Police Order.....328...../2024

Sub:- Standard Operating Procedure for Investigating Officers for Identification, Securing& Collection of Electronic Evidence and Certificate under Section 65B(4) of the Indian Evidence Act, 1872 [under Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023].

The spread of Information Technology has led to increasing use of electronic/digital medium for committing offences. Professional handling of the electronic evidence during investigation is important for detection and successful conviction of offenders. It is, therefore, necessary that investigating officers understand the nature of electronic evidence and procedures to be followed while handling them. This Police Order lays down the procedures to be followed by investigating officers while identifying, securing and collecting the electronic evidence as well as obtaining certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023]. Certificate under Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023 will be applicable in place of certificate under Section 65B(4) of the Indian Evidence Act, 1872 for the cases registered with effect from 01-07-2024.

2. By nature, electronic evidence is time sensitive, can be easily transmitted beyond borders, is volatile, fragile, and can be easily altered, damaged or destroyed. The police officer reaching first at a scene of crime/premises, where the electronic evidence is located, shall be responsible for securing the said premises. The investigating officer or the officer authorised by the investigating officer or a forensic expert notified by the State Government under section 176(3) of the Bharatiya Nagarik Suraksha Sanhita, 2023 shall be responsible for action with regard to identifying and seizing the electronic evidence and should keep in mind that his actions should not change / alter the evidence. Where required, a trained police officer / forensic expert should be engaged for handling electronic evidence and seizure, transfer, storage or examination of electronic evidence should be properly documented in order to maintain the chain

of custody. Any error committed while securing, collection or preservation of electronic evidence may result in damage to electronic evidence affecting the evidentiary value of the evidence before the Court of law.

3. As per the Indian Evidence Act, 1872, for proving/disproving a fact through **secondary** electronic document, it is essential that the investigating officer submits a certificate as mandated by Section 65B(4) of the Indian Evidence Act, 1872. It may be noted that when a fact is sought to be proved/disproved through **primary** electronic evidence, there is no need for submitting certificate under the Indian Evidence Act. For example, where a mobile phone is seized in a criminal case, if the mobile phone seized itself is produced before the Court for proving/disproving a fact, there is no need for submitting certificate under Section 65B(4) of the Indian Evidence Act. However, if the investigating officer decides to prove/disprove a fact by downloading a file etc., from the mobile phone, a certificate under the Indian Evidence Act is mandatory. Certain conditions must be fulfilled for a certificate under the Indian Evidence Act. So, the investigating officer is required to be well versed with the contents of the certificate under the Indian Evidence Act and circumstances in which such a certificate is required to be submitted before the Court.

4. The Investigating Officer must ensure that the electronic material sought to be seized is relevant to the crime being investigated and only so much of the evidence must be seized that is sufficient to establish the crime / role of accused. Unnecessary / indiscriminate seizures must be avoided. The proper documentation of collection and seizure process is important at every stage. It must withstand validation during trial process regarding the procedure, technique and scientific method followed for evidence collection. This Police Order therefore lays down the steps to be followed while identifying, securing and collecting the electronic evidence so that the reliability and accuracy of the digital evidence is maintained and it can be produced as an admissible evidence during trial.

5. **Precautions :** In order to ensure that the evidentiary value of electronic evidence is not disturbed, it is essential that following precautions are taken by the investigating officer:-

i. Secure the premises where the electronic evidence is located.

ii. Identify the wireless connections, if any, in and around the premises.

iii. Check all the rooms in the premises and identify the available electronic devices.

iv. If required, take assistance of trained police personnel authorized by the Officer-in-Charge of the police station and identifythe users, internet access, IP addresses, storage facilities, server/s, user name & password of e-mails, webmail, blogs, social media accounts, internet messaging etc.

v. Identify the potential electronic evidence on the basis of facts of the case.

vi. Sketch the location of electronic evidence and photograph.

vii. Decide, if the entire evidence needs to be seized or a forensic copy of the evidence will be sufficient.

viii. Do not change the current status of the device.

ix. Do not turn ON a device if it is turned OFF.

x. If the device is ON, call a trained person before turning it off or doing anything.

xi. If the device is not charged, do not charge.

xii. Ensure that the device is not left in an open area or unsecured space.

xiii. Document where the device is, who has access, and when it is moved.

xiv. Do not plug in anything to the device, such as memory cards, USB thumb drives, or any other storage media that you have, as the data could be easily lost.

xv. Do not open any application, files, or pictures on the device. It may lead to accidental loss of data or overwriting.

xvi. Do not copy anything to or from the device.

xvii. Take photographs of the evidence (front, back, etc.) to prove its condition.

xviii. Make sure you know the PIN/Password pattern of the device.

xix. Precautionary measures mentioned above are only illustrative. Depending upon the location and nature of electronic evidence, the Investigating Officer may have to take additional precautionary measures. Since seizure of electronic evidence needs to be done

with abundant precaution, it is necessary that the investigating officer carries the IT Investigation Kit while going for investigating such a scene of crime.

6. **IT Investigation Kit :** While going for collecting electronic evidence, the following articles should be part of the IT Investigation Kit to be carried by the Investigating Officer :-

i. Photo / Video Camera or Mobile Phone for recording search and seizure
ii. Evidence Tape
iii. Chain of Custody form
iv. Toolkit (Screwdriver set, etc)
v. Adhesive tape
vi. Sticky note
vii. New/wiped pen drives & hard drives
viii. Gloves & static wrist band
ix. Write blockers
x. Hardware for Imaging (TD2U, Falcon, True Imager)
xi. Pen drives, hard disk, etc.
xii. Laptop with FTK (Crossover Tested)
xiii. Card readers
xiv. Magnifying glass, Flashlight, etc.
xv. Faraday bag/Aluminium foil, Bubble wraps, etc.
xvi. Non-Magnetic tools
xvii. Permanent Markers
xviii. Antistatic bags
xix. Cardboard boxes
xx. Power Bank
xxi. Other materials as required.

7. **Identification of electronic evidence :** Identification of electronic evidence enables the investigating officer to list the potential sources of electronic evidence. While identifying the electronic evidence, the investigating officer should keep in mind the nature of crime, location of crime, location of database server, custodians, site administrators, users, type of information stored in the computer, who transmitted the information & in which form, number & types of devices involved in the

commission of offence, information storage facilities available, remote login capabilities of the computer, network connections available etc. During this stage, every possible source of electronic evidence should be identified by the investigating officer. Following are generally the sources of electronic evidence:

i. Central Processing Unit
ii. Display Monitor
iii. Screens of Mobile Phones
iv. Smart Cards
v. Dongles, biometric scanners etc.
vi. Digital Cameras
vii. CCTV Cameras / DVRs
viii. Personal Digital Assistants [PDAs]
ix. Smart Phones
x. Hard Drives
xi. Local Area Network (LAN) Card/ Network Interface Card (NIC)
xii. Modem & Routers
xiii. Hubs & switches
xiv. Servers
xv. Network cables & connectors
xvi. Pagers, Printers, etc.
xvii. Removable storage media such as Hard Discs,pen drives etc
xviii. Scanners
xix. Copiers
xx. CD & DVD Drives
xxi. Credit Card Skimmers
xxii. Digital Watches
xxiii. Fax machine
xxiv. Global Positioning System (GPS)
xxv. Keyboard & Mouse
xxvi. Call Records
xxvii. e-mail
xxviii. SMS sent through mobile phones
xxix. Tape records
xxx. Digital photographs, etc.

Depending upon the nature of crime, and evidence required for proving/disproving a fact, the investigating officer may look for additional sources of electronic evidence.

8. The investigating officer should keep in mind that information gathered during identification stage may be sought by the court at a later stage. Thus, it is necessary that information gathered during identification phase are correctly documented and preserved by the investigating officer. The process followed should be documented and signed with date & time by the investigating officer. Once identification of electronic evidence is done, the investigating officer may proceed for securing the electronic evidence. It is needless to say that securing electronic evidence requires inspection/visit of the investigating officer to the place of occurrence.

9. Securing the electronic evidence : Following the procedures/ precautions mentioned above, the investigating officer may proceed for securing the electronic evidence. Securing the electronic evidence would mean physically securing the evidence for seizure, labelling, and packaging to prepare the evidence for forensic examination or storage. The investigating officer should keep in mind that sources of electronic evidence are numerous and may be in the form of stand-alone devices, networked devices, storage devices, mobile phones etc., and different kinds of electronic evidence may require different methods of securing.

10. Procedures to be followed while securing different kinds of electronic evidence are as below:

A. Mobile Phone

Use hand gloves or other clean sterile cotton cloth while recovering the mobile phone device from the scene of crime.

If the phone is in switched on

i. Keep the device isolated by selecting flight mode option.
ii. If the flight mode option is not available, use faraday bag to isolate the device.
iii. If faraday bag is also not available, wrap the mobile in aluminium foil.

iv. Plug in the mobile phone to a power bank so that the device does not get switched off.

v. If the mobile device is synced to a computer/laptop and data transfer is occurring, do not pull the phone away from the computer/laptop as data transfer will stop.

vi. Send the phone(s) to forensic lab for recovering physical evidence such as finger prints, DNA, etc and digital evidence such as call logs, SMS, etc. from the device.

vii. Document all the steps followed.

If the mobile phone is switched off

i. Remove the battery, if removable, and photograph the position of SIM(s).

ii. Pack the battery, SIM, and Handset separately.

iii. Note Down the details of SIM and handset details like Make, Model, IMEI, ICCID, etc.

iv. If the device is immersed in liquid, take the device out, remove the battery, SIM card(s),etc. Also collect a small quantity of the liquid in which device had been immersed to prove the effect of the liquid on present state of the device.

v. Send the device(s) to forensic lab for recovering physical evidence such as finger prints, DNA, etc and digital evidence such as call logs, SMS, etc. from the device.

vi. Document all the steps followed.

B. Home / Personal Computer/ Laptop:

i. Verify if the computer or laptop is networked i.e. connected to any router and modem. If so, isolate the system from the network by disconnecting the connected ethernet cable from the system or by disabling the Wi-Fi connection.

ii. Do not straightaway use the computer/ attempt to search for evidence in the computer without following due process.

iii. Photograph the computer, front and back, as well as the cords and connected devices.

iv. Photograph the surrounding area prior to moving any evidence from where it is located.

If the Computer is in switched "OFF" condition

v. If the computer is in "off" condition, do not switch it "on" under any circumstances.

vi. For laptops, etc with removable battery, remove the battery first.

vii. Do not open the laptop as some laptops switch on automatically when the lid is opened.

viii. Removing the battery pack will prevent accidental start-up of the computer.

ix. Unplug the power cord.

x. Sketch and label the cords for identification of connected devices,

xi. Disconnect all the cords and devices,

xii. Nowadays, all-in-one computers come with hard drives embedded within the monitor. In such cases where the hard drive cannot be removed from the device, then it would be prudent to seize the entire device as evidence.

xiii. Carefully open the outer casing of the CPU or Laptop and identify the hard disk.

xiv. Detach the hard disk from the motherboard by disconnecting the data transfer and power cables.

xv. Take out the storage device (hard disk) carefully and record unique identifiers such as the make, model, and serial number. Even if the entire CPU is seized, note down the unique identifiers.

xvi. Ensure that all items have been signed and have complete exhibit labels.

xvii. Search the scene of the crime for non-digital evidence that may be relevant to the case, like diaries, notebooks, invoices, bank transactions, or pieces of paper with passwords.

xviii. Take the assistance of the user in case encryption or password is adopted. Check for the passwords of the operating system present in the suspected system, the application packages, and other computer users.

xix. To avoid clock inaccuracy, note down the actual date and time on the system without causing any changes to the evidentiary value of the systems.

xx. Pack the components, including router and modem.

xxi. Seize the additional storage media, if found.

xxii. Keep all the storage/other media, away from magnets, radio transmitters and other potentially damaging elements.

xxiii. Collect instruction manuals, documentation and notes related with the computer.

xxiv. Document all the steps followed.

If the Computer is in switched "ON" condition

xxv. If the computer is "on" and something is displayed on the monitor, photograph the screen.

xxvi. If the computer is "on" and the screen is blank, move the mouse or press space bar as this will display the active image on the screen. After the image appears on the monitor, photograph the screen.

xxvii. Connect the external USB drive (Preloaded with live data acquisition/ RAM acquisition tools) to the suspect system.

xxviii. Record the make, model, serial number of the USB drive and document it, including the date and time of insertion.

xxix. Acquire RAM using the RAM memory acquisition tools (e.g., Dumpit, CAINE, etc).

xxx. After acquiring the RAM, generate hash value of the forensic image file using live hashing tools (Hash My Files, HashCalc, etc).

xxxi. Take the picture of the hash value along with the hashing algorithm used or copy and paste in notepad and save in external USB drive.

xxxii. Determine whether the system drives are encrypted or not using the appropriate tools (e.g. EDD). While dealing with Windows operating system if encryption is detected, take a copy of Bit Locker recovery keys of each volume and store it in an external storage device.

xxxiii. The non-volatile (HDD/SSD) data available in the system may be acquired using the live forensic tools.

xxxiv. The person attempting to perform live acquisition of the system should be competent and trained to do so.

xxxv. In situations where the computer being seized is in "ON" condition, the imaging process (forensic copying) on-site

must be done from an external storage device and the output of the process should be stored on a sterile digital storage medium like a USB storage.

xxxvi. Perform normal shutdown, if the data on the device is stable. If Anti-forensic shutdown methods are suspected, remove the power cable.

xxxvii. Follow the remaining process as detailed above in the procedure for gathering evidence from switched OFF machine.

C. Network Server/Business Network

i. Consult a trained person/specialist for assistance

ii. Secure the scene and do not let anyone to touch except the personnel trained to handle network systems

iii. Pulling the plug may:

- Severely damage the system
- Disrupt legitimate business.

D. Storage Media

i. Collect the instruction manuals, documents and notes related with the storage media.

ii. Keep the storage media away from magnets, radio transmitters and other potentially damaging devices.

iii. Document all the steps involved in seizure of storage media.

E. Personal Digital Assistant (PDA), Digital Camera, etc

i. If the device is "off", do not turn it "on",

ii. With PDAs, if the device is on, leave the device on. Powering down the device could enable password preventing your access to the evidence,

iii. Photograph the device and display screen, if available.

iv. Label and collect all the cables, including power cords, and transport with the device.

v. Keep the device charged.

vi. If the device cannot be kept charged, examination by the expert must be completed prior to discharge of battery. Else, the data may be lost,

vii. Seize additional storage media such as memory sticks, compact flash, etc., if available.

viii. Document all the steps followed.

F. Cloud Based Digital Evidence

While dealing with cloud-based data for an investigation, it is important to note that cloud computing involves the storage and processing of data on remote servers owned/maintained by third-party service providers. Examples of cloud service providers include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, etc. Steps for handling cloud-based data during an investigation are as below:

i. Identify the cloud services relevant to your investigation. Common cloud storage are: Google Drive, Dropbox, email services etc.

ii. Gather information about the user accounts associated with the relevant cloud services. This may include usernames, email addresses, account identifiers, etc.

iii. Issue a preservation request to the cloud service provider. This request helps the provider to preserve the specified data and prevents its deletion or alteration.

iv. Different service providers may have different processes and requirements and follow the procedure prescribed by the service provider.

v. Some cloud service providers offer forensic tools or APIs (Application Programming Interfaces) that can be used to access and collect data in a forensically sound manner. Such facilities can be used.

vi. Collect relevant metadata associated with the cloud-based data, such as creation dates, modification dates, and access logs. These metadata can be valuable for establishing a timeline of events.

vii. Document each step of the data collection process and include details such as dates, times, methods used, and any challenges encountered.

viii. Follow chain of custody procedures to maintain the integrity of evidence.

ix. In case where the recovery of email-id/password is not possible, the Investigating Officer may send a request to the cloud service provider for preservation of the cloud data.

x. Cloud storage may be accessible from devices if not password protected. The owner may be examined for obtaining password.

xi. If there is access to the cloud storage, data may be imaged using write blockers procedure.

xii. The downloaded data be stored in a fresh storage device and hash value of the data be calculated.

xiii. Password for access to cloud data should be changed in the presence of independent witnesses to prevent alteration or deletion by the owner. New password must be recorded after successful login test and stored in sealed cover along with the seizure memorandum.

xiv. Security question and security phone number for the cloud account also should be changed in order to prevent access by the owner.

xv. Document all the steps followed.

G. CCTV

With the advent of Smart City concepts and increasing use of Closed Circuit Television (CCTV) Surveillance systems, both in personal and institutional settings, the recordings available from these systems have become an important part of crime investigation. An examination of CCTV footage would provide the Investigating Officer with information about the sequence of events, the entry and exit points of the accused persons, etc. To use the footage from CCTV systems as evidence in the court of law, it has to be secured and collected in the following manner :-

Procedures while handling CCTV/DVR/NVR surveillance systems:

i. The investigating officer should survey the site where the subject CCTV system in installed and document the following:
   - Photograph/ sketch depicting the interconnections between CCTV cameras and DVR/NVR.
   - Number of cameras connected to the DVR/NVR system.
   - Check if the system is stand-alone/PC-based or networked.
   - Identify whether the footages are stored on-premise/remote/cloud.

- Determine which camera views are essential for investigation.
- Decide the best method of seizure based on the requirement and situation at the site.
- DVR/ NVR system date and time and actual date and time.

ii. The investigating officer may seize the original hard disk, if feasible, along with the DVR/ NVR systems. If the seizure of the original is not required or not feasible, for instance in cases of CCTVs at railway stations, public places, traffic police camera, etc., then the Investigating Officer should obtain the copy of the relevant footage.

iii. If the entire DVR/ NVR system is required to be seized, check for any Password/PIN enabled in the system. If possible, collect it.

iv. Get details regarding the setup of the system such as
- How is the system configured to record?
- What policy is adopted for overwriting the hard disk space?
- Is there any motion sensor technology adopted?
- Whether the system is protected with a password/PIN or not?

v. Take assistance of the technical person who installed the DVR/NVR system, if feasible.

vi. If the DVR system is not seized, the following steps should be taken:
- The Investigating Officer should issue a preservation notice to the owner/ in-charge to not make any changes in the system.
- Certificate under section 65B(4) of the Indian Evidence Act, 1872 should be obtained from the person who owns or is in-charge of the system.
- Besides other points, the certificate should mention the following technical details:
  - Manufacture of the DVR system
  - Hard disk used in the DVR system
  - Serial number/product number of DVR and hard disk
  - Date & time shown in the DVR system to record the clock inaccuracy
  - The DVR system was functioning properly at the time of incident.

vii. In case, Investigating Officer decides to extract the relevant footages, it is recommended to plug-in a sterile pen drive or external HDD after recording its unique identifiers.

viii. Study the DVD/NVR system and export features. Enter relevant camera frame's start time and end time, select supported download format and download/export in front of witnesses.

ix. While taking the copy of the relevant footage, ensure that there is no mismatch in the frame rate of recorded and retrieved copy.

x. Normally the DVR/NVR stores information on proprietary format, it is advisable to create a copy of the original proprietary format as well as the converted format (e.g. MP4)

xi. Compute and record hash values along with hashing algorithms used. Preview the footage to ensure it is in an accessible format.

xii. If required, the video playback software required to view the video should also be taken into possession.

xiii. Ideally, Investigating Officer should document the complete seizure process through videography /photography and proper documentation.

xiv. The CCTV clipping obtained during the investigation can be directly submitted before the court along with a certificate provided by the owner/in-charge of the CCTV system

xv. The DVR/ NVR system may be sent to Forensic Science Laboratories in below mentioned situations:

   a. Cases where the recovery of the deleted footage is required.
   b. Comparison of photographs/ footages is essential.
   c. Enhancement of the image to identify a person or vehicle number.
   d. To check if there is any video frame disturbance to rule out tampering.

xvi. Document all the steps followed.

H. IoT Devices

i. Identify the IoT devices at the premises/ place of seizure. IoT devices, can be separated into several classes, or groups of devices which include wearable's (e.g. smart watches, fitness bands, smart ring etc), smart speakers, smart displays, control

systems (e.g. smart door lock), virtual assistant (e.g. Alexa, Siri, Bixby etc.) etc.

ii. Different IoT devices are available in the market and new devices are added regularly, the usage and capabilities of these devices can be determined by looking up information online or referring to user manuals.

iii. Take photograph of the IoT device including the peripherals connected to it.

iv. Before taking any action on the device, capture the content/status, if any, displayed on its screen.

v. Examine whether the system is connected to the network, if yes, isolate the devices.

vi. During the isolation process, the investigating officer must be careful of trigger events. These events may result in manipulation of the device itself. Such events may include motion or movement caused by the investigating officer, that may be detected by connected sensors, vocalizing wake-words like saying you found an Alexa device, and "Alexa" is also the wake-word, making sounds above a detectable threshold, or such other actions or trigger events.

vii. Disconnecting the Ethernet wire or turning off the Wi-Fi connection will isolate the IoT device from the network.

viii. Determine if there is a presence of a hub or a router or if the device connects directly to the internet and document the same. In case a hub or a router is connected to an IoT device, those items should also be seized.

ix. Unplug the device's power or take its battery out to isolate from the network. If these methods fail to turn off the device, use a faraday bag or other network isolation techniques.

x. Take a photograph and record the make, model, serial, number, and Media Access Control (MAC) address of the device. This serves as useful documentation in matching the appropriate connections to other devices such as smart phones. It may be noted that identifiers in an IoT Standard include object identifiers, communication identifiers and application identifiers.

xi. Volatile memory can contain useful information that should not be overlooked, if it exists. Due to the limited RAM/storage in some IoT devices, data/files, may get overwritten at frequent intervals.

xii. If the date is stored in cloud or third-party apps, collect the date from the cloud.

xiii. Identify the cloud service providers and learn about the services they offer and the types of information they collect.

xiv. Request data from the service provider, if linked, as data may exist in a proprietary format, so the service provider may provide the data in a common file format.

xv. After extraction of the date from IoT Devices, or associated apps, or connected devices or cloud, compute and save hash values of the collected data.

xvi. Preview the acquired data to ensure it is in an accessible format.

xvii. Document the item as received if the date is in physical media (e.g., an optical disc or a hard drive).

xviii. Ensure to send preservation notice to the concerned cloud service providers for captured data that is stored in the cloud, on mobile and other linked devices, and with other parties.

xix. Seized IoT devices should remain in power-off mode and isolated from the network throughout the process of packaging, transporting, pre-examination storage, etc.

xx. Document all the steps followed.

I. CDRs/ IPDRs/ etc.

i. CDRs/ IPDRs obtained from the Telecom/ Internet Service Providers come within the category of electronic documents and have to comply with the provisions of Indian Evidence Act regarding admissibility.

ii. Where the Investigating Officer obtains these directly through the Nodal Officer of the TSP/ISP, whether in hard copy or soft copy, the same has to be accompanied by a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] issued by the Nodal Officer.

iii. Where the Investigating Officer obtains these through the DIU or another officer, who in turn obtains it through the Nodal Officer of the TSP/ISP, whether in hard copy or soft copy, in that case the

CDR/ IPDR so obtained has to be accompanied by a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] issued by the Nodal Officer of the TSP/ISP as well as a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] issued by the System Administrator of the DIU or the concerned officer.

iv. The Investigating Officer should not analyse / use the original so obtained for analysis by CDR Analysis software but should make a copy thereof for the purpose of analysis. The copy of hardcopy can be made through normal photocopying process. In case of softcopies received, the copy must be done from the storage device containing the soft copy using write blocker so that the original remains secure and the output of the process should be stored on a sterile digital storage medium like a USB storage, Pen drive, etc that can be used for further analysis.

v. The original CDR /IPDR received with the requisite certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] has to be submitted directly as an electronic document / evidence along with the charge sheet in the court.

vi. Document all the steps followed.

J. Audio / Video Clips received through other sources

i. Any Audio / Video clip received by Police through sources such as open sources, internet, informers, viral clips, etc, is also an electronic document.

ii. The admissibility and evidentiary value would depend on the manner of taking it on record. Such clips should not be downloaded from personal mobile phones or randomly from any computer system. The DIU in a district should have a dedicated computer system for receiving such clips.

iii. Such clips should be downloaded from this dedicated computer system along with a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] issued by the system administrator of the said system. The original clips received should be kept stored in the

system for future retrieval, if required. A working copy of the clip should also be downloaded on a sterile digital storage medium like a USB storage, Pen drive, etc that can be used for further analysis by the Investigating Officer.

iv. Investigating Officer should immediately send the downloaded clip for forensic examination regarding the authenticity of the said clip to rule out tampering / editing, etc.

v. Voice spectrography and /or image analysis may also be got done to confirm identity of suspects featuring in such audio / video clips.

vi. Simultaneously, efforts should be made to trace the source of the said clip by carefully analysing the contents. Evidentiary value of the clip would be greater if the origin is traced.

vii. When source / origin is traced, steps as indicated in paras above regarding collection of the electronic evidences, as applicable, should be followed.

viii. Document all the steps followed.

K. Lawfully Intercepted Material

i. Section 5(2) of the Indian Telegraph Act, 1885, Rule 419A of the Indian Telegraph Rules, 1951 and Section 69 of the Information Technology Act, 2000 provide for lawful interception.

ii. The information obtained through such lawful interception comes within the ambit of electronic evidence.

iii. The interception should be done through a secure Voice Logger Machine and the designated system administrator should handle all requests pertaining to sharing of inputs as per the SoP.

iv. Any material obtained through lawful interception must be shared with the concerned Investigating Officer after approval of the Nodal Officer. For this purpose, the system administrator must export only the relevant material and provide it to the concerned Investigating Officer along with a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] in a sterile pen drive or external HDD after recording its unique identifiers.

v. The original of the entire interceptions related to that number / IP or entity must be retained in the secure Voice Logger Machine till

conclusion of the trial. The SoP for Retention / Destruction of Intercepts issued by the Home Department in this regard should be scrupulously followed. Even in case of replacement of the Voice Logger Machine, the original hard disks must be kept preserved till requirement is over.

vi. The Nodal Officer should also provide a copy of the orders of the competent authority authorizing the interceptions under Section 5(2) of the Indian Telegraph Act, 1885, Rule 419A of the Indian Telegraph Rules, 1951 and Section 69 of the Information Technology Act, 2000 as the case may be to the Investigating Officer.

vii. Investigating Officer must also obtain CDR/ IPDR of the relevant phone number / IP address as the case may be to link it with intercepted material. SoP for obtaining CDR /IPDR needs to be followed as already indicated in paras above.

viii. Document all the steps followed.

11. After securing the electronic evidence, the following sequence may be followed for collecting the evidence:

A. Using write-blocker.

B. Extraction of forensic image, and

C. Generating Hash Value.

A. Using write-blocker

Write blockers are hardware/software tools that allows read-only access to the storage media. Write blockers are essential tools in digital forensics to prevent the alteration or modification of data on the original storage media during the process of evidence collection. These tools help the investigating officer to access and analyse the files/data without inadvertently making changes to the evidence. General guidance on how to use write blockers during the collection of electronic evidence is as below:

i. Choose a write blocker that is appropriate for the type of storage media you are dealing with (e.g., hard drives, USB drives, SSDs).

ii. Before connecting the evidence storage media to the write blocker, power down the system where the evidence is located.

This will help to prevent any accidental alterations during the connection process.

iii. Connect the write blocker to the original evidence storage media. If a hardware write blocker is used, ensure that the hardware is properly connected between the storage device and the forensic workstation.

iv. Connect the evidence storage media (via the write blocker) to the forensic workstation/Laptop.

v. Power on the forensic workstation/Laptop and confirm that the write blocker is functioning correctly. Most write blockers have indicator lights or displays to show their status.

vi. Before conducting any forensic examination, ensure that the storage media is in read-only mode. This ensures that no data can be written back to the original source.

vii. Document the use of write blocker and mention details such as type of write blocker used, serial numbers, and any pertinent information about the hardware or software etc.

viii. Once the write blocker is in place, proceed with your forensic analysis. Use specialized forensic tools to examine and collect data from the evidence storage media.

ix. When your analysis is complete, power down the forensic workstation before disconnecting the evidence storage media.

x. Document the removal of the evidence storage media from the write blocker and note the time, date, and any relevant details about the removal process.

B. Extraction of Forensic Image

If the investigating officer plans to extract forensic copy of the electronic device at the scene of crime, he should first identify and document the details of the electronic device of which forensic image is required to be taken. Details such as make, model, and any relevant serial numbers may be correctly documented. Also, the investigating officer should ensure that he has the necessary tools for the extraction the forensic image. Following steps may be taken to extract forensic copy of electronic device.

i. Isolate the electronic device from any network or external connections to prevent remote tampering or data destruction, and

ii. Power-off the device and take steps to preserve its original state. This may even require placing the device in a Faraday bag to block electromagnetic signals,

iii. Document the physical environment where the extraction is taking place. Note the condition of the device, any external storage media, and the presence of any peripherals,

iv. Choose appropriate forensic tools for the extraction process. Common tools include software like FTK Imager, EnCase, or dd (a command-line tool for creating a bit-for-bit copy),

v. Connect the electronic device to the forensic workstation using write-blocking hardware or software to ensure that the extraction process is read-only and does not modify the original data,

vi. Use the selected forensic tool to create a bit-for-bit forensic image of the entire storage media (hard drive, SSD, etc.). Ensure that the tool used is capable of creating a forensically sound image,

vii. Generate hash values (MD5, SHA-1, SHA-256, etc.) for the forensic image. Compare these hash values with those of the original device to verify the integrity of the extracted image,

viii. Record details of the extraction process, including the start and end times, tools used, and any issues encountered during the process,

ix. Store the forensic image in a secure manner, ensuring that it is protected from unauthorized access, tampering, or loss. Follow best practices for evidence handling and storage,

x. If the device has multiple storage media (e.g., multiple hard drives, USB drives), repeat the extraction process for each storage device.

C. Generating Hash Values

Generating and recording the hash values during the collection of electronic evidence is a critical step for establishing data integrity and to maintain the chain of custody. Hash values are unique identifiers

generated by cryptographic algorithms (such as MD5, SHA-1, or SHA-256) and can be used to verify the integrity of electronic files. General guidance as how to collect hash values during the evidence collection process is as below:

i. Document the evidence collection process, including details such as date, time, location, individuals involved, and the purpose of the collection,
ii. Always use specialized forensic tools for evidence collection. These tools often include hash calculation features. Example: EnCase, FTK (Forensic Toolkit), Autopsy, Sleuth Kit etc.,
iii. Forensic tools which can automatically generate hash values during file extraction or imaging processes may be used for convenience,
iv. Choose a secure hash function (e.g., MD5, SHA-1, SHA-256),
v. Make a bit-for-bit copy or forensic image of the entire storage media, preserving the original evidence,
vi. Calculate the hash value for the forensic image,
vii. Calculate hash values for individual files and directories and properly document the hash values generated/calculated,
viii. After collection, verify the hash values of the original evidence against the hash values of the forensic image or collected files. Mismatch, if any, indicates data tampering,
ix. Use write-blockers to prevent any accidental changes to the original media,
x. Maintain a detailed chain of custody record mentioning the hash value,
xi. Safely store the original media in a secure location to maintain its integrity.

12. Labelling, Seizure, Packaging, Transportation and Storage of electronic evidence:

A. Labelling:

After securing the electronic evidence, the investigating officer should properly label the evidence for documentation and identification purposes. The following guidelines may be followed while labelling the electronic evidence.

i. Label the items with unique number/letter/mix and appropriately document the number in the seizure list.

ii. Label at appropriate place on the evidence.

iii. Label the main device together with all its connected devices.

iv. If the cables are also seized, ensure that the cables are properly labelled for future reconstruction.

The investigating officer should ensure that the computer system is photographed as found on site, including the image displayed on the monitor, if the computer system was powered on. Further, the report prepared by the investigating officer should also include other computer systems/data and digital devices identified on site but not seized.

B. Seizure, package, transportation and storage of electronic evidence:

This stage shall start after the evidence has been properly labelled. Procedure given for seizure of evidence need to be strictly followed while seizing the electronic evidence. The evidence must then be packaged with anti-static bag or other materials such as bubble wrapper or plastic bag as electronic evidence may get altered/destroyed by magnetic/radioactive forces. While packing the evidence, the investigating officer must ensure that packaging does not damage the evidence. During transportation, chain of custody should strictly be followed. The following general precautions should be taken by the investigating officer while seizing, packing, transporting and storing the electronic evidence.

i. Do not place the computer systems, computer data and digital devices next to magnetic sources or radio transmitters.

ii. Do not store the computer systems, computer data and digital devices in humid places.

iii. Transport the computer systems, computer data and digital devices without shock or excessive or lengthy vibrations.

iv. Pack the digital evidence in signal-blocking bags such as Faraday isolation bags and radio frequency-shielding material to prevent data/ messages from being sent or

received by the devices. It may be noted that keeping devices in signal-blocking packaging may reduce the battery life significantly. In cases of low battery power, consider putting devices into "flight-mode" wherever possible.

v. Packing the electronic evidence with materials that can produce static electricity (such as Styrofoam) should be avoided.

vi. While transportation, protect the evidence from magnetic sources, moisture, dust and other harmful particles or contaminants.

vii. Various types of evidence need special packaging, so Investigating Officer should have a variety of evidence envelopes, bags, and containers.

viii. The packaging should also be clean, and preferably new, to avoid contamination.

ix. In addition, each piece of evidence should be packaged separately and documented.

x. Proper entry should be made in the Malkhana Register as provided in the Police Manual before storing the electronic evidence in the Malkhana.

13. Chain of custody

Chain of custody is an important requirement for proving the integrity of electronic evidence. The chain of custody for electronic evidence is crucial in maintaining the integrity and admissibility of the evidence in legal proceedings. As per section 193(3)(i) of Bharatiya Nagarik Suraksha Sanhita, 2023 it is mandatory to mention the sequence of custody in case of electronic evidence in the Police report. A well-documented and secure chain of custody ensures that the electronic evidence has not been tampered with, altered, or compromised during its collection, preservation, and analysis. Chain of custody ideally involves documenting the persons who handled the evidence, the date and time when such evidence was collected, and the purpose of collection of such evidence in the case.

Once the evidence is collected and subsequently each time the evidence is transferred, it should be documented and no one else other than the person entrusted with the exhibit should have access to the

evidence. It is important to maintain the chain of custody of evidence to establish the integrity of electronic evidence and to prevent the evidence from getting contaminated. If the chain of custody is not established, the evidence presented in the Court of law might be challenged. The transfer of electronic evidence from one person/location/agency to another should properly be recorded in the Chain of Custody Form, annexed herewith as **Annexure-1** this Police Order.

14. Forwarding the electronic evidence to Forensic Science Laboratory

If the seized electronic evidence requires forensic examination, the investigating officer should send the exhibit to forensic science laboratory for examination. While forwarding an electronic exhibit to a Forensic Science Laboratory (FSL), it is essential to follow specific steps for ensuring integrity, security, and admissibility of the evidence. Below are guidelines to be followed by the Investigating Officer while forwarding electronic evidence for forensic examination.

i. Mention case related information, including the exhibit's description, case number, date and time of collection, and any other pertinent details in your request form.
ii. Obtain necessary authorization/orders from Court.
iii. Establish and maintain a clear chain of custody for the exhibit. Document who has possession of the evidence and when, and ensure the continuity of custody.
iv. Pack the electronic exhibit securely to prevent physical damage during transportation. Use anti-static bags or containers designed for electronic devices.
v. Clearly label the packs with case information, exhibit description, and any handling instructions. Include any specific precautions that the FSL should be aware of while handling the evidence,
vi. Seal the package securely to prevent tampering during transportation. Consider using tamper-proof seals.
vii. Provide details about the exhibit to FSL, the case, and any specific instructions/requirements. Detail of examination to be

conducted, evidence required, key words for making searches etc., may also be provided.

viii. FSLs may have their own protocol of receiving electronic exhibits. While selecting a FSL, also understand the specific protocol to be followed.

ix. Take confirm report/receipt/acknowledgment from the FSL that they have received the exhibit.

x. Update the case file with information about the submission, including the date and time of submission, and any other relevant details.

xi. Be in regular contact with the FSL. Provide any additional information that may assist them in the examination.

xii. Indicative list of Forensic Science Laboratories available in India for examination of electronic evidence has been given in Annexure-2 of this order.

15. Certificate under the Indian Evidence Act, 1872 / Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023.

Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] governs the admissibility of electronic evidence, and specifies the requirement for a certificate to accompany electronic records.

A. When a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [under Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] is required?

When the original device itself is produced before the Court as evidence, no certification under Section 65B(4) of the Indian Evidence Act is required. It is only in cases where a fact is sought to be proved/disproved through **secondary** electronic evidence, a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] is required.

B. Person competent to issue certificate under Section 65B(4) of the Indian Evidence Act,1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023].

Any person occupying responsible position in relation to the operation of the device or the management of the relevant activities may issue the certificate. For example, operator of the device/computer, owner of the computer, officer of the service provider, user of the computer/device, Head of Department in which the computer device is being used etc., are competent to issue certificates under the Indian Evidence Act. It may be noted that under section 63(4) of Bharatiya Sakshya Adhiniyam, 2023 "Part-A" of the certificate will be issued by the person who produces the electronic evidence and "Part-B" will be issued by the expert who examined the electronic evidence. It may be further noted that under section 63(4) of Bharatiya Sakshya Adhiniyam, 2023, mentioning Hash value has been made part of certificate.

C. Requirements of certificate under Section 65B(4) of the Indian Evidence Act, 1872 [under Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023].

For admissibility of a secondary electronic record, the following need to be established:

- Integrity of the data
- Integrity of the hardware/software, and
- Security of the system.

The aforesaid requirements are taken care of by Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] for proving secondary electronic evidence. However, a certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] is about admissibility and not authenticity of the document. The proforma certificate under Section 65B(4) of the Indian Evidence Act, 1872 and under Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023 are annexed herewith as Annexures-3, 4 and 4A of this Police Order.

D. Since the 65B(4)/63(4) certificate is focused on regularity of the input rather than correctness of the input, all the conditions mentioned in the respective certificates must be fulfilled in

order to make an electronic document admissible in evidence. In effect, the 65B(4)/ 63(4) certificate must establish that the computer / communication device was

- Operating properly,
- Regularly used for processing/storing data by the person having lawful control over the use of the computer/ communication device, and
- The electronic output was derived from information fed in the ordinary course of use of the computer/ communication device.

E. Further, the 65B(4)/63(4) certificate should**,**

i. Identify the record such as CD, DVD, Memory card, How was it secured etc.,

ii. Identify the particulars of devices involved in the production of electronic document,

iii. Show that the person issuing the certificate occupies a responsible position in relation to operation of the relevant device or management of the relevant activities,

iv. Mention "best of my knowledge" if in control of the device and "to the best of my belief" if not in control of the device.

It may be noted that a secondary electronic evidence will not be adduced as evidence until the evidence is supported by certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023].Thus, the investigating officer must take all the efforts to submit the certificate under Section 65B(4) of the Indian Evidence Act, 1872 [Section 63(4) of Bharatiya Sakshya Adhiniyam, 2023] while submitting charge sheet.

16. Since Information Technology keeps evolving, it is, therefore, necessary that training and technology requirements are continuously reviewed and updated. The Economic Offences Unit, Bihar shall be nodal unit for research and training for Investigating Officers and supervisory officers on all aspects where cyber medium is involved in the commission of

crime. The Economic Offences Unit, Bihar will standardise the tools/investigation kit required by police stations for crime scene investigation and the Superintendent of Police concerned shall make available the necessary tools to police stations.

17. This order comes into force with immediate effect. ADG CID / ADG EOU / ADG Railways / ADG ATS / Range IsG /DIsG and District SSPs /SPs (including Railways) shall ensure compliance.

Enclosure:-as mentioned above.

3/6/2024

Director General of Police,
Bihar.

Memo no.....19(A).....L2
Bihar Police Headquarters,
Sardar Patel Bhawan, Patna.

Patna, Date: 03/06/2024

Copy to:-

1. Director General, Vigilance Investigation Bureau/ Bihar Home Guards and Fire Services/Training/BSAP for information and necessary action.
2. Director, BPA / Additional Director General of Police, HQ /Mod &SCRB / W&TS/ Prohibition / WS(CID) / Traffic/ EOU/ SVU/ CID / Special Branch/ Budget, Appeal & Welfare/ Railways/ Provisions/ L&O/ Operations and ATS Bihar, Patna for information and necessary action.
3. All IsGP/DIsG (including Range/Railways), Bihar for information and compliance.
4. All SSPs/SPs (including Railways/Units), Bihar for information and compliance.

3/6/2024

Director General of Police,
Bihar.

Annexure-1

Chain of custody form

Details of Electronic Evidence					
Case no. and Police Station					
Name of Investigating Officer with ID and e-mail/mobile number.					
Date of seizure					
Time of seizure					
Description of Electronic Items seized.					
Technical information of each electronic items seized.					
Item no	Manufacturer	Model	Serial No	Date and time of seizure	
Chain of Custody (for each electronic item seized above)					
Item No.	Reason for the movement of electronic item.	Received from	Received by	Date	Time

Annexure-2

Indicative list of Cyber Forensic Lab facilities available in India

i. Forensic Science Laboratory, Bihar, Patna

ii. National Cyber Forensic Science Laboratory :https://ncfl-i4c.mha.gov.in/

iii. CFSL (CBI), CGO Complex, New Delhi, Email: dcfsl@cbi.gov.in

iv. CFSL, Chandigarh, E-Mail: dircfl_chd@dfs.gov.in

v. CFSL, Hyderabad, Email: dircfl_hyd@dfs.gov.in

vi. CFSL, Kolkata, Email: dircfl_kol@dfs.gov.in

vii. ACD, Baba Atomic Research Centre, Mumbai,

viii. State Forensic Science Laboratory, Red Hills, Hyderabad, Telengana,

ix. State Forensic Science Laboratory, Gandhi Nagar, Gujarat,

x. State Forensic Science Laboratory, Kerala,

xi. State Forensic Science Laboratory, Karnataka.

Annexure-3

CERTIFICATE Under Section 65B(4) of Indian Evidence Act, 1872.

Case No._____, Police Station_____, District_____

I, _____, S/O_____, Aged about___ years, resident of _____ do hereby solemnly affirm and state as below:

1. I state that I have produced the printouts of (Mention which document) _____

2. The printouts and other digital documents were taken from the computer owned, maintained, managed and operated by me and the said computer device and the printer details are as follows:

OS Name _____
Version _____
OS Manufacturer _____
System Name _____
System Manufacturer _____
System Model _____
Start-up disk _____
Installed Physical Memory _____(RAM)

3. I state that the computer output containing the information was produced by the Computer during the period over which the Computer was used regularly to store or process information for the purposes of the acts referred to in the evidence regularly carried on over that period by me having lawful control over the use of the computer.

4. I state that 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 in the ordinary course of my correspondences with the Respondent.

5. I state that throughout the material part of the said period the computer was operating properly without affecting the contents of the electronic record or its accuracy or its contents.

6. I state that the information contained in the electronic record is derived from such information fed into the computer in the ordinary course.

Place: Deponent.
Date:

Verification:

Verified on _____at _____ that the contents of the above stated affidavit is true to my best of knowledge/belief.

Deponent.

Annexure-4

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: —

1. Corresponds to Section 167 of the Indian Evidence Act, 1872 (1 of 1872).

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/soft he electronic/digital record/sis _____,

obtained through the following algorithm: —

☐ SHA1:
☐ SHA256:
☐ MD5:
☐ Other_____ (Legally acceptable standard)

(Hash report to been closed with the certificate)

(Name and signature)

Date(DD/MM/YYYY):_____

Time (IST)_____ hours (In 24 hour's format)

Place: _____

Annexure-4A

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/soft he electronic/digital record/s is_____, obtained through the following algorithm: —

☐ SHA1:

☐ SHA256:

☐ MD5:

☐ Other_____(Legally accept able standard)

(Hash report to been closed with the certificate)

(Name, designation and signature)

Date(DD/MM/YYYY):_____

Time(IST)_____hours (In 24 hour's format)

Place:_____