Chhattisgarh State Judicial Academy, Bilaspur(C.G.)

Divisional Judicial Seminar of Bilaspur Division

Held on 08.02.2025

Topic

Electronic Evidence and its admissibility. Appreciation of Electronic Evidence -Challenges and Best Practices

In the guidance of

Respected Shri Satyendra Kumar Sahu Sir,

Principal District and Session Judge, Korba (C.G.)

Presented by:

-Dr. Mamta Bhojwani

District and Additional Session Judge,F.T.S.C (POCSO) Korba

- Richa Yadav

Ist Add.judge to the court of Civil Judge Junior Division, Korba

-Lov kumar Lahare

II Civil Judge Junior Division, Korba

ACKNOWLEDGEMENT

We feel highly elated to work on the topic " ***Electronic evidence and its admissibility. Appreciation of electronic evidence -challenges and best practices .”*** The practical realization of this presentation has obligated the assistance of many persons. First of all, we would like to thank the Hon'ble High court of Chhattisgarh and Chhattisgarh state judicial Academy for organizing this divisional conference and providing us a platform to discuss on such crucial legal points.

We would like to express our deepest regard and gratitude for Hon'ble Shri Satyendra Kumar Sahu, Principal District and Session Judge, Korba, Chhattisgarh. His consistent supervision, constant inspiration and invaluable guidance have been of immense help in understanding and carrying out the nuances of the preparation of paper.

-Dr. Mamta Bhojwani

District and Additional Session Judge,F.T.S.C (POCSO) Korba

- Richa Yadav

Ist Add.judge to the court of Civil Judge Junior Division, Korba

-Lov kumar Lahare

II Civil Judge Junior Division, Korba

Table of Contents

Electronic Evidence and its admissibility – Appreciation of Electronic Evidence -Challenges and Best Practices .

INTRODUCTION

In February 2010, the city of Pune was endangered by a terrorist attack in a much-frequented bakery. The 'German Bakery blast' accused were finally identified by the police on the basis of a CCTV recording. The question, therefore, arises as to whether such a recording, which is neither on paper nor on a camera negative , in fact, not available in any tangible form at all, can be introduced in court as evidence. The only proof available will be that recorded in the computer system controlling the CCTV unit. This incident illustrates the significance of electronic evidence in criminal trial. (**The State of Maharashtra Vs Mirza Himayat Baig 2016 SCC OnLine Bom 2864**)

Electronic evidence has been the most significant form of evidence in the 21 century. This is because of the rapidly developing technological environment, whereby technological gadgets like cell phones, tablets, laptops, etc. have become necessities and this has resulted in the way communications and transactions are made and stored.

In the year 2000 , certain amendments were incorporated in criminal laws. Section 65 A and Section 65 B were added in the Indian Evidence Act,1872.

Sec 3 IEA 1872 widened the definition of documentary evidence by adding **electronic records** in it and certain other words like electronic signature, electronic form, electronic records, information, secure digital signature, etc were also added by mentioning that they will have the same meaning which is assigned to them in IT Act ,2000.

- **Admissibility of Electronic Evidence under the Old Act**

Under Sec-4 of Information Technology Act, 2000 - Legal recognition of electronic records:

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is- (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.

Section 65B of the erstwhile Indian Evidence Act,1872 was introduced through an amendment in 2000 primarily to deal with the admissibility of electronic records.

The following are some of the key provisions of the Sec 65B of Evidence Act,1872:

a) Admissibility - Sec 65B(1) of IEA,1872 provides that the information contained in an electronic record which is stored in the computer shall be deemed to be a document if it meets certain conditions provided in the section and shall be admissible in any proceedings.

b) Conditions to be satisfied - Sec 65B(2) of IEA,1872 deals with the conditions relating to the computer output, i.e the information stored in an electronic record. It states that the computer into which the computer output is present must be operating properly, should have been used regularly and must be fed into the computer during the ordinary course of the said activities for which the computer was used. Similarly, Section 65B(3) provides for conditions relating to the computer system.

c) Certificate requirement - Under Section 65B(4) of IEA,1872, a certificate from a person in a responsible official position is mandatory for the admissibility of electronic records.

For the purpose of admissibility of electronic record, a three prong test is important:-

1. Document in question is an electronic record [as defined under S.2(1)(t) of the IT Act, 2000] ;

2. Produced by a computer: The term "computer" is defined under S.2(1)(i) of the IT Act, 2000 which means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulation of

electronic,magnetic or optical impulses,and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

3. Accompanied by a certificate: fulfilling the conditions laid down under section 65 (B) of Indian Evidence Act,1872 / Section 63 of the Bhartiya sakshaya adhiniyam,2023.

- **The Development of Law of Electronic Evidence through case laws**

1. State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru [(2005) 11 SCC 600] (The Parliament Attack Case) .

Facts of the Case :- On 13th December , 2001 , five heavily armed persons practically stormed the Parliament House complex and inflicted heavy casualties on the security men on duty. In the gun battle that lasted for 30 minutes , these five terrorist who tried to gain entry into the Parliament when it was in session were killed.

Relevancy of electronic evidence :- The links between the slain terrorists and the masterminds of the attack were established only through phone call transcripts obtained from the mobile service providers.

One of the major issue raised from the side of the accused was the inadmissibility of the electronic records (mobile phone call records)

because there was no certificate produced by the prosecution which is necessary for admitting any electronic record .

Judgment :- The Apex Court concluded that the cross-examination of competent witness acquainted with the functioning of the computer during the relevant time and the manner in which the printouts of the call records were taken was sufficient to prove the call records. Irrespective of the compliance of the requirements of Section 65B which is a provision dealing with admissibility of electronic records, there is no bar to adducing secondary evidence under the other provisions of the Evidence Act, namely Sections 63 & 65.

2. Anvar P.V. Vs. P.K. Basheer and Others [(2014) 10 SCC 473]

Facts of the Case :- In the present case , appellant had filed election petition to set aside the election of first respondent on ground that alleged songs, announcements , and speeches made as part of election propaganda of first respondent , amounted to corrupt practices.

Relevancy of Electronic Evidence :- alleged songs, announcements , and speeches were recorded using some instrument and by feeding them into computer, CDs were made which were produced in the court. However, certificate in terms of section 65-B was not produced in respect of such CDs.

Judgment :- A three-Judge Bench of the Hon‘ble Supreme held that CDs concerned, not being the original CDs themselves, cannot be

admitted in evidence since the mandatory requirements of section 65-B of Evidence Act are not satisfied. Hon'ble Court further held that the Computer Output is not admissible without compliance of Section 65B. It overruled the judgment in State (NCT of Delhi) v. Navjot Sandhu alias Afzal Guru [(2005) 11 SCC 600] by the two judge Bench of the Supreme Court. The court observed that "the Judgment of Navjot Sandhu, to the extent, the statement of the law on admissibility of electronic evidence pertaining to electronic record of this court, does not lay down correct position and is required to be overruled.

Hon'ble Apex Court in ***Anvar P.V vs. P.K.Basheer*** held that under Section 65B(4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:

(a) There must be a certificate which identifies the electronic record containing the statement;

(b) The certificate must describe the manner in which the electronic record was produced;

(c) The certificate must furnish the particulars of the device involved in the production of that record;

(d) The certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act; and

(e) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.

The objective behind aforesaid step-by-step processes is to identify whether the computer in question was properly processed, stored and reproduced whatever information it received.

- **Genuineness of Electronic Records**

In Anvar P.V. Vs. P.K. Basheer, **(2014) 10 SCC 473**), in para 16, the Hon'ble Supreme Court said, "if the electronic record is duly produced in terms of Section 65B of the Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A Indian Evidence Act, opinion of examiner of electronic evidence."

Section 45A of IEA/ 39(2) of BSA provides- ***Opinion of Examiner of Electronic Evidence*****.** When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 in a relevant fact.

Explanation.- For the purposes of this section, an Examiner of Electronic Evidence shall be an expert.

Section 79A Information Technology Act, is also relevant to be mentioned here which says- ***Central Government to notify Examiner of Electronic Evidence*** The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette,

any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation.- for the purposes of this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

A combined reading of Section 45A Indian Evidence Act and Section 79A Information Technology Act makes it clear that the genuineness of an electronic record can be verified by an examiner of electronic evidence, who is to be appointed by the Central Government. The expert can be any body or agency of Central Government or State Governments, like Central Forensic Science Laboratories or State Forensic Science Laboratories.

Hence , the examiner of electronic record will explain to the court about the contents of the electronic evidence which is sought to be presented before court and certify to the court that the electronic evidence is not tampered with or in any way manipulated. The **person** certifying under Section 65B and the **'expert'** certifying under Section 45A are not certifying the same thing and at the same time. Whereas the person certifying under Section 65B is certifying the accuracy and sanctity of the process of taking computer printout or making a copy for the purposes of producing secondary electronic evidence, from original 'electronic record', the examiner of 'electronic records' under Section 45A is certifying about the genuineness of the electronic records itself.

- **Exhibiting the electronic record before court**

In **Anvar P.V. Vs. Basheer** , it is held by Hon'ble Supreme Court that certificate under Sec.65B must accompany the electronic record like Computer Printout, Computer Disc (CD), Video Computer Disc (VCD), Pen Drive etc. pertaining to which a statement is sought to be given in evidence when the same is produced by evidence. We may analyze this statement to say that the person, who has given the certificate U/s. 65B should be called in court to testify the factum of entire process undergone while a computer printout or copy was taken from original source and about which he issued a certificate U/s 65B. During his testimony he is also required to certify Sec.65B certificate which will be marked a specific exhibit number.

During his testimony he is also required to certify computer printouts (in cases of call detail reports or CDR and any other textual or email messages, printed on paper) and the CD, VCD, Pen Drive etc. filed as an electronic record, which shall also be marked as exhibit number.

3.**Tomaso Bruno & Anr. Vs. State of UP** [(2015) 7 SCC 178]

Facts of the case :- Appellants were foreigners , who were tourist in India , charged with having murdered their companion in a hotel. The prosecution case was based on circumstantial evidence that it were appellants alone who could do this because all the three were lodged in

a single room . Per contra, the version of the appellants was that they were out of hotel for a couple of hours while the deceased stayed back because he was not well and when the appellants returned , they found deceased in serious condition.

Relevancy of electronic evidence :- Appellants location at material time was crucial to unravel the truth and this could be determined with the help of CCTV recordings in the hotel and movement of mobile phones.

Judgment :- The Hon'ble Court set aside the conviction of the appellants under section 302/34 of IPC on the ground that CCTV footage and call records was not produced by the prosecution . Further , without referring to the judgment passed in Anwar PV case, the Hon'ble Court held that secondary evidence of the contents of a document can be led under section 65 of the Evidence Act.

4. Shafhi Mohammad vs The State Of Himachal Pradesh [(2018) 2 SCC 801]

Facts of the case :- Use of the videography of the scene of crime is the subject matter of consideration herein.

Judgment :- A two Judge Bench of the Hon‘ble Supreme Court held that requirement of certificate under Section 65B (4) is not always mandatory.

As there was dichotomy of decisions in between Anwar PV‘s case and Shafhi Mohammad‘s case, in the year 2019, a two-Judge Bench of the apex court referred the matter to a another three-judge bench for clarification on the point.

5. <u>The leading case law on this is the judgment of “Arjun Panditrao” (Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors 2019 SCC OnLine SC 1553 , delivered on 14th July , 2020) .</u>

Facts of the case :- The Hon’ble Court had to adjudicate on an election petition which challenged the election of Mr. Arjun Panditrao Khotkar from Jalna-101 Legislative Assembly Constituency, on the ground that the nomination papers were filed after the stipulated deadline. The Respondents wished to rely on video camera recordings of the office of Returning Officer to prove that the candidate had filed his nomination after the stipulated deadline. The Election Commission produced CDs which contained a copy of the video camera recordings, in accordance with the direction given by the Hon’ble High Court. However, the necessary certificates were not produced in accordance

with Section 65B(4) by the Election Commission, despite multiple requests made by the Petitioner.

Relevancy of electronic evidence :- The question arises whether the Video Compact Disk containing video recordings could be admitted in the absence of certificate .

Judgment :- The Hon'ble Supreme Court upheld the impugned judgment of the High Court wherein during the cross examination , an officer of the Election Commission testified that the video camera recordings were authentic. Based on this testimony, the High Court admitted the evidence of the video recordings even though the certificate in accordance with Section 65B (4) had not been produced. The High Court held that it was satisfied that there was "substantial compliance" with Section 65B, as a competent officer had testified that the video recordings were authentic. Moreover , apart from electronic record , other evidence was also relied upon by High Court.

- ***Arjun Panditrao Khotkar Case also considered three key issues with regards to Section 65B of the IEA.***

A - Whether or not section 65B constitutes the complete code in India as to the admissibility of secondary digital evidence ?

Answer :- Special provisions of ss.65A and 65B are a complete Code in themselves when it comes to admissibility of evidence of information contained in electronic records.

B - Whether the requirement of a certificate was mandatory in all cases ?

Answer :- A written certificate u/s.65B(4) is a sine qua non for admissibility of such evidence – Oral evidence in place of such certificate cannot suffice as s.65B(4) is mandatory. Further, the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4).

C Finally at which stage of the proceedings in a criminal or civil trial would the certificate need be produced ?

Answer :- It has been held in Arjun Panditrao Case that "So long as the hearing in a trial is not yet over, the requisite certificate can be directed to be produced by the learned Judge at any stage, so that information contained in electronic record form can then be admitted and relied upon in evidence ."

The Overruling- Hon'ble Supreme Court in **ARJUN PANDITRAO KHOTKAR Vs. KAILASH KUSHANRAO GORANTYAL AND ORS.** [2020 SCC OnLine SC 571] by Judgment dated July 14, 2020, held that Anvar P.V. (supra), is the law declared by this Court on Section 65B of the Evidence Act. The judgment in Tomaso Bruno (supra), being per incuriam, does not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as Shafhi Mohammad (supra) (2018) 5 SCC 311, do not lay down the law correctly and are therefore overruled.

A NEW ERA- THE BHARTIYA SAKSHYA ADHINIYAM, 2023

The Arjun Panditrao ruling, on one hand, had affirmed the provisions relating to admissibility of electronic evidence to be a self-sustained and comprehensive "complete code", and effectively prevented creation of two parallel procedural pathways within the existing legal framework of the law on electronic evidence. The approaches outlined in the earlier decisions in Navjot Sandhu and Shafhi Mohammad were deemed divergent, making the verdict in Arjun Panditrao a foundational step towards uniformity in this area of law — a step that now stands settled in light of the recently enacted the BSA, 2023. Though the Adhiniyam offers a refreshing change, it now remains to be seen if this new beginning will warrant the Court to revisit its previous decisions, and reconsider the discarded approaches as viable

options in this evolving landscape. While we await the response from the Court, we can either wait for solutions to the issues identified or actively pursue to seek those solutions.

Arguably, it is easier to identify problems than to propose solutions, but in the realm of law, it is crucial to recall Einstein's wisdom, who is famously quoted having said that if he had one hour to save the planet, he would spend 59 minutes defining the problem and only one minute on the solution. So, for now, it is hopefully acceptable to sit with the problems so identified.

• Meaning of Electronic Evidence

Document as defined under section 2(d) of *The Bhartiya Sakshya Adhiniyam, 2023* includes both electronic and digital records. Illustration (vi) of section 2(d) of BSA states that electronic records on emails, server logs, documents on computers, laptop or smart phone, messages, websites and voice mail messages stored on digital devices are documents .

"***Evidence***" as defined under section 2(e) of Bharatiya Sakshya Adhiniyam, 2023 includes all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; and all documents including

electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence.

The Bhartiya Sakshya Adhiniyam, 2023 does not define the term '**electronic record'**, however , **Sec 2(t) of the IT Act**, **2000** defines it as "any data, record, image, or sound that is generated, stored, received, or sent in electronic form, including microfilm or computer-generated microfiche;; essentially encompassing any digital data or information stored electronically.

In other words , electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use it at trial. Hence, electronic evidence is a documentary evidence.

- **Sources of Electronic Evidence**

Every kind of electronic/digital data/information which can be saved in the electronic/digital media storage, the same can be used as evidence. Source of such data/information/records may be:

i. Hardware: Computers, mobile devices, storage media, network peripherals.

ii. Software: Operating systems, applications, firmware, malicious code.

iii. Data: Documents, emails, images, audio/video files, logs, metadata.

iv. Online Evidence: Social media, cloud storage, websites, internet activity logs.

- **Some Devices and their importance in evidence-**

At this juncture, it is better to understand certain important devices and its uses.

- **CPU:** The device itself may be evidence of component theft, counterfeiting etc. The device contains digital devices with all the files and folders stored including deleted files and information, which may not be seen normally. Cyber Forensic is used to image, retrieve and analyze the data.
- **Display Monitor (CRT/LCD/TFT etc.) screens of Mobile Phones, if switched on:** All the graphics and files that are open and visible on the screen in switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and through description in seizure memo.
- **Smart Cards, Dongles and biometric scanners etc:** The device itself, along with the identification/authentication information of the card and the user, level of access, configurations and permissions.
- **Digital Cameras:** The device can be looked for images, videos, sounds, removable cartridges, time & date stamps.
- **Smart Phones:** Much information can be obtained from these devices like address book, appointment calendars/information, documents, emails, phone book, messages (text & voice), emails passwords etc.
- **Hard Disc Drives:** The basic storage location of any computer is HDD. The HDD can be both internal and as well as external.

Internal HDD is integrated into the computer system. External HDD can be attached though USB portals and includes like pen drive or flash drive. It is generally referred to as secondary storage of the computer system. The primary being the Random Access Memory (RAM).

- **Local Area Network (LAN) Card or Network Interface Card (NIC):** The device itself and also MAC (Media Access Control) address can be obtained.
- **Modems, Routers, Hubs and Switches:** In routers, configuration files contain information related to IP addresses etc.
- **Servers:** Information like last logins, mails exchanged, contents downloaded, pages accessed etc. can be obtained.
- **Network cables and connectors:** Network cables are used to trace back to their respective computers. Connectors help in identifying the types of devices that are connected to the computers.
- **Printers:** The device has data like number of prints last printed and some maintain usage logs, time & date information. If attached to a network, they may store network identity information. In addition, it can also be examined for figure prints.
- **Scanners:** The device itself, having the capability to scan, may help to prove illegal activity.
- **Copiers:** Copies may contain some documents both physical and electronic, user usage logos, time and data stamps.

- **CD & DVD Drives:** These devices store files/data in which evidence can be found.
- **Digital Watches:** Some latest digital watches contain information like address book, notes, appointment calendars, phone numbers, emails etc.
- **Fax machine:** These devices contain some documents, phone numbers, send/receive logs, film cartridges that can be considered.
- **Global Positioning System (GPS):** The device may provide travel logs, home location, previous destinations, way point coordinators, way point name etc.
- **Keyboard & Mouse:**
  These devices can be examined for fingerprints.

- **<u>Classification of Electronic Evidence as Primary and secondary evidence-</u>**

➢ **<u>Primary Evidence:</u>**

Section 57 of BSA defines primary evidence as the original document presented for the court's inspection. This encompasses documents **executed in parts or counterparts,** as well as those produced through uniform processes such as printing or photography. Importantly, electronic or digital records are recognized as primary evidence when stored concurrently or sequentially across multiple files,

and video recordings in electronic form are also classified as primary evidence

Explanation 4. of S.57 of BSA—Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.

For example :- Email Threads:- A conversation unfolds over several email messages sent and received at different times. Each email in the thread (including attachments) is primary evidence as they collectively show the chronological exchange of information.

Explanation 5. of S.57 of BSA —Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.

Electronic records are said to be in proper custody if they are in the place in which, and looked after by the person with whom such document is required to be kept; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render that origin probable **(Explanation of section 81 of the BSA).**

For example :- CCTV Footage from secured recorder: The footage stored on the system's secure recorder, accessible only to authorized personnel, is considered primary evidence.

Explanation 6. of S.57 of BSA —Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or

transferred to another, each of the stored recordings is primary evidence.

For example :- Live Streaming being broadcasting and recorded at different storage media: A live event like a concert or a sports game is broadcasted simultaneously through a streaming platform and recorded locally by the organizer. Both the streamed recording and the local recording are considered primary evidence as they capture the same event from different perspectives.

Explanation 7. of S.57 of BSA —Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.

For example :- Web Browsing History :- An investigation into online activity examines the user's web browsing history, including cached images, cookies, and temporary internet files. These temporary files, alongside the main browsing history, can reveal visited websites, searched keywords, and downloaded content, serving as primary evidence of online activity.

- **Secondary Evidence-**

Section 58 of BSA defines secondary evidence, encompassing certified copies, copies produced by mechanical processes, oral and written admissions, oral accounts of document contents, and testimony from individuals who have examined documents.

- This **applies particularly** when the original consists of many impractical accounts or documents to examine in court.
- Secondary evidence is **deemed relevant** when the original document cannot be presented for court inspection.

Admissibility of Electronic Records under the New Act-

Section 61 of BSA provides for the admissibility of electronic or digital Records

➔ This section confirms that electronic or digital records cannot be denied as evidence merely because they exist in electronic form.

➔ If the requirements of Section 63 are met, electronic records hold the same legal weight as physical documents or records.

➔ This provision enables courts to accept digital evidence like emails, whatsApp chats, social media posts, and digital contracts in legal proceedings.

Section 62 of BSA provides that the contents of electronic records may be proved in accordance with the provisions of section 63. –

Note:"Standard of proof " in the form of electronic evidence should be "more accurate and stringent" compared to other documentary evidence " has been held in Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329.

Section 63 of BSA, 2023 provides for admissibility of electronic records:-

Section 63(1) provides that notwithstanding anything contained in this Adhiniyam, **any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original,** as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible

Section 63(2) provides that the conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:

- The computer output containing the information **was produced by the computer or communication device during the period over which the computer or communication device was used regularly** to create, store or process information for the purposes of any activity regularly carried on over that period by the

person having lawful control over the use of the computer or communication device.

- During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was **regularly fed into the computer or communication device in the ordinary course of the said activities.**

- Throughout the material part of the said period, the computer or communication device was **operating properly** or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, **was not such as to affect the electronic record or the accuracy of its contents.**
- The i**nformation contained in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities.**

Section 63(3) provides that where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a)

of sub-section (2) was regularly performed by means of one or more computers or communication device, whether—

- In standalone mode; or
- On a computer system; or
- On a computer network; or
- On a computer resource enabling information creation or providing information processing and storage; or
- Through an intermediary,

All the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly.

Section 63 (4) provides that in any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:—

- Identifying the electronic record containing the statement and describing the manner in which it was produced.

- Giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3).
- Dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, **and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert** shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.

Section 63 of the BSA governs the admissibility of electronic evidence in courts wherein the format of the certificate under Section 63 has been changed and divided into two parts, where part A concerns basic details to be filled by the person who is filing for evidence.

The technical part arises in Part B which has to be now filled by an 'Expert' which has been mentioned under Section 63(4)(c) as *"an expert shall be evidence of any matter stated in the certificate."*

This ‘expert’ means any other person with necessary expertise who has to fill in the details of the electronic record. The new procedure under this form is filling in of *hash function* of the electronic evidence being submitted.

This Section provides for certificate requirements to prove the authenticity of the documents in digital form. Though, this inclusion is a significant step towards addressing the technological intervention in the justice system.

Comparison between Section 65(B), of the IEA & Section 63 , of the BSA

One of the significant steps in the admissibility of evidence is the inclusion of section 63 of BSA which reflects section 65B of Indian Evidence act, 1872 with slight modifications. Some of the common elements between the two sections regarding the admissibility of electronic evidence are:

i Both the sections permit the admissibility of information contained in an electronic record and the conditions to be satisfied are the same.

ii They both are ‘non-obstante clauses’ meaning their special provisions prevail over any other sections of their respective acts.

iii) The certificate requirement is present in both sec 65B of erstwhile Evidence act, 1872 and in sec 63 of the new Bharatiya Sakshya Adhiniyam,2023.

The legislative intent and the crux of these sections are same. However, few additions and modifications are done in Sec 63 of BSA without disrupting the scope of the section - admissibility of electronic record.

Section 63(1) of the BSA has included into its admissibility, the communication devices along with computers to cover telephonic conversations, social media texts, posts, tweets etc as documents admissible into evidence.

In the erstwhile sec 65B(3), the conditions to be satisfied by devices covered only storage and processing operation, however in Sec 63(3), it includes creation operation also. This is done in order to include the intermediaries into the evidential jurisprudence.

Regarding the certificate requirement, Section 63(4) provides that whenever an electronic record is submitted for evidence in those instances, a certificate shall be submitted accompanying it, thereby making it a mandatory requirement.

This section has also brought two factor authentication of electronic records - **first by the person in charge of the computer or communication device and then by an expert.** This has removed the confusion regarding the who, when and what of the certificate requirement. Thus, Section 63 of BNS provides better clarity which will in turn reduce the judicial burden and higher stability by improving the authentication requirement of electronic records as compared to Section 65B of Indian evidence Act.

APPRECIATION OF ELECTRONIC EVIDENCE

The evidentiary value of an electronic record can be judged on these two parameters-

(1) Admissibility / Proof of electronic records (as hereinabove discussed in this paper)

(2) Genuineness of electronic records. (Part B of the certificate as mentioned in section 63 of the BSA , 2023)

In this paper , we are citing some of the important case laws wherein electronic evidence has been appreciated by Hon'ble Apex Court and Hon'ble High Courts , so that we can have clarity as to how electronic evidence is to be appreciated :-

- **LATEST CASE LAWS**

1.The importance of comparison of hash value of a source data and CD produced in court was underlined by Punjab and Haryana High Court in the case of **Ram Kishan Fauji Vs State of Haryana (2016 SCC OnLine P&H 14198)** that if the CD cannot stand the test of authenticity by its comparison with its hash value with the source, then the transcript of what has been obtained through its audio footage or what it purports to capture cannot be taken as of value.

Hence , so far as authentication of CD is concerned, it needs to be noted that comparison of hash values of original data and the data copied on CD is an important means of authentication.

2.An interesting question arose as to when and how the admissibility of CDR can be questioned before the Court of law. The question is answered in **Sonu @ Amar v/s State Of Haryana, (2017) 8 SCC 570 .**

Facts of the case :- The appellants were found guilty of abduction and murder and sentenced for life imprisonment. Their conviction and sentenced was confirmed by the High Court. One of the main ground for these appeals was lack of a certificate under section 65-B of the Indian Evidence Act for CDR which was relied upon in evidence .

Issue :- Objection regarding mode or method of proof of CDR of mobile phones recovered from the accused was raised for first time before appellate court.

Judgment :- The Hon'ble Supreme Court upheld the judgment of the High Court and held that an objection as to the admissibility of CDR must be taken at the time of marking of document as an exhibit i.e. at trial stage and it cannot be raised at the appellate stage as the objection relates to the method of proof. The following observations are also significant :-

*** The objections as to admissibility of documents in evidence may be classified into two classes :-**

(i) an objection that the document which is sought to be proved is itself inadmissible in evidence; and

(ii) where the objection does not dispute the admissibility of the document in evidence but is directed towards the mode of proof alleging the same to be irregular or insufficient

- **That objections regarding admissibility of documents which are per se inadmissible can be taken even at the appellate stage.** Admissibility of a document which is inherently inadmissible is an issue which can be taken up at the appellate stage because it is a fundamental issue.
- **The mode or method of proof is procedural and objections, if not taken at the trial, cannot be permitted at the appellate stage**. If the objections to the mode of proof are permitted to be taken at the appellate stage by a party, the other side does not have an opportunity of rectifying the deficiencies. **The crucial test, as affirmed by this Court, is whether the defect could have been cured at the stage of marking the document.**

3. Section 88-A of the Evidence Act 1872 (Sec 90 of the BSA, 2023) provides for presumption about electronic message. It is necessary to understand that the presumption merely states that the mesaage received by the addressee is the same, which was fed into the originator's computer for trasmission. As held by Madras High Court in **S.Karunakaran Vs Srileka , 2019 SCC Online Mad 1402**, the court shall not make any presumption as to the person by whom such

message was sent. Therefore , it is clear that mere filing of email does not raise a presumption that it is sent by the originator.

4. The Hon'ble the Punjab and Haryana High Court , in the case of **Sunil vs State Of Haryana (2022 SCC OnLine P&H 1343)** held that the evidence of the CCTV footage, which has been converted to a CD could not be read in evidence in the absence of the certificate under Section 65 B (4) of the Evidence Act.

5. Ravinder Singh Vs State of Punjab (2022) 7 SCC 581

Facts of the case :- In this case , two children were kidnapped and murdered by three accused persons.

Relevancy of electronic evidence :- Call records were produced by the prosecution without certificate relating to phone calls between appellant accused and other co-accused that they share intimate relationship , which became root cause of offence committed.

Judgment :- Oral evidence in place of such certificate cannot possibly suffice as section 65-B(4) of the Evidence Act is a mandatory requirement of law.

6. Duleshwar Verma Vs State of Chhattisgarh (Criminal Appeal No. 321 of 2013 , Judgment dated 03.01.2023 , 2023 Latest Caselaw 35 Chatt.)

Facts of the case :- The appellant along with a co-accused (later acquitted) strangulated the deceased. Call details linked the appellant to the deceased and his wife.

Relevancy of electronic evidence :-The prosecution relied on call details , however , these record lacked a mandatory certificate under Section 65B(4) of the Evidence Act.

Judgment :- The Hon'ble High court held that call details cannot be said to be proved in absence of required certificate ,therefore , conviction and sentence imposed upon the appellant was set aside.

7. State of Karnataka Vs T.Naseer @ Nasir , 2023 Livelaw (SC) 965, delivered on 06-11-2023

Facts of the Case:- The Hon'ble Supreme Court granted leave to hear the appeal filed by the State of Karnataka, challenging the High Court of Karnataka's decision to uphold the Trial Court's rejection of the prosecution's application. The initial proceedings involved a heinous case of serial bomb blasts in Bangalore on July 25, 2008, resulting in fatalities and injuries. During the investigation, various electronic devices were seized and later analyzed by the Central Forensic Science Laboratory (CFSL), Hyderabad. The CFSL report, dated November 29, 2010, was initially rejected by the Trial Court for lacking a Section 65-B certificate. The prosecution subsequently

obtained the certificate and sought to admit the report into evidence through an application under Section 311 of the Code of Criminal Procedure (Cr.P.C.), which was denied by both the Trial Court and the High Court.

Issue :- Whether the trial court refusal to admit certain electronic evidence due to the absence of the mandatory Section 65-B certificate at the time of its initial presentations is valid ?

Judgment :- A certificate under section 65-B of the Indian Evidence Act to prove electronic evidence can be produced at any stage of the trial. Hence, an application filed by the prosecution under section 311 of Cr.P.C. was allowed.

8. Sundar @ Sundarrajan vs State By Inspector Of Police ,2023 SCC OnLine SC 310 , Review Petition (Crl.) Nos. 159-160 of 2013 , 21-03-2023

Facts of the case - The applicant was a convict on death row. He moved this court for a fresh look at his petition seeking a review of his conviction for the offence of murder and the award of the sentence of death.

Some of the grounds of challenge-

-That the 15-digit IMEI number for the cell phone, allegedly belonging to the petitioner containing the SIM with mobile number ending with XXX5961, mentioned in the seizure memo differs from the IMEI number mentioned in the call detail record.

-The certificate under Section 65B of the Indian Evidence Act 1872 for the call detail records was not furnished.

Observation :- The Hon'ble Court held r**egarding difference of IMEI No**.-

" **In para 23**:- " Similarly, the contention based on the difference in the IMEI number recorded in the seizure memo and the call detail records does not affect the prosecution's case for the following reason. The difference in the IMEI number recorded in the seizure memo and the call detail record pertains to the last digit of the 15-digit IMEI number. Every device has a unique IMEI number identifying the brand owner in the model. The first 8 digits are the Type Allocation Code (TAC) digits of which the initial 2 digits identify the reporting body and the next 6 identify the brand owner and device model allocated by the reporting body. The next 6 digits are the unique serial number assigned to individual devices by the manufacturer..

Para 24. These 14 digits in the petitioner's case match in both the seizure memo and the call detail record. The last digit in the IMEI number is the 'Luhn check digit' based on a function of the other

digits using an algorithm. Technically, the last digit, which is the only digit that is different in the seizure memo and the call detail record, can be calculated through the algorithm on the basis of the first 14 digits which are the same in both the documents. Accordingly, it can be conclusively said that a difference in only the last digit of the IMEI number cannot imply that it represents the IMEI number of a separate device."

Regarding certificate being not furnished- the court held as:-

Para 44 :- " Therefore, we are inclined to agree with the ratio in **Sonu** by not allowing the objection which is raised at a belated stage that the CDRs are inadmissible in the absence of a Section 65B certificate, especially in cases, where the trial has been completed before 18 September 2014, i.e. before the pronouncement of the decision in Anvar P.V**."**

Para 45 :- " However, since the instant matter pertains to award of death sentence, this review petition must be considered in light of the decisions made by this Court in Anvar P.V. and Arjun Panditrao. Consequently, we must eschew, for the present purposes, the electronic evidence in the form of CDRs which was without any appropriate certificate under Section 65-B(4) of the Evidence Act.**"**

Para 46 :- " Accordingly, we too deem it appropriate to consider this review petition by eschewing the electronic evidence in the form of CDRs as they are without the appropriate certificate under Section 65B

even if the law, as it was during the time the trial in the present case was conducted, allowed for such electronic evidence to be admitted."

9. The Hon'ble Delhi High Court, in the case of **Dell International Services Private Limited V. Adeel Feroze & ors (2024 SCC OnLine Del 4576)** held that screenshots of conversations on WhatsApp cannot be admitted as evidence unless it is accompanied by an electronic evidence certificate under Section 65B of the Evidence Act.

10. Shankar Vs State of Haryana (CRA-D-118-2019 , Judgment pronounced on 12.09.2024 , Latest Caselaw 16941 P&H)

Facts of the Case :- Five persons murdered the guard of the company to commit dacoity. CCTV footage showed that five to six persons had entered the company by scaling the wall and committed the murder of Laxman Singh, Guard. The Trial Court convicted the accused under Sections 457, 396, 120-B and 412 of IPC and sentenced them to life, observing that "the CCTV footage had captured the entire occurrence, showing the manner in which, the deceased was being overpowered by the accused and he was ultimately murdered."

Relevancy of electronic evidence :-The Findings of the trial Court are based on the CCTV footage, but while producing the said CCTV footage in evidence, it is not accompanied by the certificate .

Judgment :- Hon'ble High Court upheld the conviction awarded by the trial court which convicted the accused persons on the basis of CCTV footage wherein they were clearly seen committing the crime.

The High Court noted that since the footage was produced without a certificate it is not admissible evidence but the presence of other corroborative evidence is sufficient to prove guilt. In the instant case , The recovery of looted bundles of cloths and the vehicle TATA Ace used while committing the said crime coupled with the sale proceeds of the looted articles clearly connects the chain of evidence to hold that it was the accused persons who had committed the crime in question.

- **CYBER CRIME AND ELECTRONIC EVIDENCE**

Cyber crime :- Any criminal activity that involves a computer or networked device. This can include hacking, financial fraud , cyber stalking , cyber bullying , phishing, identity theft, and more. Collecting and preserving electronic evidence presents a significant challenge in cybercrime investigations.

The dynamic nature of digital data, coupled with the rapid spread of cybercrime, makes the timely identification and retrieval of electronic evidence essential. Effectively managing electronic evidence is crucial for successful cybercrime investigations and ensuring its admissibility in court proceedings

The Shifu App Case :- In the Shifu App case, a notorious banking Trojan named Shifu infected numerous computers, leading to financial fraud. Law enforcement agencies collaborated with cybersecurity experts to investigate the case. Through meticulous electronic evidence collection and preservation, including network

traffic analysis and forensic examination of infected systems, investigators successfully traced the origins of the malware and identified the perpetrators.

The IPL Spot-Fixing Case :- The IPL Spot-Fixing case involved a high-profile cricket betting scandal. Law enforcement agencies, with the assistance of digital forensic experts, collected electronic evidence from mobile phones, laptops, and communication networks. The investigators extracted call records, text messages, and financial transactions, which served as crucial evidence in establishing the involvement of players, bookies, and other individuals. The effective management of electronic evidence played a pivotal role in exposing the illegal activities and ensuring successful prosecutions.

Challenges

The electronic evidences are though admissible in the court of law but they are not free from the challenges regarding admissibility and authenticity of the electronic evidence , such as :-

1 **Authentication of electronic evidence** :- There are no sufficient safeguards to prevent tampering of electronic evidence during investigation. The possibility of originals getting lost, damaged or destroyed cannot be ruled out.

2 **Data Protection and Privacy** :- Electronic evidence is very important for the investigation of cyber crimes. However , it may cause threats to people's privacy rights.

3 **Search, Seizure and Seizure Authority** :- The court will admit the electronic evidence if the methods used to obtain it are in line with legal procedures. The challenge arises when electronic evidence is obtained without proper authority. There is no uniform standard of procedure regulating such search and seizure of electronic evidence .

4 **Lack of technical expertise :-** There are a lot of difficulties faced by the investigating officers due to lack of technical expertise and insight into electronic evidence . Hence , the agencies are seriously handicapped in some respects.

5 **Forensic challenges** :- Electronic Evidence often undergoes forensic examination in order to determine its authenticity . However, challenges can arise due to the rapidly growing technology. Outdated forensic tools present a challenge during the examination, potentially impacting the court's confidence in the accuracy of electronic evidence.

6 **Technological Advancement** :- The evolving technology has posed many challenges for defining and controlling digital technologies like artificial intelligence etc. The rise of AI technologies means courts must now reconsider traditional methods of

evidence authentication to address the complexities of AI manipulation.

7 **Fixing the liability of Social Media intermediaries** :- social media intermediary' means an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services . Robust legal framework and policies are required to ensure availability of evidence from social media intermediaries such as Whatsapp , Instagram , Youtube, etc. since intermediaries are not providing information in respect of the originator of the communication/content on the platforms provided by the intermediaries.

8 **Chain of Custody**: Maintaining a proper chain of custody for digital evidence is crucial to demonstrate that the evidence has not been tampered with or altered during its collection, preservation, and presentation in court. Any breaks or inconsistencies in the chain of custody can weaken the admissibility of evidence.

(**Explanation 5. of S.57 of BSA** —Where an electronic or digital record is produced from proper custody, such electronic and digi tal record is primary evidence unless it is disputed.)

9 **Cross-Border Considerations**:- Digital evidence might be stored across different jurisdictions, which can complicate issues of jurisdiction, data protection laws, and international legal cooperation.

BEST PRACTICES

Ram Ramaswamy v Union of India , Writ Petition(s)(Criminal) No(s). 138/2021:- is pending before the Hon'ble Supreme Court of India urging the Court to pass guidelines regulating the seizure of electronic devices. Since the Government has formed a committee on this issue, which will be coming up with revised guidelines and for the time being at least the CBI manual of 2020 will be followed by all the Central Government agencies.

GENERAL GUIDELINES OF CBI MANUAL

i Procedures for search are envisaged in Section 100 CrPC, 1973 as well as Section 80 of the Information Technology Act, 2000 (if it is applied).

ii During incident response, the biggest challenge is to retain and document the state and integrity of items (digital or otherwise), at the crime scene. The right procedure for identification and seizure of electronic evidence has been dealt with in Chapter 4.

iii Make sure that the panchas have some knowledge and ability to identify various digital devices.

iv Brief the witnesses regarding the tools used to perform search and seizure of the electronic evidence.

v Ensure taking proper toolkit to the crime scene and validation of all the tools.

vi Maintain integrity of electronic evidence. Hash value of electronic evidences should be computed to prove its integrity.

vii It should be kept in mind that the evidences from digital devices connect device to the crime. Additional evidences may be required to connect suspect to the device as well as crime.

viii The exhibits recovered should be properly packed and sealed in presence of independent witnesses. The specimen of the seal used should be affixed on the seizure memo. A separate sample may also be prepared on a sheet of paper, which should be signed by the witnesses and this fact should also be incorporated in the seizure memo. It will be used while forwarding the exhibits to FSL/CFSL for examination by the experts.

ix The seal used should be handed over to one of the independent witnesses for its safe custody after the entire seizure proceeding is completed, under acknowledgement. It is done to ensure proper chain of custody.

x Identity of each electronic evidence should be established in the panchnama. The make, model and serial number should be carefully noted in the panchnama.

xi In order for the evidence to be accepted by the court as valid, chain of custody for electronic evidence must be kept,

or it must be known who exactly, when and where came into contact with evidence in each stage of the investigation.

xii The phrase "chain of custody" refers to the accurate auditing control of original evidence material that could potentially be used for legal purposes. The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed throughout the phases, and must include documentation on how evidence is gathered, transported, analysed and presented.

xiii Knowing the current location of original evidence, is not enough for court, there must be accurate logs tracking evidence material at all time. Access to the evidence must be controlled and audited. The make, model and serial number of the evidence noted in the panchnama, should also be noted in chain of custody forms.

xiv As far as possible, effort should be made to seize primary or original electronic evidence. If secondary electronic record is seized, requirement of Section 65-B of the Indian Evidence Act, 1872 should be complied with. Certificate under Section 65-B of Evidence Act (the subject has been dealt with in detail in Chapter 2) is mandatory for admissibility of secondary electronic record as envisaged by the Hon'ble Supreme Court in Anvar P.V. v. P.K. Basheer'. The said certificate should normally be filed in the court

along with the charge-sheet, however not producing such certificate at the time of filing the charge-sheet is only an irregularity that can be cured at a subsequent stage (Paras Jain v. State of Rajasthan).

xv At the time of charge-sheet, ensure filing of all the relied upon electronic evidences along with Section 65-B certificate for secondary electronic evidence. Also ensure that opinion of expert is included.

- **Standard Operating Procedure (SOP) for Audio-Visual Recording of Scene of Crime :-Released by Bureau of Police Research & Development , Ministry of Home Affairs , Government of India.**

Considering the risk of manipulation of evidence, the mandatory inclusion of audio-video recording in search and seizure proceedings is an important inclusion in BNSS. Section 105 of BNSS contemplates that the process of conducting search of place or taking possession of any property, article or thing including the list of all things seized in the course of such search and seizure and signing of such list by witnesses, shall be recorded through any audio-video electronic means preferably by cell phone and the police officer shall without delay forward such recording to the District Magistrate, Sub-Divisional Magistrate or Judicial Magistrate of the first class.

Issuance of Certificate of Part A of Section 63(4) (c) of the BSA :- In case of audio-video recording(s) done on a Mobile phone, (wherein it is stored on mobile's internal memory or on memory card), the police officer/ operator, should apply hashing software through app/web-based tool on the mobile itself and generate the hash value, note it down and transfer the recording to the expert in the police station, on to the local designated desktop - via Cable or Bluetooth or other default file transfer methods. Police officer shall produce a Part-A certificate of section 63(4)(c) to the officer in-charge of the police station/investigation unit as his part of execution is complete.

- **<u>Checklist at the stage of filing of charge sheet</u>**

1. Search and seizure via audio-video electronic means (section 105 of BNSS) should be accompanied by Chain of Custody proforma in the chargesheet showing how the evidence was collected , stored , and sent for examination to ensure integrity and authenticity of electronic evidence**. (Chain of Custody proforma has been enclosed vide Annexure- 1)**

2. Details of technical persons /cyber expert who identified , collected , and analyzed the electronic evidence should be mentioned

3. Electronic record produced at the stage of filing of charge sheet should be accompanied by the certificate(**PART A**) to be filled by the party who has produced electronic record taken from digital device and the certificate (**PART B**) to be filled by the expert as provided under section 39(2) of the BSA i.e. the opinion of the Examiner of Electronic Evidence referred to in section 79A of the IT Act , 2000. **(Certificate A and B has been enclosed vide Annexure -2)**

4. Hash Report must be enclosed with the certificate. The certificate must mention the hash values (MD5, SHA-1, SHA256, or other legally accepted standard) of the electronic record to prove data integrity.

Note :- **How to calculate hash value of any electronic document-**

a) To get the hash value of an electronic document download an application from the following website under the name of WINmd5/HashCalc.

b) Open the downloaded file and run the application under the name of WinMD5/ HashCalc.

c) Now just drag and drop the file you want to extract the hash value from or select the file from browse menu from file explorer and the MD5 hash value / other hash values will appear**.**

(Screenshot of calculation has been enclosed vide Annexure 3)

5. Serial number or Unique identification number of the digital devices must be mentioned in the certificate to ensure identity of the digital devices.

Note :- How to check IMEI number of any mobile phone. IMEI number of any mobile phone displays at the screen by entering or calling on *#06# .

6. It should be ensured that copy of the electronic evidence has been made in order to supply to the accused person and prosecution .

- **Suggestive measures**

The admissibility of digital evidence is a dynamic field influenced by technological advancements and evolving legal standards. Here are some future trends and policy considerations that may shape the admissibility of electronic evidence:-

1 **Machine Learning and Artificial Intelligence :** For instance, AI-powered image recognition algorithms can be used to assess whether digital images or videos have been manipulated in the case of multimedia evidence. AI can identify possible cases of picture manipulation or forensic tampering by examining pixels, patterns, and discrepancies in the visual data. As AI and machine learning systems generate and analyze more data, courts will need

to address the admissibility of evidence produced by these systems. Policy considerations might include establishing standards for validating the reliability and accuracy of AI-generated evidence.

2 **Blockchain:-** Blockchain technology offers a tamper-proof and transparent way to record transactions. It could play a significant role in ensuring the integrity and authenticity of digital evidence. Courts may need to consider the admissibility of evidence stored on blockchains and the legal status of blockchain records.

3 **Cloud and Remote Storage**: As more data is stored remotely on cloud servers, challenges related to access, authenticity, and jurisdictional issues may arise. Policies might be developed to address these challenges and ensure fair and reliable use of cloud-stored evidence

4 **Expert Testimony and Education:-** Courts may increasingly rely on expert witnesses to explain the technical aspects of digital evidence to judges. Policymakers might consider standards for qualifying and training such experts to ensure accurate and unbiased information is presented.

5 **Continuous Learning & Adaptation and open to innovation -** Given the rapid pace of technological change, legal professionals, judges, and policymakers need to stay informed about the latest developments in digital technology and its implications for evidence.

CONCLUSION

It is necessary that the law should follow the development of science & technology. The *Arjun Panditrao case* has made clarity on the issue of the admissibility of electronic evidence . The production of a certificate under Section 63 of the BSA may be a necessary safeguard to ensure authenticity, although there is a need to formulate other safeguards as well to ensure that privacy and confidentiality of the information contained in electronic records is protected. Also , robust rules for the retention of data involved in trial of offences , preservation, retrieval and production of electronic record, is required to be framed . It's high time for judicial officers to upgrade themselves keeping in tune with latest technological advancements otherwise we would be failing in our sacred duty to sub-serve the ends of justice.

"One may lose evidence not because of 'lack of technology', but because of 'lack of appreciation of technology"

Annexure-1

CHAIN OF CUSTODY FORM

अप.क.....धारा .....

थाना.....जिला.....

जांचकर्ता / विवेचक (नाम / नंबर).....

पीड़ित का नाम पता.....

संदेही / आरोपी का नाम पता.....

जप्ती दिनांक समय.....जप्ती स्थान.....

साक्ष्यों का विवरण			
क.	सामाग्री	संख्या / मात्रा	समाग्री का विवरण

Chain Of Custody				
क.	दिनांक / समय	प्रेषक (हसताक्षर एवं पदनाम)	प्राप्तकर्ता (हसताक्षर एवं पदनाम)	रिमार्क / स्थान

Annexure-2

THE SCHEDULE

[*See* section 63(*4*)(*c*)]

CERTIFICATE

PART A

(To be filled by the Party)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable)
and any other relevant information, if any, about the device/digital record____(specify).

The digital device or the digital record source was under the lawful control for regularly creating, storing or processing information for the purposes of carrying out regular activities and during this period, the computer or the communication device was working properly and the relevant information was regularly fed into the computer during the ordinary course of business. If the computer/digital device at any point of time was not working properly or out of operation, then it has not affected the electronic/digital record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐

by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is _____, obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): _____

Time (IST): _____hours (In 24 hours format)

Place: _____

PART B

(To be filled by the Expert)

I, _____ (Name), Son/daughter/spouse of _____ residing/employed at _____ do hereby solemnly affirm and sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐

CD/DVD ☐ Server ☐ Cloud ☐ Other ☐

Other: _____

Make & Model: _____ Color: _____
Serial Number: _____
IMEI/UIN/UID/MAC/Cloud ID_____ (as applicable)
and any other relevant information, if any, about the device/digital record_____(specify).

I state that the HASH value/s of the electronic/digital record/s is _____,
obtained through the following algorithm:—

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

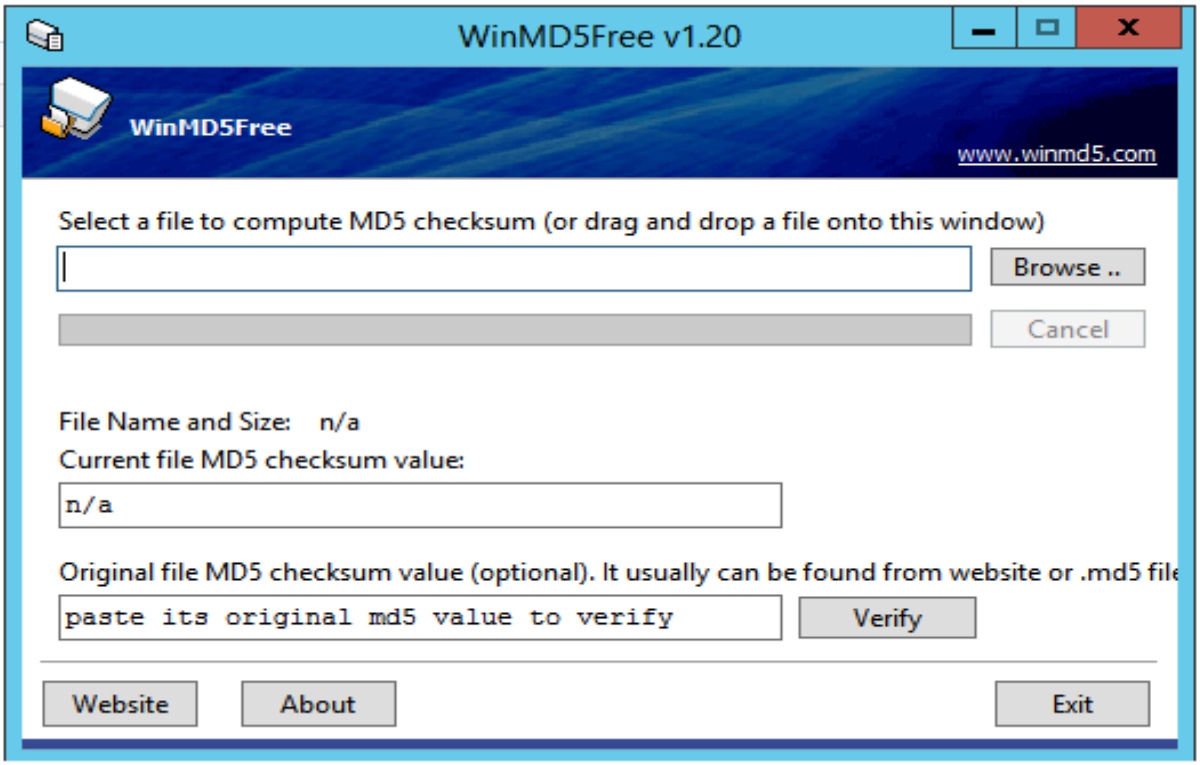
(Name, designation and signature)

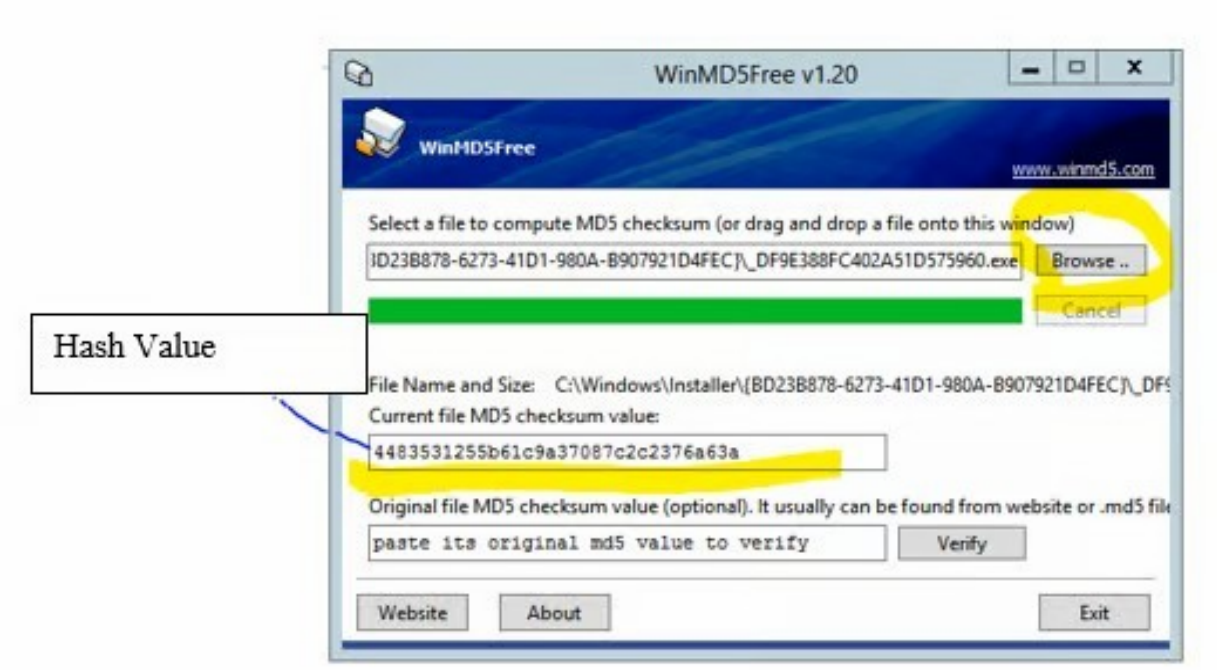
Date (DD/MM/YYYY): _____

Time (IST): _____hours (In 24 hours format)

Place: _____

Annexure -3


WinMD5Free v1.20
WinMD5Free
www.winmd5.com
Select a file to compute MD5 checksum (or drag and drop a file onto this window)
Browse ..
Cancel
File Name and Size: n/a
Current file MD5 checksum value:
n/a
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file
paste its original md5 value to verify
Verify
Website
About
Exit


Hash Value
WinMD5Free v1.20
WinMD5Free
www.winmd5.com
Select a file to compute MD5 checksum (or drag and drop a file onto this window)
Browse ..
Cancel
File Name and Size: C:\Windows\Installer\{BD23B878-6273-41D1-980A-B907921D4FEC}_DF
Current file MD5 checksum value:
4483531255b61c9a37087c2c2376a63a
Original file MD5 checksum value (optional). It usually can be found from website or .md5 file
paste its original md5 value to verify
Verify
Website
About
Exit