Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach--[Part-II]

Sanjay Rambhau Salkute

B.Sc.; LL.M.; M.B.A.; D.C.S.A.
Retired District Judge, Pune (Maharashtra), India

Abstract:

Section 65B of the Indian Evidence Act, 1872 did not require that a statutory certificate be issued by an expert. Although the provision was computer-centric and deals with electronic records, it was only required a certification by a person who was a responsible position in relation to the operation or management of the computer system. Now, the Bharatiya Sakshya Adhiniyam, 2023 updates Indian evidence law to address electronic and digital records in a technology-neutral manner. Section 63(4) prescribes a statutory method requires a dual certificate to be filed at each instance when an electronic record is submitted before the Court for admission. Under the Bharatiya Sakshya Adhiniyam, 2023, one of the statutory certificates must be issued by an expert, thereby expressly incorporated the expert's role through the Part-B certificate at the stage of submitting an electronic record for admission. Thus, when the original device is not produced before the Court, Section 63 shifts the compliance framework from a device-centric approach to a data-centric one, with the object of strengthening the authenticity, integrity, and reliability of the electronic record.

Under the Indian Evidence Act, 1872, when the original device was produced before the Court, a statutory certificate was not required. However, the party relying on the original device could seek the assistance of a technical expert to facilitate and demonstrate the device and its contents to the Court. The same principle will applicable under the Bharatiya Sakshya Adhiniyam, where no certificate is required, if the original device itself is produced before the Court

This is a preliminary paper for Law Students which examines Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam and shows that the scheme is not expert-centric in adjudication though role of expert is introduced under Part-B Certificate. It is studied that, the Court has a continuing duty to independently apply its judicial mind to ensure that electronic evidence is authentic, intact, relevant, reliable, and possesses sufficient probative value to support a judicial conclusion.

This study paper also examines basic provisions to explain important phrases in Section 63 and related provisions of the Bharatiya Sakshya Adhiniyam. The illustrations are only to aid understanding, and no empirical data has been relied upon, no forensic concepts are studied little concepts are discussed but

that may be suitable in certain circumstances. This paper is not an in-depth study of all issues. It examines only selected provisions of the Bharatiya Sakshya Adhiniyam, 2023 and does not cover all related laws. In this paper, section II from the main study paper, 'When Statutory certificate is not Required' is studied for more clarification in illustrations and note, and also illustration as to why trial court role is important as a guardian, but conclusion of the paper is same. The views are personal and generic.

Keywords: Section 63(4) BSA 2023, digital records, Hash value, Secure Hash Value, custody of electronic records, Expert opinion, statutory certificates, AI admissibility.

1. Introduction:

When an electronic or digital record is extracted or derived from an original device or source and submitted before the Court for admission, it is required to prove that the extracted electronic record comes from the original device/ source and that its integrity is the same as that of the original device or source. Under the Indian Evidence Act, 1872, electronic records were extracted or derived from an original device or source and when submitted before the Court, then it was required to be admitted in accordance with Sections 65A and 65B along with a mandatory statutory certificate. Such electronic records were treated as document and as secondary evidence. Under Sections 65A and 65B of the Indian Evidence Act, the mandatory statutory certificate was required to be issued by a person occupying a responsible position in relation to the operation of the computer, and not necessarily by an expert. The scheme of those provisions was entirely computer-centric. Then later judicial interpretation, the practice of mentioning mirror image, hash values of extracted electronic records were introduced to ensure integrity, and thereafter it was also clarified that the statutory certificate could be filed at a later stage.

The Bharatiya Sakshya Adhiniyam, 2023 updates Indian evidence law to deal with electronic and digital records in a technology-neutral manner. Under the BSA, electronic and digital records are treated as document and as primary evidence when they come from proper custody and are admitted through the statutory method. Section 63(4) makes it mandatory to file a dual statutory certificate at each instance when an electronic record is submitted before the Court for admission. One of the statutory certificates must be issued by an expert. The secure hash value of the electronic record must be mentioned in both certificates.

If the original device itself is produced before the Court, no dual statutory certificate is required, as the device itself constitutes the primary electronic record and there was no process of extraction or derivation involved. The party relying on the original device must still prove the provenance of the data, including its source and authenticity. Since this involves technical matters, the party may take the assistance of an expert, and not as a certifier.

Although the Bharatiya Sakshya Adhiniyam changes the procedural structure, it retains the basic legal principles and jurisprudence developed under Section 65B of the Indian Evidence Act.

In both situations, whether only the electronic record is produced or the original device itself is produced, the Court must ensure fairness to both parties and assess the relevance and evidentiary value

of the material. The Court must independently apply its judicial mind to determine the authenticity, integrity, reliability, and probative value of the evidence.

2. Study:

Definition: "Document": Under the Indian Evidence Act, 1872, "document" and "evidence" had separate definitions, and electronic records were not specifically included as "documents," but Section 65B(1) later added a non-obstante clause to address it.

The Bharatiya Sakshya Adhiniyam, 2023 removes this structural ambiguity by expressly defined "document" in Section 2(1)(d) to include electronic records and digital records. However, the BSA does not define "digital record." The term 'digital record' is introduced for the first time to cover information encoded in digital or binary form. Based on the definitions of "digital signature" and "digital audio" in the Information Technology Act, 2000, following illustrative examples are possible.

Illustration:

• **Electronic record:** A physical cheque that is scanned and stored in a computer system or server. The original paper document already existed, and it is converted into electronic form by scanning or imaging.

• **Digital record:** Data that is created and exists only in digital form, such as a truncated cheque generated directly through banking software, a database entry, or an invoice created and issued through an online accounting system. There is no original paper document. The record is digital from the moment of its creation.

Illustration:

• A paper document that is scanned and stored on a computer remains an electronic record, as it originates from a physical document.

• A spreadsheet, or dataset that is created directly on a computer and stored in binary or digital form is a digital record, as it is digital from its inception and has no physical original.

Illustration: A book or PDF downloaded from a private website or through a search engine such as Google. It does not carry any statutory presumption of authenticity under the Bharatiya Sakshya Adhiniyam, 2023. Such material is not a public document. It may be relied upon only if its source, authorship, integrity, and lawful acquisition are properly proved. If it is produced in printed form, it must satisfy the rules applicable to secondary evidence for paper documents. If it is produced as an electronic record, it must strictly comply with Sections 61 to 63 of the BSA, including statutory certifications and integrity requirements. In the absence of such proof, a downloaded PDF may not be relied upon to prove the truth of its contents [1].

Illustration: WhatsApp chats are born-digital electronic records, as they originate directly on a digital device and do not exist in any non-electronic form.

Primary Evidence: Under the Indian Evidence Act, 1872, primary evidence refers to the actual document itself produced for the Court's inspection, a concept originally based on physical documents.

The Bharatiya Sakshya Adhiniyam, 2023 expressly recognises electronic or digital records as primary evidence when produced under the Act, unless disputed. It includes multiple files created or stored together or in sequence, audio and video recordings, and electronic data stored, processed, or transmitted across multiple systems or locations, even in temporary or transient storage.

Secondary Evidence: Under the Indian Evidence Act, 1872, secondary evidence included certified copies, mechanically produced copies, copies compared with the original, counterparts of documents against non-executing parties, and oral accounts by someone who had seen the document. After Sections 65A and 65B were introduced, electronic records were treated as a special form of secondary evidence, admissible only if the mandatory certification requirements were met.

The Bharatiya Sakshya Adhiniyam, 2023 makes a big change because secondary evidence now only applies to paper or physical documents. Electronic or digital records needs follow the provisions of sections 61to 63 and it is primary evidence, only if they are lawfully extracted, their integrity is verified, and dual statutory certificates are submitted. The law also expands primary evidence to include digital copies, backups, cloud data, and replicated files, keeps secondary electronic evidence very limited, and makes Section 63 compliance is the only way to use electronic records that are now primary evidence [9] Anvar P.V.

Illustration: Where an electronic or digital record is produced in court in the form of a copy, printout, downloaded file, or an extracted file stored on a pen drive, hard disk, or other storage device, such production does not by itself make the record admissible. The statutory dual certificate under Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 is a mandatory pre-condition. Without this certificate, the court cannot treat the electronic record as primary evidence, irrespective of its relevance or contents.

Illustration: An Excel sheet printout is a computer output and merely a representation of underlying electronic data. Under the Bharatiya Sakshya Adhiniyam, 2023, electronic and digital records are not proved through the doctrine of secondary evidence. A printout does not automatically substitute the original electronic record. It becomes admissible only if it strictly complies with Section 63(4), including proof of authenticity, integrity, source, and statutory certification. In the absence of such compliance, the printout has no evidentiary value.

3.Admissibility of Court-Issued Electronic Judgments as Public Documents: An electronic copy of a court judgment downloaded from a court official website is admissible because it is a public document with statutory authenticity. Its admissibility comes from Section 61 of the BSA, with Section 79 creating a presumption of genuineness for judicial records. Moreover, as per sections 75 to 78 allow public documents and certified copies to be produced without formal proof. Therefore, official electronic judgments can be used in court without following the Section 63 certification rules [2][3].

4. Certified Copy of Electronic & Digital records / Exhibits by Court: Neither the Bharatiya Sakshya Adhiniyam, 2023 nor the criminal procedural manuals presently provide a clear statutory mechanism for the issuance of certified copies of exhibited electronic records by the court. This conceptual gap is studied [4] and highlights the need for specific procedural provisions, including the use of forensic safeguards such as write-blockers during supplying copy or certified copy, to ensure that court-issued

copies of electronic records preserve integrity and do not result in alteration or creation of a new electronic record.

Section-I: When dual certificate is Required:

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 introduces a dual certification system (Part A and Part B). The Bharatiya Sakshya Adhiniyam, 2023 modernises the law by treating electronic and digital records as documents and primary evidence, making it technology-neutral and future-proof. It requires dual certification for each instance when submitted, including a secure hash, and allows certifiers to be device custodians, responsible managers, technical experts. This shift from device-focused to data-focused rules improves the authenticity, integrity, and reliability of electronic evidence.

The admissibility the formula Under BSA:

Integrity = Hash Consistency + Forensic Extraction + proper Continuous Custody

Authenticity = Lawful Source + Identifiable Creator/System

Admissibility (BSA applicable) = Section 63(4) Certification + Relevance + Integrity + Authenticity + Proper Custody+ Fair Opportunity to Challenge.

5. Certificates with Secure Hash Value in Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023: Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023, along with the Schedule has prescribed the dual certificate format. Both certificates introduce the secure hash value as a statutory mechanism to ensure the integrity and authenticity of electronic and digital records. Part A statutory certificate deals with legal and procedural compliance, while Part B statutory certificate issued by expert deals with technical and integrity compliance, such as secure hashing and verification. The Schedule also specifies the specific algorithm for hash value to be used, while making the certification process, clear, reliable, and standardized.

Note: A hash value is a fixed-length alphanumeric string generated by applying a mathematical algorithm to data, which acts as a digital fingerprint of that data.

Note: A secure hash value is generated using a cryptographically secure hash algorithm (such as SHA-256 or SHA-512) that is resistant to collision, pre-image attacks, and tampering.

Note: For a forensic copy, the hash is essential and done in way (SHA-256, documented in Part-B certificate). It proves bit-by-bit accuracy of the copy.

Note: For a clone copy, the hash may match visible files, but hidden, deleted, or system-level data may be missing, so the hash does not guarantee full forensic integrity.

"Is a secure hash value, by itself, sufficient?": A secure hash value is a cryptographic fingerprint that uniquely represents the contents of a digital file at a specific time. If the secure hash calculated during extraction, matches the hash verified at a subsequent check, it shows that the data has not been altered. By requiring secure hash values in statutory certifications, the Bharatiya Sakshya Adhiniyam, 2023 goes beyond procedural formalities to provide a technological guarantee of data integrity, reducing disputes over tampering. This brings Indian law closer to international digital forensic standards and is especially

important for modern electronic evidence like cloud data, forensic images, blockchain records, and large digital datasets.

Under the Bharatiya Sakshya Adhiniyam, 2023, a secure hash value alone does not prove an electronic record's genuineness, authorship, or lawful origin. Hash value only shows that the data has not changed since the hash value was created. To ensure both integrity and authenticity, Section 63(4) and the Schedule require the secure hash as part of full certification. Part-A covers statutory and procedural details like identifying the record, describing its production, showing the source, and confirming integrity, while Part-B covers technical aspects, including generating and disclosing secure hash values using a prescribed algorithm. The Part-B expert creates the secure hash for each record, including files, audit logs, or other digital content. In short, a secure hash is not a "magic seal" of truth, it is just a timestamped snapshot of the data.

Secure Hash Value = Algorithm + Original Data + Single Point of Hashing.

· **Part-A Certificate** = Lawful Control + Identified Source + Mode of Production + Custody Declaration+ Secure Hash Value.

·**Part-B Certificate** expert = Forensic Method + secure Hash Generation + System Reliability + Technical Assurance

6. **Part-A: Role of the Person Issuing Statutory Certificate Under Schedule (section 63(4)) (To be filed by the Party to establish source, lawful control, regular use, and system integrity):**

1. **Source Authentication:** The certifying person confirms the identity of the source of the electronic or digital record. It may include a server, computer system, mobile device, CCTV system, email server, or cloud platform etc. The certificate also confirms that the data originated from a lawful and identifiable source.
2. **Regular Use and Lawful Control:** He affirms that the computer or communication device was regularly used in the ordinary course of activities during the relevant period. He also confirms that he had lawful control or responsibility over the operation or management of the device.
3. **System Functionality Assurance**: He confirms that the system was operating properly during the material period. Alternatively, he confirms that any malfunction did not affect the accuracy or integrity of the electronic or digital record.
4. **Data Input and Creation Confirmation:** He certifies that the information contained in the electronic or digital record was regularly fed into, created, stored, or processed by the system. This was done in the ordinary course of business or official activity.
5. **Source Hash Certification:** Where secure hash values are generated at the source, the person certifies, the hash value itself, the algorithm used [secure hash value], and the date and time of generation.

6. **Custody and Access Control:** He affirms that the data remained under controlled access. He identifies the authorized users. He confirms that no unauthorized access, alteration, or deletion occurred during the relevant period.
7. **Compliance with Statutory Conditions:** He certifies compliance with the conditions set out in Section 63 & Schedule Part-A of the BSA.

Expert-Part-B: Role of Expert in Establishing Electronic/Digital Record under BSA, 2023- (To be filled by the Expert): -

A] **Validation of Secure Hash Generation and Matching:** To certify that secure hash values were generated using a secure algorithm specified in the Schedule. He has to confirm that the source hash and extracted hash match exactly. If examined as a witness, he has to demonstrate the methodology of hash generation and verification. He must establish that the data has not been altered or changed.

B] **Assessment of Extraction Methodology:** He has to verify that extraction or copying was done in a forensic or read-only mode. To identify reliable tools or software used, including version details. To ensure that the process did not change, overwrite, or contaminate the original data.

C] **Technical Verification of System Integrity:** He has to evaluate whether the source system or device was functioning properly. To examine the operating system and application environment for stability. To assess whether any system anomalies could affect data accuracy.

D] **Interpretation of Logs, Metadata, and Audit Trails**: He has to examine access logs, timestamps, metadata, and audit trails. To confirm continuity of the data and detect gaps or anomalies. To certify that no unauthorized access or manipulation occurred.

E] **Chain of Custody Assurance:** He has to correlate timestamps, secure hash values, and storage details with custody records. To confirm that the electronic or digital record remained secure and unaltered from source to Court.

F] **Verification of Source Authenticity:** He has to confirm the origin of data, such as server, device, cloud account, or IoT device. To ensure that the record came from a lawful and identifiable source.

G] **Assessment of Data Completeness:** He has to ensure that all relevant segments, attachments, and components are included. To identify missing portions or gaps in logs, database snapshots, or cloud exports.

H] **Evaluation of Cloud and Remote Data:** He has to confirm lawful access to cloud-hosted or remotely stored data. To verify that extraction preserved integrity across distributed nodes. To identify multi-location or transient data and assess reliability.

I] **Blockchain and Distributed Ledger Verification:** He has to confirm integrity of blockchain transactions or smart contract records. If examined, he has to demonstrate transaction hash matching, block confirmations, and immutability.

J] **Verification of AI-Generated Records:** He has to identify the algorithm, model version, and input data. To certify that outputs correspond to the input and remain unaltered.

K] **Simulation or Reproduction of Data:** If examined as a witness, he has to reproduce processes such as call logs, software executions, or CCTV playback etc.

L] **Assessment of System Logs and Error Handling:** He has to examine system warnings, error logs, and alerts, to validate that the system operated properly during the relevant period.

M] **Identification of Anti-Tampering Measures**: He has to confirm whether encryption, digital signatures, or tamper-proof mechanisms were applied. If examined as a witness, he has to demonstrate effectiveness in preventing unauthorized alterations.

N] **Correlation Across Multiple Devices or Sources:** He has to correlate timestamps, secure hashes, and logs for distributed data (e.g. mobile, cloud, workstation). To establish continuity and a complete chain of integrity.

O] **Support to the Statutory Certificate:** He has to strengthen and corroborate the certificate issued by the responsible person Part-A. Especially important for complex cases like cloud data, blockchain, CCTV, large databases, AI outputs etc.

P] **Expert Reporting and Certification Best Practices:** He has to ensure the certificate is clear, detailed, and in the prescribed format. To record methods, tools, timestamps, and secure hash values for transparency and reproducibility.

R] **Witness:** If examined, he has to reply challenges during cross-examination regarding tampering, fabrication, or system reliability etc.

S] **Advisory Role for Court Strategy:** He has to advise on procedural options to preserve electronic record. He may provide guidance on lawful retention, sealing, and secure transmission of electronic records.

Note: Expert under Part-B of the Bharatiya Sakshya Adhiniyam is a person with technical expertise whose role is to ensure statutory compliance in relation to an electronic record and digital record. This certification operates only as a statutory and foundational precondition enabling the Court to consider the electronic record for admissibility. The expert may need to appear before court to give oral evidence on technical matters, whether data has been tampered with, fabrication, or system reliability and be cross-examined by opponent. AI might have been used in forensic testing only to help experts in their forensic work /tool but it should not be to used replace human experts or their opinion.

Note: The list of above roles is indicative due to continuous changes in technology therefore as illustrative above points are stated, and is not intended to be exhaustive because sometimes it may be necessary to demonstrate how record was generated in the system. **Ex.** In cases of truncated cheques, [as per illustration] it may be required to explain whether the inputs used in the truncation process was sufficient to ensure that the final output is accurate and valid. It must also be shown that the process was properly validated and applied in the same manner as in other similar cases. **Ex.** In computer generated system, the expert must identify the system that generated the data, explain how the process normally operates, and show that the system was functioning properly at the relevant time. He should demonstrate

that the data was produced automatically in the ordinary course of operation, without manual interference, and that appropriate safeguards existed to prevent alteration. The expert must also explain how the record was stored, retrieved, and preserved, and confirm the continuity of the data through a proper chain of custody.

Note: At present, there is no specific judicial precedent dealing directly with AI and the role of experts, [15] Selvi v. State of Karnataka is relevant for guidance. In that case, the Hon'ble Supreme Court discussed that ''scientific techniques cannot bypass constitutional safeguards, procedural legitimacy and voluntariness are essential and courts cannot treat scientific methods as inherently reliable''. Applying this principle to AI-generated records, it becomes necessary for the expert to explain not only the output but also the logic behind it. The expert may also require to act as a "translator" of the AI system by disclosing how the algorithm works, how the data was processed, and what safeguards were in place. This may include explaining the algorithm used, multi-file or cross-source and artifact analysis, human verification steps, and known error rates. To ensure fairness and effective defence, the party relying on AI-generated evidence may require (where feasible) to provide the opposing party with access to the forensic image of the data and disclose the specific version of the AI software used. The Court may assess algorithmic transparency ("why"), data integrity and processing method ("how"), system reliability, and compliance with procedural safeguards before relying on such evidence.

Note: Section 63 of the Bharatiya Sakshya Adhiniyam does not expressly distinguish between electronic records created by humans and those generated by artificial intelligence. However, keeping view and object of the Act, it becomes the expert's task to explain not only 'what the content is', but also 'how it was created'. This includes examining the source and origin of the record, the process of its creation, and the chain of custody. The expert should demonstrate source integrity, explain the creation path of the data, and verify whether safeguards such as cryptographic signatures, blockchain-based timestamps, or immutable audit trails were used. The expert must also cross-check the record with independent logs or external records to confirm that it is genuine and was actually generated or sent by a real system or person. Technical verification may include detecting visual, audio, or textual anomalies, checking metadata for a complete provenance trail, assessing system reliability such as validation methods, error rates, and possible bias, and corroborating the record with other independent sources. In short, the expert's role is to assist the Court in assessing authenticity and reliability through a multi-layered verification process.

Thus, Secure hash proves that the data is the same, certificate proves its source and custody proves trustworthiness.

Sr No	Legal Test for Admissibility	Established	Effect
1	Integrity	Data was not altered.	Yes
2	Authenticity	The source was genuine.	Yes
3	Custody	Lawfully handled.	Yes

4	Admissibility	All above (1 to 3) Satisfied?	Allowed for Admissible Record.

Illustrations: When data is extracted from a mobile handset onto a pen drive, each category of data, such as audio files, application data, system logs, metadata, and other forensic artefacts, constitutes a separate electronic record. For forensic reliability, a secure hash value must first be generated for each item of data on the original mobile handset. The same data, after extraction onto the pen drive, must then be re-hashed and the hash values compared to verify that the data has not been altered during extraction.

In addition, the pen drive as a storage medium must be treated separately. Before extraction, the blank pen drive should be hashed to establish its clean state. After completion of extraction from mobile handset, the pen drive must again be hashed to generate a final hash value. Verification of these hash values of the pen drive ensures that the complete collection of extracted records stored on the pen drive remains intact and untampered after extraction [5].

Note: The above procedures and illustration on secure hash generation, file-level and container-level hashing, extraction methods, and forensic steps are illustrative and not exhaustive. They explain the principles of integrity, authenticity, and reliability of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023. As technology evolves, extraction methods, datasets, logging, and hashing practices may change. Therefore, the required technical steps will depend on the specific system or digital environment, and must be evaluated according to applicable technological standards, accepted forensic practices, and the facts of the case.

7. Hash value of Source/ Device: The Hon'ble Supreme Court has consistently held that the general rules on secondary evidence under Sections 63 and 65 of the Indian Evidence Act, 1872 do not apply to electronic records. In ordinary cases, secondary evidence is allowed only when the original (primary evidence) once existed but cannot be produced for valid legal reasons. However, electronic evidence is different. Its admissibility and proof were governed only by Section 65-B, which is a special and self-contained provision. This means that electronic records could be proved only in the manner prescribed under Section 65B, and not by using the general rules of secondary evidence.

As per BSA, if the secure hash value of the extracted data does not match the hash value of the original source, it means the data has changed during extraction. This creates a clear presumption that the integrity of the data is lost. Such a mismatch shows that the extracted record is not an exact copy of the original and therefore does not meet the legal requirement of integrity under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. As a result, the extracted electronic record cannot be treated as primary evidence. When the extracted record is not faithful, the legal conditions for admitting electronic evidence are not satisfied, and the Court cannot overlook or cure this defect by treating the material as supporting or corroborative evidence. A secure hash mismatch therefore undermines the very foundation of the electronic evidence, because it fails to prove that the electronic record submitted in Court is the same as the data that existed at the original source.

Illustration: If a pen drive has a forensic image with a secure hash, that hash proves the image hasn't changed since creation, and the opponent may verify this by recalculating and comparing the hash, even without the original device. But the opponent may verify the original data's integrity only if records show the hash was made during acquisition and used to create the forensic image, typically via extraction reports, logs, timestamps, and custody records; if the image was copied read-only from the device, it can be considered reliable. If acquisition logs are missing, incomplete, or show hashing done after processing, the forensic image only proves integrity from that point onward, not of the original device, and gaps or inconsistencies may show a broken chain of integrity. Even if a forensic copy is given, the opponent can check it only on the basis of the materials supplied by the relying party, and if there is no clear proof of how the data was taken from the original device, the risk of unreliability remains with the party relying on the electronic record.

8.Preservation of the Original Source: The BSA 2023 does not set a fixed time for keeping electronic records by the parties. Section 93 specifically deals with preserving electronic signature data. For all other electronic records, once a party wants to rely on them, they must preserve the original device, system, or account in its original state for the duration of the case, as far as reasonably possible. This duty comes from the need to prove authenticity and integrity, and to let the court and the opposing side examine the record, metadata, hash values, and chain of custody. But if the original record is lost may be due to delays in trial, technology changes, deleted cloud data, or lost devices, the party relying on it bears the risk. Therefore, the party must act reasonably and in good faith, inform the court and opposing side if preservation becomes impossible with its explanation. It is studied that, the best practical way to preserve an electronic record is to make a forensic copy with a verified secure hash, a proper chain of custody, and expert certification. This creates a reliable copy of the original, though it may still be examined and challenged in court.

9.Minor Procedural Defects: Judicial precedents clarify that under the BNSS, 2023 and the Civil Procedure Code, only minor procedural defects in a statutory certificate may be corrected. It is only if the original electronic record has been properly preserved, remains intact, and is available for forensic verification.

Note: Minor procedural defects relate to format of certificate , description, or clerical clarity only. But the integrity defects relate to the integrity data itself and are incurable under the BSA.

Illustrations: For WhatsApp messaging record: (1) The certificate omits the IMEI Number but the handset is produced and may be verified. (2) In the certificate the secure hash value is stated but the algorithm (e.g.SHA-256) was not mentioned. (3) The date or time of extraction is incomplete but system logs confirm it. (4) The chat export file name is wrongly described but the hash matches the produced file. (5) In the certificate only mentioned, 'WhatsApp chats but Chat ID and phone numbers are clarified through the same device/ handset.

Illustrations: For e-mail record: (1) The certificate does not mention mail server name but the header and server logs are intact. (2) The sender / recipient domain is misstated but message headers conclusively identify it. (3) The mailbox export format (.pst/.mbox) is not specified but the hash and contents match. (4) The time zone used in timestamp is not stated, but metadata clarifies it.(5) The

certificate refers to ‘email record’ instead of ‘email with header and attachments but the complete file is produced.

Illustrations: For CCTV / Audio-Video record: (1) The camera location is described improperly but it may be clarified through site inspection documents. (2) The DVR Model number is omitted but the DVR/ Medium (original) is produced and examined. (3) The clip duration is misstated but the secure hash matches the admitted clip. (4) The export software version is not mentioned but DVR logs confirmed standard export. (5) The certificate mentions ‘video file’ without naming codec but later clarified by expert testimony.

10.Stage of filing dual certificates: In Arjun Khotkar case [12], Hon’ble the Supreme Court clarified that, the statute does not prescribe the exact stage at which the certificate must be filed, but it must accompany the electronic record when the record is produced in evidence. It was also pleased to observe that the Court may exercise discretion to permit production of a belated certificate at the trial if the hearing is not yet over and doing so will not cause prejudice to the accused.

The above flexibility was recognised to avoid procedural rigidity, particularly in criminal trials where fairness to the accused is paramount. The discretionary power arises from the Court’s duty to balance statutory compliance with fairness. A certificate may be produced later in the trial provided the electronic record remains the same and no serious prejudice is caused. In short, Arjun Khotkar [12] permits the late filing of the certificate at any stage of the trial to cure a procedural defect. The above situation was concluded for filing statutory certificate and not for filing electronic record. In that case the Election Commission produced the video recordings (CDs/VCDs) following a court order. Despite multiple requests from the petitioner and orders from the High Court, the Election Commission and the Returning Officer failed to provide the Section 65B certificate The Hon’ble Bombay High Court admitted the videos anyway, observed that, there was "substantial compliance" because the Returning Officer gave oral evidence confirming the videos were authentic. The Hon’ble Supreme court observed that oral evidence cannot replace the written certificate. The certificate is a sine qua non (absolute essential). ‘Lex Non Cogit Ad Impossibilia’- the petitioner tried everything to get the certificate and the authorities refused, the Court held the party should not be punished for something impossible to perform. Therefore, the Hon’ble Court held that a Judge can direct the production of the certificate at any stage of the trial before the hearing is over.

Under the new BSA statutory regime, the text of Section 63(4) states, “a certificate shall be submitted along with the electronic record at each instance where it is being submitted for admission…” meaning the certificate must accompany the electronic record every time it is produced for admissibility. The three elements. ‘Shall’, ‘along with’, ‘at each instance’ is a material phrase.

This language.’ at each instance’ in BSA is stricter and more exact than Section 65B of the IEA. The use of “each instance” means that every time an electronic record is submitted for admission. The statutory wording prevents strategic delay or piecemeal certification. It strengthens transparency at each stage of evidence production for admission. The use of the word ‘shall’ is mandatory and not directory, because the provision deals with admissibility and is meant to ensure procedural fairness, transparency, and proper judicial scrutiny at the time when the electronic or digital evidence is produced at each instance.

In short Arjun Khotkar [12] relied on the absence of specific timing language in Section 65B to permit flexibility. Section 63(4) removes that gap by explicitly mandating "at each instance'' and adopted the jurisprudence from Arjun Khotkar. It clearly demonstrates that, electronic record with secured hash value needs to be filed, while filing the document. The certificates can be filed at the time of admissibility.

Note: Electronic record with secure hash value filing is transparency (let the other side to know what relying party have and to prepare for defence by opponent). But Admission is about integrity (proving the document hasn't been tampered with). The Section 63 (4) Certificate is the "gate pass" required to cross the gate from filing to admission.

11.Repeal & Saving Under BSA: When the Bharatiya Sakshya Adhiniyam, 2023 came into force on 1 July 2024, Section 170 provides that cases already started before that date will follow the Indian Evidence Act, 1872, while cases instituted on or after that date must follow the BSA's evidentiary rules.

12.Death or Unavailability of Certificate Issuer under BSA, 2023: Under Section 32 of the Indian Evidence Act, 1872, statements by persons who are dead or unavailable can be admissible in certain cases.

Under Section 26(b) the Bharatiya Sakshya Adhiniyam, 2023, if the Part-A person who issued certificate is deceased, the record may still be admitted as primary evidence, if its integrity is verified by other means. This can include checking the secure hash values or testimony from someone familiar with the deceased's signature or management of the relevant activities.

For Part-B certificates, the certificate remains a relevant fact even if the expert is deceased. Another competent expert may testify to supplement examination in chief and cross-examination. This Expert may confirm that the procedures in the certificate Part-B were standard. He may also verify that the secure hash value in the certificate Part-B matches the current secure hash of the electronic record. He may confirm that the certificate part-B is technically sound on the basis of records preserved by the deceased expert. It may include the identification of the deceased expert (person's) signature or handwriting may support admissibility.

13.Exhibiting Electronic Evidence under the BSA, 2023:

Points for prima facie admission u/s 63 (4) of record:

1. **Lawful Control:** The Court checks lawful control by checking whether the certifying person had legal authority and access to the device or system at the relevant time.
2. **Source of the Record:** The Court verifies the source by identifying the specific device, server, or account from which the electronic record originated.
3. **Production of the Record:** The Court assesses production as to how the record was obtained, preserved, and submitted before the Court without alteration.

4. **Integrity of the Record:** The Court checks the integrity of a record by verifying its secure hash value, which shows that the record has not been changed from the source to when it is submitted.
5. **Authenticity and Technical Reliability:** The Court checks whether a record is authentic and reliable by looking at system working, metadata, logs, and experts to make sure there was no tampering or malfunction.

Note: The list of above points is indicative and illustrative, and is not intended to be exhaustive.

Under Section 63(4) of the BSA, if an electronic or digital record does not meet the statutory requirements, the Court cannot treat it as primary evidence, if it is disputed. The Court cannot postpone the admissibility decision merely on allowing identification number to the electronic record. The purpose of the BSA is to exclude doubtful or unreliable electronic evidence at the threshold, and it does not permit liberal view while admission of non-compliant electronic records.

The Court evaluates the electronic record using the following parameters: -

- **Existence of Electronic/Digital Record:** Whether a specific electronic or digital record exists on a device, server, system, or storage environment as a factual assertion under Section 57.
- **Lawful Source and Control:** Whether the record originates from a lawful, identifiable, and explained source, and whether the producing party had lawful access and control over the system or data.
- **Proper Custody:** Whether the electronic record was produced from proper custody, including continuity of possession, secure storage, and absence of unauthorized access.
- **Statutory Mode of Proof:** Whether the electronic record is accompanied by a valid Section 63(4) statutory certificates, in the prescribed form, at the time it is tendered for admission.
- **Completeness of Certification:** Whether all mandatory particulars are disclosed, including device/system description, method of extraction, date and time, hash value, and identity of the certifying persons.
- **Source Authenticity:** Whether the electronic record is shown to be what it claims to be, by linking it to its original device, account, application, or system through metadata, logs, and testimony.
- **Technical Integrity:** Whether the data has remained unchanged from creation or extraction to production, verified through secure hash values, forensic methods, and uninterrupted chain of custody.
- **Reliability of System and Process:** Whether the system, software, or automated process that generated, stored, or extracted the record was functioning properly at the relevant time.
- **Forensic Soundness of Extraction:** Whether copying or extraction was conducted in a read-only or forensic manner, using reliable tools, without overwriting or contaminating the original data.

- **Expert Authentication:** Whether technical aspects beyond ordinary understanding are supported by Expert or testimony, particularly for cloud data, CCTV, blockchain, large databases, or AI-generated records.
- **Chain of Custody Continuity:** Whether timestamps, storage details, secure hash values, and custody records together demonstrate uninterrupted preservation from source to Court.

Note: The above points are indicative, and are not intended to be exhaustive. Mere exhibiting a document does not make it admissible. It is admissible only if the law allows it and it is free from statutory bars.

Note: Due to continuous change in technology, it is necessary to consider the types of digital forensic evidence as per the technology at the relevant time.

14.Inspection of record by opponent, under BSA, 2023: If an opponent wants to inspect an electronic record before the witness is examined, the Court may allow it under controlled supervision to ensure integrity and prevent tampering, subject to privacy issues. The Court should especially help laypersons who are unfamiliar with electronic records. This inspection promotes transparency and lets the Court assess authenticity, integrity, and reliability before admitting the record as primary evidence.

15.Objection by Opponent and Filing Expert Opinion: As noted in Arjun Khotkar [12] (para 54), the Hon'ble Supreme court observed that, 'if the accused seeks to produce a certificate as part of their defence, the Court must exercise its discretion in accordance with law and fairness.'

The opponent may challenge a produced electronic record, both statutory certificates, metadata, or any visible inconsistencies without filing their own expert report, simply by highlighting non-compliance, gaps, or procedural defects.

The opponent may submit an expert opinion to point out technical issues, reliability concerns, or non-compliance with statutory requirements, helping the Court decide whether the electronic record meets the BSA standards of authenticity, integrity, and admissibility. However, since the opponent's expert does not have direct access to the original device, system, server, or storage media, they may not perform independent forensic verification. Their opinion is based mainly on the supplied electronic record, dual statutory certificates, and outputs, and may highlight internal inconsistencies or gaps in methodology.

Form-B Expert	**Expert Opinion**
Certifies statutory requirements and facts of compliance.	Provides assisting (opinion) on the basis of supplied material.
Does not give any opinion in the certificate.	Gives a reasoned expert opinion.

If examined, in evidence he may prove how the electronic or digital record was created, extracted, preserved, and verified etc.	Opinion helps the Court understand, analyse, or evaluate the record. If examined, in evidence the expert may demonstrate his opinion and its grounds.
Mandatory condition for admissibility.	Not mandatory.
Cannot be replaced by any other expert opinion.	Cannot cure absence of statutory certificate.

Note: Expert's Opinion is an expert forming a technical opinion may or may not examine the original device or system. But he draws conclusions and inferences from technical material produced on record. He must evaluate the material, give opinion, its reasoning, process and grounds for opinion. He places his conclusions before the Court. Such opinion is purely advisory and persuasive.

16. Appoint neutral examiner Under section 93(2) of BSA: In cases where the party relying on an electronic record has examined the expert Part-B and the opposing party has examined its own expert, and from their evidence, if court think that, a technical conflict persists that goes to the root of the record's integrity, authenticity, or reliability then the Court may appoint a neutral Examiner of Electronic Evidence under Section 39(2) BSA. The role of the neutral examiner is limited to assisting the Court in evaluating the reliability, integrity, and probative value of an otherwise statutorily compliant electronic record. Such an appointment cannot cure any absence or defect in mandatory certification under Section 63(4), nor can it be used to bypass statutory conditions of admissibility or to fill up lacuna in any process. It is useful in exceptional circumstances.

Illustration: In a criminal case, the accused is alleged to have sent incriminating emails from a particular computer. The prosecution provides a forensic copy of the hard drive, but there are conflicting claims about whether the emails were deleted or altered. The Court may seek the opinion of a neutral examiner to check the forensic copy, metadata, and logs. The neutral examiner reports that the hash values match, the emails were not altered, and the timeline of creation is consistent. The Court may then use this opinion to form its own conclusion about the authenticity and reliability of the emails but the Court itself will decide whether to accept the emails as evidence.

Note: The electronic record must stand or fall on the evidence led by the parties. In no circumstance, the Judge decides the case, step into the role of an expert and determine issues of authenticity, integrity, or technical correctness based on personal or his own assumed technical knowledge. The electronic record and digital record must be proved by statutory compliance and expert evidence, or it fails.

Note: If a party could have produced an expert but did not do so, the court should not normally appoint neutral examiner to help that party. Here, the court's power to appoint a neutral examiner is meant to assist the court in understanding the evidence. It is not meant to cure a party's failure to prove its case. It cannot be used to dilute or bypass statutory requirements. In this process, both parties have the right to cross-examine the court-appointed expert under Section 39(2).

Suo motu appointment under Section 39(2): If the Court needs expert technical insight on electronic evidence, the opinion of such a neutral examiner is treated as relevant evidence for the purpose of Court's own opinion forming process. It does not mean the neutral examiner decides anything. The examiner's role is purely advisory. The Court still forms its own assessment.

Illustration (Telecom Records): If an accused cannot get electronic records or certificates from a telecom company, the Court may lawfully summon those records from the company's nodal officer under statutory powers, and the company must then produce them with proper certification. When a telecom company produces records under court summons, it acts as a statutory custodian-witness issuing certificates, not as a neutral examiner under Section 39(2) BSA.

Illustration: In a civil suit for breach of contract, the plaintiff relies on emails and server log files stored on a cloud platform to prove timely performance of the contract. The defendant does not admit these electronic records. He states that he does not have technical knowledge or independent access to the plaintiff's cloud system to verify the data. The defendant applies to the Court seeking inspection of the electronic records and access to relevant technical details, so that he may prepare his defence. The Court allows limited inspection and statutory certificates produced by the plaintiff but, due to practical constraints relating to cloud servers, third-party control, and data confidentiality, does not permit direct access to the live cloud system. While examining the record, the Court notices that the electronic data originates from cloud servers located outside India, that the log files are automatically generated across multiple servers, and that the material on record does not clearly explain the process of creation, storage, and preservation of the data. Even though the defendant has not filed an expert objection and no direct technical dispute is raised, the Court finds that it cannot confidently assess the technical reliability of the electronic evidence on its own. Therefore, acting suo motu under Section 39(2) of the Bharatiya Sakshya Adhiniyam, 2023, the Court may seek the opinion of a neutral technical examiner to explain how the cloud system generates and stores logs, whether the timestamps and metadata are system-reliable, and whether the data could have been altered during syncing or storage. The neutral examiner submits a technical opinion explaining the system process and integrity safeguards. The Court uses this opinion only to assist itself in forming its own judicial conclusion on the authenticity and reliability of the emails and log files. But the burden of proof remains on the plaintiff, and the examiner's opinion does not cure any statutory non-compliance or replace the evidence that the parties are required to produce. Because Section 136 BSA limits compulsory access to third-party electronic systems, a neutral examiner usually works only with the records produced in court, and the Court treats the opinion as assistance, not as proof.

Note: The neutral Examiner's role under Section 39(2) of the Bharatiya Sakshya Adhiniyam, 2023 is to assist the Court in assessing the reliability and probative value of an electronic or digital record, after statutory admissibility under Section 63(4) is addressed. In this process, both parties have the right to cross-examine the court-appointed expert under Section 39(2).

Section-II: When Statutory certificate is not Required:

17. Under the Bharatiya Sakshya Adhiniyam, 2023, statutory certification under Section 63(4) (Part-A and Part-B) is required where the relies is on an extracted, copied, or otherwise derived electronic record. But when the original device itself is produced before the Court and the electronic record is relied upon in its native form then such statutory certification is not mandatory as a condition of admissibility. In such cases, the burden of proving authenticity, integrity, and reliability rests entirely on the party relying on the electronic record of the device and must be discharged through procedural transparency and adversarial testing rather than statutory certification. This includes proving lawful control, regular use, system functionality, data creation, access control, metadata, logs, chain of custody, and absence of tampering. Where necessary, technical aspects may be explained through expert. The expert may assist and helps the court to show / demonstrate the data that is already physically present in the device.

To give a fair opportunity to the opposing party, the person relying on the original device must allow inspection of the device and relevant technical details such as file properties, timestamps, metadata, logs, and system information. The opponent must be permitted to examine the device or seek forensic access under court supervision. Any secure hash values relied upon should be disclosed in advance, or generated in court, to ensure transparency and also supply copies of relying documents.

If the relying party, has examined expert who assisted, the opponent must equally have the opportunity to cross-examine. In such cases, production of the original device may satisfy admissibility under Section 57, but the authenticity, integrity, and reliability of the contents in it must still be proved through witness testimony. Being a witness, the expert has to reply challenges during cross-examination regarding tampering, fabrication, or system reliability, if challenged. The opponent has opportunity to file his expert's opinion. The court may also appoint neutral examiner. Both parties have the right to cross-examine the court-appointed expert under Section 39(2).

Note: Expert's Assistance means**,** when an original electronic device or system is produced before the Court, the role of the expert is also to help the Court understand the electronic and digital evidence. His assistance is facilitative, explanatory. The expert shows the technical route to the data. The expert explains technical facts. He explains the process and pathway through which the electronic and digital evidence appears before the Court, but he may give any opinion on the meaning, intention, truth, or legal effect of the data when examined. His assistance helps the Court understand whether the digital environment appears intact (environmental integrity), how metadata reflects creation, access, or modification of data (metadata navigation), and how hardware and software work together to store and display information (hardware–software interaction). He proved the device was not tampered with (Integrity) and shows the data it held (Fact). In the oral testimony he has to prove all facts.

Note: The authenticity of the device and the authenticity of the contents stored in the device are two distinct concepts, and both must be proved. Authenticity of the device means proving that the device produced before the Court is genuine, properly identified, and is the same device from which the electronic data is claimed. Authenticity of the contents means proving that the data stored in the device is genuine and originates from the stated source. Admissibility depends on compliance and fair procedure, including opportunity for the opposing party to inspect, challenge, and test the evidence. Proving the

device alone does not automatically prove the contents, and proving contents without ensuring integrity and reliability does not make the evidence admissible.

Note: Under section 57 speaks that the document itself produced for the inspection of the court. Section 61 speaks word, 'Notwithstanding. In the case of Arjun Khotkar at paragraph72(b) the position of production of original device is discussed,'' (b) The clarification referred to above is that the required certificate under Section 65 B (4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him.''. e.g. physical devices with direct storage (mobile phones, laptops, cameras, USB drives) where data can be directly inspected without extraction or format conversion. e.g. Accused's personal mobile phone handset, Witness's laptop, Photographer's camera memory card, USB drive seized from crime scene.

Illustration: If police seized a mobile phone handset from the accused as per section 105,106,185 of BNSS 2023. The section 176(3) BNSS enables forensic examination of evidence, including collection where necessary, but does not make the forensic expert's presence at the time of seizure. The expert can examine evidence later, including collecting data from already-seized devices. The forensic expert who will present data, is not a statutory expert and he will give his opinion for the contents in the seized mobile phone because expert might have performed the extraction (technical process), verified device working properly etc and provided secured hash values. His expert opinion is supportive, not foundational. The investigating officer needs to prove chain of custody since seizure to till production before court. The investigating officer may present data, but he does not become an expert unless he is independently qualified and examined as one.

Note: In the case of Arjun Khotkar at paragraph72(b) further observed that, 'In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B (4). ''. e.g. virtual environments, cloud infrastructure, distributed storage systems, or multi-tier architectures etc. It is clear that, now under BSA the dual certificate is required.

Illustration: If accused was using a big server system that cannot be moved / produced before the court, OR, when Data/Contents from Seized Mobile was extracted by FSL or Expert. In the case of State of Karnataka v. T. Naseer @Nasir @Thandiantavida Naseer @Umarhazi @Hazi & Ors. [17], It only mentions that a certificate under Section 65-B of the Act as per Indian Evidence Act. The judgment T. Naseer @Nasir, does not clearly specify whether both Part-A and Part-B are required or who issues them because it was based on 65-B. But now, according to BSA 2023, the certificate 65-B already covered details (Part-A type requirements) and expert verification (Part-B requirements) will be covered by expert, if expert extracted the data, then he will have to issue certificate Part-A and Part-B [functional requirements only in two separate formats]. However, the Investigating officer needs to prove chain of custody since seizure to till production before court. The investigating officer may extract data, certify facts, and also prove custody, but he does not become an expert unless he is independently qualified and examined as one.

Note: The concept functional requirements only in two separate formats [i.e. combine certificate for both parts] may be developed in future by jurisprudence.

Note: Secure hashing proves integrity only if the original evidence was preserved in a forensically sound manner before hashing. In reality, handling modern devices is much more complicated. Unlike a paper notebook, a computer or phone is "live" and reacts when you touch it. Even the process of creating a secure hash value can be risky. If an investigating officer runs hashing software directly on the seized device without safeguards, the system may update logs or timestamps in the background. That means the very act of checking integrity could unintentionally change the evidence. To avoid this, investigating officers use special forensic tools such as write-blockers, which allow them to take a secure hash value without altering the original device. But this isn't something an ordinary officer can do casually. It requires special knowledge and training. Investigators must understand not only what a write-blocker is, but also how to use it correctly, along with other forensic methods. Without that expertise, even the act of secure hashing can unintentionally change the evidence.

Therefore, if the investigating officer does not have the necessary technical knowledge, the correct procedure is to seize the device and send it to a forensic laboratory. The forensic experts, who are trained to use specialized tools and methods, will then create the secure hash value and preserve the evidence properly. But, if the device is connected with a virtual machine, cloud service, or remote environment, mere seizure of the physical device is not sufficient. In such cases, the investigating officer must ensure that the virtual environment and its data are preserved, which requires the presence of forensic experts at the time of seizure. Only by preserving both the local device and the virtual/remote environment can the evidence remain intact and admissible in court.

Note: A secure hash value only shows that a digital file has not changed. It proves that the copy is exactly the same as the file that was seized. It does not prove that the data itself is genuine or truthful. There is an important difference between a file being "unchanged" and a file being "authentic." To prove authenticity, it must be shown that the file was created in the manner claimed, at the stated time, and by the stated source, and that it was not fabricated, manipulated, or generated by artificial intelligence. This can be done only by examining digital footprints such as metadata, system logs, and file-system records. Such examination requires specialised forensic knowledge and tools. An ordinary investigating officer can confirm that hash values match, which proves hash value process integrity and reproducibility, but cannot determine whether the contents are genuine or truthful. Only a qualified forensic expert can analyse technical indicators and certify the authenticity of digital data. The Investigating Officer's role is limited to lawful seizure, sealing, and custody of the device. Through forensic examination, including safe hashing and analysis of digital footprints, the expert connects the integrity of the handling process with the authenticity of the data and certifies that the evidence is genuine and reliable.

Illustration: Illustration: Hash values establish only the post-seizure integrity of electronic data and do not prove its pre-seizure authenticity. A matching hash merely confirms that the image was extracted correctly and that the copied file is a bit-perfect replica of what existed on the device at the time of extraction. It does not establish how, when, or by whom the image was created. Consequently, a forensic expert can testify only to the existence and integrity of the extracted image, not to its genuineness or truthfulness. A perfect extraction of a forged or planted image remains a forgery. To determine authenticity, the forensic examination must extend beyond hash verification to an analysis of the digital

environment, including metadata, system and application logs, and file-system artifacts that reveal the origin and history of the data.

Even when the handset itself is produced in court and the image is viewed directly on the screen, such visual confirmation proves only existence and display, not authenticity. Just as a document expert examines ink, paper, and writing characteristics to verify a signature, a digital forensic expert must analyze the handset's technical traces to certify that the data represents a genuine and truthful record rather than a fabrication.

Thus, in both circumstances, whether the handset is produced or not, the forensic expert must, through examination of the technical artifacts, demonstrate that there are no indicators of fabrication, planting, or post-creation manipulation and that the image is consistent with having been generated in the ordinary course of the handset's operation.

Note: Section 176(3) of the BNSS, 2023 requires a forensic examination only in serious offences punishable with imprisonment of seven years or more. However, Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023, read with Schedule Part-B, makes it clear that electronic evidence must be certified and signed by a forensic expert. The purpose of the BSA, 2023 is to ensure the technical reliability of electronic evidence. This requirement depends on the nature of the evidence, not on the severity of the offence. Therefore, even in cases punishable with less than seven years' imprisonment, electronic evidence cannot be properly proved unless it is examined and certified by a qualified expert. The seriousness of the offence does not remove the technical requirement laid down under the BSA, 2023.

18. Certificate u/s 63(4) is not mandatory before Tribunal where Evidence Act is not strictly Applicable: In certain proceedings such as Family Courts, strict compliance with Section 65-B of the Indian Evidence Act (Now section 63(4) BSA)) may not be mandatory because the formal rules of evidence do not fully apply. However, this relaxation does not mean that the requirements of authenticity and integrity may be ignored. Authenticity concerns whether the electronic record is genuine and originates from the source it claims. Integrity concerns whether the data has remained unchanged. Even before the decision in Anvar P.V. v. P.K. Basheer, courts tested integrity in a practical manner by examining factors such as system reliability, official or lawful custody, internal consistency of the record, and whether the opposing party had a fair opportunity to challenge it. After Anvar, forensic practices such as hash value verification evolved to address disputes relating to data alteration. If expert/ experts/ neutral examiner is appointed then parties have right to cross examine. In disciplinary proceedings as well, directions have been issued to supply electronic material and follow basic forensic verification practices to ensure fairness and reliability. [8,9,10]. In short for electronic record, basic verification should be done, authenticity, integrity must be established and opponent must have opportunity to challenge

Admissibility (Where BSA not strictly applicable) = Relevance + Integrity+ Authenticity + proved provenance (Source) + Fair Opportunity to Challenge.

Illustrations: The case was for evidence. In this case, the husband filed an affidavit along with memory cards/chips from mobile phones, a compact disc (CD), and transcripts of recorded conversations. The

wife challenged the admissibility of these electronic records, but the Family Court allowed their production. The High Court overturned this, but the Supreme Court directed that the Family Court should take the records on evidence, provided they are relevant and authenticated. The Court emphasized that for recordings to be admissible, they must be relevant to the dispute, authentic, accurately represent the conversation, voices must be identifiable, and the record must be untampered and reliable. Mere filing of electronic media is insufficient; these foundational requirements must be satisfied. If the respondent wished to challenge the recordings' technical aspects, the proper approach would have been to call a forensic or voice identification expert at trial or upon remand [11].

Illustrations: In a divorce petition on the ground of adultery, the Family Court granted divorce relying on photographs showing the wife in compromising situations. The wife claimed the photographs were originally on her mobile phone, later transferred to the husband's device, and that the husband had broken her phone. She denied authenticity but did not explain fabrication or identify who might have manipulated the images, merely asserting they were "created by some trick." The photographer who developed the photographs was examined, corroborating the authenticity and context of the images. On appeal, the wife argued that the photographs were secondary electronic evidence and inadmissible for lack of a Section 65B certificate. The High Court held that the wife had ample opportunity to cross-examine and challenge the evidence, and noted that Family Courts have wide discretion to consider evidence that assists in truth-finding in matrimonial disputes, even if it is not strictly admissible under the Indian Evidence Act [8].

Illustration: The difference between data integrity and authenticity is best understood through the analogy of a mobile handset as explained above illustration is equally applicable to Tribunal where Evidence Act is not strictly Applicable.

Section-III - Trial Court as Guardian of Digital Evidence under BSA, 2023:

19.Under the Bharatiya Sakshya Adhiniyam, 2023, the Trial Court is not a passive receiver of electronic or digital evidence. It has an active duty to ensure legality, integrity, authenticity, reliability, procedural fairness, and justice at every stage of the proceedings.

Following are steps to play role of guardian: -

- The Court must verify that the electronic record is supported by a valid statutory certificate, issued by a person in lawful control of the system, disclosing the source, method of creation or extraction, and integrity of the data, and must assess the nature of the record before admitting it in evidence.
- The Court must ensure that the electronic record is complete, accurate, and not selectively extracted, and that it represents the full and relevant data without truncation or manipulation.
- The Trial Court must ensure the defence has a fair opportunity to examine electronic records, raise admissibility or integrity objections, and, especially for unrepresented parties and also provide guidance and access to prevent technical disadvantage.

- The Court must scrutinize evidence of expert, methodology, computational process, compliance, and reliability, compare conflicting experts objectively, and treat opinions without direct access to original devices as assistive, not conclusive.
- A neutral examiner may be appointed only when necessary to help the Court understand or verify technical aspects of electronic records. Such appointment is only for judicial assistance and may not replace party-appointed experts or cure any statutory non-compliance.
- The Court must clearly distinguish between incurable defects that affect the integrity of the electronic record and curable procedural defects. Incurable defects must lead to exclusion of the record, while curable defects may be permitted to be corrected if the original record remains intact and no prejudice is caused.
- After admission, the Court evaluates the electronic record's relevance, authenticity, integrity, and reliability, weighs its probative value with corroboration, and decides whether it is proved and trustworthy.
- The court must independently apply judicial mind and determine authenticity, integrity, relevance, reliability, and probative value.

Illustration: In a criminal case alleging that the accused sent a threatening WhatsApp message. The prosecution produced certified forensic extracts supported by valid Part-A and Part-B certificates under Section 63(4) BSA, 2023. Handset of complainant was not produced. The accused denied authorship of his own handset and WhatsApp account and raised theoretical possibilities of manipulation. The Court independently examined statutory compliance, verified matching hash values at seizure, analysis, and production, scrutinised WhatsApp databases, message IDs, timestamps, metadata, chat continuity, backups, multi-device logs, and chain-of-custody records. On finding consistent technical data and the absence of any concrete proof of tampering, the Court accept the electronic record as authentic, reliable, and admissible, and concluded that the message was sent by the accused. The court has independently applied judicial mind and determine authenticity, integrity, relevance, reliability, and probative value. But the Court did not treat the Part-B expert's opinion and Expert's opinion for defence as conclusive or decisive by itself. The expert opinion serving only as an aid and not as a substitute for judicial determination. Thus, the judicial satisfaction was reached through the Court's own assessment.

Note: The above illustration is only imaginary wherein facts for electronic record which court may require to assess are stated. It has not considered other factors need of CDR, SDR etc or any other witness to corroborate authorship and account of handset holder etc. which generally arises. The illustration is only imaginary on technical points which court may require to independently assess.

Note: Metadata gives basic information about digital data, such as when a file was created, sent, received, or modified. Courts may look at this information themselves to check whether electronic evidence appears genuine. While experts help the Court understand technical details, the judge must decide reliability by considering all the surrounding facts and evidence together, not only the expert's opinion. Expert evidence is also relevant. The judge cannot hand over the responsibility of deciding authenticity or admissibility to experts. The final and independent duty to assess electronic evidence always lies with the Court.

Note: Where the relying party admits the use of AI tools in the creation, enhancement, or alteration of the electronic record, then question arises its reliability, accuracy, and evidentiary weight, and where the record is produced (alleged) as a natural or original record and the opponent objected for AI use, then authenticity and integrity may require to look in addition to basic principle of the jurisprudence as laid down in Arjun Khtokar.

Illustrations: Mohammed Ajmal Mohammad Amir Kasab [7], The Hon'ble Court did not rely on expert opinion. It independently examined whether the CCTV footage CD, call records, intercepts, and other digital materials came from official and lawful sources, such as government CCTV systems, telecom service providers, and investigating agencies, and not from private or doubtful origins. The Court itself verified whether the electronic evidence was properly seized, sealed, stored, and transferred, by examining seizure memos, custody records, and continuity of possession, and considered that there was no manipulation. The Court also assessed whether the systems generating the electronic records were regularly used official systems, operating in the normal course of business, and not specially created for the case. Independently of expert opinion, it checked whether timestamps, call sequences, video timelines, and internal data were chronologically consistent and matched the sequence of events proved by other evidence. The court scrutinised what was visible on the CD footage and recognised the conditions under which these copies were made (e.g., automatic deletion after a week) also weighed the probative value. The Court cross-verified electronic evidence with eyewitness testimony, medical evidence, recoveries, movement of the accused, and other proved facts. Expert testimony was treated as assistive. While experts explained technical aspects, the final conclusions on integrity, authenticity, and admissibility were drawn by the Hon'ble Court itself after an overall evaluation of the entire evidence.

Illustrations: K. Ramajayam @ Appu [13**]** [DVR was produced], The Hon'ble Court itself viewed and evaluated the CCTV recording, examined whether the footage clearly depicted the accused entering the jewellery shop, committing theft, and murdering the victim, and whether the facial features and physical movements were sufficiently clear and identifiable. The Hon'ble Court independently considered the continuity of the footage, the natural sequence of events, and the absence of breaks or suspicious edits, and correlated the visual evidence with surrounding circumstances such as timing, location, recovery of stolen articles, and other oral and documentary evidence. The forensic opinion regarding the CCTV footage was treated as assisting the Court in understanding technical aspects, but the final satisfaction regarding authenticity, reliability, and evidentiary value was reached by the Court itself after personally examining the footage and testing it against the totality of evidence on record.

Illustration: Anil Kumar Yadav [14] [CD was produced]- The Hon'ble Court itself viewed the CCTV footage/CD, examined its contents directly, and noted what was actually visible and what was not, including whether the alleged use of a weapon (such as a baseball bat) could be clearly seen. The Court independently assessed the clarity, continuity, and probative value of the footage, and compared it with the prosecution version and other evidence on record. The decision shows that the Hon'ble Court did not leave its judgment to experts. The experts only assisted the Court, and the final decision on reliability and evidentiary value was made by the Hon'ble Court after its own examination of the electronic record.

Illustration: Ambalal Sarabhai [16] it was held that, the digital conversations can evidence negotiations, but they do not automatically create a contract. Courts must read emails and WhatsApp messages as a

whole, examine whether all essential terms were finally agreed upon, and apply strict evidentiary standards before treating such communications as proof of a concluded contract.

Note: In civil cases, which are to be decided on the preponderance of probabilities, courts may admit electronic evidence despite minor certificate defects if the record is not disputed. In criminal cases, where proof must be beyond reasonable doubt, strict compliance with admissibility requirements is essential, and defective or partial electronic evidence is ordinarily not admissible.

Illustration-Case Study for 65-B: Devashish Rai vs State of Uttar Pradesh, by Special CJM (Customs) in Lucknow **[**W/S Case No.-75759/2024 decided on 16-07-2025] [18] is a fact-based decision of the Chief Judicial Magistrate, Lucknow, arising out of a "digital arrest scam." The importance of the case does not lie in it being a binding precedent, but in the manner in which the trial court examined electronic evidence.

What electronic record was produced: (a)video call logs and recordings (b) bank transaction metadata (c) digital footprints such as IP address records and IMEI details of devices used, (d) hash values (e) certificates under Section 65B of the Indian Evidence Act for some electronic record.

What documents were provided to the defence: (a) Mirror images of the seized storage devices (b) forensic report (c) Section 65B certificate (d) Equal access to digital material.

What role played by the Expert: (i) Identity mapping: The expert established identity mapping by correlating multiple digital identifiers. The IMEI number was shown to correspond to the seized mobile device, the IP address activity was traced to the same device, and the use of that device was linked to the accused. (ii) Device linkage: The expert further proved device linkage by showing that several forged bank accounts were operated from the same device. The IMEI remained constant, the usage pattern was similar, and the operational behaviour across accounts showed uniformity. (iii) Non-repudiation. The combination of logs, metadata, recorded hash values, and certified forensic reports created a situation where the accused could not plausibly deny involvement.

The trial Court relied upon: (A) Video call logs and recordings: The video call logs and recordings were treated as electronic records under Section 2(1)(t) of the IT Act. They directly demonstrated impersonation and were admitted because they were supported by Section 65B certification and protected by recorded hash values at the time of seizure. (B) Bank transaction metadata: The court relied not merely on bank statements, but on transaction metadata such as timestamps, device access information, and transaction origination details. (C) Digital footprints: IP, IMEI, and tower data: The digital footprints, IP logs showed the origin of internet activity, IMEI identified the physical device used, and tower location data established geographical presence. For the purpose of the traditional concepts of "last seen" and "exclusive possession." (D) Hash value recorded at seizure: Enabled the court to rely on the electronic evidence with confidence as to its unchanged condition after seizure.

Trial Court Observations: The court observed that the digital evidence was properly preserved by maintaining a clear chain of custody. It noted that SIM cards were obtained using forged Aadhaar documents and that the mobile numbers were linked to fake firms. The video call recordings clearly showed the accused impersonating a CBI officer. The bank transaction records established a continuous money trail, showing transfers of about ₹85 lakh over a period of ten days. The testimony of the victim,

Dr. Soumya Gupta, a senior physician at KGMU, further supported the prosecution case. The court observed that although the accused used fake names and forged identity documents to open bank accounts, such personation could not hide the digital trail. Technical surveillance, including IMEI data, tower location records, and IP logs, created an airtight link between the electronic activity and the accused, making the disguise ineffective.

Why the Trial Court's role is important: The Trial Court convicted to accused. The Appellate Court, in Appeal No. 208 of 2025 decided on 11-09-2025, remanded the case because the investigation suffered from serious legal defects. The investigating officer wrongly removed the charge of criminal conspiracy under Section 120B IPC without proper justification. The investigation failed to collect crucial electronic evidence. No Call Detail Records of the victim or the accused mobile numbers 9714898541 and 7997087395 were obtained. No internet or WhatsApp records were collected from service providers. No screenshots from the victim's mobile device were taken with a valid certificate under Section 65B of the Evidence Act.

Important financial documents were also not properly proved. NEFT and RTGS forms, bank statements, and account opening forms of several first-layer accounts were either improperly seized or not verified. These documents were placed on record but were never proved through competent witnesses. The alleged fake documents were verified only through Google and open-source searches by the investigator. No forensic examination was conducted. No confirmation was obtained from banks or issuing authorities to establish that the documents were forged.

The Trial Court failed to perform its statutory duty under Section 313 of the CrPC. It asked only general questions to the accused. It did not put specific incriminating circumstances to him. The Trial Court wrongly applied Section 106 of the Evidence Act and shifted the burden of proof onto the accused.

The prosecution also failed in its duty. It did not examine essential witnesses such as bank officials, technical experts, or nodal officers. It allowed electronic and documentary evidence to remain improperly proved. There was no clear money trail of the alleged amount. Several important documents and testimonies were left unexamined.

Because of these failures, the trial became a mere formality. The Appellate Court held that justice could not be served in such a manner. It therefore ordered a fresh trial. The Court directed that the case be reconsidered after proper examination of electronic and documentary evidence and after examining all necessary witnesses.

Recommendations for Further Study:

1] Examine cryptographic hash methods and accepted digital forensic standards to assess and verify the integrity of electronic records.

2] Examine the respective roles of expert witnesses and neutral examiners in resolving technical disputes relating to digital evidence, while ensuring that judicial decision-making is not replaced by technical opinion.

3] Investigate challenges in proving authenticity and integrity of cloud, blockchain, and decentralized digital records.

4] Examine the admissibility of AI-generated content and assess whether current BSA mechanisms ensure reliability.

5] Study the Trial Court's guardian role in inspection, retendering, and verification of electronic evidence.

6] Conduct empirical surveys of trial and appellate decisions to assess trends in acceptance or rejection of electronic evidence.

7] Practical difficulties in terms of infrastructure deficiency, technical support, and privacy issues including uniform set of digital forensic standards and trained individuals.

8] With the rise of AI substantive safeguards of the Bharatiya Sakshya Adhiniyam, 2023 to electronic record [except certificates] are required even where the BSA Act does not strictly apply and it also due to applicability of Information Technology Act,2000 and any other Act relating to IT, on this concept more study is required.

9] Re-extraction of electronic or digital record with the permission of court OR Forensic examination by court-appointed expert for re-extraction of electronic or digital record.

Limitations of the study:

1] This study paper is based on the text and scheme of the Bharatiya Sakshya Adhiniyam, 2023. As there are presently no judicial precedents interpreting Section 63 of the BSA, the jurisprudential principles evolved under Section 65-B of the Indian Evidence Act, particularly those relating to authenticity, integrity, source reliability, and the mandatory nature of certification, are likely to continue to guide courts in evaluating electronic evidence. However, the procedural requirements prescribed under Section 63 of the BSA must be strictly complied with in proceedings to which the BSA applies, in accordance with Section 170 of the BSA, which provides that the new law applies prospectively to trials, inquiries, and proceedings commenced on or after its enforcement on 1 July 2024, while earlier proceedings continue to be governed by the Indian Evidence Act, 1872.

2] The issue of oral evidence to prove the authenticity of the electronic record is not studied. 3] The study is not carried out in depth separately regarding judicial principles applicable to criminal cases, civil cases and tribunal where natural justice needs to be followed.

4] This study is not carried out for scientific standards and ground level implementation, standardized forensic robust infrastructure, privacy violations,

5] This study is not carried out regarding AI-Generated and other advanced technology Evidence and Its Admissibility by Courts.

Conclusion: Under the Bharatiya Sakshya Adhiniyam, 2023, the earlier system of a single certificate under the Indian Evidence Act has been replaced by a requirement of two certificates. The BSA also requires a secure hash value instead of a simple hash value, which improves data integrity. The principle laid down in Arjun Panditrao Khotkar is continued by requiring the certificate to be filed but at the time of admission of the electronic record. By including the role of an expert through the Part-B certificate, the BSA brings more transparency and technical clarity. This will help Courts to assess electronic

evidence not only in the present AI environment but also as digital technology advances further in the future.

The BSA does not permit the Court to cure or validate non-compliant electronic records on its own, the certificates is a gate pass. Any correction of minor procedural lapses is permissible only where jurisprudence allows it and only if the original electronic record remains intact. In the absence of compliance with Section 63(4), the burden of proof remains entirely on the party producing the evidence, and the Court has no authority to authenticate or verify the record independently.

Expert's opinion cannot substitute the mandatory statutory certificate issued by expert Part-B, nor can conflicting expert reports cure foundational defects. The Trial Court must therefore apply strict threshold scrutiny at the admissibility stage, supervise proper exhibition of records, and allow effective examination, cross-examination, and re-examination.

If the original device is produced or in the circumstances where the BSA is not strictly applicable the basic principles need to be scrutinized. In any circumstance, mere production of electronic or digital material or device is insufficient because the admissibility and reliability depend on strict technological compliance.

The Court should not admit expert evidence merely because it is scientific or originates from a government forensic laboratory or any other forensic / technical expert. It must examine the methodology used, the reliability of the process, and the integrity of collection and analysis, and insist on full disclosure of underlying data, methods, and assumptions. This approach preserves judicial neutrality, statutory discipline, and the right to a fair trial. If parties use AI or any other technology, an expert should assist the Court by explaining the technology so that the Court may independently assess fairness, accountability, integrity, and reliability. The Court must examine electronic or digital evidence step by step. Each step must be carefully checked, and the evidence should not be accepted as true merely on its face. In all circumstances, the court must independently apply judicial mind and determine authenticity, reliability, accuracy, integrity, relevance, reliability, and probative value / evidentiary weight of the electronic record.

References:

1. Excitel Private Limited vs The Registrar Of Trade Marks https://indiankanoon.org/doc/141399920/
2. The Hon'ble Delhi High court issued a Notification April 22, 2024 for E-True Copy Rules of high court of Delhi, 2024, https://www.delhihighcourt.nic.in/files/announcements/1543372878666302c0c45fa.pdf
3. Shital Krushna Dhake v. Krushna Dagdu Dhake https://www.casemine.com/judgement/in/5dc077be3321bc77c509170c
4. Supply of copy of electronic evidence - Suggested system for District Courts, by Sanjay Rambhau Salkute, Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/research-paper.php?id=3213
5. Yuvaraj vs State Rep. By https://indiankanoon.org/doc/57531294/

6. State of Karnataka v. T. Naseer @ Nasir @ Thandiantavida Naseer @ Umarhazi @ Hazi and Others , https://www.supremecourtcases.com/state-of-karnataka-v-t-naseer-nasir-thandiantavida-naseer-umarhazi-hazi-and-others/.
7. In Mohammed Ajmal Mohammad Amir Kasab @ Abu Mujahid vs. State of Maharashtra https://www.casemine.com/judgement/in/5609af15e4b01497114158b6
8. [8] Lumeshwari@ Pinky vs Rajesh Dubey, First Appeal No.866 of 2021 decided on 11-11-2025 by M.P. High Court https://www.casemine.com/commentary/in/relaxed-electronic-evidence-requirements-in-matrimonial-cases:-section-14-family-courts-act-vs.-section-65-b-evidence-act-in-lumeshwari-@-pinky-v.-rajesh-dubey/view
9. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 https://indiankanoon.org/doc/187283766/
10. Toman Lal Sahu S/o Panth Ram Sahu vs State of Chhattisgarh, WPS No. 5287 of 2012, 26.03.2021 https://www.indianemployees.com/judgments/details/toman-lal-sahu-versus-state-of-chhattisgarh
11. Vibhor Garg v. Neha (2025 INSC 829) https://www.scobserver.in/wp-content/uploads/2025/07/SCOLR-Vibhor-Garg-v.-Neha.pdf
12. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1 https://indiankanoon.org/doc/172105947/
13. K. Ramajayam @ Appu v. Inspector of Police (2016) - Madras High Court https://indiankanoon.org/doc/26760633/
14. Anil Kumar Yadav v. State of NCT Delhi (2017) - Supreme Court https://indiankanoon.org/doc/57105555/
15. Selvi v. State of Karnata**ka** https://indiankanoon.org/doc/338008/
16. Ambalal Sarabhai Enterprise Limited v. KS Infraspace LLP Limited https://indiankanoon.org/doc/51304221/
17. State of Karnataka v. T. Naseer @Nasir @Thandiantavida Naseer @Umarhazi @Hazi & Ors. https://www.verdictum.in/court-updates/supreme-court/bangalore-bomb-blasts-fair-trial-not-that-should-be-fair-to-one-of-the-parties-1503542https://www.verdictum.in/court-updates/supreme-court/bangalore-bomb-blasts-fair-trial-not-that-should-be-fair-to-one-of-the-parties-1503542 .
18. Devashish Rai vs State of Uttar Pradesh, by Special CJM (Customs) in Lucknow , CNR: UPLK040860602024https://services.ecourts.gov.in/ecourtindia_v6/?p=casestatus/index&app_token=a0794bb46af947d3ad61b46e8fb0ef037ca038cd6738bb3e70e5eff6e2d54fd3# Appeal: CNR UPLK010136422025https://services.ecourts.gov.in/ecourtindia_v6/?p=home/index&app_token=4fa159b9b53ef47172a88ceb2ddab55bc25a089a6446a57418319d7abc3c5cb3#

Other Cases:

19. Supreme Court of India's White Paper on AI and Judiciary (Nov 2025) https://cdn.s3waas.gov.in/s3ec0490f1f4972d133619a60c30f3559e/uploads/2025/11/2025112244.pdf
20. P. Gopalkrishnan @ Dileep v. State of Kerala (2020) 9 SCC 161 https://indiankanoon.org/doc/188011203/

    Ritesh Sinha v. State of Uttar Pradesh (2019) 8 SCC 1 https://indiankanoon.org/doc/18061439/
21. Trimex International FZE Ltd. v. Vedanta Aluminium Ltd. (2010) 3 SCC 1 https://indiankanoon.org/doc/658803/
22. State of Maharashtra v. Praful Desai (2003) 4 SCC 601 https://indiankanoon.org/doc/560467/

23. P. Gopalkrishnan @ Dileep v. State of Kerala https://indiankanoon.org/doc/188011203/
24. Implementation of Policy Regarding Use of Artificial Intelligence Tools in the District Judiciary - Reg. Dated 25-07-2025 https://images.assettype.com/theleaflet/2025-07-22/mt4bw6n7/Kerala_HC_AI_Guidelines.pdf
25. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach https://www.academia.edu/150287956/Trial_Court_as_Guardian_of_Electronic_and_Digital_Record_Under_Section_63_of_the_Bharatiya_Sakshya_Adhiniyam_2023_A_Modern_Approach