INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

EVOLUTION OF FORENSIC TOOLS: A TECHNICAL AND HISTORICAL OVERVIEW

AUTHOR - KANNAN KARLMARX* & MS. ANNA JOHN**

* STUDENT AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

** ASSISTANT PROFESSOR AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

BEST CITATION – KANNAN KARLMARX & MS. ANNA JOHN**,** EVOLUTION OF FORENSIC TOOLS: A TECHNICAL AND HISTORICAL OVERVIEW, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (6) OF 2026, PG. 653-665, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I6467

ABSTRACT

Digital forensic tools constitute the indispensable epistemological bridge between latent electronically stored information and admissible evidence in a court of law. This chapter advances a comprehensive technical and jurisprudential analysis of the four generational epochs of digital forensic tool development — spanning disk-imaging utilities of the 1990s, network and volatile-memory forensics of the early 2000s, the mobile-device and cloud extraction paradigm of the 2008–2018 decade, and the contemporary era of Artificial Intelligence and Machine Learning-driven forensic analytics — and critically evaluates their corresponding legal ramifications within the Indian criminal justice architecture. The analysis demonstrates that while forensic tool capabilities have advanced through four distinct and increasingly complex technological generations, the Indian evidentiary framework — most notably Sections 65A and 65B of the Indian Evidence Act, 1872, and their successor provisions under the Bharatiya Sakshya Adhiniyam (BSA), 2023 — has remained tethered to procedural hardware authentication rather than demanding substantive scientific validation of the software algorithms employed. Drawing upon comparative analysis of the United States' Daubert standard, the NIST Computer Forensics Tool Testing (CFTT) programme, and the epistemological debate between open-source and proprietary forensic paradigms, the chapter identifies a structural validation deficit at the heart of Indian digital evidentiary doctrine. It further examines the constitutional tensions generated by memory forensics under Article 21 of the Indian Constitution as interpreted in *K.S. Puttaswamy v. Union of India* (2017), the sovereignty challenges posed by cloud-based evidence extraction, and the profound "algorithmic black box" crisis introduced by AI forensics into courtroom admissibility standards. The chapter concludes with a normative argument for the immediate legislative establishment of an independent Digital Forensic Tools Regulatory Authority, mandated to conduct mandatory empirical validation of all forensic software prior to its deployment in criminal proceedings, thereby restoring the constitutional integrity of digital evidence in India.

Keywords: *Digital Forensic Tools; Electronic Evidence; Section 65B; Bharatiya Sakshya Adhiniyam; EnCase; FTK; Cellebrite UFED; Volatility Framework; Artificial Intelligence Forensics; Daubert Standard; NIST CFTT; Open-Source Forensics; Cloud Forensics; Algorithmic Black Box; India.*

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

I. INTRODUCTION: THE EPISTEMOLOGICAL INTERSECTION OF COMPUTATIONAL CAPABILITY AND EVIDENTIARY JURISPRUDENCE

The hermeneutics of digital evidence within the criminal justice system are inextricably linked to the technological capabilities of the forensic tools utilised to acquire, preserve, analyse, and present electronically stored information (ESI). What commenced as a rudimentary discipline relying on standard operating system commands in the late 1980s has metamorphosed into a highly sophisticated, multi-billion-dollar global industry encompassing volatile memory forensics, decentralised cloud data extraction, and artificial intelligence-driven predictive analytics.[1170] This evolutionary trajectory presents a profound epistemological and jurisprudential challenge for legal frameworks globally, and particularly for the Indian legal regime governing digital evidence. While digital forensic tools have advanced through four distinct and increasingly complex technological generations, the corresponding legal paradigms — most notably Sections 65A and 65B of the Indian Evidence Act, 1872, and the contemporary Bharatiya Sakshya Adhiniyam (BSA), 2023 — have largely remained tethered to procedural authentication rather than demanding substantive scientific validation.[1171]

The dichotomy between accelerating forensic tool capabilities and relatively static evidentiary doctrines fundamentally threatens the integrity of criminal adjudications. Digital forensic software is not merely a passive, objective conduit for data retrieval; it is an active agent that interprets, reconstructs, parses, and sometimes irreversibly alters the digital fabric of the evidence it processes.[1172] Consequently, the uncritical judicial reliance on these tools, absent rigorous independent validation protocols akin to the United States' Daubert standard or the National Institute of Standards and Technology (NIST) Computer Forensics Tool Testing (CFTT) programme, creates an environment ripe for tool-induced errors, algorithmic bias, and subsequent wrongful convictions.[1173]

The transition from physical to digital evidence has fundamentally altered the nature of forensic investigation. Unlike physical evidence, which is tangible and subject to the laws of Newtonian physics, digital evidence is latent, fragile, and infinitely replicable. To make latent digital data visible and intelligible to a court of law, investigators must employ intermediate software applications. The reliability of the evidence presented in court is therefore entirely contingent upon the reliability of the software tool used to extract and format it.[1174] This chapter provides an exhaustive technical and historical exposition of the four generations of digital forensic tools, delineating the specific architectures of industry-standard software, analysing the epistemological debates surrounding open-source versus proprietary models, and evaluating the cascading legal ramifications for the Indian criminal justice system.

II. FIRST-GENERATION FORENSIC TOOLS (1990s–2000s): THE ERA OF DISK IMAGING AND FOUNDATIONAL ARCHITECTURES

The foundational architecture of modern digital forensics was established during the late 1980s and the 1990s, driven by the mass proliferation of personal computing and the urgent requirement for law enforcement agencies — such as the Federal Bureau of Investigation's Computer Analysis and Response Team (CART) — to standardise search, seizure, and chain-of-custody procedures for fragile digital media.[6] Prior to the advent of specialised, non-destructive forensic software, investigators relied on highly risky "live" analyses using the subject's own operating

[1170] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Academic Press 2011) 3–4.

[1171] Indian Evidence Act 1872, ss 65A–65B; Bharatiya Sakshya Adhiniyam 2023, s 63.

[1172] Brian Carrier, *File System Forensic Analysis* (Addison-Wesley 2005) 11–14.

[1173] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993); National Institute of Standards and Technology, CFTT Programme Overview (NIST SP 500-307, 2014).

[1174] Simson Garfinkel, Digital Forensics (IEEE Security and Privacy, 2010) 59–62.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

system or utilised Unix-based dd (disk dump) commands to create raw, sector-by-sector bit-stream copies of storage media. This early methodology was inherently perilous; accessing a live, running system invariably altered file metadata, modified critical timestamps, executed background processes, and risked the absolute spoliation of crucial evidence.

The paradigm shifted fundamentally in 1998 with the release of EnCase by Guidance Software (now integrated into OpenText), followed shortly thereafter by the introduction of AccessData's Forensic Toolkit (FTK) (now owned by Exterro).[7] These first-generation commercial tools pioneered the concept of the non-destructive forensic environment. By utilising specialised hardware write-blockers to intercept and deny any write commands sent to the source drive, these platforms allowed investigators to create mathematically verifiable, strictly read-only images of digital media without altering a single bit of the original evidence.

The technological cornerstone of this generation was the introduction of the Expert Witness Format (E01), pioneered by Guidance Software for EnCase. The E01 architecture represents a highly sophisticated evidentiary container designed specifically to ensure absolute data integrity and court admissibility.[8] The structure embeds CRC checksums between every single 32 KB data block, and the container is sealed with a comprehensive cryptographic hash value — traditionally utilising MD5 or SHA-1 — calculated across the entire acquired bit-stream. Cryptographic hashing acts as an infallible digital fingerprint; an identical hash value proves beyond mathematical doubt that the digital evidence has remained wholly unaltered since the moment of its acquisition, satisfying the most stringent chain-of-custody requirements in a court of law.

Feature	RAW (dd) Format	EnCase (E01)	Advanced Forensic Format (AFF)
Architectural Structure	Exact bit-for-bit raw copy without metadata.	Proprietary structured container with embedded case metadata.	Open-source container integrating extensive custom metadata.
Compression	No native compression; massive file sizes.	Native compression heavily supported.	High-efficiency compression via open algorithms (zlib).
Data Integrity	External hashing required post-acquisition.	Embedded CRC per 32 KB block + global footer hash.	Integrated cryptographic hashing within file structure.
Vendor Independence	Universal compatibility across all OS.	Requires compatible commercial software	Open standard; wide interoperability.

		(EnCase/FTK).	

Table 1: Comparative Analysis of First-Generation Forensic Image Formats

The legal integration of these powerful first-generation tools within the Indian jurisdiction was characterised by a delayed, highly reactive adoption curve. Following high-profile national security incidents — such as the 2001 Parliament attack — apex institutions like the Central Forensic Science Laboratory (CFSL) in Hyderabad rapidly procured EnCase and FTK to investigate complex digital trails.[9] However, this rapid adoption lacked a crucial corollary: the establishment of a domestic, rigorous testing and validation regime. While the United States established the NIST CFTT programme in 1999 to empirically test these tools against standardised cases and publicly publish known error rates, India adopted the tools purely based on vendor marketing representations and general international reputation, demonstrating an alarming institutional deference to proprietary algorithms.[10]

6 Federal Bureau of Investigation, CART (Computer Analysis and Response Team) History and Overview (FBI Publications 2003).

7 Guidance Software, *EnCase Forensic Version 8 User Guide* (OpenText Corp 2018) 1–3; AccessData Group, *FTK Forensic Toolkit User Guide* (Exterro Inc 2020) 2.

8 Guidance Software, *EnCase Evidence File Format Specification* (OpenText Corp 2009) 5–9.

9 Ministry of Home Affairs, *Guidelines on Cyber Forensics for Law Enforcement Agencies* (Government of India 2007) 12.

10 National Institute of Standards and Technology, NIST SP 500-240: *An Overview of Issues in Testing Forensic Software* (NIST 1999).

III. SECOND-GENERATION FORENSIC TOOLS: THE EPHEMERAL SHIFT TO NETWORK AND VOLATILE MEMORY FORENSICS

The exponential growth of the global Internet and the rapid proliferation of highly sophisticated malware in the late 1990s and early 2000s exposed the profound limitations of first-generation, purely disk-centric forensics.[1175] The rise of hacking collectives and the devastating spread of self-replicating viruses like Melissa and ILOVEYOU underscored the urgent need for new investigative methodologies. Cybercriminals rapidly evolved, executing advanced persistent threats (APTs), silent data exfiltrations, and utilising "fileless" malware that resided entirely in a system's RAM, leaving virtually no retrievable traces on the physical hard drive.

Wireshark, an open-source packet analyser originally released as Ethereal in 1998 and rebranded in 2006, became the foundational tool of network forensic investigation.[1176] Operating primarily at the data link layer of the OSI model, Wireshark leverages the promiscuous mode of network interface controllers to capture raw binary data traversing network infrastructure. By automatically recreating complete TCP streams from thousands of fragmented packets, investigators could visually reconstruct the exact sequence of an unauthorised network intrusion, identify clandestine command-and-control (C2) server communications, and isolate specific payloads of exfiltrated proprietary data.

Concurrently, the Volatility Framework, first introduced in 2007 as a completely free, open-source Python-based tool, revolutionised volatile memory forensics.[1177] Maintained by the

[1175] Kevin Mandia and Chris Prosise, *Incident Response and Computer Forensics* (2nd edn, McGraw-Hill 2003) 89–92.
[1176] Gerald Combs and others, *Wireshark Network Protocol Analyser: Developer's Guide* (Wireshark Foundation 2021) 1–2.
[1177] Volatility Foundation, *The Volatility Framework: Volatile Memory Artifact Extraction Utility Framework* (Volatility Foundation 2020).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Volatility Foundation, this framework utilises an extensible, modular plugin architecture to parse highly complex memory structures across multiple versions of Windows, Linux, and macOS operating systems. Volatility plugins allow analysts to examine the Windows Virtual Address Descriptor (VAD) tree, extract running processes and dynamic-link libraries (DLLs) from memory, reconstruct the active Windows Registry without accessing the disk, and identify sophisticated rootkits explicitly designed to hide their presence from traditional anti-virus software and disk analysis tools.

The advent of second-generation forensics introduced severe legal complexities into the Indian jurisprudential landscape. The bulk interception of network traffic directly implicates the fundamental constitutional right to privacy, explicitly recognised as intrinsic to the right to life and personal liberty under Article 21 of the Indian Constitution in the landmark nine-judge bench decision of *K.S. Puttaswamy v. Union of India* (2017).[1178] Indian courts, relying predominantly on the rigid procedural certification mandates of Section 65B of the Indian Evidence Act, have historically struggled to articulate clear standards for the admissibility of evidence derived from inherently destructive and state-altering memory acquisition processes.

IV. THIRD-GENERATION FORENSIC TOOLS: THE MOBILITY REVOLUTION, CLOUD COMPUTING, AND DECENTRALISED DATA GEOGRAPHIES

The decade spanning 2008 to 2018 fundamentally and permanently reorganised the locus and geography of digital evidence. The release of the Apple iPhone in 2007, quickly followed by the mass global proliferation of the Android operating system, precipitated a massive societal shift away from traditional desktop computing.[1179] Simultaneously, vast quantities of corporate and deeply personal data migrated en masse from localised hard drives to highly decentralised cloud storage infrastructure provided by hyper-scalers such as Amazon Web Services (AWS), Google Cloud, and Microsoft Azure.

Advanced tools like the Universal Forensic Extraction Device (UFED) by Cellebrite, alongside powerful alternatives from Oxygen Forensics and MOBILedit, developed a highly structured, tiered extraction hierarchy.[1180] This mobile extraction methodology is universally classified into five distinct levels of increasing technical complexity, invasiveness, and cost, ranging from manual screen photography at Level 1 through to Micro-Read electron microscopy at Level 5.

[1178] *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1, para 144 (nine-judge bench).

[1179] Arie Engelsman and others, "Smartphone Forensics: A Practical Handbook" in *Handbook of Digital Forensics and Investigation* (Elsevier 2010) 301–305.

[1180] Cellebrite, *UFED Ultimate Product Description and Technical Specification* (Cellebrite Mobile Synchronisation Ltd 2022) 4–7.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Level	Methodology	Technical Description	Evidentiary Recoverability
Level 1	Manual Extraction	Photographing data displayed on device screen.	Extremely limited; no deleted data recovery.
Level 2	Logical Extraction	Communicating via manufacturer-approved API.	Active user data only; cannot recover deleted files.
Level 3	File System / Physical	Bit-by-bit flash memory dump via bootloader exploits (checkm8, Qualcomm EDL).	Highly comprehensive; recovers deleted data, SQLite WAL files.
Level 4	JTAG / Chip-Off	Hardware-level intervention; direct binary reading of desoldered chip.	Bypasses software locks; destructive and expensive.
Level 5	Micro-Read	Electron microscopes to view physical state of memory logic gates.	Theoretical/extreme national security cases only.

Table 2: Mobile Device Forensic Extraction Hierarchy

The ability of Cellebrite UFED to perform Physical Extractions by aggressively bypassing user passcodes and inherent device encryption fundamentally challenges long-standing constitutional protections against self-incrimination and unreasonable search and seizure.[1181] In India, the complex interplay between the fundamental right to informational privacy and the broad investigative powers granted to law enforcement under Sections 91 and 100 of the Code of Criminal Procedure (CrPC), 1973 (now updated under the Bharatiya Nagarik Suraksha Sanhita, 2023), creates a highly volatile constitutional landscape.

Cloud forensics compounds these mobile complexities exponentially. When critical evidentiary data is stored exclusively in the cloud, physical acquisition of server hardware is impossible, rendering traditional disk-imaging procedures obsolete.[1182] A smartphone lawfully seized in New Delhi may contain a valid OAuth token granting instantaneous access to a server physically located in Ireland, managed by a tech conglomerate headquartered in the United States, and governed by corporate data privacy policies rather than Indian criminal law. Indian law enforcement agencies frequently attempt to circumvent heavily bureaucratic MLAT procedures — which can routinely take 12 to 18 months — by issuing direct emergency data disclosure requests to tech conglomerates, creating a massive asymmetry in the administration of justice.[1183]

V. FOURTH-GENERATION FORENSIC TOOLS: ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND THE ALGORITHMIC BLACK BOX PARADIGM

The sheer volume, relentless velocity, and staggering variety of digital evidence generated by modern digital society have definitively rendered traditional, manual forensic analysis mathematically intractable. A contemporary financial fraud or counter-terrorism investigation may routinely involve processing

[1181] Code of Criminal Procedure 1973, ss 91, 100; Bharatiya Nagarik Suraksha Sanhita 2023, ss 94, 103.
[1182] Josiah Dykstra, *Essential Cybersecurity Science: Build, Test, and Evaluate Insecure Software* (O'Reilly Media 2016) 141–144.
[1183] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (UNODC 2013) 197–199.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 6 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

petabytes of data across dozens of deeply interconnected devices, cloud accounts, and decentralised communication platforms.[1184] To overcome this fundamental cognitive limitation, the forensic industry has decisively entered its fourth generation, characterised by the deep integration of Artificial Intelligence (AI) and advanced Machine Learning (ML) algorithms into leading forensic platforms such as Nuix Workstation, Relativity, and Magnet AXIOM Cyber.

AI-driven forensic tools deploy sophisticated Natural Language Processing (NLP) pipelines to semantically analyse millions of intercepted emails for hidden sentiment and criminal intent, utilise deep convolutional neural networks (CNNs) for rapid facial recognition and the detection of manipulated deepfake media, and deploy complex behavioural ML classifiers to instantly identify anomalous file modifications indicative of zero-day malware infections.[1185] While these immense capabilities drastically reduce processing times, they introduce an unprecedented, systemic epistemological crisis into the courtroom: the algorithmic "black box" problem. Deep learning models — consisting of multiple interconnected layers of artificial neurons — learn patterns by adjusting millions of internal weights based on vast historical training datasets, rendering the underlying logic entirely opaque and unintelligible even to the scientists who programmed the software.[1186]

This algorithmic opacity collides violently and irreconcilably with established evidentiary standards. Under the United States Supreme Court's Daubert standard, scientific evidence must be rigorously testable, subjected to extensive peer review, possess a known and acceptable error rate, and enjoy general acceptance within the relevant scientific community.[1187] A purely black-box AI algorithm fundamentally fails these criteria because its internal logic cannot be meaningfully tested or cross-examined by the defence. Furthermore, ML classifiers are notoriously susceptible to severe training data bias, resulting in devastating false positives that may disproportionately target specific demographics, misidentify faces, or wrongly flag benign file configurations as malicious, leading directly to wrongful convictions.

To salvage the legal admissibility of AI forensics, the highly specialised sub-discipline of Explainable

Artificial Intelligence (XAI) has emerged. Prominent XAI methodologies include LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations).[1188] SHAP, grounded in cooperative game theory, quantifies the exact marginal contribution of each individual feature to the model's final prediction. By integrating SHAP and LIME, forensic AI systems can generate transparent decision explanations, mitigating their black-box nature and attempting to satisfy legal admissibility standards regarding transparency.

[1184] Jason Sachowski, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (Syngress 2016) 67–69.

[1185] Liliana Pasquale and others, "Artificial Intelligence in Digital Forensics" (2021) 18 *Digital Investigation* 301168.

[1186] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015) 1–5.

[1187] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 592–594 (1993).

[1188] Marco Tulio Ribeiro and others, "Why Should I Trust You?: Explaining the Predictions of Any Classifier" in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (2016) 1135–1144; Scott Lundberg and Su-In Lee, "A Unified Approach to Interpreting Model Predictions" in *Advances in Neural Information Processing Systems* vol 30 (2017).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

AI Characteristic	Traditional Deterministic Forensics	AI "Black Box" Forensics	Explainable AI (XAI) Forensics
Nature of Output	Exact, Binary, Highly Deterministic	Probabilistic, Statistico Opaque	Probabilistic with specific mapped feature attribution
Interpretability	Exceptionally High (matching a mathematical hash value)	None (opaque neural weights distributed across hidden layers)	Moderate to High (via LIME/SHAP mapping algorithms)
Primary Error Source	Distinct code bugs, human logic errors	Training data bias, imbalanced datasets, overfitting	XAI model approximation errors, misinterpretation of SHAP values
Court Legal Status	Broadly accepted; rarely challenged	Highly contested; extremely vulnerable to Daubert cross-examination	The emerging gold standard for court admissibility and GDPR compliance

Table 3: Comparative Analysis of Deterministic, Black-Box, and Explainable AI Forensic Paradigms

Within the specific context of Indian jurisprudence, the impending influx of AI-generated forensic outputs exposes the severe, structural inadequacy of Section 65B of the Indian Evidence Act. Section 65B(4) strictly demands a signed certificate verifying that the "computer was operating properly" during the generation of the electronic record.[1189] However, a computer executing a deeply flawed, racially biased, or statistically inaccurate machine learning algorithm is, strictly from a hardware perspective, operating perfectly according to its programmed instructions. Indian courts, entirely lacking a statutory or judicial mechanism to rigorously probe algorithmic logic, are currently forced to accept AI outputs based purely on the immense deference afforded to state-appointed expert witnesses under Section 45 of the Evidence Act, creating a profound risk of miscarriages of justice in cases involving predictive policing or AI forensic analysis.

VI. THE EPISTEMOLOGICAL DEBATE: OPEN-SOURCE VERSUS PROPRIETARY SOFTWARE PARADIGMS

Underpinning the rapid evolution of these four generations of forensic tools is a fierce, ongoing epistemological debate regarding the optimal paradigm for forensic software development: open-source versus proprietary commercial models.[1190] This debate extends far beyond mere technical preference; it dictates the fundamental parameters of an accused person's constitutional right to a fair trial, transparency, and the ability to conduct an effective cross-examination of the evidence presented against them.

[1189] Indian Evidence Act 1872, s 65B(4); *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473, para 24.

[1190] Vassil Roussev, *Digital Forensic Science: Issues, Methods, and Challenges* (Morgan and Claypool Publishers 2016) 33–37.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 6 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Advocates for deeply proprietary software — such as AccessData's FTK, OpenText's EnCase, and Cellebrite's UFED — forcefully argue that massive commercial backing provides the necessary financial resources and dedicated engineering teams for rapid, continuous research and development.[1191] However, proprietary vendors vigorously and legally guard their source code as highly valuable corporate trade secrets. When a proprietary tool produces a specific forensic artefact in court, the underlying algorithmic logic retrieving and interpreting that artefact is completely hidden behind a corporate firewall, inaccessible to both the prosecution and the defence.

Conversely, open-source forensic tools — such as Autopsy, The Sleuth Kit, Wireshark, and the Volatility Framework — publish their complete, unredacted source code for the world to scrutinise.[1192] Proponents of the open-source paradigm argue that true scientific validity absolutely requires open peer review, which is only possible when the computational algorithms are entirely transparent and subject to independent, rigorous academic auditing. Empirical academic research and rigorous testing repeatedly demonstrate that properly validated open-source tools consistently produce highly reliable, repeatable results with error rates strictly comparable to their expensive commercial counterparts.

This fundamental clash of paradigms creates severe friction within the adversarial judicial system. Indian procedural law, heavily influenced by colonial-era drafting, lacks a definitive, modern mechanism for a defendant to compel the disclosure of a proprietary forensic tool's source code during a trial.[1193] This contrasts sharply with certain jurisdictions in the United States, where courts — such as in the landmark case of *State v. Underdahl* — have forcefully compelled the disclosure of proprietary software source code under protective orders to ensure a defendant's fundamental constitutional right to confront the scientific evidence levied against them.

VII. THE CRUCIBLE OF VALIDATION: THE NIST CFTT PROGRAMME AND GLOBAL REGULATORY STANDARDS

To bridge the dangerous gap between opaque software paradigms and ensure a baseline of scientific reliability for court admissibility, international regulatory bodies increasingly rely on standardised, empirical testing frameworks. The United States National Institute of Standards and Technology (NIST) Computer

Forensics Tool Testing (CFTT) programme represents the undisputed global gold standard in this domain.[1194]

Established in 1999 directly in response to the rigorous demands of the Supreme Court's *Daubert* ruling, the NIST CFTT programme systematically and empirically tests forensic tools for critical functions including disk imaging, deleted file recovery, mobile device acquisition, and hardware write-blocking. The methodology is exhaustive: NIST first develops highly specific tool category specifications and rigorous assertions, designs standardised test cases using known datasets — such as the CFReDS reference data sets — and executes these tests against both open-source and proprietary software. By publicly publishing detailed, peer-reviewed performance reports, the CFTT provides the objective, scientific data absolutely required by judges conducting Daubert gatekeeping hearings.[1195]

The Indian forensic ecosystem is structurally and dangerously deficient in this specific regard. India currently possesses no domestic equivalent whatsoever to the NIST CFTT programme.[1196] While resource-constrained

[1191] Cellebrite, *Annual Digital Intelligence Report* (Cellebrite 2022) 6.
[1192] Brian Carrier, "Open Source Digital Forensics Tools: The Legal Argument" (2002) @stake Research Paper accessed 1 April 2025.
[1193] *State v. Underdahl*, 767 N.W.2d 677 (Minn. 2009) (compelling disclosure of Intoxilyzer source code under analogous principles).
[1194] James Lyle, *NIST CFTT: Testing Disk Imaging Tools* (NIST Special Publication 500-254, 2003) 1.
[1195] National Institute of Standards and Technology, *Computer Forensics Tool Testing Program: Test Results for Disk Imaging Tools* (NIST SP 500-280, 2007).
[1196] Department of Electronics and Information Technology, Information Technology Act 2000: Section 79A — Examiners of Electronic Evidence (Ministry of Electronics and Information Technology, Gazette Notification, 2009).

Indian state forensic science laboratories (SFSLs) increasingly rely on free open-source tools like Autopsy to manage massive caseloads, the absolute lack of a standardised, government-backed validation framework leaves this critical evidence highly vulnerable to aggressive judicial scepticism and dismissal. Furthermore, Section 79A of the Indian Information Technology Act, 2000, establishes a dangerous monopoly by empowering the Central Government to designate official "Examiners of Electronic Evidence," yet it mandates absolutely zero quality control or validation standards for the actual digital forensic tools these examiners utilise.

VIII. CONCLUSION: THE IMPERATIVE FOR STRUCTURAL REFORM IN INDIAN FORENSIC JURISPRUDENCE

The sweeping technical evolution detailed across these four generations highlights a systemic, critical vulnerability within the Indian criminal justice system's heavy reliance on digital evidence. The entire edifice of digital admissibility in India rests precariously upon the outdated procedural conformity dictated by Section 65B of the Evidence Act, as rigidly interpreted by the Supreme Court in the *Anvar P.V. v. P.K. Basheer* and

Arjun Panditrao Khotkar line of jurisprudence.[1197]

This archaic legal framework essentially creates a legal fiction wherein the correct functioning of the silicon hardware automatically guarantees the scientific validity of the highly complex, potentially flawed, and inherently biased software algorithms executing upon it. Section 65B is entirely blind to the substantive reliability of the forensic tool itself. It simply cannot account for a silent hashing bug in FTK, an undocumented and invasive bootloader exploit utilised by Cellebrite, or the devastating demographic bias embedded within a machine learning classifier used for digital triage.[1198]

In conclusion, the unceasing, exponential evolution of digital forensic tools — from rudimentary Unix disk imagers to profoundly opaque AI prediction engines — dictates that mere procedural legal safeguards are no longer remotely sufficient.[1199] To prevent an impending crisis of wrongful convictions stemming directly from tool-induced errors and algorithmic bias, the Indian legal system must urgently pivot from superficial procedural authentication to rigorous, substantive scientific scrutiny. This necessitates the immediate legislative establishment of an independent, statutory Digital Forensic Tools Regulatory Authority, mandated to execute mandatory, peer-reviewed, empirical testing of all forensic software prior to its use in a criminal trial, thereby ensuring that the epistemological foundation of digital evidence in India is robust, transparent, and constitutionally sound.

REFERENCES

I. PRIMARY SOURCES

A. Statutes and Codes

Indian Evidence Act, 1872 (Act 1 of 1872).

Information Technology Act, 2000 (Act 21 of 2000).

Code of Criminal Procedure, 1973 (Act 2 of 1974).

Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

Constitution of India, 1950.

B. Subordinate Legislation and Notifications

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

[1197] *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

[1198] Eoghan Casey, *Handbook of Digital Forensics and Investigation* (Academic Press 2010) 15–17.

[1199] Law Commission of India, *185th Report on Review of the Indian Evidence Act 1872* (Law Commission 2003) Chapter 6.

Information Technology (Examiner of Electronic Evidence) Notification, 2009 (Ministry of Electronics and Information Technology, Gazette Notification No. SO 2291(E), 2009).

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

C. Judicial Decisions

Indian Courts

Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1. *K.S. Puttaswamy v. Union of India* (2017) 10 SCC 1.

State of Maharashtra v. Dr. Praful Desai (2003) 4 SCC 601.

Shafi Mohammad v. State of Himachal Pradesh (2018) 5 SCC 311.

Tomaso Bruno v. State of Uttar Pradesh (2015) 7 SCC 178.

Foreign Decisions (Persuasive Authority)

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Kumho Tire Co. Ltd v. Carmichael, 526 U.S. 137 (1999).

State v. Underdahl, 767 N.W.2d 677 (Minn. 2009).

United States v. Llera Plaza, 188 F. Supp. 2d 549 (E.D. Pa. 2002).

II. BIBLIOGRAPHY

A. Books

Brian Carrier, *File System Forensic Analysis* (Addison-Wesley Professional 2005).

Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd edn, Academic Press 2011).

Casey E (ed), *Handbook of Digital Forensics and Investigation* (Academic Press 2010).

Dykstra J, *Essential Cybersecurity Science: Build, Test, and Evaluate Insecure Software* (O'Reilly Media 2016).

Garfinkel S and Spafford G, *Practical Unix and Internet Security* (3rd edn, O'Reilly Media 2003).

Mandia K and Prosise C, *Incident Response and Computer Forensics* (2nd edn, McGraw-Hill 2003).

Nelson B, Phillips A and Steuart C, *Guide to Computer Forensics and Investigations* (5th edn, Cengage Learning 2014).

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

Roussev V, *Digital Forensic Science: Issues, Methods, and Challenges* (Morgan and Claypool Publishers 2016).

Sachowski J, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (Syngress 2016).

B. Journal Articles and Book Chapters

Garfinkel S, "Digital Forensics" (2010) 8(4) *IEEE Security and Privacy* 59.

Garfinkel S, "Lessons Learned Writing Digital Forensics Tools and Managing a Large Corpus of Digital Evidence" (2013) 10 *Digital Investigation* S80.

Lundberg S and Lee S-I, "A Unified Approach to Interpreting Model Predictions" in *Advances in Neural Information Processing Systems* vol 30 (2017).

Pasquale L and others, "Artificial Intelligence in Digital Forensics" (2021) 18 *Digital Investigation* 301168.

Ribeiro M T, Singh S and Guestrin C, "Why Should I Trust You?: Explaining the Predictions of Any Classifier" in

Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (ACM 2016) 1135.

Turner P, "Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)" in *Proceedings of the 5th Annual Digital Forensic Research Workshop* (2005) 223.

C. Reports and Policy Documents

Cellebrite, *Annual Digital Intelligence Report* (Cellebrite 2022).

Law Commission of India, *185th Report on Review of the Indian Evidence Act 1872* (Law Commission of India 2003).

Ministry of Home Affairs, *Guidelines on Cyber Forensics for Law Enforcement Agencies* (Government of India 2007).

National Institute of Standards and Technology, NIST SP 500-240: *An Overview of Issues in Testing Forensic Software* (NIST 1999).

National Institute of Standards and Technology, NIST SP 500-254: *Test Results for Disk Imaging Tools* (NIST 2003).

National Institute of Standards and Technology, NIST SP 500-280: *Computer Forensics Tool Testing Program* (NIST 2007).

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (UNODC 2013).

Volatility Foundation, *The Volatility Framework: Volatile Memory Artifact Extraction Utility* (Volatility Foundation 2020).

WEBLIOGRAPHY

A. Government and Regulatory Websites

Ministry of Electronics and Information Technology, Government of India — IT Act, Notifications, and Examiner of Electronic Evidence Gazette Orders <https://meity.gov.in>.

Ministry of Home Affairs — Cyber and Information Security Division, Guidelines and Reports <https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division>.

Central Forensic Science Laboratory (CFSL), Ministry of Home Affairs <https://cfsl.gov.in>.

Supreme Court of India — Judgments and Orders <https://main.sci.gov.in>.

National Crime Records Bureau — Cyber Crime Statistics and Reports <https://ncrb.gov.in>.

Telecom Regulatory Authority of India — Interception and Surveillance Policy Documents <https://trai.gov.in>.

B. International Standards and Organisations

National Institute of Standards and Technology (NIST) — Computer Forensics Tool Testing (CFTT) Programme, All Published Test Reports and Specifications <https://www.nist.gov/system-forensics/cftt-program>.

National Institute of Standards and Technology — Computer Forensic Reference Data Sets (CFReDS) Project <https://cfreds.nist.gov>.

Scientific Working Group on Digital Evidence (SWGDE) — Best Practice Documents and Standards <https://swgde.org>.

International Organisation of Computer Evidence (IOCE) — Digital Evidence Standards <https://ioce.net>.

INTERPOL — Digital Forensics and Cybercrime Technical Resources <https://www.interpol.int/Crimes/Cybercrime/Digital-forensics>.

European Union Agency for Cybersecurity (ENISA) — Forensics and Evidence Collection Guidelines <https://www.enisa.europa.eu>.

C. Forensic Tool Vendors and Open-Source Communities

OpenText (formerly Guidance Software) — EnCase Forensic Tool Documentation and Whitepapers <https://www.opentext.com/products/encase-forensic>.

Exterro (formerly AccessData) — Forensic Toolkit <https://www.exterro.com/forensic-toolkit>.

Cellebrite — UFED Product Documentation, Technical Specifications, and Digital Intelligence Reports <https://cellebrite.com/en/ufed>.

Autopsy Digital Forensics Platform (The Sleuth Kit) — Open-Source Documentation and Source Code <https://www.autopsy.com>.

Volatility Foundation — Framework Documentation, Plugin Repository, and Research Publications <https://www.volatilityfoundation.org>.

Wireshark — Network Protocol Analyser Official Documentation and Developer's Guide <https://www.wireshark.org/docs>.

Magnet Forensics — AXIOM Cyber Product Documentation and Research Blog <https://www.magnetforensics.com>.

D. Legal Databases and Academic Resources

SCC Online — Supreme Court Cases Database (Subscription Required) <https://www.scconline.com>.

Manupatra — Supreme Court, High Court and Tribunal Decisions (Subscription Required) <https://www.manupatra.com>.

Indian Kanoon — Open-Access Database of Judicial Decisions <https://indiankanoon.org>.

Digital Investigation Journal (Elsevier) — Peer-Reviewed Digital Forensics Research <https://www.sciencedirect.com/journal/digital-investigation>.

USENIX Security Symposium — Proceedings on Digital Forensics and Security Research <https://www.usenix.org/conference/usenixsecurity>.

ACM Digital Library — SIGKDD and CCS Proceedings on Machine Learning and Security <https://dl.acm.org>.

E. Specific Documents and Reports (Direct URLs)

National Institute of Standards and Technology, CFTT Test Results for Disk Imaging (2007) <https://www.nist.gov/sites/default/files/documents/2017/05/09/DI-SP-UTSA-Results.pdf>.

Brian Carrier, "Open Source Digital Forensics Tools: The Legal Argument" (2002) <https://www.digital-evidence.org/papers/opensrc_legal.pdf>.

MEITY Notification — Examiners of Electronic Evidence u <https://meity.gov.in/writereaddata/files/GSR_702(E)_0.pdf>.

K.S. Puttaswamy v. Union of India (2017) — Full Text <https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf>.

Anvar P.V. v. P.K. Basheer (2014) — Full Text <https://indiankanoon.org/doc/31543338>.

Volatility Foundation GitHub Repository — Com <https://github.com/volatilityfoundation/volatility3>.

Cellebrite Digital Intelligence Blog — Technical Research <https://cellebrite.com/en/blog>.