INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ISSN: 2582-6433

COMPUTER FORENSICS: CONVICTING CRIMINALS BASED ON COMPUTER USAGE EVIDENCE

AUTHORED BY - MS. PRIYANKA GEHLOT[1] MR. ABHIJEET SINGH[2]

ABSTRACT

In the contemporary Indian legal landscape, the transition from traditional physical evidence to digital artifacts has redefined the parameters of criminal prosecution. This paper examines the critical role of computer forensics in convicting criminals, framed within the transformative legislative shift from the Indian Evidence Act (IEA) to the Bharatiya Sakshya Adhiniyam (BSA), 2023. As digital footprints become ubiquitous, the investigation of computer usage evidence - including system logs, registry entries, volatile RAM data, and application-specific artifacts - serves as the primary mechanism for establishing *mens rea* (guilty mind) and *actus reus* (guilty act). The research analyzes the procedural rigors required under Indian law to ensure that digital evidence is admissible and untainted. Central to this is the evolution of the mandatory certification process, formerly under Section 65B of the IEA, and the increasing reliance on Section 79A of the Information Technology Act for expert testimony. Through a synthesis of technical forensic methodology and judicial precedents - such as the landmark *Arjun Panditrao* ruling - this paper explores how Indian Law Enforcement Agencies (LEAs) utilize tools like Autopsy and Magnet AXIOM to extract evidence from encrypted environments and cloud-native architectures.

Furthermore, the study addresses unique indigenous challenges, including the forensic analysis of UPI (Unified Payments Interface) transaction metadata, the handling of Aadhaar-linked digital identities, and the jurisdictional hurdles of Digital Arrest scams. By evaluating the role of the Indian Cyber Crime Coordination Centre (I4C) and Central Forensic Science Laboratories (CFSLs), the paper concludes that while AI-driven anti-forensics poses a growing threat, a robust adherence to the Chain of Custody and standardized hash-value verification remains the bedrock of securing convictions in India's digital age.

[1] Assistant Professor, Jagannath University, Jaipur
[2] LLM Student, Jagannath University Jaipur

ISSN: 2582-6433

Keywords: Computer Forensics, Bharatiya Sakshya Adhiniyam (BSA), Digital Evidence, Section 65B Certificate, Indian IT Act, Cybercrime Conviction, Chain of Custody, UPI Forensics.

I. Introduction

1.1 Definition and Scope

Computer forensics is defined as the methodical application of scientifically proven investigation and analysis techniques to identify, preserve, and document digital evidence in a manner suitable for a court of law. In India, this scope is strictly governed by the Information Technology Act, 2000, and the procedural mandates of the Bharatiya Sakshya Adhiniyam (BSA), which require a seamless link between binary data and criminal intent.

1.2 Historical Evolution

The field has undergone a radical transition:

a. **Traditional Forensics (Dead Box):** Seizing physical hardware and performing offline analysis on static hard drives.
b. **Modern Forensics:** Live-system analysis, mobile device extraction, and cloud-native forensics (Basharat, 2025).
c. **The Indian Context:** The shift from treating digital evidence as secondary to the current status where electronic records are primary evidence under the BSA, 2023, provided their integrity is verified by hash values and mandatory certifications.

1.3 Research Problem

Despite the advanced capabilities of modern forensic tools, a critical gap exists between technical discovery and legal admissibility in the Indian judicial system.

The core research problem focuses on the following dimensions:

1. **The Certification Hurdle:** While investigators can extract computer usage evidence (e.g., browser history, deleted WhatsApp databases, or UPI logs), these often fail in court due to improper adherence to Section 65B of the IEA (now replaced by Section 63 of the BSA). The problem lies in the lack of a standardized SOP for Examiners of Electronic Evidence to certify cloud-stored data.
2. **Attribution vs. Possession:** In a country with high device sharing and public Wi-Fi usage, proving that a specific *person* (not just a device) committed an act remains a

ISSN: 2582-6433

significant forensic challenge. Establishing exclusive possession of digital evidence is a recurring point of failure in prosecutions.

3. **Anti-Forensics and Encryption:** The rise of end-to-end encryption (E2EE) and self-destructing messages creates dark data that remains inaccessible to standard CFSL (Central Forensic Science Laboratory) tools, leading to a high rate of acquittals in cyber-terrorism and financial fraud cases.
4. **Technological Lag:** The rapid evolution of Digital Arrest scams and deepfake-based extortion often outpaces the legal frameworks and the technical training of local police officers, creating a "forensic backlog" that compromises the Chain of Custody.

1.4 Research Question: How can the Indian legal system and forensic laboratories integrate automated AI-profiling and cloud-native forensic protocols to ensure that computer usage evidence survives the rigors of the Bharatiya Sakshya Adhiniyam to secure higher conviction rates?

2. Technical Foundations of Digital Evidence

Evidence is categorized into persistent and transient data, each requiring specific handling to maintain integrity.

2.1 File System Artifacts:

Recovery & Carving: Even when a criminal deletes files or formats a drive, forensic "data carving" can recover headers and footers of files from unallocated space.

Registry Analysis: Analyzing Shellbags and LNK files allows investigators to prove that a suspect navigated specific folder, even if those folders no longer exist. This establishes knowledge and intent.

File Signature Analysis: This prevents criminals from hiding data by changing extensions (e.g., renaming a .jpg incriminating photo to .dll). Forensic tools identify the true file type via the hex header.

2.2 User Activity Logs:

Internet & Browser History: Crucial for proving premeditation (e.g., searching for how to bypass OTP or poisonous chemicals).

Application Objects: Analyzing the .db files of apps like WhatsApp or Telegram. In India, metadata from these apps is often used to establish cyber-presence at the time of a crime.

ISSN: 2582-6433

2.3 Volatile Data (Live Forensics):

RAM Captures: Contains active passwords, decrypted chat messages, and running processes that disappear when the device is powered off.

Network Flow Metadata: Essential in IP-spoofing cases to trace the origin of a packet back to a specific Indian ISP gateway.

2.4 Forensic Toolkits

To ensure evidence is not tampered with during analysis, Indian labs use internationally validated toolkits that generate automated logs and hash reports.

Autopsy/Sleuth Kit: An open-source standard used by many state SFSLs for disk imaging and keyword searching.

Magnet AXIOM: Highly effective for Cloud Forensics, allowing Indian LEAs to pull data from Google Drive or iCloud when provided with a legal warrant.

Hash Filtering (SHA-256/MD5): Every piece of evidence is assigned a digital fingerprint (hash). If a single bit of data is changed, the hash changes, alerting the court to potential evidence tampering.

2.5 Relevant Case Laws

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020):[3] The Supreme Court of India clarified that a certificate under Section 65B(4) is a *condition precedent* to the admissibility of electronic records. In computer forensics, this means the forensic report is useless unless accompanied by a certificate from the person in charge of the computer/server.

Anvar P.V. v. P.K. Basheer (2014):[4] Established that if an original electronic record (the actual device) is produced in court, a 65B certificate is not required. However, since devices are usually kept in forensic labs, "usage evidence" is almost always presented as a copy (secondary evidence), making the forensic process and certificate mandatory.

State of Delhi v. Mohd. Afzal (2003):[5] One of the earliest cases where computer usage evidence (laptop logs and printouts) was used to establish the conspiracy in the Parliament Attack case. The court held that electronic records are admissible if the system was operating properly during the period of evidence creation.

[3] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[4] Anvar P.V. v. P.K. Basheer & Others, (2014) 10 SCC 473.
[5] State (N.C.T. of Delhi) v. Navjot Sandhu @ Afshan Guru (Parliament Attack Case), (2005) 11 SCC 600

ISSN: 2582-6433

3. The Legal Framework for Admissibility

3.1 Foundational Rules: The Best Evidence Rule in the Digital Era

The Best Evidence Rule traditionally required the production of the original document to prove its contents. In the digital context, this posed a challenge: is the original the server, the hard drive, or the data itself?

a. **Primary Evidence (BSA Section 57):** Under the Bharatiya Sakshya Adhiniyam (BSA), 2023, electronic records are now explicitly classified as primary evidence. If data is stored in multiple locations (e.g., cloud synchronization), each instance is considered an original.[6]

b. **The Printout Standard:** For a printout or output of computer usage evidence to be considered an original, it must be shown to be a direct reflection of the data stored in the source device.

3.2 Admissibility Hurdles: The Indian Validation Standard

While Western jurisdictions often use the Daubert Challenge to test the scientific validity of forensic software, India relies on a strict Certification and Expert Opinion model.

a. **The Section 63 Certificate (formerly 65B IEA):** This is the gatekeeper of digital evidence. A conviction cannot be sustained based on a digital usage log (like a Google search history or a UPI transaction) unless it is accompanied by a certificate stating that the computer was operating properly and the data was not tampered with.[7]

b. **Expert Testimony (Section 39 BSA / Section 79A IT Act):** Courts rely on the "Examiner of Electronic Evidence" to provide an opinion on the integrity of the data. The forensic investigator must prove that the Hash Value (MD5/SHA-256) recorded during seizure matches the value during analysis.

3.3 Jurisdiction and Digital Borders

The borderless nature of cybercrime remains a primary hurdle for Indian Law Enforcement Agencies (LEAs).

a. **Extra-Territoriality:** Section 75 of the IT Act allows India to prosecute a criminal even if the crime was committed outside India, provided it involved a computer system

[6] Bharatiya Sakshya Adhiniyam, 2023, Section 57, Explanation 4: Where an electronic or digital record is created and stored, and such record is transmitted and transferred through any means... each such record shall be primary evidence.

[7] Ryan, D. J., & Shpantzer, G. (n.d.): *Legal Aspects of Digital Forensics*. This highlights that "usage evidence" is only as strong as the witness who can testify to the reliability of the system that generated it.

ISSN: 2582-6433

located in India.

b. **The MLAT Process:** To obtain usage evidence from foreign-based service providers (like Meta or Google), Indian authorities must navigate Mutual Legal Assistance Treaties (MLAT), a process that can take months and often leads to evidence cooling (data being deleted before it can be seized).[8]

4. Case Analysis: From Evidence to Conviction

4.1 Timestamp Integrity: Defeating Anti-Forensics

A common defence strategy involves claiming a digital alibi by manually altering the system clock to make it appear that incriminating files were created at a different time or that the suspect was not logged into the machine.

a. **Correlation of Time Sources:** Investigators do not rely solely on the local system clock. They compare local timestamps against Network Time Protocol (NTP) logs, router logs, and server-side metadata.

b. **Logfile Analysis:** Modern operating systems maintain deep-level logs (such as the Windows Event Viewer or iOS .logarchive) that record System Time and Network Time separately. Even if a user timestomps a file (altering the Created/Modified dates), the file system journal often preserves the true entry time (Forensic Focus, 2025).

4.2 Establishing Knowledge and Intent (Mens Rea)

For a successful conviction, the prosecution must prove that the act was intentional. Computer usage patterns provide a window into the mind of the accused.

a. **Search History & Premeditation:** Browser history serves as a chronological map of intent. Repeated searches for specific fraud methods, untraceable poisons, or how to delete CCTV footage provide evidence of planning.

b. **Artifact Chaining:** Forensics can show not just that a file existed, but that it was actively engaged with. Analyzing Jump Lists, Shellbags, or Recent Documents proves that the suspect navigated to, opened, and viewed the evidence, refuting claims of accidental downloads or background malware activity.

4.3 Attribution: Linking the User to the Activity

The most significant challenge in digital forensics is the Keyboard Problem" - proving exactly

[8] Raburu, G., et al. (2020): *Legal issues in computer forensics*. Explains the friction between local law enforcement and international data privacy laws (like GDPR) during cross-border evidence collection.

ISSN: 2582-6433

who was sitting at the computer when the crime occurred.

a. **Identity Graph Analysis:** Since IP addresses only identify a connection, investigators use Identity Graphs. This involves mapping saved browser credentials, auto-fill profiles, and synchronized cloud accounts (Gmail, iCloud) to a specific physical person (Basharat, 2025).
b. **Biometric Synchronization:** By linking a specific user login time on a laptop to a simultaneous biometric unlock event (fingerprint or Face ID) on a synchronized mobile device, forensics can create an attribution chain that makes it nearly impossible for a suspect to claim that an unauthorized person used their account.

5. Emerging Challenges and SOTA (2025-2026)

5.1 Cloud-Native Forensics and Ephemeral Data

As India pushes toward a "Cloud-First" digital economy, traditional device seizure is becoming secondary to cloud acquisitions.

a. **Shifting Focus:** Investigations now prioritize IAM (Identity and Access Management) events and API activity logs. In Indian corporate fraud cases, who accessed a cloud bucket is often more important than what is on the suspect's laptop (Basharat, 2025).
b. **The Container Challenge:** With apps running in containers (like Docker or Kubernetes) that delete themselves after use, forensic experts must use Live Capture tools to grab data before it vanishes into the ephemeral ether.

5.2 AI-Powered Forensics and Automated Profilers

The sheer volume of data in India - driven by the world's highest mobile data consumption - makes manual review impossible.

a. **Automated Evidence Profilers (AEP):** Indian labs are integrating AI to perform Anomaly Detection. AI can scan millions of files to instantly flag a single hidden encrypted folder or a pixel-shifted deepfake image (Jain, 2026).
b. **Predictive Analysis:** Using AI to correlate cross-jurisdictional data from the I4C (Indian Cyber Crime Coordination Centre) to identify patterns in Sextortion or Digital Arrest scams across different Indian states.[9]

[9] R Kaur, A Kashyap, D Kumar," Computer Vision Detection Of Submerged Object Through Machine Learning", Elementary Education Online, Vol:20, Issue: 5, Pg: 5013-5019.

ISSN: 2582-6433

5.3 Rapid Data Degradation and Mobile Acquisition

Modern smartphones are now designed with Security by Default, which actively fights forensic extraction.

a. **The AFU (After First Unlock) Window:** In India, investigators emphasize the Quicker, The Better approach. If a seized phone reboots or stays idle for too long, it enters a Before First Unlock (BFU) state, where data becomes mathematically impossible to decrypt (Forensic Focus, 2025).
b. **USB Restrictions:** New OS updates (iOS/Android) frequently disable data transfer through the charging port after a period of inactivity, forcing Indian LEAs to use Signal Blockers and Power Sustainers during transit to the lab.

5. Conclusion

The landscape of criminal investigation in India has undergone a tectonic shift, moving from the tangible world of physical evidence to the intricate, binary world of computer forensics. As this research has demonstrated, the conviction of criminals in the modern era is no longer solely dependent on eyewitness testimony or physical fingerprints, but rather on the digital fingerprints left behind during the course of computer usage. The successful prosecution of cyber-enabled crimes now rests at the precarious intersection of high-level technical extraction and rigid legal admissibility.

In the Indian context, the year 2026 marks a pivotal moment of maturation for this discipline. The transition from the antiquated Indian Evidence Act to the Bharatiya Sakshya Adhiniyam (BSA) has fundamentally redefined the status of digital records. By elevating electronic data to the status of primary evidence, the Indian legislature has acknowledged the reality of a Digital India. However, as explored in this paper, this elevation does not imply a relaxation of standards. The mandatory requirement for certification - now under Section 63 of the BSA - remains the procedural bedrock. Without a scientifically validated chain of custody and a transparent hash-value verification process, the most incriminating computer usage evidence remains legally inert.

Technically, the shift from dead-box forensics to cloud-native and identity-centric analysis reflects the increasing complexity of criminal behavior. The ability of forensic investigators to bypass anti-forensic measures, such as time stomping and data wiping, through the analysis of unified logs and volatile RAM data, has proven decisive in establishing *mens rea*. In high-

ISSN: 2582-6433

profile cases of financial fraud and conspiracy, the correlation of search histories, application metadata, and UPI transaction logs has provided courts with a window into the mind of the accused that physical evidence could never offer. Furthermore, the emergence of Identity Graph Analysis has finally begun to solve the Keyboard Problem, allowing investigators to attribute digital actions to specific individuals with a degree of certainty that survives judicial scrutiny.

However, the future of computer forensics in India is not without its hurdles. The rapid evolution of end-to-end encryption, ephemeral containerized data, and AI-driven anti-forensics presents a constant challenge to Law Enforcement Agencies (LEAs). The forensic backlog in Central and State Forensic Science Laboratories remains a bottleneck that can lead to data degradation or procedural lapses. To maintain the integrity of the judicial process, India must continue to invest in Automated Evidence Profilers (AEP) and AI-driven anomaly detection to handle the sheer volume of data generated by its population.

Ultimately, the power of computer forensics to convict lies not just in the software used, but in the credibility of the forensic scientist as an expert witness. As the Indian judiciary becomes increasingly tech-savvy, the demand for scientific validity over mere technical possession will grow. This paper concludes that while the tools of the trade - from Magnet AXIOM to Autopsy - are essential, the ultimate guarantor of a conviction is a seamless, transparent, and legally compliant forensic workflow. As we look toward the remainder of the decade, the synergy between robust legislative frameworks like the BSA and cutting-edge forensic technology will be the primary deterrent against the rising tide of digital criminality in India. The foundation of trust in digital evidence is the new cornerstone of justice.