce.
- National Institute of Standards and Technology (NIST) (2014) Special Publication 800-101 revision 1: Guidelines on mobile device forensics. Gaithersburg, MD: U.S. Department of Commerce.
- Sharma, G.K. (2024) Importance and advantages of digital forensics for law enforcement and business protection. Available at: https://ijarmt.com.