Deconstructing Section 61 of the BSA,2023: The Procedural Vulnerabilities of Hashing, Mirroring, and Chain-of-Custody in Cryptographic & Cyber-Syndicate Investigations

Deepak Sharma[1]*, Dr. Rinu Saraswat[2]

1 Research Scholar, Apex School of Law, Apex University, Jaipur, Rajasthan, India

wolkgeist@gmail.com

2 Supervisor, Apex School of Law, Apex University, Jaipur, Rajasthan, India

Abstract: This paper critically deconstructs Section 61 of the Bharatiya Sakshya Adhiniyam, 2023 in the context of cryptographic and cyber-syndicate investigations. While the provision recognizes electronic and digital records as admissible evidence, its practical application depends upon the integrity of hashing, mirroring, metadata preservation, forensic imaging, and chain-of-custody protocols. The study examines how procedural lapses, technological manipulation, inadequate certification, and weak investigative documentation may compromise authenticity, reliability, and evidentiary value. It argues that digital admissibility must be supported by robust forensic standards, judicial scrutiny, and investigator accountability to ensure fair trial, due process, and cyber-evidence integrity within modern Indian criminal courts.

Keywords: Section 61, Bharatiya Sakshya Adhiniyam 2023, Digital Evidence, Electronic Records, Hashing, Mirroring, Chain of Custody, Cryptographic Evidence, Cyber-Syndicate Investigation, Forensic Integrity

INTRODUCTION

The Digital Frontline of Organized Crime and the Statutory Architecture of the Bharatiya Sakshya Adhiniyam, 2023. Criminal groups today have advanced technologically at an alarming pace, moving from operations based in physical structures to those conducted in encrypted digital spaces. Organized gangs, transnational cartels, and localized cyber-syndicates regularly use encrypted communication channels, decentralized applications, and peer-to-peer cryptocurrency networks to carry out complex extortion schemes, run illicit supply chains, and launder the proceeds of crime. In this complex environment, traditional physical evidence is often absent, and law enforcement agencies are left almost exclusively

with digital traces. Today's criminal investigations increasingly focus on transient server logs, volatile mobile device artifacts, cryptocurrency transaction trails, and metadata.

In order to bring India's legal system in conformity with these technological developments, the legislature enacted the Bharatiya Sakshya Adhiniyam, 2023 (BSA), which officially repealed and replaced the colonial-era Indian Evidence Act, 1872 (IEA), on 1 July 2024. This legislative change is more than just a cosmetic update; it fundamentally alters the nature of how digital evidence is defined, authenticated, and admitted into trials.

This transition is driven by Section 61 of the BSA, 2023 a new addition to the BSA that creates a rule that electronic or digital records are not disqualified from being useful for evidentiary purposes solely because they are electronic or digital. Section 61 accords electronic documentation the same legal validity as traditional paper documents. But this equality is not natural. The admissibility of any information contained in a digital record is subject only to the provisions of the law relating to the admissibility of evidence provided under Section 63 of the BSA, as explicitly stated in Section 61.

Section 63 of the BSA, which replaced the former Section 65B of the IEA, is the route to secondary electronic evidence. It determines if "computer outputs" (printouts, copies on optical media, and extractions from semiconductor memory) are permissible without the requirement of producing the physical source device. Section 63 is designed to facilitate the presentation of digital evidence, but it also lays down strict technical and procedural requirements. In the context of investigations involving highly organized, tech-savvy cyber-syndicates, these statutory demands reveal deep systemic weaknesses in the investigative machinery of state police forces.

Défense counsel has increasingly exploited procedural weaknesses in cryptographic hashing, device mirroring, and chain-of-custody documentation during cross-examination, sometimes leading to the collapse of sophisticated prosecutions, from unscientific device seizures on the scene to the long-standing technical backlogs of forensic laboratories.

The Ontological Divide: Explanations to Section 57, the Redefinition of Primary Evidence, and Tensions with Arjun Panditrao

The legal treatment of electronic evidence has been complicated for a long time by a fundamental conceptual challenge: a physical document has a tangible, singular physical form,

whereas a digital record is a dynamic sequence of binary states stored on physical media. Digital data is extremely flexible. It can be copied very easily and can be altered without any physical evidence.

This challenge was sought to be addressed in a three-judge bench of the Supreme Court of India in *Arjun Panditrao Khotkar v. Kailash Kushalrao Gorantyal (2020)* under the old IEA framework. The Court held that "primary electronic evidence" is the original electronic record in the particular computer or device in which the information was first stored. The Court adopted a strict source test. Any output from that device, whether a printout, a copy on CD-ROM, or a forensic mirror image on an external drive, was considered secondary electronic evidence and required a mandatory certificate of authenticity.

The BSA attempts to take account of the dynamic nature of computer records by changing this classification. The explanations to Section 57 define certain classes of automated, sequential, and replicated digital records as primary evidence, and the BSA has incorporated these explanations.

Explanation 4 in particular relates to electronic or digital records created or stored simultaneously or successively in more than one file and treats each file as primary evidence. This provision is intended to make clear that automated backups, mirror systems, and sequential database writes are valid primary evidence. However, this classification often ignores metadata discrepancies and temporary file drift during rapid sequential writes.

Explanation 5 is about electronic or digital records taken from proper custody, and these are primary evidence unless challenged. This means there is no need for Section 63 certification for public or corporate records kept routinely, but it opens a big legal loophole for digital evidence held by the state or seized by the police.

Explanation 6 is about video recordings that are stored in electronic form and transmitted, broadcast, or transferred to another medium, with each stored recording being considered the primary object. This is good for live-streamed media, CCTV feeds, and synchronized broadcasts. However, such records are highly susceptible to network latency, packet loss, compression artifacts, and frame injection.

Finally, Explanation 7 relates to electronic or digital records stored in several storage spaces within a computer resource and states that each such automated storage, including temporary

files, is primary evidence. It recognizes RAM dumps, cache files, and virtual memory swap spaces, but volatile memory is extremely ephemeral, and extracting it is inherently destructive and changes the physical state of the system.

The categories of primary evidence are extended under Section 57, and a major procedural tension is created, especially with regard to Explanation 5. The legislature has established a presumption of authenticity for records in the custody of public officials and law enforcement agencies by providing that any digital record produced from proper custody is primary evidence unless challenged. This classification enables the prosecution to avoid the strict two-tier certification requirements of Section 63 by simply stating that the seized and extracted digital files are in lawful police custody or with a government-notified cyber portal.

This presumption of proper custody runs counter to the fundamental principles of digital forensics. In forensic practice, there is no presumption of the authenticity of a digital record. The process of identifying, preserving, extracting, and analyzing digital data is highly intrusive. If an investigating officer takes a mobile phone during a raid and copies the contents to an external hard drive and does not use hardware write-blockers or immediately generate a hash value, then the data is changed.

By treating state-extracted files as primary evidence under the guise of proper custody, the BSA dilutes the constitutional protections of the accused and compromises the equality of arms at trial. This forces defence counsel to reactively challenge and demonstrate tampering ex post facto instead of requiring the state to cryptographically prove the integrity of its evidence as a condition of admissibility. This change is particularly disturbing in complicated trials involving encrypted communications and cryptocurrency wallets, where the state itself is a litigant and has the ability and motivation to change digital structures to make its prosecution easier.

Mathematical and Cryptographic Protocols under Section 63: Hashing, Mirroring, and the Two-Tier Certification Framework

The BSA in section 63(4) offers a cryptographic protection against the potential risk of tampering with digital evidence by mandating the disclosure of hash values. The hash value is a unique alphanumeric digital fingerprint of a specific data set. Mathematically, a

cryptographic hash function is a function that takes an input of arbitrary length and returns a unique output string of a fixed length.

This mathematical mapping is based on three fundamental properties that make hashing extremely reliable for legal authentication:

1. Pre-image Resistance, or the one-way property, is that for any given output string, it is computationally infeasible to reconstruct the original input file.

2. Second pre-image resistance (or weak collision resistance): It is computationally infeasible to find a second input that produces the same output as a given input.

3. Collision resistance or strong collision resistance means it is computationally infeasible to find any two different arbitrary inputs that hash to the same output.

One of the most important properties in cryptographic hashes is the avalanche effect. For example, changing one bit of an input file will produce a completely different and unpredictable hash value. For example, changing a letter in an extortion message or a timestamp in a cryptocurrency transaction log would change the SHA-256 output completely. This shows how sensitive the algorithm is when checking the data integrity.

The mathematical validation is provided by the schedule to Section 63 of the BSA, which sets out a standard two-tier certification format. Part A is to be completed by the person legally responsible for the computer output-producing device or system, i.e., the investigating officer or system administrator. This section contains device details, normal operation, and host baseline hash value.

Part B includes certification by an independent technical expert to validate the technical environment, the tools used, and the integrity of the data extraction. This expert report describes the forensic toolchain, the scientific auditing process, and the expert validation. The parties will calculate and record the identical cryptographic hash value of the digital evidence using a hashing algorithm such as MD5, SHA-1, or SHA-256.

The two-tier certification process was challenged on its constitutional validity in *Pune Bar Association v. Union of India & Ors. (2026).* The petitioners argued that the requirement of both a Part A and a Part B certificate, along with the accompanying disclosure of the cryptographic hash, imposed an undue and impractical burden on litigants and state agencies.

The Supreme Court of India rejected the challenge to the statutory design of Section 63(4). The court observed that digital evidence is a special form of evidence that is especially vulnerable to tampering, deepfakes, cloning, and AI-assisted alterations. The integrity of digital evidence can be reasonably and necessarily secured by means of cryptographic validation, hashing, and expert supervision. The Court observed that the standard procedure to prove that a file has not been altered from the time it is seized to when it is presented before the Court cannot be legally guaranteed in the absence of the reliability of digital evidence.

Section 105 BNSS and the Mandate of Videography: e-Sakshya, Technical Hurdles, and Field Execution Realities

The legislative design of the BSA and the procedural mandates of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, are of high scientific standards, but their implementation is suffering due to an operational gap in the law enforcement agencies of India. The gap in operations is marked by serious deficiencies in specialized equipment, technical training, and forensic laboratory capacity in state police departments.

An example of this operational friction is the mandatory videography requirement under Section 105 of the BNSS. Section 105 stipulates that the entire process of conducting a search or seizure of any property, including the preparation and signing of the seizure memo by witnesses, shall be recorded through audio-video electronic means. Police are directed to use the e-Sakshya mobile application, a digital evidence management platform developed by the government, to record, timestamp, geotag, and upload the footage immediately to a centralized portal.

Furthermore, Section 193(2)(i) of the BNSS provides an important safeguard, requiring that the final police report must contain a detailed chronology of custody of any seized electronic devices. Every physical hand-to-hand transfer of the device from the time of seizure to the time of delivery at the forensic laboratory must be included in this chronology.

However, the mandatory deployment of e-Sakshya has faced serious real-life challenges. Officers frequently work in rural and semi-urban jurisdictions that may have poor network connectivity, low-light conditions, and adverse weather conditions. In case the raid is carried out in a remote area where the e-Sakshya app does not have connectivity to upload the recorded

file, the officers would have to save the raw footage locally on their personal smartphones. This breaks the chain of custody and makes data vulnerable to tampering.

Also, personal smartphones do not have write-blocking and secure storage architecture. This results in broken recordings when the batteries die or the storage space of the device runs out during the search. It also allows for background system processes to alter critical file metadata.

Systemic Bottlenecks: Laboratory Under-Resourcing, Staffing Deficits, and the Forensic Backlog Crisis

There are serious structural bottlenecks in the implementation of the BSA in the form of under-resourced forensic infrastructure and lack of professional technical training for investigating officers. The structural deficits are very strong at the level of state cyber cells and forensic labs.

State Forensic Laboratories' Capacity Less than thirty percent of the state forensic laboratories in India have the technical infrastructure required to perform the cryptographic hash-value verification required under Section 63 of the BSA. This is a major deviation from the desired benchmark of full capacity in all state and regional laboratories. The technical divide means backlogs in laboratories, stale evidence and long periods of pre-trial detention.

Less than fifteen percent of investigating officers have ever received any formal training in digital evidence handling, write-blocking, cryptographic hash verification or Section 63 certification procedures write, All investigating officers will be required to undergo forensic training under the BNSS and BSA. The training gap results in high rates of metadata corruption, improper device shutdowns and unsealed packaging in transit.

These under-resourcing challenges are further compounded by a severe FSL operational backlog where the average laboratory turnaround time ranges between eighteen to thirty-six months. This backlog persists despite the new legislation which mandates a forensic report within ninety days. This leads to delay in criminal proceedings and that is why over seventy six percent of Indian prisoners are undertrials.

Moreover, the national prison occupancy rate is over one hundred and thirty one percent, well above the goal of less than one hundred percent occupancy that is based on accelerated trial proceedings. Finally, the digital forensics market in India is expected to grow at a compound

annual growth rate of forty percent and reach close to twelve thousand crore rupees by the financial year 2029-30, but stark differences in funding between states threaten to create regional imbalances in the quality of justice delivered.

These infrastructure gaps frustrate the legislative intent of the BSA. The law requires scientific validation. The state's ability to provide this validation is limited." In investigations of cyber-syndicates, local police units often lack standard write-blockers or spot-forensic kits. Therefore, metadata is often corrupted by on-site unscientific data extraction performed by first responders.

The technical gap is also widened by slow laboratory turnaround times. If a device is placed in a chronically backlogged state FSL, it is stored for months at a time, during which time the defence may challenge its physical and logical integrity.

Tactical Vulnerabilities in Trial: Deconstructing the Chain of Custody and the Write-Blocker Paradox in Cross-Examination

The defence counsel will attack the operational and procedural errors during cross-examination at trial proceedings. When prosecuting a cryptographic network, or an encrypted communication platform, the case is often determined by the integrity of a copy or mirror image from a seized device. If the defence can demonstrate that the extraction process did not employ proper forensic safeguards, they could try to argue that the data was changed and is thus inadmissible under Section 63.

A major weakness exploited during cross examination is the lack of use of a hardware write-blocker during data acquisition. When you plug in a storage device (like a SATA hard disk, an NVMe SSD, or a USB flash drive) into a computer, the workstation operating system automatically starts background write operations. These automated processes index files, update access times, change registry hives, and modify system logs. This automatically alters the device's cryptographic hash value, meaning the hash calculated at the time of seizure will not be the same as the hash calculated during the forensic extraction process. In order to avoid such automated modifications a forensic examiner needs to use a hardware write-blocker. The write-blockers provide a controlled interface.

They intercept write commands from the workstation 's operating system, but allow read-only access to copy the data. Baseline integrity of evidence is lost if the investigating officer cannot

demonstrate that a certified hardware write-blocker was used during the extraction.The following transcript shows how defence counsel can systematically exploit these technical and procedural weaknesses during cross-examination:

Trial Court of Delhi: Cross-Examination of the Investigating Officer

Defense Counsel: Officer, in your deposition you said that on October 12, 2024, during the raid at the suspect's house, you copied the contents of the desktop computer that had the ledger of the alleged extortion syndicate. Is that right?

Investigating Officer: Yes. That's right. "I did a full forensic copy of the hard drive at the scene."

Defense Counsel: You took the suspect's hard drive and put it into your investigative laptop and made a copy of it. What is the physical connection between the two machines?

Investigator: I have taken the hard drive out of the suspect's desktop computer and connected it to a standard SATA to USB adapter and plugged it directly into the USB port of my investigative laptop. Afterwards I copied the files with standard copy software.

Defense Counsel: Officer, in the course of this process, did you use a hardware write-blocker between the suspect's hard drive and your investigative laptop?

Investigating Officer: "No, I did not have a hardware write blocker. But I was careful not to write to or alter any files on the suspect's drive.

Defence Counsel: Do you know that if a storage device is connected to a Windows or macOS workstation, the operating system will automatically do background write operations without any action on the user 's part?

Investigator: I don't know much about the automatic background processes of the OS. But I do know I did not copy any files manually to the suspect's drive.

Defense Counsel: Let's be clear on the technicality. Did you know that the OS on your laptop will automatically update access timestamps, modify file system allocation tables, index files for search, and modify registry entries on any drive you plug in?

Investigating Officer: I can't say that was done by the operating system.

Defense Counsel: So, during your extraction process, the suspect's drive was altered, if these system files and metadata were changed by the operating system? I am correct?

Investigating Officer: I don't think there was any big change.

Defense Counsel: A change is a big deal in digital forensics. Did you generate a crypto hash value of the drive before you inserted the suspect's hard drive into your laptop?

Investigator: No, we generated the hash value after the copy was completed and stored on our forensic drive.

Defense Attorney: That's a material omission, officer. You didn't generate a hash value before plugging in the drive. You did not use a hardware write blocker to prevent the drive from auto writing to the disk. And you can't mathematically prove that the contents of the drive did not change during your extraction. You agree?

Investigating Officer: That's our job.

Defense Counsel: Your SOPs did not prevent the metadata from being changed. Are you absolutely sure there was no data 'written to', or modified 'on', or deleted 'from' that hard drive while it was connected to your laptop?

The Investigating Officer: Nothing I wrote myself.

Defense Counsel: But you can't prove that your laptop didn't automatically alter the data on the drive. Also, you must keep a record of the chain of custody of this device as required by Section 193(2)(i) of the BNSS. Who physically had this hard disk from the time it was taken away from the desktop till the time it was handed over to the cyber cell?

Investigating Officer: I kept it overnight in the glove box of my personal vehicle and handed it over to the cyber cell the next afternoon.

Defense Counsel: Was the hard drive during this transit period maintained in an anti-static, sealed, cryptographically signed tamper-evident bag?

Investigating Officer: No, bubble wrap

Defense Counsel: So, no physical evidence, no cryptographic evidence that this drive wasn't accessed, wasn't connected, wasn't modified overnight. The chain of custody was not

maintained, a write-blocker was not used, and a baseline hash value was not obtained at the time of seizure. Officer I am telling you the digital ledger that you have presented before this honorable court is unauthenticated, corrupted and legally inadmissible under Section 63 of the BSA.

This line of questioning illustrates how the failure to meet technical standards can undermine the veracity of the prosecution's case. The baseline cryptographic hash must be taken at the point of immediate seizure or any subsequent cryptographic hash generated in the laboratory is legally meaningless. Without a baseline, there's no mathematical way to show that the data that was presented in court is the same data that was seized. Failure to preserve data integrity could lead to the dismissal of key evidence and the failure of the prosecution's case.

Judicial Post-Mortem: Analysing Systemic Failures in Landmark Indian Precedents

Some landmark judicial pronouncements in India reflect these procedural loopholes and technical glitches. In these cases, courts have been increasingly looking at digital evidence, and have pointed out the consequences of incomplete documentation and poor forensic practices. State of Kerala Versus XXXX [2023].

In the case of State of Kerala v. XXXX (2023) the prosecution had proved its case by way of video recordings stored on a memory card. However, during the trial, forensic analysis showed that the cryptographic hash value of the memory card had been altered multiple times while in the possession of the court and law enforcement. More specifically, the forensic report concluded that there were events of unauthorized access on January 9, 2018, December 13, 2018 and July 19, 2021.

The High Court of Kerala opined that the media had been tampered with in terms of its cryptographic fingerprint, which vitiates the integrity of the evidence. The court found that a change in the hash value of a storage medium while in official custody is evidence of possible tampering. The altered digital evidence, therefore, was not safe to rely on to sustain a conviction.

Shadab vs. State of U.P. (2024)

In Shadab v. State of U.P., 2025, forty stolen motorcycles were allegedly recovered in a police raid in which the applicant was arrested. The defence claimed that the recovery was fabricated

as the police did not conduct mandatory video graphing or prepare a digitized seizure list at the spot as required under Section 105 of the BNSS.

It was a serious procedural lapse and a showing of negligence on the part of the police to not undertake the mandatory audio-video recording under Section 105, the Allahabad High Court said. The Court observed that such omissions cast a doubt on the prosecution's narrative and may allow real offenders to get bail/acquittal due to avoidable procedural loopholes. The Court, accordingly, directed the Director General of Police, Uttar Pradesh to issue standard operating procedures for mandatory compliance of Section 105 through the e-Sakshya portal and granted bail to the accused.

Ravi Verma v. State of Uttar Pradesh (2025)

In Ravi Verma v. State of Uttar Pradesh (2025) prosecution failed due to incomplete digital documentation of seizure of narcotics. During the raid, officers used a personal unofficial smartphone to record the search instead of videography equipment. The phone ran out of storage halfway through the search so the second half of the operation was not documented. The Allahabad High Court has observed that partial video footage without verifiable metadata and continuous coverage is not admissible under Section 105 of the BNSS. The Court held that the digital recordings were incomplete and failed to satisfy the legal standard of an unbroken chain of custody resulting in the acquittal of the accused.

State v. Aadil Khan (2024)

However, unlike the failures in Ravi Verma, State v. Aadil Khan (2024) is a good example of the successful application of Section 105 of the BNSS. In this case the Delhi Police had used body worn cameras to record a raid which gave an uninterrupted and unedited footage of the entire search and seizure operation.

The defence claimed the police had planted evidence. The prosecution played the raw footage, keeping the metadata and timestamps in place and synchronized. The court accepted the digital record as reliable and admitted it under Section 105 of the BNSS and a conviction was secured within six months.

Arif Mollah vs Kolkata Police (2025)

Digital Evidence: Calcutta HC in Kolkata Police v. Arif Mollah (2025) deals with a technicality in digital evidence. The police were wearing body cameras recording the search in the arms raid, but the footage had no embedded timestamps. The defense argued the video is inadmissible on this ground.

The Calcutta high court accepted the footage as evidence applying the "best evidence" principle and said minor procedural lapses should not invalidate otherwise reliable and authenticated digital evidence. This move ensured a conviction in eight months and demonstrates that courts will not be deterred by minor technical lapses if the overall integrity of the evidence is established.

Reena Sharma v. State of Delhi (2023)

Reena Sharma v. State of Delhi (2023) The court debated the issue of mandatory videography versus individual privacy rights. Police recorded video of a home search and upset female family members, and a complaint of a privacy violation was filed.

The court chastised the officers and ordered a partial redaction of the video. The judgment emphasized the need to balance the transparency of investigation with the privacy rights guaranteed by the Constitution while using videography under Section 105 of the BNSS, and said sensitive or non-probative visuals should be masked.

Structural and Policy Recommendations for Forensic-Admissible Digital Prosecutions

These systemic vulnerabilities warrant targeted structural reforms in India's criminal justice system to meet the admissibility standards of the BSA for digital evidence.

Standardized Mobile Forensic Units (MFUs)

State governments should prioritise fully equipped Mobile Forensic Units in each district. These units should be mobile extensions of state FSL's, bringing advanced tools to the crime scene.

Each MFU shall include licensed hardware write blockers, anti-static Faraday bags for device isolation and forensic duplication software. First responders need training in how to quickly isolate devices that are seized from cellular and wireless networks to prevent remote data

erasure. Once a device is physically seized, it is RF shielded in a Faraday bag and then duplicated on-site using write blocking under this protocol.

Integration of Permissioned Blockchain Network

State judiciaries and police departments need to implement permissioned, decentralized blockchain networks to protect the chain of custody from physical and logical tampering. For a seized digital device, the cryptographic hash value of the device baseline should be calculated on-scene and immediately written to an immutable blockchain ledger. Such digital entry should include the geotagged location coordinates, a timestamp synchronized in time, and the digital signatures of the seizing officer and independent witnesses.

Blockchain logs are tamper-evident, meaning any unauthorized access or alteration while being transmitted or stored will generate a mismatched hash value, alerting the court to any potential tampering. It all starts with a device being seized, a hash being calculated and committed to a blockchain ledger with an immutable timestamp. Once the device is delivered to the forensic science laboratory, a final audit is conducted, where the court compares the current hash to the record on the blockchain.

“Preservation Blitz” Procedure Required

Because network logs, session tokens, and IP address translations are so volatile, police departments need a standardized “Preservation Blitz” protocol. The investigating officers should be trained to obtain log preservation orders from internet service providers, cellular companies and cloud hosts within 72 hours of registering a First Information Report (FIR). Indeed, empirical evidence suggests that obtaining these orders within three days translates into a 22-percentage-point increase in compliance and data recovery, thereby preventing essential network traces from being overwritten.

Standardized Judicial Training and FSL Accreditation Requirement

The state judicial academies are entrusted with the task of developing specific training modules on digital forensics and Section 63 certification to address the digital literacy gap in the judiciary. Forensic laboratories should also be required to obtain ISO/IEC 17025 accreditation,

so that their testing methods, equipment calibration and data handling procedures are in conformance with international scientific standards.

Thus, the Indian criminal justice system can bridge the divide between statutory standards and operational field realities, by adopting these structural and technical reforms. "Getting the data right at the time of seizure is critical to protecting the constitutional rights of the accused and to ensuring reliable convictions in cyber-syndicate prosecutions."

References

1. Advocatetanwar. (2024). Understanding Section 61 of the Bharatiya Sakshya Adhiniyam, 2023. Advocatetanwar.
2. Bar and Bench. (2026). State fully capable of tampering: Former CBI judge on entrusting electronic evidence custody with State. Bar and Bench News.
3. Chambers and Partners. (2026). Trends and developments in Indian financial crime and digital extortion. Chambers Practice Guides.
4. Chhattisgarh State Judicial Academy. (2024). Introduction and changes in the Bharatiya Sakshya Adhiniyam, 2023. CSJA.
5. CorpoTech Legal. (2024). Admissibility of electronic evidence under Section 63 of the BSA. CorpoTech Legal.
6. Cyint Technologies. (2023). Write blockers: Ensuring authenticity and data integrity in digital investigations. Cyint Blog.
7. Drishti Judiciary. (2025). Mandatory videography of search and seizure: Analysis of Shadab v. State of U.P. Drishti Judiciary.
8. Economic Times Government. (2026). Pune Bar Association case: How the Supreme Court redefined digital evidence authenticity in India. ET Government.
9. Eviden. (2024). Chain of custody: The importance of correct evidence collection for the litigation process. Digital Security Magazine.
10. FICCI & Khaitan & Co. (2026). Fraud in the digital age: Legal, compliance, and enforcement challenges. Khaitan & Co Publications.

11. Government of India. (2026a). Digital evidence, hash value, and the chain of custody: Police and court guidelines. S3WaaS.

12. Government of India. (2026b). Section 63 of the Bharatiya Sakshya Adhiniyam: Hash certificates and Part A/Part B formats. S3WaaS.

13. High Court of Delhi. (2024). Disclosure of documents and right to fair trial guidelines under the new criminal acts. Delhi Judiciary Practice Guidelines.

14. Indian Express. (2026). Mobile phone snatcher in Delhi held, tried, and convicted in just 12 days using e-Sakshya. Indian Express.

15. Indian Kanoon. (2023a). Section 61 in Bharatiya Sakshya Adhiniyam, 2023. Indian Kanoon.

16. Indian Kanoon. (2023b). Section 63 in Bharatiya Sakshya Adhiniyam, 2023. Indian Kanoon.

17. Indian Kanoon. (2023c). Section 57 in Bharatiya Sakshya Adhiniyam, 2023. Indian Kanoon.

18. Indian Kanoon. (2023d). Section 57 in Bharatiya Sakshya Adhiniyam, 2023. Indian Kanoon.

19. International Journal of Creative Research Thoughts (IJCRT). (2025). Role of mobile forensic units and digital evidence management in India. IJCRT.

20. International Journal of Innovative Research in Technology (IJIRT). (2024). Section 63 of the Bharatiya Sakshya Adhiniyam: Modernizing electronic evidence in India. IJIRT, 11(1).

21. International Journal of Innovative Research in Technology (IJIRT). (2025a). Capacity heterogeneity, tooling, and log preservation timelines in India. IJIRT.

22. International Journal of Innovative Research in Technology (IJIRT). (2025b). SOP maturity and cryptocurrency tracing success rates in cyber cells. IJIRT.

23. International Journal of International Relations and Law (IJIRL). (2025a). Videography in search and seizure under BNSS 2023: Method vs. implication. IJIRL.

24. International Journal of International Relations and Law (IJIRL). (2025b). Case examples and technical hurdles of search and seizure videography under BNSS. IJIRL.

25. International Journal of Law and Legal Research. (2024). Admissibility and procedure for digital evidence in court. IJLLR.

26. International Journal of Law Management & Humanities (IJLMH). (2023). Role of forensic evidence under BNSS 2023. IJLMH.

27. International Journal of Law Management & Humanities (IJLMH). (2026a). Procedural lapses in digital forensics under the BSA. IJLMH.

28. International Journal of Law Management & Humanities (IJLMH). (2026b). Procedural lapses, laboratory capacity, and training statistics in digital forensics. IJLMH.

29. Jharkhand Judicial Academy. (2025). Digital evidence handling, hashing, and chain of custody. Jharkhand Judicial Academy.

30. Journal of Advances and Scholarly Researches in Allied Education (JASRAE). (2024). Mapping the legal and forensic scaffolding in India's criminal justice system. JASRAE.

31. Kerala Police Department. (2021). Standard operating procedure on digital evidence. Kerala Police.

32. KPMG India. (2026). Next-gen forensics: The new age of fraud investigation. KPMG Forensic Publications.

33. LawSikho. (2024). Understanding BSA Section 63 and electronic evidence framework for criminal lawyers. LawSikho.

34. Laxhar. (2023a). Your emails, chats, CCTV footage, and digital data can now speak in court. Laxhar Legal Portal.

35. Laxhar. (2023b). Your emails, chats, CCTV footage, and digital data can now speak. Laxhar Legal Portal.

36. Lawyers Club India. (2023). Admissibility of electronic & digital record as evidence. Lawyers Club India.

37. Legistify. (2024). Section 65B and the framework under the BSA 2023 for enterprises. Legistify.

38. LiveLaw. (2024a). Recording of search and seizure in electronic mode: Section 105 BNSS. LiveLaw.

39. LiveLaw. (2024b). Importance of hash values in electronic evidence under the BSA. LiveLaw.

40. MSAB. (2026). The ultimate guide to digital forensics in 2026: Workflows, tools, and legal standards. MSAB Blog.

41. Mumbai Mirror. (2026). Lawyers locked out of e-Sakshya digital evidence portal. Mumbai Mirror News.

42. Naavi. (2023). Section 63 of the Bharatiya Sakshya Adhiniyam. Naavi.org.

43. National Law School of India University. (2026a). Trimming the edges, tearing the core: Electronic evidence and definitional tensions in Arjun Panditrao and the BSA. NLSIU Journal Blog.

44. National Law School of India University. (2026b). Definitional tensions in Arjun Panditrao and the BSA. NLSIU Journal Blog.

45. National Law School of India University. (2026c). Tensions with Arjun Panditrao under the BSA primary and secondary record framework. NLSIU Journal Blog.

46. Project 39A. (2023). Criminal law bills 2023 decoded: Audio-video recordings during investigation. Project 39A Blog.

47. Reddit r/digitalforensics. (2026). Kali Linux forensic mode admissibility without a hardware write blocker. Reddit.

48. ResearchGate. (2024). The enforcement and implications of the Bharatiya Sakshya Adhiniyam (BSA), 2023. International Journal of Novel Trends and Innovation, 25(10).

49. Scribd. (2023a). Admissibility of electronic records under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA). Scribd.

50. Scribd. (2023b). BNSS and forensic experts: The role of digital forensics. Scribd.

51. Scribd. (2023c). BSA evidence law: Overviews of electronic evidence and proper custody. Scribd.

52. Scribd. (2024a). Changes in the Bharatiya Sakshya Adhiniyam, 2023. Scribd.

53. Scribd. (2024b). Section 57 BSA: Primary evidence explained. Scribd.

54. Scribd. (2024c). Section 57 BSA: Primary evidence explained and case laws. Scribd.

55. Semantic Scholar. (2023). The Bharatiya Sakshya Adhiniyam, 2023 (BSA): A comprehensive update to the Indian Evidence Act. Semantic Scholar.

56. Sikkim Judicial Academy. (2023). Challenges in electronic evidence, encryption, and dark web tracking. Sikkim Judicial Academy.

57. Stellar Info. (2024). The critical role of write blockers in digital forensics acquisition. Stellar Knowledge Base.

58. Supreme Court of India. (2024a). Chain-of-custody of digital evidence and procedural guidelines. Supreme Court Practice Guides.

59. Supreme Court of India. (2024b). Hash-value integrity disputes and rules of practice. Supreme Court Practice Guides.

60. SupremeToday AI. (2024a). Key findings on memory card hash value integrity disputes in Indian courts. SupremeToday AI.

61. SupremeToday AI. (2024b). Importance of hash values in establishing electronic evidence integrity. SupremeToday AI.

62. TaxGuru. (2026a). SC upholds Section 63(4) hash requirement, ensures authenticity of electronic evidence. TaxGuru.

63. TaxGuru. (2026b). Key details of the Supreme Court judgment in Pune Bar Association v. Union of India. TaxGuru.

64. UNODC. (2024a). Handling of digital evidence in cybercrime investigations. UNODC Education for Justice.

65. UNODC. (2024b). Volatility, fragility, and protocols for handling digital evidence. UNODC Education for Justice.

66. Vidhi Judicial Academy. (2023a). Section 61 of the Bharatiya Sakshya Adhiniyam, 2023. Vidhi Judicial Academy.

67. Vidhi Judicial Academy. (2023b). Section 61 of the Bharatiya Sakshya Adhiniyam. Vidhi Judicial Academy.

68. Vivekananda Global University. (2026a). Department of Forensic Science curriculum and lab resources. VGU.

69. Vivekananda Global University. (2026b). Department of Forensic Science admission and resources. VGU Jaipur.