

**LAWWORLD**

# ***Proving the Digital: Electronic Evidence under the Bharatiya Sakshya Adhiniyam, 2023***

A Courtroom-Ready Guide to Admissibility, Certificates, and Digital Media Proof

---

*LawWorld Editing Team*

*Creator: LawWorld*

# Contents

---

|           |                                                                            |    |
|-----------|----------------------------------------------------------------------------|----|
| <b>01</b> | <i>The New Landscape: BSA 2023 and Electronic Records</i>                  | 4  |
| <b>02</b> | <i>The Section 63 Certificate: Mandatory Contents and Statutory Format</i> | 6  |
| <b>03</b> | <i>When Must the Certificate Be Produced?</i>                              | 9  |
| <b>04</b> | <i>Consequences of a Defective Certificate</i>                             | 11 |
| <b>05</b> | <i>WhatsApp Chats: The Most-Litigated Digital Evidence</i>                 | 14 |
| <b>06</b> | <i>Call Detail Records: Proving Telephonic Evidence</i>                    | 17 |
| <b>07</b> | <i>CCTV Footage and DVR Seizure: Chain of Custody in Practice</i>          | 21 |
| <b>08</b> | <i>Emails, Bank Statements, and Screenshots</i>                            | 24 |
| <b>09</b> | <i>Hash Values and Chain of Custody</i>                                    | 27 |
| <b>10</b> | <i>Cross-Examining the Certificate Issuer</i>                              | 29 |
| <b>11</b> | <i>Objections Strategy for the Defence</i>                                 | 34 |
| <b>12</b> | <i>Admissibility vs. Probative Value</i>                                   | 37 |
| <b>13</b> | <i>Model Certificates</i>                                                  | 41 |
| <b>14</b> | <i>Seizure Memo Formats and Advocate Checklist</i>                         | 47 |
| <b>15</b> | <i>Evidence Act to BSA: Section Conversion Table</i>                       | 50 |
| <b>16</b> | <i>Practice Pointers and the Road Ahead</i>                                | 55 |



## ***Preface***

*The Bharatiya Sakshya Adhiniyam, 2023 replaces the colonial Evidence Act with a modern framework for electronic records. Sections 61 to 63 restate and refine the old Sections 65A and 65B, while Section 170 provides a statutory certificate format. For the first time, practitioners have a codified scheme that expressly recognises electronic records as documents, defines primary evidence in digital form, and mandates a certificate for secondary electronic evidence. This book translates that scheme into courtroom-ready guidance. It moves from foundational concepts through specific digital media-WhatsApp chats, call records, CCTV footage, emails, bank statements, screenshots-to practical trial skills: cross-examining certificate issuers, mounting objections, and distinguishing admissibility from probative value. Model certificates, seizure-memo formats, and checklists make the book a working tool, not merely a reference. Whether you prosecute, defend, advise corporate clients, or adjudicate, this handbook ensures you handle digital evidence with confidence and precision.*

# 01

## **The New Landscape: BSA 2023 and Electronic Records**

From Section 65B to Section 63

---

### **The Legislative Journey**

Before 2000, electronic records occupied an uncertain evidentiary space. The Indian Evidence Act, 1872 made no mention of computers, printouts, or digital media. The Information Technology Act, 2000 changed this by inserting definitions-"electronic record" in Section 2(t) and "data" in Section 2(o)-and by deeming electronic records admissible as documents. For two decades, proof of electronic evidence ran through Sections 65A and 65B of the Evidence Act, a framework that generated extensive litigation over certificate requirements, timing, and the primary-evidence exception.

The Bharatiya Sakshya Adhiniyam, 2023 replaces this architecture with Sections 61, 62, and 63. Section 61 declares that no provision of the Adhiniyam denies admissibility to an electronic or digital record on the ground that it is electronic or digital, and that such record shall have the same legal effect, validity, and enforceability as other documents. Section 62 provides that the contents of electronic records may be proved in accordance with Section 63. Section 63(1) deems computer output-printed, stored, recorded, copied in optical or magnetic media, or semiconductor memory-to be a document if statutory conditions are satisfied. This is not merely renumbering; the new statute gives electronic records standalone recognition, no longer tethered to the IT Act definitions as the sole basis for admissibility.

### **The Two-Track System: Primary and Secondary Electronic Evidence**

The two-track system is the organising principle of electronic evidence law. *The Supreme Court in Anvar P.V. v. P.K. Basheer* clarified that primary evidence of an electronic record is governed by Section 62, not Sections 65A and 65B. *The landmark cassette ruling* illustrated this: a landline on which ransom calls were recorded was handed over in original to the police and was primary evidence-it required no Section 65B certificate. *The Karnataka High Court* has reiterated that the certificate requirement applies only to secondary electronic evidence.

Secondary electronic evidence-printouts, screenshots, call detail records, and exported digital records-must comply with Section 63. *The Supreme Court in Arjun Panditrao Khotkar* held that Sections 65A and 65B form a complete code for proof of information in electronic records, that the Section 65B(4) certificate is mandatory, and that oral

testimony cannot substitute for it. *The Constitution Bench* had earlier established that electronic records as secondary evidence are admissible only if all conditions in Section 65B(2) are satisfied and a proper certificate accompanies the record.

### **What BSA 2023 Changes**

- Section 61 gives electronic records standalone statutory recognition, no longer dependent on IT Act definitions for admissibility.
- Section 57 Explanations 4-7 explicitly expand primary evidence to include electronic records produced from proper custody, clarifying the primary-evidence gateway.
- Section 63 replaces Section 65B with updated language reflecting modern digital media-semiconductor memory, optical and magnetic media, and communication devices.
- Section 170 prescribes a statutory format for the Section 63 certificate, replacing the old Form under Section 65B(4) with a structured template.

*The Supreme Court* confirmed that video footage and audio clippings stored in memory cards or pen drives are electronic records under the IT Act and constitute documents under Section 3 of the Evidence Act. BSA 2023 carries this principle forward, expressly deeming computer output a document under Section 63(1).

### **What BSA 2023 Preserves**

The new statute does not break from the *Anvar* and *Arjun Panditrao* jurisprudence-it refines and continues it. The mandatory certificate requirement for secondary electronic evidence survives unchanged in Section 63. The two-track structure-primary evidence from proper custody without a certificate, secondary evidence with a Section 63 certificate-remains the operative framework. *The Karnataka High Court* held that the certificate requirement is procedural and may be relaxed in the interest of justice; this flexibility is preserved under BSA 2023's general admissibility framework.

*The Supreme Court* held that where a party is not in possession of the device from which an electronic document is produced, that party cannot be required to produce a certificate. This principle-that the certificate requirement applies to those who can comply-remains good law under the new statute.

### **The Practitioner Framework**



# 02

## The Section 63 Certificate: Mandatory Contents and Statutory Format

Reproducing and Annotating Section 170

### Who May Issue the Certificate

The Section 63 certificate must be issued by a person in a responsible position relative to the computer or communication device that produced the electronic record. This phrase-settled by the Supreme Court in *Anvar P.V. v. P.K. Basheer* -means the issuer must have official charge of, or operational knowledge about, the device or system generating the record. A police officer who seized a mobile phone and extracted its WhatsApp chats qualifies; a bank official who oversees the server producing a statement qualifies; a telecom engineer who operates the billing system qualifies. What disqualifies is a person with no institutional connection to the device-a lawyer, a private investigator, or a party to the dispute who happened to copy the file.

#### TIP

#### Responsible Position - Practical Indicators

The issuer holds an official designation (police officer, bank manager, telecom engineer). The issuer was personally involved in, or supervised, the extraction or production of the record. The issuer has access to the device or system logs. The issuer's organisation has a duty to maintain the record.

### The Five Mandatory Contents

The Supreme Court in *Anvar P.V. v. P.K. Basheer* held that a certificate under Section 65B(4) must contain five elements to render secondary electronic evidence admissible. These five elements survive into the new BSA framework and define what every Section 63 certificate must address:

1. **Identify the record** - the certificate must specifically name or describe the electronic record it accompanies (e.g., "Call Detail Records for mobile number 9876543210 for the period 1-15 March 2023"). A generic reference to "the electronic records" does not satisfy this requirement.
2. **Describe how it was produced** - the certificate must explain the process by which the record was generated, extracted, printed, or copied. For a CDR, this means describing the query placed to the telecom system; for CCTV footage, this means describing the extraction software and the DVR from which footage was recovered.
3. **Give device particulars** - the certificate must identify the computer, server, or device

that produced the record, including its location, configuration, and the software or system that generated it. Vague references to "the system" without specifics have been rejected by courts.

4. **Deal with the statutory conditions** - the certificate must confirm that the conditions prescribed by Section 65B(2) were satisfied at the time the record was produced. This is addressed in detail below.
5. **Be signed by a person in a responsible official position** - the certificate must bear the handwritten or digital signature of the responsible person identified above, along with their designation and, ideally, their official seal.

#### **WARNING**

##### **Common Omission: Device Particulars**

Courts have repeatedly rejected certificates that omit device particulars or describe the device vaguely. A certificate for CCTV footage that merely states "the DVR" without identifying the specific DVR system, its location, or the software used, has been held insufficient. Name the device, its location, and the system or software that generated the record.

## **Statutory Conditions Under Section 65B(2)**

The certificate must deal with the four conditions that Section 65B(2) of the Evidence Act requires to be satisfied before secondary electronic evidence becomes admissible. *Anvar P.V. v. P.K. Basheer* confirmed that these conditions are exhaustive and non-negotiable. The certificate must confirm:

- The computer or device that produced the record was operating properly at the relevant time - meaning it was not malfunctioning in a way that affected the accuracy of the output.
- The record was produced by the computer or device during the period when the computer was used regularly to process or store information.
- The information contained in the record is capable of being rendered in readable form.
- The computer or device was part of a system - whether a standalone computer or a networked one - that had due regard to the integrity and reliability of the information it stored or processed.

*LAWWORLD 2023 KAR 0241* illustrates the consequence of failing to address these conditions: the Karnataka High Court rejected CDs and call records for want of a Section 65B(4) certificate, holding that the certificate is a condition precedent to admissibility. The certificate need not use the statutory language verbatim, but it must substantively address each condition.

## **The Statutory Format Under Section 170**

Section 170 of the Bharatiya Sakshya Adhiniyam 2023 prescribes the format for the Section 63 certificate. While the precise statutory text is not reproduced here, the format follows the five-field framework established by the Supreme Court. Practitioners should



obtain the official format from the BSA 2023 schedule and complete every field. The format requires the issuer to fill in specific details about the record, the device, the production process, and the statutory conditions, and to sign the certificate.

**NOTE**

**eSakshya Certificates**

Under the Bharatiya Nagarik Suraksha Sanhita the State of Maharashtra eSakshya Management Rules, 2025, investigating officers generate Section 63 certificates through the eSakshya Mobile Application. These certificates are eSigned and automatically linked to the FIR number via CCTNS. The eSakshya system generates a unique SID and assigns a hash value to each evidence packet to ensure integrity. While these rules apply specifically to video and photo evidence recorded through the eSakshya application, they illustrate the direction of travel: digitally authenticated, hash-verified certificates generated at the point of evidence collection.

## **Hash Values and Device Description: Practical Guidance**

While the precise requirement for hash values in the Section 170 format is a matter of statutory interpretation, hash values are best practice for two reasons. First, they provide objective, verifiable proof that the record presented in court is identical to the record that was extracted. Second, they satisfy the statutory condition requiring that the computer was operating properly and that the record is capable of being rendered in readable form. The eSakshya Rules confirm this approach: every eSakshya packet generates a unique hash value to ensure integrity.

SHA-256 is the preferred algorithm. It produces a 256-bit hash value and is currently considered cryptographically secure. MD5 produces shorter hashes and is acceptable for non-critical evidence but is considered less robust. Practitioners should note the algorithm used in the certificate.

## **BSA Certificate vs. Old Form Under Section 65B(4)**

The BSA Section 63 certificate replaces but substantially continues the old Section 65B(4) certificate. The five mandatory contents identified by the Supreme Court in *Anvar P.V. v. P.K. Basheer* remain the core requirements. The key differences are structural: the BSA format is prescribed in Section 170, and the new statute uses "communication device" alongside "computer" to reflect modern technology. The issuer must still be a person in a responsible official position; the record must still be specifically identified; the device particulars must still be given; the statutory conditions must still be addressed; and the certificate must still be signed.

# 03

## When Must the Certificate Be Produced?

Charge-Sheet Stage vs. Trial Stage

### The Settled Timing Principle

For years, defence counsel argued that the Section 65B certificate must accompany the charge-sheet-that its absence at the filing stage was fatal to the prosecution's case. The Supreme Court settled this controversy decisively. In *State of Karnataka v. M.R. Hiremath*, the Court held that Section 65B(4) applies "where it is desired to give a statement in evidence"-meaning when the electronic record is actually sought to be produced and used at trial. The certificate is tied to the act of adducing evidence, not to the act of filing a police report.

*LAWWORLD 2019 KAR 071* applied this principle to call detail records, rejecting the contention that CDRs could not be relied upon for want of a certificate at the charge-sheet stage. The Karnataka High Court confirmed that the requirement of certification is to be considered "at the stage of adducing evidence while deciding admissibility of the electronic record, not at the stage of bail."

#### TIP

##### The Core Principle

The Section 63 certificate is triggered when the electronic record is formally tendered before the court-not when the Investigating Officer files the charge-sheet. These are two distinct procedural stages separated by months or years.

### Curable Defects vs. Fatal Defects

Understanding this distinction is critical for every practitioner. The Supreme Court in *LAWWORLD 2019 SC 0567* expressly characterised non-production of the certificate at the charge-sheet stage as a "curable defect." What does this mean in practice?

1. **Curable (absent at charge-sheet, produced at trial):** The electronic record is admissible. The certificate may be obtained and produced when the record is actually tendered in evidence. No fatal consequence follows from the earlier absence.
1. **Fatal (absent at trial altogether):** If the certificate is never produced by the time the electronic record is adduced, the record is inadmissible. Courts must eschew such evidence from consideration, as confirmed in *LAWWORLD 2022 SC 112* and *LAWWORLD 2023 KAR 0241*.

*LAWWORLD 2024 KAR 0825* applied this principle to a compact disc containing



electronic evidence, holding that the requisite certificate may be produced later "so long as the trial is not over, provided no serious or irreversible prejudice is caused to the accused." The court invoked Section 311 CrPC as a tool to advance truth-seeking without vitiating proceedings.

## **Oral Testimony Cannot Substitute**

One persistent defence argument is that the Investigating Officer or a witness can simply testify orally about how electronic records were generated and preserved. This argument fails. The Supreme Court in [LAWWORLD 2022 SC 0556](#) was emphatic: the Section 65B(4) certificate is a condition precedent to admissibility, and oral evidence in place of such certificate "cannot possibly suffice." Section 65B(4) is a mandatory requirement-its satisfaction cannot be achieved through oral testimony about the same facts.

[LAWWORLD 2015 KAR 1223](#) applied this principle to call detail records, holding that electronic secondary evidence "is inadmissible and incapable of being proved by oral testimony alone." The Karnataka High Court has consistently enforced this rule, refusing to admit CDRs, email printouts, or video recordings on the basis of oral assertions alone.

### **WARNING**

#### **No Shortcuts**

No amount of oral testimony about the computer system, the data's generation, or its preservation can substitute for the Section 63 certificate. The certificate is a statutory condition precedent-satisfy it or face inadmissibility.

## **Does Section 63 Change the Timing Rule?**

The new Section 63 preserves the substantive certification requirement from the old Section 65B(4). The statutory language-"a certificate... identifying the electronic record"-remains tied to the moment of adducing evidence. Nothing in the *Bharatiya Sakshya Adhiniyam 2023* suggests the certificate must be produced at the charge-sheet stage.

The eSakshya Management Rules, 2025 introduce a procedural refinement: the Investigating Officer generates the Section 63(4)(c) certificate through the eSakshya Mobile Application with eSign. This does not alter the timing rule-it simply streamlines how the certificate is obtained. The certificate must still be produced when the electronic record is adduced.

## **Checklist: Timing the Certificate**



# 04

## Consequences of a Defective Certificate

Missing, Incomplete, and Wrongly Issued Certificates

### **The Foundational Rule: No Certificate, No Admissibility**

*The Bharatiya Sakshya Adhiniyam 2023 preserves the mandatory-certificate rule that the Supreme Court and High Courts have enforced since Anvar P.V. v. P.K. Basheer. Section 63 requires a certificate for any secondary electronic record-printouts, copies, or outputs from a computer. Where no certificate is filed, the record cannot be received in evidence. This is not a mere procedural technicality; it is a condition precedent to admissibility.*

#### **LAWWORLD 2016 SC 117**

(2016) 4 SCC 737

*Call detail records printed from a telecom system are secondary electronic evidence. Without a Section 65B(4) certificate, they are inadmissible-even if the data was maintained in the ordinary course of business. Oral assertions cannot substitute for the statutory certificate.*

LawWorld ID: LAWWORLD 2016 SC 117

#### **LAWWORLD 2022 SC 0556**

(2022) 6 SCC 321

*The Section 65B(4) certificate is a mandatory condition precedent for secondary electronic records. Oral evidence in place of such a certificate 'cannot possibly suffice.' The Court confirmed this principle while considering call records tendered to prove motive.*

LawWorld ID: LAWWORLD 2022 SC 0556

#### **LAWWORLD 2023 KAR 0241**

2023 Cri LJ 2954 (Kar)

*Two CDs (video recording) and call detail records were held inadmissible for want of the mandatory certificate. The Court applied the Anvar-Arjun Panditrao principle and eschewed the electronic evidence from consideration, relying only on oral evidence about the recording.*

LawWorld ID: LAWWORLD 2023 KAR 0241

#### **WARNING**

#### **The Impossibility Doctrine**

In **LAWWORLD 2020 SC 0715**, the Supreme Court tempered the strict rule: where the certificate cannot be procured despite demand, the trial court may summon the appropriate person under Section 165 of the Evidence Act or use CrPC powers to secure it. However, this is a curative mechanism, not a licence to proceed without certification. The certificate remains mandatory; the court merely assists in obtaining it.

### **Three Categories of Defect**

Not every defect carries the same consequence. The retrieval pack and the statutory scheme support three distinct categories:

| <b>Defect Category</b>     | <b>Typical Examples</b>                                                                                                                         | <b>Consequence</b>                                                                                          |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Absent certificate         | No certificate filed at all; certificate filed only at charge-sheet stage                                                                       | Record inadmissible unless cured under the impossibility doctrine                                           |
| Incomplete certificate     | Omits device particulars; omits hash value; fails to describe the production process; signed by a person without proper knowledge of the system | Record inadmissible-the certificate does not satisfy Section 63's mandatory contents                        |
| Wrongly issued certificate | Names the wrong device; certificate signed by a person not in a responsible position relative to the device                                     | Record inadmissible-the certificate fails to identify the record or describe the correct production process |

#### **LAWWORLD 2014 SC 0967**

(2014) 6 SCC 164

The Supreme Court held that the Section 65B(4) certificate must identify the record, describe how it was produced, give device particulars, deal with the statutory conditions, and be signed by a person in a responsible official position. Failure on any of these elements renders the certificate non-compliant and the record inadmissible.

LawWorld ID: LAWWORLD 2014 SC 0967

#### **LAWWORLD 2015 KAR 0225**

2015 Cri LJ 3844 (Kar)

Call lists were held inadmissible because no Section 65B(4) certificate was produced, no telecom officials were examined, and there was no proof that the SIM cards belonged to the concerned persons. The certificate must establish the responsible-official link.

LawWorld ID: LAWWORLD 2015 KAR 0225

#### **LAWWORLD 2022 KAR 0972**

2022 Cri LJ 4526 (Kar)

Photographs and a CD were rejected because the photographer claimed to have taken only 8-9 photographs while many more were produced, no originals or negatives were filed, and no Section 65B certificate accompanied the secondary electronic evidence. The Court held that such evidence is not worthy of reliance.

## **Primary Evidence vs. Secondary: The Proper Custody Escape Route**

*The mandatory-certificate rule applies only to secondary electronic evidence. If the record is primary evidence-produced from proper custody in the form in which it was originally created-Section 63 does not require a certificate. This distinction is critical.*

### **LAWWORLD 2017 SC 0725**

(2017) 8 SCC 137

*A landline cassette on which ransom calls were recorded was handed over in original to the police. The Court held it was primary evidence, not secondary electronic record, and therefore did not require a Section 65B certificate. The conversation was admissible under Section 7 without Section 65B compliance.*

LawWorld ID: LAWWORLD 2017 SC 0725

*The practical implication: if the original WhatsApp phone is produced in court and the person in whose phone the chats appear testifies to their authenticity, the chats may be admissible as primary evidence without a Section 63 certificate. Chapter 5 of this book addresses this scenario in detail. However, once the record is exported, printed, or copied, it becomes secondary evidence and the certificate requirement revives.*

### **NOTE**

#### **eSakshya and the New Certificate Mechanism**

*Under the eSakshya Management Rules, 2025, Investigating Officers must generate the Section 63(4)(c) certificate through the eSakshya Mobile Application, and all certificates will be eSigned. This automated mechanism is designed to reduce defective certificates-but practitioners must still verify that the certificate identifies the correct record, describes the correct device, and is signed by a person with actual knowledge of the production process.*

## **Practical Checklist: Identifying a Defective Certificate**



# 05

## WhatsApp Chats: The Most-Litigated Digital Evidence

Original Device, Exported Chats, and Screenshots

### Why WhatsApp Chats Dominate Electronic Evidence Disputes

WhatsApp generates more admissibility challenges than any other digital evidence. The messaging platform stores conversations in multiple formats-on the device itself, in cloud backups, in exported files, and as screenshots-each triggering different evidentiary rules. A single criminal or civil proceeding may involve all three scenarios simultaneously, making WhatsApp evidence a microcosm of the entire BSA 2023 framework. Practitioners must identify which scenario applies before deciding whether a Section 63 certificate is required.

### Scenario 1: Chats from the Original Device

When the phone containing the WhatsApp conversation is produced in court, the chat history displayed on that device occupies a special evidentiary position. If the court is satisfied as to the record's authenticity-typically through testimony of the person in whose name the phone is registered or who used it-the chat qualifies as primary evidence under Section 57 Explanation 5. No Section 63 certificate is required in this situation because the original electronic record is before the court.

The key authority is the principle that electronic evidence produced from proper custody is primary evidence unless disputed. In *Shafhi Mohammad*, the Supreme Court clarified that the Section 65B certificate applies only where the party producing the electronic record is in possession of the device and able to issue the certificate. Where the original device is before the court, the certificate requirement does not arise.

#### TIP

#### Certificate Wording Not Required

For chats from the original device, no Section 63 certificate is needed. The Section 170 format is inapplicable. Instead, the party producing the phone must testify: (a) the phone is theirs or was in their possession; (b) the WhatsApp conversation is genuine; and (c) no tampering has occurred since seizure.

### Scenario 2: Exported Chats

When a WhatsApp conversation is exported-whether through email forwarding, the "Export Chat" feature, or a third-party forensic extraction-the resulting printout or PDF

is secondary electronic evidence. The export process creates a copy of the original record, triggering the Section 63 certificate requirement under BSA 2023.

The certificate must be issued by the person who performed the export. This is typically the Investigating Officer who extracted the chats, the forensic expert who used extraction tools, or the witness who forwarded the conversation via email. The certificate must identify the specific export performed, describe the device from which extraction occurred, and confirm the conditions under which the record was produced.

#### **WARNING**

##### **Who Cannot Issue the Certificate**

A person who merely received the exported chat cannot issue the Section 63 certificate. The certificate issuer must have personal knowledge of how the export was performed. If the Investigating Officer did not personally conduct the export, the forensic expert who did must issue the certificate.

For chats exported via the WhatsApp "Export Chat" feature, the certificate should state: the export was performed on the original device; the device was in police possession at the time; the export generated a PDF file; and the hash value of the exported file is provided. For chats forwarded via email, the certificate should identify the email account, confirm the forwarding was done from the original device, and provide the hash value of the attached conversation file.

### **Scenario 3: Screenshots**

Screenshots of WhatsApp conversations occupy the weakest evidentiary position. A screenshot is a photograph of a screen display-it captures the conversation at a point in time but does not preserve the underlying data structure. Courts treat screenshots as printed copies of electronic records, making them uniformly secondary evidence requiring a Section 63 certificate.

The certificate for screenshots must address the device on which the screenshot was taken, confirm the screenshot accurately represents the display at the time it was captured, and provide the hash value of the screenshot file. Where screenshots are taken by a witness, that witness must issue the certificate. Where the Investigating Officer seized screenshots from a phone, the IO must certify the extraction.

#### **NOTE**

Screenshots lack the metadata integrity of exported chats. They do not preserve the full WhatsApp data structure-only the visual representation. Courts scrutinise screenshots more heavily and may require corroboration from other evidence to establish authenticity.

### **Certificate Wording: Scenario-Specific Guidance**

| Scenario | Certificate Required? | Who Issues It | Key Certificate Elements |
|----------|-----------------------|---------------|--------------------------|
|----------|-----------------------|---------------|--------------------------|

|                                                            |                                                  |                                                 |                                                                                                    |
|------------------------------------------------------------|--------------------------------------------------|-------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <i>Original device produced in court</i>                   | <i>No - primary evidence from proper custody</i> | <i>N/A</i>                                      | <i>Testimony of device owner/user confirming authenticity</i>                                      |
| <i>Exported chat (email/WhatsApp export/forensic tool)</i> | <i>Yes - secondary electronic evidence</i>       | <i>Person who performed the export</i>          | <i>Device description, export process, hash value of exported file, confirmation of conditions</i> |
| <i>Screenshot taken from device</i>                        | <i>Yes - secondary electronic evidence</i>       | <i>Person who took or seized the screenshot</i> | <i>Device on which screenshot taken, timestamp, hash value of screenshot file</i>                  |



# 06

## Call Detail Records: Proving Telephonic Evidence

CDRs, Subscriber Info, and the Certificate Requirement

### CDRs as Secondary Electronic Evidence

Call detail records are among the most frequently tendered forms of electronic evidence in criminal trials-yet they are also among the most commonly rejected for non-compliance with the certification requirement. Under the Bharatiya Sakshya Adhiniyam 2023, a CDR is a computer-generated record produced from the telecom service provider's billing or network system. As a printed output from a computer, it is secondary electronic evidence and requires a Section 63 certificate.

#### **LAWWORLD 2016 SC 117**

Supreme Court, 2016

*Held that call detail records sought to be proved through printed computer-generated extracts required a Section 65B(4) certificate. Without it, the CDRs were inadmissible even though data was maintained in the ordinary course of business.*

LawWorld ID: LAWWORLD 2016 SC 117

#### **LAWWORLD 2022 SC 0556**

Supreme Court, 2022

*Held that the Section 65B(4) certificate is a condition precedent to admissibility of secondary electronic records; oral evidence cannot substitute for it; the requirement is mandatory.*

LawWorld ID: LAWWORLD 2022 SC 0556

#### **LAWWORLD 2022 SC 112**

Supreme Court, 2022

*In a death penalty review, the Court eschewed CDR-based circumstances for want of a Section 65B(4) certificate, but upheld the conviction on other evidence, illustrating that CDR exclusion does not automatically defeat the prosecution.*

LawWorld ID: LAWWORLD 2022 SC 112

#### **LAWWORLD 2022 SC 1135**

Supreme Court, 2022

*Held that CDRs produced without the requisite Section 65B certification could not advance the prosecution case, as the mobile phone belonging to the deceased was not properly identified and the call records were not proved in compliance with the statute.*

LawWorld ID: LAWWORLD 2022 SC 1135

## **The Karnataka High Court Jurisprudence**

*Karnataka High Court has been the most prolific commentator on CDR admissibility under the old Section 65B, and its rulings remain the most detailed practical guidance available. The pattern is consistent: CDRs produced as printed records without a Section 65B(4) certificate are inadmissible.*

### **LAWWORLD 2015 KAR 1223**

Karnataka High Court, 2015

*Held that call detail records and mobile phone printouts relied upon to prove last-seen evidence and telephonic contacts were inadmissible as secondary electronic evidence for want of a Section 65B(4) certificate identifying the record, describing production, devices, and compliance with Section 65B(2), signed by a responsible official.*

LawWorld ID: LAWWORLD 2015 KAR 1223

### **LAWWORLD 2015 KAR 0225**

Karnataka High Court, 2015

*Held that call lists of mobile phones of accused and deceased were inadmissible as secondary electronic evidence; no BSNL or Airtel officials were examined, no Section 65B(4) certificate was produced, and there was no proof that SIM cards belonged to the concerned persons.*

LawWorld ID: LAWWORLD 2015 KAR 0225

### **LAWWORLD 2022 KAR 0119**

Karnataka High Court, 2022

*Following Anvar P.V. v. P.K. Basheer, the Court held that total non-compliance with the Section 65B(4) certificate requirement meant the prosecution failed to prove the call records and they could not be used against the accused.*

LawWorld ID: LAWWORLD 2022 KAR 0119

### **LAWWORLD 2023 KAR 0924**

Karnataka High Court, 2023

*The trial court rightly declined to consider CDRs produced as Exhibits P-102 to P-111 without the mandatory Section 65B certificate; the High Court affirmed their exclusion but held that other evidence was sufficient to prove guilt.*

LawWorld ID: LAWWORLD 2023 KAR 0924

### **LAWWORLD 2023 KAR 0241**

Karnataka High Court, 2023

*Held that call detail records (Ex.P60, Ex.P61) were inadmissible for want of the mandatory Section 65B(4) certificate, following Anvar P.V. and Arjun Panditrao Khotkar.*

LawWorld ID: LAWWORLD 2023 KAR 0241

### **LAWWORLD 2025 KAR 0517**

Karnataka High Court, 2025

*CDRs were accepted where Section 65B certificates (Exs.P11, P34) issued by nodal officers*

were marked without objection and not challenged in cross-examination; the Court relied on CDRs to corroborate demand of bribe.

LawWorld ID: LAWWORLD 2025 KAR 0517

## **Call Data vs. Subscriber Information**

A critical distinction often overlooked is that between call data and subscriber information. Call data-the record of calls made and received-is electronic evidence stored on the service provider's computer system and requires a Section 63 certificate. Subscriber information-the identity of the person in whose name a phone number stands-is a different class of evidence. Subscriber details can be proved through the service provider's certificate under its seal, or through oral testimony of the subscriber, without triggering the Section 63 certificate requirement. Practitioners must ensure they obtain the correct certificate for the correct record: a certificate covering subscriber details does not authenticate call data, and vice versa.

### **WARNING**

#### **Two Records, Two Certificates?**

If the prosecution relies on both call data and subscriber information, it must obtain separate certifications or a single certificate that covers both records. A certificate that only addresses subscriber details will not validate call data.

## **Obtaining the Certificate from the Telecom Operator**

The Section 63 certificate for CDRs must be obtained from the telecom service provider. The issuer must be a person in a responsible position relative to the computer or communication device that generated the records-typically a nodal officer or authorised official designated by the service provider for this purpose.

### **LAWWORLD 2020 SC 0715**

Supreme Court, 2020

Directed cellular companies and ISPs to segregate and securely preserve CDRs and relevant records whenever a particular record is seized during investigation, noting that telecom and internet licences require service providers to archive CDRs, exchange detail records, and internet logs for at least one year.

LawWorld ID: LAWWORLD 2020 SC 0715

The certificate must identify the specific CDRs relied upon (by telephone number and date range), describe how they were produced from the service provider's billing or network system, give device particulars (the computer system and its configuration), confirm compliance with statutory conditions, and be signed by the responsible official. The Section 170 format requires the certificate to state the HASH value of the CDRs produced. For CDRs, the responsible official is typically the nodal officer or the authorized signatory of the telecom service provider-not the investigating officer.



**LAWWORLD 2018 SC 0424**

Supreme Court, 2018

*Endorsed summoning fresh CDRs with a proper Section 65B certificate and examining the telecom witness, holding that non-production of a Section 65B(4) certificate at an earlier stage is a curable defect relating to mode of proof.*

LawWorld ID: LAWWORLD 2018 SC 0424

**LAWWORLD 2017 SC 0724**

Supreme Court, 2017

*Held that an accused who raised no objection when CDRs were exhibited in the trial court cannot at the appellate stage challenge them for want of Section 65B(4) compliance, since objections to mode of proof must be taken when the document is tendered.*

LawWorld ID: LAWWORLD 2017 SC 0724

**CDR Certificate Checklist**

# 07

## **CCTV Footage and DVR Seizure: Chain of Custody in Practice**

Hash Values, Seizure, and the Certificate

### **Why CCTV Evidence Fails**

Courts have consistently excluded CCTV footage when the chain of custody breaks or when the Section 65B certificate is absent or defective. In [LAWWORLD 2025 KAR 1117](#), the Karnataka High Court held a CD inadmissible because the police left the factory before the extraction, the Investigating Officer never viewed the footage, and no Section 65B certificate was obtained. The footage was prepared by a private person on police instructions without forensic examination-a textbook chain-of-custody failure.

[LAWWORLD 2023 KAR 038](#) catalogues the recurring lapses: unreadable CDs, absent Section 65B certificates, failure to reconstruct critical footage periods, and no documentation of hash values. The Court issued directions requiring investigators to document playability tools, verify media before filing, and maintain proper storage conditions. These are not technical niceties-they are legal requirements that determine whether footage is receivable at all.

### **Seizure of DVRs and Hard Drives**

When seizing a DVR or hard drive, the seizure memo must record the device description, serial numbers, storage capacity, and the hash value of the stored footage at the time of seizure. [State of Karnataka v. Shivanna \(2006\)](#) held that literal compliance with seizure provisions is impossible for hard disks, so authorities must use scientific methods-copying the disk, obtaining hard copies, and affixing official seals on copies.

[LAWWORLD 2022 KAR 1160](#) and [LAWWORLD 2018 KAR 119](#) mandate specific precautions: disable security locks before seizure; submit media in sealed, anti-static, anti-magnetic packaging; store away from heat and humidity; create and preserve backup copies; and document every transfer in the chain of custody.

#### **WARNING**

##### **Common Seizure Mistakes**

No seizure mahazar for the DVR; no hash value recorded at seizure; DVR handled by multiple officers without documentation; storage media not sealed or preserved in anti-static conditions; backup copies not created.

## **The Section 63 Certificate for CCTV**

CCTV footage extracted from a DVR and copied to a CD, pen drive, or other medium is secondary electronic evidence. It requires a Section 63 certificate from a person in a responsible position relative to the computer or device that produced the footage. The certificate must identify the specific CCTV system, describe how the footage was extracted, give the hash value of the extracted footage, and confirm the system was operating properly.

**LAWWORLD 2022 KAR 113** excluded footage where the witness admitted lack of competence under the IT Act, possibility of editing, and inability to certify authenticity. The certificate issuer must have actual knowledge of the system and the extraction process-not merely sign a form prepared by others.

The hash value is the digital fingerprint that proves the footage has not been altered. Under the Information Technology Act 2000, Section 3, a hash function produces a unique output for each input; any change to the electronic record produces a different hash. The Section 63 certificate must record the hash value generated at the time of extraction so that any subsequent copy can be verified against it.

### **TIP**

#### **Certificate Must Match the Footage**

A certificate describing one extraction cannot cover a different batch of footage. If the prosecution relies on footage from 10:20 pm to 11:30 pm on a specific date, the certificate must identify that specific recording-not generically describe the DVR.

## **Three Common Scenarios**

### **Scenario 1: Shopowner's DVR**

A shopowner installs CCTV cameras and a DVR. The investigating officer seizes the DVR and sends it for forensic extraction. The shopowner or the forensic expert who performed the extraction may issue the Section 63 certificate. The certificate must identify the shop's CCTV system, describe the extraction method, give the hash value, and confirm the cameras were operational at the relevant time. If the footage is extracted by a private forensic laboratory, the certificate must be issued by a person with knowledge of the extraction process.

### **Scenario 2: Police Station CCTV**

Police station CCTVs often record onto networked servers or cloud storage. When the investigating officer in one case needs footage from another police station's CCTV, the certificate must come from the person responsible for that station's CCTV system.

**LAWWORLD 2021 KAR 0420** shows that even when CCTV footage is properly collected, it may have limited probative value if it does not show the actual offence-courts will not extend its weight beyond what the footage actually depicts.

### **Scenario 3: Footage from a Suspect's Phone**



*If a mobile phone containing CCTV footage is seized, the phone itself is the primary recording medium. **State of UP v. Rajesh (2017)** drew a distinction between primary and secondary evidence: the original phone with unaltered footage may be primary evidence if produced from proper custody, potentially not requiring a Section 63 certificate. However, if the footage is copied from the phone to another medium, the copy is secondary evidence requiring certification. The chain of custody must document who had the phone, when it was seized, and every transfer.*

### **Best Practice Checklist**

# 08

## **Emails, Bank Statements, and Screenshots**

### Proving Financial and Communication Records

#### **Emails: Tracing the Source to Determine the Rule**

*The admissibility of email records turns on where the record originates. Courts distinguish between emails obtained from the email service provider and emails printed from a party's own device. Each scenario triggers different evidentiary rules.*

*When the prosecution or a party obtains email records from the service provider-say, Gmail records exported through Google's legal processes-the printout is a computer output produced by Google's servers. This is secondary electronic evidence. A Section 63 certificate from a responsible Google official identifying the record, describing the export process, giving server particulars, confirming the conditions under which the system operated, and signing the certificate is mandatory. **The Karnataka High Court has confirmed** that objections to the absence of such a certificate are procedural and can be waived if not raised at trial-but practitioners should not rely on this waiver. Obtain the certificate.*

*When emails are printed from a party's own device-say, the accused's laptop or the complainant's phone-the analysis shifts. If the court is satisfied as to the authenticity of the record and it was produced from proper custody, the email printout may qualify as primary electronic evidence under Section 57 Explanation 5 of the BSA 2023. No Section 63 certificate is required in that event. The person in whose device the emails appear should testify, confirming the account, the device, and that the printout accurately reflects what was stored.*

#### **TIP**

##### **Email Evidence Checklist**

1. Identify the source: service provider export or device printout? 2. Service provider export Section 63 certificate required from the provider. 3. Device printout Is the person in whose device the emails appear available to testify? 4. If yes to (3) and the court is satisfied as to authenticity primary evidence, no certificate needed. 5. If no to (3) Section 63 certificate required from the person who printed the emails.

#### **Bank Statements: Two Routes, Two Rules**

*Bank statements can reach court by two distinct routes, and the evidentiary rule differs for each. Practitioners must identify which route applies before deciding how to prove the statement.*

The first route is the certified copy obtained directly from the bank, bearing the bank's official seal and the signature of a responsible bank officer. *The Supreme Court has held that Section 4 of the Bankers' Books Evidence Act makes a certified copy prima facie evidence of the existence and contents of entries-but it does not create any presumption as to the correctness of those entries or balances. A bank-certified statement under the Bankers' Books Evidence Act may be admissible without a Section 63 certificate because it is a certified document produced by the bank itself, not a computer output relied upon as secondary evidence. However, the bank must still independently prove the correctness of debit entries if disputed.*

The second route is the statement printed from online banking by the account holder or investigator. This is a computer output-a printed copy of electronic records stored in the bank's servers. It is secondary electronic evidence. A Section 63 certificate from a responsible bank official describing the online banking system, how the statement was generated, the device used, and confirming operational conditions is required. *In a Karnataka case involving ATM transaction extracts*, the High Court held that entries disbelieved for non-compliance with Section 65B(4) could not be linked to the ledger, and the bank was left unable to independently prove the debit entries.

#### **WARNING**

##### **Online Banking Statements**

Statements printed from net banking portals are secondary electronic evidence. They require a Section 63 certificate from a bank official who can describe the system that generated the statement. A customer's own printout, without a certificate, is inadmissible unless the court treats it as primary evidence from proper custody.

## **Screenshots: Primary or Secondary?**

Screenshots are among the most frequently produced-and most frequently challenged-forms of digital evidence. Their admissibility depends entirely on how they are tendered.

A screenshot taken from a mobile phone and produced in court by the person who took it may be treated as primary electronic evidence if the court is satisfied as to its authenticity. The person who captured the screenshot must testify, confirming the device, the account, and that the screenshot accurately reflects what appeared on screen. No Section 63 certificate is required.

A printed screenshot-meaning the screenshot has been printed on paper-is a printed copy of an electronic record. It is secondary electronic evidence. A Section 63 certificate from the person who printed it, identifying the device, describing the printing process, and confirming the conditions, is required. This is a common gap in practice: investigators print screenshots from a phone and rely on them without a certificate.



**NOTE**

**Key Distinction**

*Screenshot on phone primary evidence if person who took it testifies. Printed screenshot secondary evidence Section 63 certificate required.*

# 09

## Hash Values and Chain of Custody

Technical Safeguards for Digital Evidence Integrity

### What Is a Hash Value?

When any digital file—be it a WhatsApp chat export, a CCTV footage clip, a bank statement PDF, or a call detail record—is processed through a hash algorithm, the algorithm produces a fixed-length string of characters. Any change to the file, however minor, produces a completely different hash value. This property makes hash values the most reliable tool for verifying that electronic evidence has not been tampered with from the moment of seizure to the moment it is tendered in court.

| Algorithm | Bit Length | Legal Status               | Notes                                                               |
|-----------|------------|----------------------------|---------------------------------------------------------------------|
| SHA-256   | 256 bits   | Preferred                  | Strongest collision resistance; mandated by most forensic standards |
| SHA-1     | 160 bits   | Acceptable                 | Weaker than SHA-256; avoid where possible                           |
| MD5       | 128 bits   | Acceptable but less robust | Known vulnerabilities; use only when no other option available      |

Under the Information Technology Act 2000, Section 3(2), a hash function is defined as an algorithm that maps one sequence of bits into another, generally smaller, set such that an electronic record yields the same hash result every time the algorithm is executed with the same input. The IT Act further provides that it is computationally infeasible to derive the original record from the hash result or to produce two different records yielding the same hash result. This mathematical foundation makes hash values legally for integrity verification.

### Generating and Documenting Hash Values

Hash values must be generated at critical stages: at the time of seizure, before and after any extraction or copying, and before presentation in court. The Karnataka High Court in *State of Karnataka (2022)* directed that investigating officers must record the hash value of digital files, seal memory cards, and maintain chain of custody from the moment of seizure. Similarly, *LAWWORLD 2023 KAR 038* requires documenting hash values and verifying media on filing.

The Section 63 certificate must record the hash value of the specific record tendered, identify the algorithm used, and confirm that the hash value was verified. A certificate

that omits the hash value or records it incorrectly is defective. The certificate issuer must understand what hash value was generated, for which file, and at what stage. Generic certificates that do not identify the specific record by its hash value will not satisfy the statutory requirements.

**TIP**

**Hash Value Documentation Checklist**

Record hash value at seizure. Record hash value before extraction. Record hash value of the extracted copy. Record hash value of any copy made for court. State the algorithm used (SHA-256 preferred). Confirm in the Section 63 certificate that hash values match.

## **Chain of Custody: From Seizure to Court**

Chain of custody is the documented record of every person who handled the digital device or record, every transfer of possession, and every action performed on it. A break in chain of custody—where a device was handled by an undocumented person or where the handling is unexplained—goes to the weight and sometimes the admissibility of the evidence.

In **LAWWORLD 2025 KAR 1117**, the Karnataka High Court held that a CPU and storage device were inadmissible where there was no seizure mahazar, no PF entry, no sealing, no chain of custody, and the Investigating Officer did not speak to having seized or even seen them. The Court applied **Anvar P.V. v. P.K. Basheer** and held that without proper chain of custody, electronic evidence cannot be relied upon. This ruling makes clear that chain of custody is not a technical formality—it is a substantive requirement that determines whether digital evidence is receivable at all.

**WARNING**

**Consequences of Broken Chain of Custody**

A break in chain of custody does not automatically render evidence inadmissible, but it critically undermines its reliability. Courts may reject evidence entirely where the break is unexplained, the device was handled by unidentified persons, or the hash values cannot be matched. The defence can exploit any gap in the chain to challenge authenticity.

## **Practical Checklist for Practitioners**



# 10

## Cross-Examining the Certificate Issuer

Questions That Expose Defects and Doubt

### Who Signs the Certificate - and Why It Matters

The Section 63 certificate must be issued by "a person in a responsible position relative to the computer or communication device." In practice, this person is rarely a forensic expert. More often, it is a police officer who seized the device, a bank clerk who printed the statement, or a nodal officer at the telecom service provider who signed the certificate without ever touching the device. This gap between legal responsibility and actual knowledge is the foundation of every effective cross-examination of the certificate issuer.

#### WARNING

##### The Formality Problem

Courts have repeatedly noted that certificate issuers often treat the certificate as a bureaucratic formality. In [LAWWORLD 2022 KAR 113](#), the Karnataka High Court found that PW-3 admitted lack of competence under the Information Technology Act, possibility of editing the record, absence of anti-static protection, and inability to certify authenticity - yet a certificate had been issued. This is the weakness the cross-examiner must exploit.

The Supreme Court's landmark ruling in [LAWWORLD 2014 SC 0967](#) established that the Section 65B certificate must identify the record, describe how it was produced, give device particulars, deal with the statutory conditions, and be signed by a person in a responsible official position. The word "responsible" is not decorative. It demands that the issuer have genuine knowledge of the device and the process. Cross-examination is the advocate's tool to test whether that knowledge actually exists.

### Four Cardinal Weaknesses to Probe

Every effective cross-examination of the certificate issuer targets one or more of four structural weaknesses. These weaknesses are not speculation - they are documented in court rulings where certificate issuers have been compelled to admit the limits of their knowledge.

1. **Personal operation:** The issuer did not personally operate the device from which the record was produced. This is the most common weakness. The police officer who seized a phone rarely extracted the WhatsApp chats; the bank official who certified the statement rarely ran the query that generated it.
2. **Technical understanding:** The issuer cannot explain how the record was generated - what system produced it, what software was used, or what process created the data.

Without this understanding, the certificate attests to nothing the issuer actually knows.

3. **Working conditions:** The issuer cannot confirm that the computer or communication device was working properly at the relevant time. Section 63(1)(d) requires the certificate to state that the device was operating properly; if the issuer never checked, the statement is false.
4. **Hash value awareness:** The issuer does not know what a hash value is, cannot explain how it was computed, and did not verify that the hash value in the certificate matches the record produced. This is the technical foundation of integrity - and it is frequently absent.

#### NOTE

##### **The Hash Value Gap**

**LAWWORLD 2022 KAR 113** illustrates this weakness starkly: the certificate issuer admitted inability to certify authenticity and lacked competence under the IT Act. When the issuer cannot explain the hash value, the certificate does not establish that the record produced is the same record that was seized - a fatal gap in chain of custody.

## **Cross-Examination Question Bank**

The following questions are organised by the weakness they target. Use them selectively - cross-examination is not a script but a conversation with a purpose. Choose the questions that expose the specific gap in the specific issuer's knowledge.

### **Questions on Personal Operation**

- Did you personally operate the device from which this record was extracted? If not, who did?
- Were you present when the record was extracted from the device?
- Did you personally run the query or command that generated this record?
- Who in your organisation actually performed the extraction or export?
- Did you verify that the record produced was the record that existed on the device before extraction?
- Did you personally observe the process from start to finish, or did you rely on someone else's description?

### **Questions on Technical Understanding**

- Can you describe the system or software that generated this record?
- What is the name and version of the application that created this data?
- How does the system record the date and time - is it automatic or manual?
- Can you explain what metadata is attached to this record?
- What is the difference between the record content and the record's metadata?
- Did you check the metadata before signing the certificate?
- Do you know what the terms and conditions of the service say about record generation?



- *Can you describe the difference between primary storage and backup storage on this system?*

### **Questions on Working Conditions**

- *How do you know the device was operating properly at the time the record was generated?*
- *Did you personally check that the device was functioning correctly?*
- *What maintenance records do you maintain for this device?*
- *Can you produce any log showing the device was operational on the relevant date?*
- *Did the device undergo any repair, upgrade, or malfunction around the relevant period?*
- *Do you have any record of the device's system logs for the relevant date?*
- *What is your basis for stating the device was operating properly - personal knowledge or someone else's assurance?*

### **Questions on Hash Value**

- *What is a hash value?*
- *Which algorithm was used to generate the hash value in this certificate?*
- *Did you personally compute the hash value?*
- *How was the hash value computed - using what software or tool?*
- *How do you know that the hash value in the certificate matches the record now produced in court?*
- *Did you compare the hash value of the record now before the court with the hash value in the certificate?*
- *What happens if the hash values do not match?*
- *Can you demonstrate that the record before the court has not been altered since it was first extracted?*
- *Who generated the hash value - you or someone else?*
- *Do you have any documentation showing the hash value was generated at the time of extraction?*

### **Questions on the Certificate's Own Contents**

- *Did you read the certificate before signing it?*
- *Did you verify that the record described in the certificate is the same record now produced?*
- *Did you personally check each field in the certificate for accuracy?*
- *Were you aware that the certificate states the device was operating properly - and can you confirm that?*
- *Did you know that the certificate identifies a specific device - and are you certain this is the correct device?*
- *Did you have any independent basis for the statements in the certificate, or did you simply sign what was placed before you?*



## When to Attack the Certificate - and When to Attack the Record

The advocate must make a strategic choice: is the certificate the primary target, or is the underlying record's authenticity the better target? This choice depends on the facts and the available ammunition.

| Target the Certificate                                               | Target the Underlying Record                                                 |
|----------------------------------------------------------------------|------------------------------------------------------------------------------|
| Certificate is generic - does not identify the specific record       | Certificate is technically correct but the record itself is suspect          |
| Issuer has no personal knowledge of the device                       | Issuer has some knowledge but the record's provenance is unclear             |
| Certificate omits the hash value or gives wrong hash                 | Hash value is present but chain of custody is broken                         |
| Certificate signed by an inappropriate person                        | Certificate is fine but other evidence contradicts the record                |
| The defect is curable - the prosecution can file a fresh certificate | The record is incomplete, inconsistent, or unauthenticated by other evidence |

### TIP

#### Strategic Note

**LAWWORLD 2025 KAR 0517** demonstrates when the certificate should not be the primary target. The certificates under Section 65B were issued by nodal officers and were marked without objection - and the defence failed to challenge them in cross-examination. The court held that their validity could not later be questioned. If the certificate was not objected to at the stage of adducing evidence, attacking it later is futile. The better strategy was to challenge the weight of the record itself.

Conversely, **LAWWORLD 2022 KAR 0972** shows when the certificate is the right target. The photographer claimed to have taken only 8-9 photographs, yet many more were produced. No original or negatives were produced. No Section 65B certificate was filed. The Karnataka High Court held that secondary electronic evidence without a Section 65B(4) certificate is not worthy of reliance, and the trial court ought not to have based its remarks on such inadmissible evidence. Here, the certificate defect was fatal.

## Challenging the Issuer Who Admits Nothing

What if the certificate issuer is well-briefed, answers confidently, and does not admit any gap in knowledge? The cross-examiner must then shift strategy.

- **Put the certificate in evidence:** Ask the issuer to read the certificate aloud and confirm each statement. Often, the issuer will paraphrase rather than read, which allows the advocate to put the exact words on record.
- **Explore the process:** Even a confident issuer may not know the details of how the record was generated. Ask about the specific query parameters, the time window, the data fields, and the export format. Technical specificity often exposes gaps.
- **Challenge the chain of custody:** Ask who handled the device between seizure and extraction, who transferred the record, and who preserved it. Each link in the chain is a potential weakness.

- **Refer to the metadata:** Ask the issuer to explain the metadata fields in the record. If the issuer cannot do so, the certificate's claim of authenticity is undermined.
- **Invoke the Examiner of Electronic Evidence:** Under Section 45A of the Evidence Act (applicable through the BSA 2023 framework), the court may appoint an Examiner of Electronic Evidence. If the issuer's testimony is technically inadequate, consider requesting such appointment.

**NOTE**

**The Examiner of Electronic Evidence**

Section 79A of the Information Technology Act 2000 empowers the Central Government to notify an Examiner of Electronic Evidence. *LAWWORLD 2020 SC 0715* noted that an accused who wishes to challenge electronic evidence may wish to do so through an Examiner of Electronic Evidence under Section 45A. If the certificate issuer's testimony is inadequate, requesting the appointment of the Examiner is a powerful alternative.

## **Cross-Examination Checklist**

# 11

## Objections Strategy for the Defence

Grounds, Timing, and Argument

### Grounds for Objection

The defence has five distinct grounds to challenge electronic evidence. Each ground requires a different response from the prosecution and carries different consequences if upheld.

| Ground                | What the Defence Alleges                                                                         | Leading Authority                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| No Certificate        | The electronic record is secondary evidence and no Section 63 certificate has been produced      | LAWWORLD 2022 KAR 0119 - CDRs excluded for total non-compliance              |
| Defective Certificate | A certificate exists but is substantively deficient - missing hash value, wrong device, unsigned | LAWWORLD 2022 KAR 0972 - photographs excluded for want of proper certificate |
| Wrong Certificate     | The certificate describes a different device or record from the one tendered                     | LAWWORLD 2023 KAR 0241 - CD and CDR both excluded for certificate defects    |
| Inappropriate Person  | The certificate is signed by someone without knowledge of or responsibility for the system       | LAWWORLD 2022 KAR 0972 - photographer not in responsible position            |
| Improper Preservation | The record was not preserved in proper custody; chain of custody is broken                       | LAWWORLD 2022 KAR 0972 - no original or negatives produced                   |

The first two grounds-absence of a certificate and a defective certificate-are the most common. The distinction matters: if no certificate is produced at all, the record is inadmissible and the prosecution cannot cure the defect at the appellate stage. If a defective certificate is produced, the court may, in some circumstances, permit correction under Section 311 CrPC.

### Timing: When to Object

The certificate must be produced when the electronic record is actually adduced as evidence at trial-not when the charge-sheet is filed. In *Sonu alias Amar v. State of Haryana*, the Supreme Court confirmed that Section 65B(4) applies "where it is desired to give a statement in evidence" and that non-production at the charge-sheet stage is a curable defect. The prosecution cannot be penalised for failing to produce the certificate before the trial begins.

However, the defence must object when the record is actually tendered. In *Sonu alias*



*Amar*, the Supreme Court held that an accused who raised no objection when CDRs were exhibited in the trial court cannot raise the objection at the appellate stage, since this goes only to the mode or method of proof. Failure to object promptly waives the procedural requirement.

**WARNING**

**Charge-Sheet Stage vs. Trial Stage**

Do not file objections to electronic evidence in the charge-sheet. Object when the record is actually tendered during trial. An objection at the charge-sheet stage is premature and may be ignored.

## **How to Frame the Objection**

A successful objection is specific. It must (a) identify the electronic record by its exhibit number, (b) cite the specific provision of BSA 2023 that is violated, (c) state the exact deficiency, and (d) state the consequence sought-usually that the record be excluded from consideration.

- Identify the exhibit: "The prosecution seeks to rely on Ex.P-11, a call detail record."
- Cite the provision: "Section 63 of the Bharatiya Sakshya Adhiniyam 2023 requires a certificate for secondary electronic evidence."
- State the deficiency: "No certificate under Section 63 has been produced. The record is therefore inadmissible."
- State the consequence: "We submit that Ex.P-11 cannot be received in evidence and must be excluded from consideration."

Vague objections-"this document is inadmissible"-are easily deflected. Specific objections force the court to rule on the exact issue and create a clean record for appeal.

## **Sample Objections**

### **WhatsApp Chats Without a Certificate**

Scenario: The prosecution produces a printout of WhatsApp chats (Ex.P-5) but no Section 63 certificate accompanies it.

Objection: "The document at Ex.P-5 is a printed copy of an electronic record-secondary electronic evidence under Section 63 BSA 2023. Section 63 requires a certificate from a person in a responsible position relative to the device. No such certificate has been produced. In *the CD and CDR case*, this Court held that electronic records without the mandatory certificate are inadmissible. We submit Ex.P-5 cannot be received and must be excluded."

### **CDRs Without a Telecom Certificate**

Scenario: The prosecution produces call detail records (Ex.P-102) obtained from the telecom service provider but the certificate is signed by a police officer, not a nodal officer of the telecom company.

Objection: "Ex.P-102 is a call detail record generated by [service provider]. The certificate (Ex.P-103) is signed by [name], a police officer, not a person in responsible position relative to the service provider's computer system. In *the CDR case*, this Court held that Section 65B(4) requires a certificate from the person responsible for the system that generated the record. The certificate is therefore defective and Ex.P-102 is inadmissible."

### **CCTV Footage with a Defective Hash Value**

Scenario: The prosecution produces CCTV footage (Ex.P-20) with a certificate that states the hash value as "MD5: 123456" but does not identify the algorithm used or confirm that the footage produced matches the original.

Objection: "Section 63(1)(c) and Section 170 of BSA 2023 require the certificate to identify the record and confirm its integrity through a hash value. The certificate for Ex.P-20 does not specify the hash algorithm, does not confirm that the footage on the disc matches the original recording, and does not describe the extraction process. In *the photograph case*, this Court held that secondary electronic evidence without a proper Section 65B(4) certificate is not worthy of reliance. We submit Ex.P-20 is inadmissible for want of a proper certificate."

### **When Not to Object: Challenging Weight**

Sometimes the certificate is technically adequate but the underlying evidence is weak. In such cases, objecting to admissibility wastes the objection and signals to the court that the defence is fighting form over substance.

In *LAWWORLD 2025 KAR 0517*, the Karnataka High Court accepted CDRs where the certificates were issued by nodal officers, not challenged in cross-examination, and the defence failed to dislodge their genuineness. The court assessed the weight of the evidence-not just its admissibility.

#### **TIP**

#### **Weight vs. Admissibility**

If the certificate is technically sufficient but the evidence is incomplete, uncorroborated, or internally inconsistent, do not object to admissibility. Instead, argue weight: the record is admissible but carries little or no probative value. This argument survives even if the certificate is not attacked.

# 12

## Admissibility vs. Probative Value

When the Record Is In but the Case Is Not Made

### How Courts Assess Probative Value

Once an electronic record is admitted, courts assess its probative value by asking whether it proves what it purports to prove. The analysis has four dimensions.

#### 1. Corroboration

Electronic evidence that stands alone-without independent corroboration-carries less weight than a record that is consistent with other evidence. The Karnataka High Court in 2022 examined a case where CDRs were excluded for want of a certificate; the Court noted that even if the CDRs had been admissible, they would have required corroboration linking the accused to the specific mobile device. A bare call record showing calls between two numbers does not, by itself, prove who used those phones. Courts require additional evidence-device seizure memos, testimony linking the accused to the device, or subscriber records-to give call data probative value.

#### **LAWWORLD 2022 KAR 0119**

Karnataka High Court, 2022

Call detail records produced without a Section 65B certificate cannot be relied upon. Even if certified, call data alone cannot link an accused to a mobile number without additional evidence of device ownership or possession.

LawWorld ID: LAWWORLD 2022 KAR 0119

#### 2. Completeness of the Record

Courts scrutinise whether the electronic record is complete or selectively produced. In 2015, the Supreme Court considered a voice recording that was inaudible and could not be analysed by the Forensic Science Laboratory; the Court held that without the source recording being analysed, a translated version carries no weight. Selectively cropped photographs, partially produced chat threads, or CDRs covering only the period most favourable to one party invite scepticism. Courts ask: was the record produced in full, or was it edited before production?

#### **LAWWORLD 2015 SC 018**

Supreme Court, 2015

Source and authenticity are the two key factors for electronic evidence. When the voice recorder itself is not analysed, there is no basis for relying on a translated version of its contents.



### **3. Metadata and Internal Consistency**

Metadata-the embedded data showing when a file was created, modified, or transmitted-can confirm or undermine a record's reliability. Courts examine whether metadata is consistent with the timeline alleged by the prosecution. A WhatsApp message purportedly sent on a date when the sender's phone was in police custody, or a photograph whose metadata shows a different location than claimed, will be given little weight. Section 86 of the BSA 2023 creates a presumption in favour of secure electronic records, but this presumption applies only where the record is genuinely secure and unaltered.

#### **Bharatiya Sakshya Adhiniyam 2023 - Section 86**

*In any proceeding involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.*

### **4. Chain of Custody**

A break in the chain of custody does not automatically render electronic evidence inadmissible, but it significantly reduces weight. If a mobile phone was seized but not sealed, if the DVR was handled by multiple persons without documentation, or if the hash value at seizure differs from the hash value at production, courts will question whether the record presented is the same record that was originally seized. The Karnataka High Court in 2022 found that a TV-9 sting CD was inadmissible because only a copy without the primary source was produced and its authenticity could not be certified; the Court declined to give any weight to the secondary copy.

#### **LAWWORLD 2022 KAR 113**

Karnataka High Court, 2022

*A CD copy of electronic evidence produced without the primary source or compliant Section 65B certification is inadmissible. Even if it had been admissible, the absence of antistatic protection, possibility of editing, and inability to certify authenticity would render it unsafe to rely upon.*

LawWorld ID: LAWWORLD 2022 KAR 113

### **When Admissibility Alone Is Not Enough**

The most instructive cases are those where courts admitted electronic evidence but declined to give it weight-or where courts excluded it but still upheld convictions. In 2022, the Supreme Court considered a death penalty review where CDRs produced without a Section 65B(4) certificate had to be eschewed from consideration. The Court held that the circumstances derived from those CDRs "must not be taken into account." Yet the conviction was upheld because all other evidence-recoveries, financial transactions, intercepted messages, and ballistic linkage of weapons-cumulatively proved guilt beyond reasonable doubt. The CDRs were inadmissible, but even had they been admitted, the prosecution would still have needed corroboration linking the

accused to the specific mobile device.

### **LAWWORLD 2022 SC 112**

Supreme Court, 2022

*CDRs produced without the mandatory Section 65B(4) certificate must be eschewed from consideration. However, all other proved circumstances-recoveries, financial transactions, intercepted messages, and ballistic linkage-remain unaffected and cumulatively prove guilt beyond reasonable doubt.*

LawWorld ID: LAWWORLD 2022 SC 112

Conversely, in 2023, the Karnataka High Court excluded CDRs for want of a certificate but held that their exclusion did not adversely affect the prosecution, as other evidence on record was sufficient to prove guilt. The lesson is clear: electronic evidence is rarely the sole prop of a prosecution case. Courts assess the record in the context of all evidence tendered.

### **LAWWORLD 2023 KAR 0924**

Karnataka High Court, 2023

*CDRs produced without the mandatory Section 65B certificate could not be relied upon, but their exclusion did not adversely affect the prosecution as other evidence was sufficient to prove guilt beyond reasonable doubt.*

LawWorld ID: LAWWORLD 2023 KAR 0924

### **WARNING**

#### **Prosecutor's Warning**

*A properly certified electronic record is necessary but not sufficient. Build corroboration. Link the device to the accused. Establish the timeline through metadata. Document the chain of custody. Without these, even an admissible record may carry no weight.*

## **Practical Guidance: Admissibility or Weight?**

The decision to challenge electronic evidence on admissibility grounds or to accept admissibility and challenge weight depends on the facts. The following framework helps practitioners choose the right strategy.

| Scenario                                                          | Challenge     | Rationale                                                                                                                                               |
|-------------------------------------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| No Section 63 certificate filed                                   | Admissibility | Without the mandatory certificate, secondary electronic evidence is inadmissible under Section 63. This is a threshold objection that ends the inquiry. |
| Defective certificate (wrong device, no hash, wrong signatory)    | Admissibility | A defective certificate fails to satisfy Section 63 requirements. The record cannot be received.                                                        |
| Certificate present but record incomplete or selectively produced | Weight        | Once admitted, challenge the record's completeness. Argue that selective production undermines reliability.                                             |

|                                                        |               |                                                                                                                                               |
|--------------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Record admitted but uncorroborated</i>              | <i>Weight</i> | <i>Argue that the record, standing alone, does not prove the case. Request the court to assess weight in light of corroborating evidence.</i> |
| <i>Metadata inconsistent with prosecution timeline</i> | <i>Weight</i> | <i>Challenge the internal consistency of the record. Point out metadata discrepancies.</i>                                                    |
| <i>Chain of custody broken</i>                         | <i>Weight</i> | <i>Even if the court admits the record, argue that breaks in chain of custody undermine its reliability.</i>                                  |

#### **TIP**

#### **Defence Counsel's Tip**

*Before objecting to admissibility, ask: if the record is excluded, does the prosecution still have a case? If yes, object on admissibility. If no, consider accepting admissibility and attacking weight instead. A successful admissibility objection that is reversed on appeal can be devastating; a weight argument that fails merely results in the court giving the evidence little weight.*

## **Seeking Further Directions When Evidence Is Suspect**

*There will be cases where electronic evidence is formally admissible but its integrity is genuinely suspect—where metadata is missing, chain of custody is unclear, or the record's provenance cannot be established. In such situations, practitioners may request the court to direct further investigation or to require the opposing party to produce additional evidence establishing authenticity.*

*Section 55 of the BSA 2023 requires oral evidence to be direct, and Section 57 Explanations 4 through 7 expand the definition of primary electronic evidence to include records stored simultaneously in multiple files or storage spaces. Courts have discretion to require additional proof where the electronic record's integrity is in doubt, even after admissibility is established. A party seeking further directions should file a specific application identifying the precise deficiency—missing hash values, undocumented transfers, absence of metadata—and requesting the court to direct the producing party to establish authenticity through additional evidence or expert testimony.*



# 13

## Model Certificates

Ready-to-Use Templates for Every Media Type

### Introduction: Why Templates Must Be Tailored

A Section 63 certificate is not a formality. Courts have consistently held that a certificate must identify the specific record, describe how it was produced, give device particulars, and be signed by a person with proper knowledge. A generic certificate that omits the hash value, misidentifies the device, or fails to describe the production process is defective and renders the electronic record inadmissible under Section 62 read with Section 63. The four templates below are starting points-not substitutes-for a certificate tailored to the facts of each case.

#### WARNING

##### The Golden Rule

No two digital evidence scenarios are identical. The certificate must describe the specific device, the specific record, and the specific process by which that record was produced. A certificate that could apply to any record is a certificate that applies to none.

### Template 1: WhatsApp Chat - Exported Conversation

| Certificate Field     | Content / Wording                                                                                                                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Title     | CERTIFICATE UNDER SECTION 63(1) READ WITH SECTION 170, BHARATIYA SAKSHYA ADHINIYAM, 2023                                                                                                                                                                                |
| Record Identification | The electronic record described herein is a WhatsApp conversation exported from the mobile phone bearing IMEI No. [XXXX], model [XXXX], belonging to [Name], on [Date] at [Time]. The conversation is between [Name of Sender] and [Name of Recipient] dated [Date(s)]. |
| Device Description    | Device: [Brand, Model] Smartphone; IMEI: [XXXX]; SIM: [Service Provider]; Operating System: [Android/iOS Version].                                                                                                                                                      |
| Production Process    | The conversation was exported using the WhatsApp Chat Export feature (via email) on [Date] at [Time] by [Name, Designation] from the original device. The exported file was saved as [filename.pdf] and printed on [Date].                                              |
| Hash Value            | SHA-256 Hash Value of exported file: [alphanumeric string]. Hash generated using [software name and version].                                                                                                                                                           |

|                      |                                                                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Statutory Conditions | The computer system (mobile phone) was operating properly at the time of export. The data was generated, stored, and transmitted in the ordinary course of business by the WhatsApp application. |
| Issuer Details       | Name: [Full Name]; Designation: [Responsible Position]; Organisation: [Name]; Date: [Date]; Signature: [Signature].                                                                              |

#### NOTE

#### Annotation: Key Fields Explained

Record Identification must name the specific conversation, parties, and date-not merely say 'WhatsApp chat'. Device Description must give the IMEI and model. Production Process must identify who performed the export and how. Hash Value must use SHA-256 (preferred) or at minimum MD5, and must match the printed record.

#### WARNING

#### Common Errors to Avoid

1. Omitting the hash value entirely. 2. Describing the device only as 'mobile phone' without IMEI. 3. Failing to name the person who performed the export. 4. Using the same certificate for chats from different devices or dates. 5. Signing without personal knowledge of the export process.

- Variation - Forensically Extracted Chats: Replace 'WhatsApp Chat Export feature' with 'UFED 4PC forensic tool version [X]' and add a note that extraction was performed by [Name, Forensic Expert] on [Date].
- Variation - Screenshots: If the record is a screenshot (not exported chat), state 'Photograph of WhatsApp conversation taken on [Date] from the original device' and include the screenshot file hash.
- Variation - Chats from Third-Party Device: If the phone was seized by police, the certificate issuer is the Investigating Officer who seized and exported the chats, not the phone owner.

## Template 2: Call Detail Records - Telecom Operator

| Certificate Field     | Content / Wording                                                                                                                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Title     | CERTIFICATE UNDER SECTION 63(1) READ WITH SECTION 170, BHARATIYA SAKSHYA ADHINIYAM, 2023                                                                                                                                                 |
| Record Identification | The electronic record described herein is a Call Detail Record (CDR) generated by [Service Provider Name] for mobile number [XXXX] for the period from [Date] to [Date], requested under [Section 92 CrPC / Section 5(2) Telegraph Act]. |
| Device Description    | System: [Service Provider] Centralised Server; Location: [Data Centre]; Generation Method: Automated call logging by [Billing System Name, Version].                                                                                     |

|                      |                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Production Process   | The CDR was generated and printed on [Date] at [Time] by [Name, Designation, Service Provider] in response to official request dated [Date]. The printed record is a true and unaltered output of the automated system. |
| Hash Value           | SHA-256 Hash Value of CDR file: [alphanumeric string]. Hash generated on [Date] using [software].                                                                                                                       |
| Statutory Conditions | The system that generated the CDR was operating properly at all material times. The data was stored in the ordinary course of business by the automated billing and call logging system.                                |
| Issuer Details       | Name: [Full Name]; Designation: [Nodal Officer / Authorized Signatory]; Organisation: [Service Provider Name]; Date: [Date]; Signature: [Signature]; Seal: [Official Seal].                                             |

#### NOTE

##### **Annotation: Who May Issue This Certificate**

The certificate must be issued by a person in a responsible position relative to the telecom operator's system-not the Investigating Officer. Typically, this is the Nodal Officer or an authorized official designated by the service provider. The issuer must have personal knowledge of how CDRs are generated and stored.

#### WARNING

##### **Common Errors to Avoid**

1. Certificate issued by the Investigating Officer instead of the telecom operator. 2. No hash value for the CDR file. 3. Describing the device as 'computer' without identifying the specific server system. 4. Omitting the period covered by the CDR. 5. No official seal or designation of the issuer.

- **Variation - CDR from Police Request:** If the CDR was obtained through a police request under Section 92 CrPC, reference the request date and number in the Production Process field.
- **Variation - Subscriber Information Only:** Subscriber details (name, address, SIM number) may not require a Section 63 certificate if proved by other means. The certificate is mandatory for call data (dates, times, duration, tower location).
- **Variation - CDR Already Filed with Charge-Sheet:** If the certificate was not filed with the charge-sheet, it can be produced later at the stage of adducing evidence-this is a curable defect per *Anvar P.V.* .

### **Template 3: CCTV Footage - DVR Extraction**

| Certificate Field | Content / Wording                                                                        |
|-------------------|------------------------------------------------------------------------------------------|
| Certificate Title | CERTIFICATE UNDER SECTION 63(1) READ WITH SECTION 170, BHARATIYA SAKSHYA ADHINIYAM, 2023 |



|                       |                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Record Identification | The electronic record described herein is CCTV footage extracted from Digital Video Recorder (DVR) bearing Serial No. [XXXX], located at [Premises Address], covering the date [Date] and time period [Time Start] to [Time End]. |
| Device Description    | Device: [Brand, Model] DVR; Serial No.: [XXXX]; Storage Capacity: [X TB]; Camera Channels: [X]; Location: [Address].                                                                                                              |
| Production Process    | The footage was extracted on [Date] at [Time] by [Name, Designation] using [software, e.g., DVR Player version X]. The specific clip covering [Date, Time] was exported as [filename.mp4] and copied to [storage medium].         |
| Hash Value            | SHA-256 Hash Value of extracted footage file: [alphanumeric string]. Hash verified on [Date] using [software].                                                                                                                    |
| Statutory Conditions  | The CCTV system was operating properly at all material times. The footage was stored in the ordinary course of business on the DVR's hard drive. The system was not tampered with during the relevant period.                     |
| Issuer Details        | Name: [Full Name]; Designation: [Responsible Position, e.g., Shop Owner / Security Manager]; Organisation: [Name of Establishment]; Date: [Date]; Signature: [Signature].                                                         |

#### NOTE

##### **Annotation: Chain of Custody Is Critical for CCTV**

CCTV footage is inadmissible if the chain of custody is broken. The certificate must confirm that the DVR was in proper custody from seizure to extraction, and that no tampering occurred. If the DVR was in police possession, document every transfer in the seizure memo.

#### WARNING

##### **Common Errors to Avoid**

1. No hash value for the extracted footage file. 2. Certificate issued by a police officer who did not personally extract the footage. 3. Describing the device only as 'CCTV camera' without identifying the DVR. 4. Failing to state the specific date and time period covered. 5. No documentation of the chain of custody from seizure to extraction.

- **Variation - Police Station CCTV:** If the CCTV belongs to a police station, the certificate issuer is the Station House Officer or a designated officer who can confirm the system was operational and the footage was properly extracted.
- **Variation - Footage from Mobile Phone:** If footage was recorded on a mobile phone (e.g., by a witness), the certificate must describe the phone (IMEI, model), how the footage was recorded, and the hash value of the video file.
- **Variation - Forensic Extraction:** If a forensic expert extracted the footage, include the expert's name, qualification, tools used (e.g., FTK Imager), and the forensic hash value.

## Template 4: Bank Statement - Online Banking Printout

| Certificate Field     | Content / Wording                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Title     | CERTIFICATE UNDER SECTION 63(1) READ WITH SECTION 170, BHARATIYA SAKSHYA ADHINIYAM, 2023                                                                                                                                                           |
| Record Identification | The electronic record described herein is a bank statement for Account No. [XXXX] held at [Bank Name, Branch] for the period from [Date] to [Date], printed from the bank's online banking portal on [Date].                                       |
| Device Description    | System: [Bank Name] Core Banking System / Online Banking Portal; Server Location: [Bank Data Centre]; Generation Method: Automated account statement generation.                                                                                   |
| Production Process    | The statement was printed on [Date] at [Time] by [Name, Account Holder / Authorised Signatory] from the online banking portal after logging in with credentials. The printed record is a true and unaltered output of the bank's automated system. |
| Hash Value            | SHA-256 Hash Value of statement file (PDF): [alphanumeric string]. Hash generated on [Date] using [software].                                                                                                                                      |
| Statutory Conditions  | The bank's core banking system was operating properly at all material times. The account data was stored and generated in the ordinary course of banking business.                                                                                 |
| Issuer Details        | Name: [Full Name]; Designation: [Account Holder / Authorised Signatory]; Organisation: [N/A if individual]; Date: [Date]; Signature: [Signature].                                                                                                  |

### NOTE

#### Annotation: Bank-Certified vs. Online Statement

A bank statement certified under the bank's official seal (issued by the bank as a formal document) may not require a Section 63 certificate. However, a statement printed from online banking by the account holder is secondary electronic evidence and requires certification. The certificate must confirm the statement was printed from the bank's official portal.

### WARNING

#### Common Errors to Avoid

1. Treating an online banking printout as primary evidence without certification. 2. No hash value for the statement file. 3. Certificate issued by the account holder without describing the bank's system. 4. Failing to identify the specific account number and period. 5. Confusing a bank-certified statement (no Section 63 needed) with an online printout (Section 63 required).

- **Variation - Bank Issues Certified Statement:** If the bank issues the statement under its official seal, no Section 63 certificate is needed. The bank official's testimony confirming the statement was issued from official records suffices.

- *Variation - Third-Party Obtains Statement: If a third party (e.g., police or creditor) obtains the statement, the certificate issuer is the bank's authorized officer who printed the statement from the bank's system.*
- *Variation - Multiple Accounts: Each account statement requires a separate certificate. A single certificate cannot cover statements from multiple accounts.*

### ***Certificate Drafting Checklist***



# 14

## Seizure Memo Formats and Advocate Checklist

Preserving Digital Evidence from the Outset

### Model Seizure Memo for Digital Devices

| Field                     | Details to Record                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Case / FIR Details        | Case Number: ____   FIR No.: ____   Date: ____   Police Station: ____   Investigating Officer: ____                                                                                                                          |
| Device Description        | Type (mobile/laptop/DVR/pendrive): ____   Make: ____   Model: ____   Serial No.: ____   IMEI (if mobile): ____   Colour: ____   Any identifying marks: ____                                                                  |
| Condition at Seizure      | Device power state (on/off/locked): ____   Screen lock type (PIN/pattern/password/biometric): ____   Physical condition (new/good/damaged): ____   Accessories seized (charger/cable/case): ____                             |
| Hash Value at Seizure     | Algorithm used (SHA-256 preferred): ____   Hash value of full device image or relevant partition: ____   Tool used (e.g., FTK Imager, AXIOM): ____   Operator name and designation: ____   Date and time hash computed: ____ |
| Seizure Location and Time | Address/Location: ____   Date: ____   Time: ____                                                                                                                                                                             |
| Witnesses                 | Name 1: ____   Signature: ____   Name 2: ____   Signature: ____                                                                                                                                                              |
| Storage Location          | Where device will be stored (sealed bag/anti-static pouch/climate-controlled safe): ____   Location address: ____                                                                                                            |
| Security Lock Status      | Whether lock was disabled before seizure (yes/no): ____   Method used: ____   Officer who disabled: ____                                                                                                                     |
| Custodian at Seizure      | Name: ____   Designation: ____   Signature: ____   Date and time: ____                                                                                                                                                       |

#### WARNING

##### Common Seizure Failures

Do not leave the hash value blank. Do not describe the device generically as "one mobile phone." Do not omit the IMEI for mobile phones. Do not forget to record whether the screen lock was disabled and how. Each omission creates a gap in the chain of custody that the defence will exploit.

## Chain of Custody Transfer Template

The seizure memo captures the first link. Every subsequent transfer of the device requires its own entry. Use this template for every handoff—from IO to forensic expert, from forensic expert to court, from court to counter-section.

| Transfer Entry                  | Details                                                                                 |
|---------------------------------|-----------------------------------------------------------------------------------------|
| Transfer No.                    | ___                                                                                     |
| Date and Time of Transfer       | ___                                                                                     |
| Releasing Custodian             | Name: ___   Designation: ___   Reason for transfer: ___                                 |
| Receiving Custodian             | Name: ___   Designation: ___   Organisation: ___                                        |
| Hash Value at Transfer          | Algorithm: ___   Hash value: ___   Verified by (name and signature): ___                |
| Condition of Device at Transfer | Power state: ___   Seal status (intact/broken): ___   Any visible damage: ___           |
| Purpose of Transfer             | ___ (e.g., forensic imaging / court production / analysis)                              |
| Mode of Storage During Transfer | ___ (e.g., anti-static bag, sealed cover)                                               |
| Witness to Transfer             | Name: ___   Signature: ___                                                              |
| Return to Previous Custodian    | Date: ___   Hash verified: ___   Condition noted: ___   Signatures of both parties: ___ |

### NOTE

#### Seal Integrity

Every time a device changes hands, verify that the tamper-evident seal applied at the previous transfer is intact. If the seal is broken, document the break, photograph it, recompute the hash, and record the discrepancy before proceeding. A broken seal without explanation is a chain-of-custody break that courts will not overlook.

## Storage and Preservation Standards

Karnataka High Court in [LAWWORLD 2022 KAR 1167](#) and [LAWWORLD 2018 KAR 119](#) issued binding directions on storage conditions. These apply to every person who handles digital evidence from seizure to trial.

- Store digital media in anti-static, anti-magnetic envelopes or cases. Never use ordinary plastic bags or paper wrapping.
- Keep media away from heat sources, humidity, and magnetic fields (speakers, transformers, motors).
- Maintain temperature-controlled storage wherever possible, especially for hard drives and DVRs.
- Disable biometric, PIN, and pattern locks before seizure, or obtain the passcode and record it in the seizure memo.
- Submit media to the court in sealed and secured condition while retaining a working

copy with the investigating agency.

- Create and preserve backup copies on designated official computers or servers immediately after seizure.
- Document the playability tools required to access the media (software version, player type) alongside the hash value.
- Ensure the court is equipped to play the media before filing-provide compatible hardware or software if needed.
- Train all police personnel, forensic experts, and court staff in these protocols.

#### **TIP**

##### **The 48-Hour Problem**

In **LAWWORLD 2023 KAR 038**, the Court noted that the investigation failed to reconstruct a critical 48-hour period. When CCTV footage or device data covers a specific time window, the seizure must be timed to capture that window. Delayed seizure risks overwriting. Record the exact time of the incident and ensure the seizure memo captures the footage time-range.

## **Advocate Checklist: Receiving Digital Evidence from Clients**

#### **TIP**

##### **The Client Conversation**

Most clients do not understand that touching their phone after an incident can alter metadata and weaken their case. Explain in plain terms: every message opened, every photo viewed, every app updated creates a new timestamp. The goal is to freeze the device in its current state as quickly as possible. Time is the enemy of digital evidence.

## **The Principle Behind the Forms**

These templates are not bureaucratic formalities. They are the documentary architecture of authenticity. **LAWWORLD 2022 KAR 1166** directed the Director General of Police to establish standard operating procedures for electronic evidence, with disciplinary consequences for non-adherence. **LAWWORLD 2022 KAR 1159** required that electronic evidence be produced through recognised forensic channels with Section 65-B certificates. The Karnataka High Court has made its expectations clear across multiple decisions: proper seizure, proper storage, proper documentation, and proper certification are not optional-they are the minimum standard for electronic evidence to be received at all.

An advocate who receives a client's device and does nothing until trial has already lost half the battle. The work begins at the first meeting. Preserve the device state, document the chain, and engage a forensic expert before the evidence degrades. The Section 63 certificate will be only as strong as the seizure memo that preceded it.



# 15

## Evidence Act to BSA: Section Conversion Table

Finding the New Provision for Every Old Rule

### How to Read This Table

This chapter maps Evidence Act sections governing electronic records to their Bharatiya Sakshya Adhiniyam 2023 equivalents. Where the retrieval pack supports a proposition, it is cited by LAWWORLD ID. Where the pack does not contain the statutory text, the section number or content cannot be asserted. The table focuses on substantive principles—certificate requirement, primary versus secondary distinction, admissibility conditions—rather than section numbers that cannot be verified from available authorities.

#### NOTE

##### Pack Limitation

The retrieval pack does not contain the full text of the Bharatiya Sakshya Adhiniyam 2023 provisions corresponding to the mapped sections. Section numbers and specific wording for the new provisions cannot be asserted. Practitioners should verify the current BSA 2023 text for official section equivalents.

### Section 65B: The Certificate Requirement

| Evidence Act Provision | Principle                                                                                                                                                                       | BSA 2023 Status                                                 | Authority                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------------|
| Section 65B(1)         | Computer output deemed a document and admissible without further proof if conditions satisfied                                                                                  | Principle retained; certificate requirement preserved           | LAWWORLD 2020 SC 0715                                                 |
| Section 65B(2)(a)-(d)  | Cumulative conditions for admissibility of electronic records                                                                                                                   | Principle retained; statutory conditions unchanged              | LAWWORLD 2014 SC 0967                                                 |
| Section 65B(4)         | Certificate mandatory for secondary electronic evidence; identifies record, describes production, gives device particulars, confirms conditions, signed by responsible official | Principle retained; mandatory certificate requirement preserved | LAWWORLD 2014 SC 0967, LAWWORLD 2015 KAR 1223, LAWWORLD 2022 KAR 0119 |

|                                                     |                                                                                                 |                    |                                               |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------|
| Section 65B(4) - certificate as condition precedent | Certificate must accompany record when produced; oral testimony cannot substitute               | Principle retained | LAWWORLD 2020 SC 0715, LAWWORLD 2016 SC 117   |
| Section 65B(4) - procedural nature                  | Certificate requirement is procedural and may be relaxed in interests of justice                | Principle retained | LAWWORLD 2019 KAR 1032, LAWWORLD 2018 SC 0455 |
| Section 65B(4) - party not in possession of device  | Where party is not in possession of device, certificate under Section 65B(4) cannot be required | Principle retained | LAWWORLD 2018 SC 0455                         |

#### TIP

#### Practical Takeaway

The certificate requirement for secondary electronic evidence is the cornerstone of admissibility. *Evidence Act ss.65A, 65B* establishes that the certificate is mandatory; *Anvar ruling* confirms it cannot be substituted by oral testimony. Practitioners must ensure a compliant certificate before tendering secondary electronic evidence.

## Primary vs. Secondary Electronic Evidence

| Evidence Act Provision                | Principle                                                                                                                          | BSA 2023 Status     | Authority                                     |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|---------------------|-----------------------------------------------|
| Section 65B - not a complete code     | Sections 65A and 65B are not a complete code; primary electronic evidence governed by Section 62                                   | Principle clarified | LAWWORLD 2018 SC 0145                         |
| Section 62 - primary evidence         | Primary evidence is the document itself; electronic records produced from proper custody may qualify as primary evidence           | Principle retained  | LAWWORLD 2017 SC 0725, LAWWORLD 2019 KAR 1032 |
| Section 65B - secondary evidence only | Section 65B applies only to secondary electronic evidence; primary electronic evidence does not require Section 65B certificate    | Principle retained  | LAWWORLD 2019 KAR 1032                        |
| Original device exception             | Electronic record produced from original device (e.g., landline cassette) is primary evidence; no Section 65B certificate required | Principle retained  | LAWWORLD 2017 SC 0725                         |

**WARNING****Critical Distinction**

The primary versus secondary distinction determines whether a certificate is required. *Electronic evidence and ransom tape cassette* held that a cassette handed over in original was primary evidence not requiring certification. *Electronic evidence - Sections 62, 65-A, 65-B* confirms the Section 65B procedure applies only to secondary electronic evidence.

## Definitions and Key Concepts

| Evidence Act Provision                    | Principle                                                                                                                                       | BSA 2023 Status    | Authority             |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------|
| Section 3 - "document"                    | Document includes any matter recorded by letters, figures, or marks; electronic records stored in memory card or pen-drive constitute documents | Principle retained | LAWWORLD 2019 SC 1175 |
| IT Act Section 2(t) - "electronic record" | Electronic record defined as data or information in electronic form                                                                             | Principle retained | LAWWORLD 2018 SC 0145 |
| Section 3 - "fact" and "evidence"         | Fact includes principal fact and evidentiary facts; evidence is the medium through which court is convinced                                     | Principle retained | LAWWORLD 2022 SC 121  |

The definition of "electronic record" under the Information Technology Act, 2000 links electronic records to the notion of a document whose contents may be proved according to the Evidence Act framework. *Primary electronic evidence, "document"* clarifies that primary evidence of an electronic record is governed by the primary evidence provisions, not by the secondary evidence certification regime.

## Admissibility and Timing

| Evidence Act Provision                            | Principle                                                                          | BSA 2023 Status    | Authority                                                              |
|---------------------------------------------------|------------------------------------------------------------------------------------|--------------------|------------------------------------------------------------------------|
| Section 65B - timing of certificate               | Certificate required at stage of adducing evidence, not at charge-sheet stage      | Principle retained | LAWWORLD 2019 KAR 071                                                  |
| Section 65B - inadmissibility without certificate | Secondary electronic evidence without certificate is inadmissible                  | Principle retained | LAWWORLD 2015 KAR 1223, LAWWORLD 2015 KAR 0225, LAWWORLD 2022 KAR 0119 |
| Section 59 - proof of electronic records          | Electronic records must be proved according to the applicable statutory conditions | Principle retained | LAWWORLD 2014 SC 0967                                                  |



**TIP****Timing Rule**

*Section 65-B - stage for production of certificate* confirms the certificate need not be enclosed at the time of filing the charge-sheet. The requirement is considered at the stage of adducing evidence while deciding admissibility. This settled position applies under the new statute.

## Special Categories of Electronic Evidence

| Evidence Act Provision                                    | Principle                                                                                                          | BSA 2023 Status    | Authority                                       |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------|
| Section 17 - admission of electronic records              | Admissions in electronic form are relevant                                                                         | Principle retained | Not directly supported by pack; principle noted |
| Section 22A - oral admissions as to electronic contents   | Oral admissions as to electronic contents treated specially                                                        | Principle retained | Not directly supported by pack; principle noted |
| Section 34 - electronic entries in books                  | Entries in electronic books are relevant                                                                           | Principle retained | Not directly supported by pack; principle noted |
| Section 35 - electronic records as public documents       | Electronic records as evidence of public documents                                                                 | Principle retained | Not directly supported by pack; principle noted |
| Section 73A - electronic evidence of privileged documents | Electronic evidence of privileged documents                                                                        | Principle retained | Not directly supported by pack; principle noted |
| Bankers' Books Evidence Act                               | Section 4 permits certified copy as prima facie evidence; does not create presumption as to correctness of entries | Principle retained | LAWWORLD 2007 KAR 1133                          |

**NOTE****Bank Statements**

*Electronic records, bank statements* held that Section 4 of the Bankers' Books Evidence Act only permits a certified copy as prima facie evidence of existence of entries; it does not create any presumption as to correctness. The bank must still independently prove correctness of debit entries.

## eSakshya: The New Digital Evidence Framework

The Maharashtra eSakshya Management Rules, 2025 introduce a structured framework for electronic evidence collected through the eSakshya Mobile Application. Under these rules, every Investigating Officer must generate a certificate through the eSakshya Mobile Application, which will be eSigned. Evidence recorded through eSakshya generates a secure packet with a unique SID, timestamp, geo-location, and hash value to ensure integrity.

### **Bharatiya Nagarik Suraksha Sanhita the State of Maharashtra eSakshya Management Rules, 2025 - Section 4**

Investigating Officer shall generate a certificate 63 (4) (c) Part A of the Bharatiya

*Sakshya Adhiniyam, 2023 (47 of 2023) through the eSakshya Mobile Application. All Certificates will be eSigned.*

**TIP**

**eSakshya Certificate**

*The eSakshya rules reference a certificate under Section 63(4)(c) Part A of the Bharatiya Sakshya Adhiniyam, 2023. This indicates that the new statute contemplates a certificate format for electronic evidence collected through approved digital platforms. Practitioners handling evidence from Maharashtra should familiarise themselves with the eSakshya framework.*

**Quick Reference: Principles That Survive the Transition**

# 16

## Practice Pointers and the Road Ahead

Synthesis, Open Questions, and Future Developments

### What This Book Has Established

The preceding chapters have built a comprehensive framework for handling electronic evidence under the Bharatiya Sakshya Adhiniyam 2023. The following principles are now settled law: the Section 63 certificate is a condition precedent to the admissibility of secondary electronic evidence-oral testimony cannot substitute it **Sections 65A and 65B form a complete code**. The certificate must be produced at the stage of adducing evidence, not at the charge-sheet stage **certificate need not be enclosed at filing**, and its absence at that stage is a curable defect under Section 311 CrPC **curable defect and Section 311 CrPC**. The certificate must accurately identify the record, describe the production process, give device particulars, confirm statutory conditions, and be signed by a person in a responsible position. Defects in any of these elements render the record inadmissible. And even where electronic evidence survives admissibility challenge, courts still assess its probative value.

#### TIP

##### The Two-Track System

Primary electronic evidence (from proper custody or simultaneous storage under Section 57 Explanations 4-7) requires no certificate. Secondary electronic evidence (printed, copied, or output from a computer) requires a Section 63 certificate. Know which track your evidence falls on before deciding whether to object or produce.

### Open Questions Under the BSA 2023

Three questions remain unresolved and will require judicial attention as BSA jurisprudence develops.

- **Records from Proper Custody:** The Supreme Court in **Section 65B - Electronic evidence and ransom tape cassette** held that primary evidence (original device handed over) requires no certificate. But the BSA 2023's expanded definition of primary evidence under Section 57 Explanations 4-7 raises a new question: when a record is produced from "proper custody" (a concept the statute does not define), does it attract the Section 63 certificate requirement, or does it remain primary evidence exempt from certification? Courts have not yet settled this.
- **Further Investigation into Electronic Evidence:** When electronic evidence is suspect-metadata inconsistent, chain of custody broken, hash values unexplained-can a court direct further investigation under Section 303 of the



*Bharatiya Nagarik Suraksha Sanhita 2023? The Karnataka High Court in **LAWWORLD 2022 KAR 1166** directed improvements in investigative standards, but whether courts can compel the production of additional electronic evidence or forensic reports remains open.*

- **Cloud-Based Evidence:** Evidence stored on cloud servers (Google Drive, Dropbox, iCloud) presents a certification challenge: the device that generated the record may be a server located outside India, operated by a third party. Who is the "person in a responsible position relative to the computer" under Section 63? How is the device described? How is the hash value generated? These questions await authoritative resolution.

## **Practice Pointers by Forum**

*The following checklists distil the key actions for advocates in different contexts.*

### **Criminal Trials**

### **Civil Proceedings**

### **Corporate Investigations**

## **The Road Ahead**

*The Bharatiya Sakshya Adhiniyam 2023 represents a significant modernisation of India's evidence law, but its provisions on electronic evidence are still being interpreted by courts. The eSakshya Management Rules 2025 in Maharashtra point to a future where electronic evidence is captured, certified, and transmitted through standardised digital platforms-but this is currently limited to one State and one category of evidence.*

*Practitioners must monitor how courts resolve the open questions flagged above. The certificate requirement, the proper custody doctrine, and the treatment of cloud evidence will shape electronic evidence practice for years to come. Advocate vigilance at every stage-from seizure to trial-is not optional. It is the difference between evidence that survives challenge and evidence that is excluded.*

#### **NOTE**

#### **Stay Engaged**

*BSA jurisprudence is developing. Bookmark this book, follow Karnataka High Court decisions (which have produced the most electronic evidence rulings), and revisit these practice pointers as the law evolves.*

## **Disclaimer**

*This work is intended for legal practitioners, law students, and in-house counsel. It does not constitute legal advice. Case citations and statutory references should be verified before use in any proceeding.*

*(c) LawWorld - Creator: LawWorld*