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-III]

Sanjay Rambhau Salkute

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

Abstract:

The Bharatiya Sakshya Adhiniyam, 2023, does not provide a specific statutory definition of the term "expert," yet judicial decisions have consistently explained that an expert is a person possessing special knowledge or skill acquired through study, practice, or experience. With the increasing use of electronic records in litigation, the role of experts has assumed greater importance, particularly under Sections 39, 50, and 63(4) of the Act. Section 63(4) mandates the filing of a Part-B certificate for the admissibility of electronic records, but the person issuing such a certificate is not necessarily a forensic analyst. The statutory scheme creates a functional distinction between two roles: the technical person who authenticates the electronic record for admissibility, and the forensic expert who analyses and interprets the record to assist the court on technical issues.

This paper (Part-III) examines the material role played by experts in relation to electronic evidence under the BSA, with special emphasis on the practical implications of Section 63(4) and the evidentiary value of expert opinions under Sections 39 and 50. It seeks to clarify the conceptual difference between authenticity and scientific interpretation, and explains how courts evaluate both aspects at different stages. The discussion is intended as a preliminary study for law students, using simplified illustrations to demonstrate the functional roles of technical and forensic experts. The illustrations are explanatory in nature and do not claim to be an exhaustive treatment of the subject and detailed forensic concepts.

Keywords: Expert, forensic expert, digital expert, certificate part-B, digital opinion expert, electronic record

1. Introductions:

Under the Bharatiya Sakshya Adhiniyam, the term "**expert**" is not specifically defined, but its meaning has been explained in various judgments. An expert is a person who, by reason of special study, training, experience, or practical knowledge in a particular field of science, art, technology, or specialized skill,

possesses knowledge beyond that of an ordinary person. Such a person assists the court in forming an opinion on technical or scientific matters which are outside the common understanding of judges and laypersons.

Thus, an expert must support his opinion with proper reasoning, data, and methodology. Thus, any person with recognized special knowledge, skill, or experience in the relevant field may be treated as an expert, provided the court is satisfied about his competence and the reliability of his opinion.

Expert Under Bharatiya Sakshya Adhiniyam, 2023:

Under the scheme of the Bharatiya Sakshya Adhiniyam, 2023, particularly Sections 39 and 63(4), the role and competence of the expert have assumed greater significance in cases involving electronic records, therefore, section 63(4) mandates the filing of Certificate Part-B, requiring technical particulars of the device, manner of production, and authenticity of the electronic record.

Thus, although the BSA does not expressly define a "forensic expert," the structure of Sections 63(4) and section 39 and 50 of BSA, creates a functional distinction: (1) The technical person authenticates the record for entry into evidence, (2) An expert analyses and explains the record to help the court decide the issues in dispute.

First role: Expert for admissibility under Section 63(4) (Part-B Certificate): Section 63(4) deals with the certificate required for electronic records. The person issuing the Part-B certificate is not necessarily a forensic analyst. He is usually the person in lawful control of the device, system, or server, or a technical person responsible for the process of extraction or copying. His duty is limited and technical in nature. He certifies how the electronic record was extracted and produced, the particulars of the device, the manner of extraction, and the generation of secure hash values. His role is to prove authenticity, integrity, and admissibility of the electronic record. He does not analyse the contents or give any opinion about the meaning of the data.

Second role: Expert giving opinion: The expert is a person with special knowledge in a particular field of science or technology, such as digital forensics. This expert examines the cloned or extracted data, performs scientific analysis, interprets logs, metadata, timelines, or communication patterns, and then gives a reasoned opinion. His function is not to certify the record, but to interpret the technical evidence and assist the court in understanding its significance. He must also explain the grounds and methodology of his opinion.

A single person my play the above both functional roles as a expert for admission of electronic record and forensic expert for opinion of the contents of the electronic record. But in digital forensics is not a single uniform discipline but comprises several specialized domains such as computer forensics, mobile forensics, cell-tower analysis, GPS data interpretation, network forensics, and video authentication. An expert in one field may not possess the necessary knowledge or practical experience in another. Thus, under the BSA framework, parties should select experts based on the nature of the electronic evidence and the specific technical issue involved, rather than expecting a single expert to cover all technological domains.

Type of Experts: Digital forensics covers several specialised areas depending on the type of device or data involved. The computer forensics deals with the examination of desktops, laptops, and storage devices such as hard drives, pen drives, and memory cards. Mobile or cell phone forensics includes the analysis of mobile phones, SIM cards, and records maintained by telecom service providers, such as call detail records and location data. GPS forensics involves examining GPS devices and location records to trace movement. Social media forensics focuses on data from messaging apps, social networks, and online accounts. Media device forensics relates to tablets, smart devices, and other digital media equipment. Specialised branches include digital video and photo forensics, which detect manipulation in images or videos, digital camera forensics, and digital audio forensics, which analyse voice recordings or sound files. There are also areas like multiplayer game forensics and online activity analysis.

In modern investigations, several advanced branches have developed: -

(i) Cloud forensics: Examination of data stored on cloud platforms such as Google Drive, AWS, or Microsoft Azure.

(ii) IoT (Internet of Things) forensics: Analysis of smart devices like smart watches, home assistants, smart TVs, and connected appliances.

(iii)Vehicle forensics: Extraction of data from car infotainment systems, GPS modules, and onboard computers.

(iv)Drone forensics: Examination of unmanned aerial vehicles and their flight logs.

(v)Memory (RAM) forensics: Analysis of live system memory to detect malware, encryption keys, or running processes.

(vi)Cryptocurrency and blockchain forensics: Tracking digital currency transactions and wallet activities.

(vii)Dark web forensics: Investigation of activities on anonymised networks such as Tor.

(viii)AI and deepfake forensics: Detection of manipulated media created using artificial intelligence.

In simple terms, digital forensics today extends far beyond computers and phones. It includes cloud systems, smart devices, vehicles, online platforms, cryptocurrencies, and AI-generated content, reflecting the growing role of digital technology in everyday life and criminal activity and it will continue in future.

Expert Area: In digital forensics, the work of an expert is generally divided into four main areas: acquisition, preservation, analysis, and presentation. Acquisition is the process of lawfully collecting the electronic record or creating a forensic image of the device or data source. Preservation means maintaining the evidence in a condition that can be safely defended in court, usually by generating hash values, sealing the original media, and maintaining a proper chain of custody. Analysis is the stage where the forensic expert examines the collected data to locate and extract evidentiary material, such as files, logs, messages, or deleted content, that may be relevant to the case. Finally, presentation involves preparing a forensic report for the court. This report typically includes the expert's background and experience, the tools used during the examination, the methods applied to verify the data, the processes

used to recover or extract the information, and a clear statement of the findings along with the supporting digital evidence.

Qualification Certificates: The court must carefully examine the qualifications, experience, and domain-specific expertise of the expert before placing reliance on such opinion. Where the issue relates, for instance, to mobile location, cell-tower data, or GPS tracking, the opinion of a general computer forensic examiner, lacking specialization in the relevant technology, would carry diminished evidentiary value. Consequently, the qualification, training and specific experience of the expert become material factors in the appreciation of electronic evidence under the BSA.

In the field of digital forensics, various international certifications such as EnCE, CFCE, GIAC (GCFA/GCFE) and CHFI are available, but none of them is legally required in India for a person to be treated as an expert. Because, under the Indian law of evidence, an expert is a person who is especially skilled by knowledge, training, or experience, and the court mainly looks at the person's practical expertise, methodology, and credibility, rather than any particular certificate.

In Indian courts, in the criminal cases, most electronic evidence is examined by experts from Central or State Forensic Science Laboratories, and their official position and experience may carry more weight than private certifications. But for becoming an expert, the international certificates like CFCE, EnCE, and GIAC are respected and add professional credibility, especially in corporate or private forensic work, while CHFI is more commonly pursued in India due to availability and cost. However, these certifications are only supporting qualifications. The decisive factors for the court remain the expert's skill, experience, scientific method, and reliability of the opinion.

Standard Procedure: In India, there is no single codified statute that prescribes a detailed step-by-step procedure for digital forensic investigation. However, investigators and forensic experts generally follow recognized technical standards and official guidelines. These include the ISO/IEC 27037 standard, which gives rules for identification, collection, acquisition, and preservation of digital evidence. Investigators also rely on NIST digital forensic guidelines, which provide internationally accepted methods for imaging, hashing, analysis, and reporting. The practical procedures are guided by CERT-In advisories, State and Central Forensic Science Laboratory (FSL/CFSL) protocols, and police cyber-crime manuals are also available.

There is no rigid rule in Indian law that only a Government FSL expert must be believed and a private expert must be rejected. The section 329 BNSS itself is clear.

In [1] **Chiranjilal Gupta v. State of Rajasthan**, '*''The report of FSL even though is admissible in evidence under Section 293 Cr.P.C., without examination of handwriting expert, the report of FSL itself is not a conclusive proof and therefore, the complainant has a remedy to demolish the credibility of the report of FSL by examining private handwriting expert as witness of the complainant.*'' *[2]* **Pravinkumar Lalchand Shah v. State of Gujarat** ,''*The accused must be given necessary materials so that he can obtain opinion of a private expert and properly defend himself.*''

The courts repeatedly hold that expert opinion is only an opinion, and the court is free to accept either a government or private expert depending on credibility, reasoning, and supporting evidence.

The best procedure in digital forensics is to ensure that the electronic evidence presented before the court is an authentic, accurate, and untampered representation of the original record. This is achieved by following lawful methods of collection, creating forensic images, generating secure hash values, maintaining a strict chain of custody, and using reliable and accepted forensic tools and techniques. Each step must be properly documented so that the court can see how the evidence was handled from the time of seizure until its production in court. In simple terms, the goal of the procedure is to satisfy the court that the electronic record is genuine, unchanged, and scientifically verified, so that it can be safely relied upon while deciding the case.

Tools: In India, there is no law that prescribes specific digital forensic tools shall be used for the production of electronic record before the court. However, in practice, many government forensic laboratories and cyber-crime units commonly use tools such as EnCase, FTK, Magnet AXIOM, X-Ways, Cellebrite UFED, MSAB XRY, and Oxygen Forensic Detective. Network analysis is often done using tools like Wireshark, while password recovery may involve tools such as Hashcat or Passware, used under lawful authority.

The Courts cannot insist on any particular brand of software. It only examines whether the forensic process was scientific, the chain of custody was maintained, and the expert can properly explain the method and findings. Thus, admissibility of electronic record depends on the procedure and credibility of the expert, not merely on the name of the tool used.

The fundamental principle of digital forensics is that the results of an examination must be capable of independent verification. The admissibility and reliability of electronic evidence do not depend upon the particular brand or name of the forensic tool used, but upon the scientific soundness and reproducibility of the process. If an examiner uses a recognized forensic tool to acquire and analyse data, another competent examiner, using a different but comparable tool with similar specifications and functions, should be able to reproduce the same results from the same source. This principle ensures transparency, accuracy, and fairness in forensic analysis, and supports the requirements of authenticity, integrity, and reliability under the Bharatiya Sakshya Adhiniyam. It also reinforces the concept of scientific testing of evidence, where conclusions are not tool-dependent but are based on verifiable data and standard forensic methods capable of independent confirmation.

Why the Role of Experts is Material: After the introduction of the Part-B certificate under Section 63(4) of the Bharatiya Sakshya Adhiniyam (BSA), any party who seeks to rely upon an electronic record must comply with the statutory requirements for its admissibility. The electronic record must be produced along with the prescribed certificate issued by a person in lawful control of the device or system, certifying the manner of production, integrity, and source of the record.

However, compliance with Section 63(4) BSA only satisfies the requirement of admissibility. It does not automatically prove the contents of the electronic record or its connection with the fact in issue. For that purpose, the role of an expert under Sections 39 and 50 of the BSA becomes material. Under Section 39 BSA, the court may rely on the opinion of a person specially skilled in digital or electronic science. Under Section 50 BSA, the expert must explain the grounds of that opinion, including the methods and processes used.

The law does not require or make restrictions that a single person must perform both roles. The roles are function-based, not person-based. One technical person may issue the Part-B certificate to prove authenticity and admissibility. Another specialist may give forensic analysis and expert opinion under Sections 39 and 50.

To asses the credibility, accept or reject expert opinions, and determine the evidentiary weight of the electronic record in light of the entire material on record the court requires forensic opinion and moreover in many cases, once one party produces an electronic record with a Part-B certificate, the opposite party may need to collect, analyse, or challenge that electronic evidence like Allegations of tampering or fabrication of digital documents , Disputes regarding call detail records, emails, or WhatsApp messages ,Cases involving edited audio or video recordings, Cyber-crime cases where technical interpretation of logs, metadata, or timelines is required, Civil disputes involving electronic contracts, digital payments, or online communications.

Legal aid is not confined merely to the appointment of a lawyer. It extends to providing all necessary assistance required for an effective and fair defence, including expert or technical support where the case involves scientific or specialised evidence. When the prosecution relies upon forensic or technical material, the accused must be given a reasonable opportunity to examine, analyse, and challenge that evidence. It is the duty of the court to maintain equality of arms between the parties and to ensure that the accused is not placed at a disadvantage due to lack of resources. Accordingly, where expert assistance is essential for a proper defence, the provision of such assistance forms an integral part of the right to a fair trial.

In any situations, an expert may be required to conduct forensic imaging or analysis, to verify hash values and detect alterations, to interpret metadata, logs, or communication patterns and to give a scientific opinion connecting the electronic record with the alleged act.

Proper Chain of Custody: The procedure is shaped by the Bharatiya Nagarik Suraksha Sanhita (BNSS), the Bharatiya Sakshya Adhiniyam (BSA), and the general procedural principles found in laws like the CPC for civil matters.

In criminal investigations under the BNSS, the process generally begins with identification and lawful collection of the electronic device or data source during search, seizure, or production before the court. After seizure, the investigator must ensure proper evidence acquisition and preservation, usually by creating a forensic image, generating secure hash values, and sealing the original device or storage media.

The next stage involves documentation and transfer, where a strict chain of custody is maintained. This means the record must clearly show who handled the evidence, when it was accessed, where it was stored or transmitted, and which forensic tools were used during imaging and analysis. These details are crucial to prove that the evidence was not altered or tampered with.

Thereafter, the forensic expert conducts analysis and examination, applying scientific methods to interpret the data and prepare an expert report under the relevant provisions of the BSA relating to expert opinion. Throughout this period, the evidence must be kept under secure storage conditions, with proper

seals and access logs. In order for evidence to be admissible, there must be a method to verify that the evidence presented is exactly the same as the original collected.

Finally, at the stage of presentation in court, the electronic record is produced along with the required Part-B certificate to establish its admissibility. The expert may also be examined to explain the technical findings. For electronic evidence to be admissible, there must be a reliable method to verify that the record produced in court is exactly the same as the original data collected, usually by means of secure hash values and proper forensic procedures.

The court then examines the authenticity, integrity, chain of custody, and scientific analysis of the electronic record before deciding its evidentiary value. In this manner, although Indian law does not prescribe a single codified forensic protocol, the combined operation of the BNSS (procedural law), the BSA (rules of admissibility and expert opinion), and general procedural principles ensures that digital evidence is lawfully collected, securely preserved, scientifically analysed, and properly proved before the court.

Ensuring Authenticity in Court Admissible Evidence: To make electronic evidence reliable and acceptable in court, certain safeguards must be followed:

1. **Lawful and proper collection**: The evidence must be collected in accordance with legal procedures. Any seizure, extraction should be done by an authorised person and in a lawful manner.
2. **Matching hash values and forensic images:** Secure hash values must be generated at the time of collection. The forensic image should produce the same hash value as the original record, proving that the data has not been altered.
3. **Strict chain of custody:** There must be a clear and continuous record showing: (1) Who collected the evidence. (2) Who handled or accessed it. (3) When and for what purpose it was accessed.
4. **Use of standard and accepted forensic methods:** The tools and techniques used for extraction, imaging, and analysis must be recognized and standardised by forensic authorities.

Stage-wise Digital Evidence Handling Under BSA: Under the BSA, electronic evidence usually enters the court in two stages.

First, the Part-B certificate ensures that the electronic record is properly produced, its source is identified, and its integrity is maintained. This certificate mainly satisfies the requirement of admissibility; it allows the electronic record to come before the court. But the admissibility alone does not prove the truth or reliability of the contents. For that purpose, the expert opinion becomes important. The expert analyses the technical aspects of the record, explains whether it is genuine, altered, or reliable, and assists the court in understanding its meaning. On the basis of this expert explanation, the Judge decides how much weight or importance should be given to that electronic evidence.

Part-B certificate = Authenticity, integrity, and admissibility of the electronic record

Expert opinion = Technical interpretation, reliability assessment, and evidentiary weight

Illustration: When a Call Detail Record (CDR) is required in a case, it is usually obtained from the Mobile Nodal Officer of the telecom company.

Expert: The Nodal Officer sends the CDR along with a secure hash value and issues the Part-B certificate. The Nodal Officer is the proper person to issue this certificate because he is in lawful control of the telecom company's system where the CDR is stored. He extracts the CDR from the company's server, generates the hash value, and certifies that the record is taken from the regularly used system and that it is an exact and untampered copy of the original data. But, when the Nodal Officer is examined in court, the questions are usually limited to: (1) Whether he is in charge of the relevant system, (2) How the CDR was generated, (3) Whether the system is regularly used in the ordinary course of business. (4) Whether the data is accurate and untampered. (5) Whether the Part-B certificate issued by him is correct.

Forensic: The forensic expert studies the call patterns, analysis's location, timing, and frequency of calls, and may reconstruct the communication pattern between the persons involved. He gives his opinion, based on scientific or technical analysis. His purpose is to connect the CDR with the alleged offence and to explain the technical aspects of the record in a manner that the court can understand. When this expert is examined in court, the questions usually relate to: (1) What the CDR actually shows including the pattern of communication between the parties and location correlation, if available, (2) Whether the calls match the prosecution version.

Trial Court: The court examines the certification of the electronic record and whether it establishes that the record is a genuine and accurate extract from the telecom system. Then the court evaluates the expert analysis of the CDR like whether the expert is qualified, whether accepted analytical methods have been used, and whether the conclusions drawn from call patterns, timings, durations, and cell-tower locations are logical and reliable. Then, the court assesses the overall evidentiary weight of the CDR along with the other evidence on record. Thereafter, the court considers whether the communication patterns and location data, when read with the surrounding circumstances, are sufficient to support the prosecution's theory of conspiracy or guilt beyond reasonable doubt.

Illustration: Computer forensic expert for fraud committed using a laptop:

Expert: He lawfully seizes or receives the laptop or electronic device, creates a forensic image of the storage media as a bit-by-bit copy, and generates secure hash values of both the original device and the copied image. He then issues the Part-B certificate, stating the particulars of the device, the manner in which the data was extracted, the technical process followed, and confirming that the electronic record is an accurate and untampered reproduction.

Forensic: He examines the forensic image of the laptop and conducts a detailed technical analysis of system logs, email data, hidden metadata, deleted files, registry entries, and browsing or access timelines. On the basis of this scientific examination, he correlates the digital activity with the alleged fraud and prepares a forensic analysis report. He also gives a reasoned expert opinion, explaining the methodology, findings, and conclusions.

Trial Court: The court considers admissibility, integrity, and chain of custody, that is, whether the Part-B certificate establishes that the electronic record is genuine, has not been tampered with, and has been properly handled from the time of seizure or collection till its production before the court. The court

looks into who collected the device, how it was stored, who accessed it, and whether the secure hash values and forensic procedures confirm the integrity of the record.

Then, the court evaluates the scientific interpretation given by the forensic expert, and checks whether the analysis is reliable, properly reasoned, and consistent with accepted forensic methods.

Thereafter, the court assesses the overall evidentiary weight, meaning whether the digital evidence, when read together with the other oral and documentary evidence on record, is sufficient to prove that the accused committed the alleged offence.

Illustration: Mobile Forensic Chain

Expert: He, lawfully seizes the mobile phone, for instance by placing it in a Faraday bag to prevent any remote wiping or interference, and then creates a forensic image of the SIM card and internal memory. During this process, secure hash values are generated to preserve the exact state of the data at the time of seizure. Then issues a Part-B certificate.

Forensic: Forensic expert does not deal with the original device directly but examines the verified forensic image created during the first stage. The expert conducts a scientific analysis of the data, which may include recovery of deleted WhatsApp messages, examination of call records and cell-tower location data, verification of timestamps and system clock settings, and study of user activity such as unlock methods. On the basis of this technical examination, the expert prepares a scientific forensic report and gives a reasoned opinion. The report explains what digital material was found, the methods used to recover or analyse it, and the technical significance of those findings.

Trial Court: The judge examines who seized the phone, the manner in which it was stored, whether there was any opportunity for tampering, and whether the hash values confirm that the data remained unchanged. The typical judicial concern at this stage is: “Could these messages have been added or altered after seizure?”

Then the judge considers what the data actually shows, whether the expert’s analysis is reliable and scientifically reasoned, and whether the digital activity can be connected to the accused.

Thereafter, such technical correlation may assist the court in linking the physical user to the digital act, subject to the overall evidence and circumstances of the case.

Illustration: CCTV footage of a crime.

Expert: The expert lawfully seizes or accesses the DVR, creates a forensic copy of the footage, generates a secure hash value, and issues the Part-B.

Forensic: The Forensic Video Analyst examines the authenticated footage. This expert applies scientific methods such as frame-by-frame analysis, detection of edits or drop-frames, metadata verification, time-synchronisation checks, and photogrammetric comparison. He prepares a forensic report and gives a reasoned expert opinion. He states, whether the person or activity in the video can be linked to the accused.

Trial Court: The court examines(1) Whether the Part-B certificate proves that the video is genuine and untampered,(2) whether the chain of custody is reliable,(3) Whether the forensic expert’s analysis is

based on accepted methods, logically reasoned, and technically reliable (4) Whether the video, along with other evidence, proves that the person shown is the accused and that the alleged offence was committed.

Illustration: Audio Recorded during bribery [Anti-Corruption] conversation.

Expert: The expert lawfully seizes the device containing the recording, extracts the audio file using forensic methods, generates a secure hash value, and issues the Part-B certificate.

Forensic: The forensic audio analyst, examined as an expert, studies the authenticated audio file, performs voice comparison, checks for editing or splicing, and prepares a scientific report explaining what was found, how it was analysed, and what it technically means. His role is to interpret the data and assist the court on technical aspects such as voice identity (as per sample voice) and continuity of the recording.

Trial Court: The court considers, (1) whether the Part-B certificate proves authenticity and integrity, (2) whether the expert's scientific analysis is reliable and reasoned, (3) whether the recording, read together with other evidence, is sufficient to prove the alleged offence.

Illustration: A video surfaces showing a politician accepting a bribe. The defence is that, it is a deepfake [AI Generated].

Expert: The expert downloads the video from the social media server or seizes the original device, extracts the file, generates a secure hash value, and issues the Part-B certificate.

Expert: Forensic expert, scientifically examines the video using specialised forensic and AI-detection techniques. He studies biological indicators such as unnatural eye-blinking, lip-sync errors, or pulse patterns; looks for digital artifacts like pixel warping, lighting inconsistencies, or face-swap traces; and analyses metadata for signs of AI-generation tools. Based on these examinations, he prepares a forensic detection report and gives a reasoned scientific opinion explaining, whether the video is genuine or manipulated and the technical grounds for that conclusion.

Trial Court: The court first checks whether the Part-B certificate establishes authenticity and integrity of the file as collected. Then it examines the expert's scientific opinion, including the methods used and the reasons given for the conclusion about deepfake manipulation. Thereafter, the court assesses the overall evidentiary weight of the video, along with other evidence in the case, before deciding whether the video can be relied upon to prove the alleged facts.

Note: *In the above illustrations, the First Stage of expert is Procedural witness to prove integrity and second stage of forensic witness is to give opinion of the collected electronic record. Hence mere integrity (the electronic record is original) does not automatically prove the truth (contents of the electronic record).*

2. Conclusion:

Under the scheme of the Bharatiya Sakshya Adhiniyam, 2023, the law recognises a functional distinction between authenticity and interpretation of electronic record. The Part-B certificate under Section 63(4)

serves the limited but essential purpose of establishing the integrity, authenticity, and admissibility of the electronic record. It is concerned only with the source and preservation of the data. In contrast, the expert opinion under Sections 39 and 50 addresses the scientific analysis and technical meaning of that data, and assists the court in understanding its relevance and probative value. The essential test of an expert is not his designation, qualification or experience only, but his special knowledge or skill acquired through study, practice, or observation, and such opinion always remains advisory, subject to the court's independent evaluation. The law does not require that both functions must be performed by the same person; one technical person may authenticate the record, while another specialist may analyse and interpret it. Ultimately, the court remains the final authority to assess credibility, accept or reject expert opinions, and determine the evidentiary weight of the electronic record in light of the entire material on record.

Limitation and Recommendations: As per Part I and Part II of the Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023.

References:

1. Chiranjilal Gupta v. State of Rajasthan, https://indiankanoon.org/doc/70971524/
2. ravinkumar Lalchand Shah v. State of Gujarat https://indiankanoon.org/doc/84924/
3. Supply of copy of electronic evidence - Suggested system for District Courts , Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/research-paper.php?id=3213
4. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approach--[Part-II], Advanced International Journal for Research, Volume 7, Issue 1 (January-February 2026), https://www.aijfr.com/research-paper.php?id=3276
5. Trial Court as Guardian of Electronic & Digital Record Under Section 63 of the Bharatiya Sakshya Adhiniyam, 2023: A Modern Approachhttps://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
6. Digital Forensics for Legal Professionals by Larry E.Daniel and Lars E. Daniel, edition 2012, Syngress Elsevier, Waltham, MA 02451, USA
7. Hidden Files, By Amit Dubey, Unbound Script, Delhi 110002