

**GOVERNMENT OF MEGHALAYA
OFFICE OF THE DIRECTOR GENERAL OF POLICE,
MEGHALAYA, SHILLONG**

**CIRCULAR No. 02/2024
(AUDIO-VIDEO RECORDING OF CRIME SCENE)**

1. One of the major changes introduced in the Bharatiya Suraksha Sanhita, 2023 is "Recording of Crime Scene through any audio-video electronic means preferably mobile phone". The use of videography in crime scene investigation is a significant step towards improving the quality of evidence and strengthening the criminal justice system. By recording the crime scene in a credible manner, issues of contradictory witness testimonies and allegations of tampering may be overcome. Transparency in search and seizure proceedings is likely to deter against fabrication of evidence and ensure the presence of independent witnesses in these proceedings. Audio - video recordings have the potential to strengthen the quality of evidence and steps have to be taken to prevent its alteration, modification, and transposition, through direct intervention or unintended corruption of a digital record. However, the effective implementation of this directive requires proper training, resources, and coordination.

2. The electronic evidence may be classified into two categories i.e., (a) Electronic Evidence acquired from the crime scene which is linked to the offence allegedly committed and obtained after search and seizure; and (b) Electronic Evidence generated by the Police Officer during investigation. The provisions of the Bharatiya Suraksha Sanhita, 2023 where Electronic Evidence become extremely significant for Police Officers are illustrated below.

Section	Role of Police	Nature
Section 54	To conduct the recording of the identification process of the arrested person by any audio-video electronic means	Mandatory
Section 63	Issue of Summons by a Court in an encrypted or any other form of electronic communication	Optional
Section 64	Service of summons by electronic communication	Optional
Section 94	An order for production of any document, electronic communication, including communication devices, which is likely to contain electronic evidence or other thing may be issued in electronic form.	Optional
Section 105	Recording of the process of conducting search of a place	Mandatory

	or taking possession of any property, article or thing including preparation of the seizure list preferably by mobile phone.	
Section 173	Information in Cognizable cases may be provided through electronic communication	Optional
Proviso to Section 173	Videography of recording of oral information of a person against whom an offence under section 64/65/66/67/68/69/70/71/74/75/76/77/78/79/124 BNS is alleged to have been committed or attempted, is temporarily or permanently mentally or physically disabled in the presence of an interpreter or a special educator, as the case may be;	Mandatory
Section 176 (1)	Recording of Statement of the victim of an offence of Rape through any audio-video electronic means including mobile phone	Optional
Section 176 (3)	Mandatory visit of crime scene for offences, which are made punishable with an imprisonment for seven years or more, by a forensic expert to collect forensic evidence and videography of the process on mobile phone or any other electronic device.	Mandatory
Section 180	Recording of Statement of witness by audio-video electronic means	Optional
Section 183 (1)	Recording of a confession or Statement by audio-video electronic means in the presence of the advocate of the person accused of an offence	Optional
Section 183 (6)	Recording of Statement of a person, who is temporarily or permanently, mentally, or physically disabled, with the assistance of an interpreter or a special educator, by a Judicial Magistrate through audio-video electronic means preferably by mobile phone	Mandatory
Section 185	Recording of search through audio-video electronic means preferably by mobile phone.	Mandatory
Section 187	Production of accused person in court (except first production, and from judicial custody) through the audio-video electronic means	Optional
Section 193 (3)	Forwarding of Charge Sheet, Final Report, or Detail Investigation Report through electronic communication	Optional

	to a Magistrate	
Section 193 (8)	Submission of copies of the Charge Sheet, Final Report, or Detail Investigation Report for supply to the accused as required under section 230 by electronic communication	Optional

3. The following are the detailed guidelines regulating the procedure to maintain authenticity and accuracy of electronic evidence generated by the Police Officer during investigation.

Pre-Requisites for Search & Seizure

4. The following items, documents, and articles must be carried by the Police Officer before proceeding for search & seizure:

- (a) Model forms related to search & seizure;
- (b) A Mobile Phone or Digital Video Camera;
- (c) A Laptop, Portable Printer, and sufficient Nos. of brand new formatted or forensically wiped Storage Media like CD-R, DVD-R, Pen Drive, SD Card, Hard Disk Drive, Solid State Drive, etc. of adequate capacity depending in the length of the file;
- (d) Packing & Sealing Materials along with Stationaries, as applicable;

Procedure for Audio-Video Recording

5. An Officer in Charge, In Charge, or Investigating Officer or any other Police Officer who has been assigned the duty to make the audio-video recording shall start the recording at the crime scene before initiating the search once the independent witnesses have been requisitioned as per procedure and their presence has been secured.

6. The Police Officer carrying the Digital Video camera or Mobile Phone shall tag alongwith the Police Officer conducting search and seizure. Immediately after starting the recording, the Police Officer conducting the search and seizure or the one recording the search shall introduce himself, independent witnesses, and date, time, and place of recording. For example - *"Audio-Vido Recording started on 1st July 2024 at 1325 hrs at House No. 100, Upper Lachumiere, Shillong in connection with Shillong Sadar PS Case No. 01/2024 u/s 103 BNS. This search is being conducted by UBSI S. K. Marak of Shillong Sadar PS and the recording is being done by UBC/325 A. Shylla. The independent witnesses present during the search are Shri S. Buam and Shri P. K. Marak."*

7. The first recording shall capture the personal search offered by the Police Officer before initiating the search and subsequent frame may capture a 360-degree view of the

place to be searched. The recording should focus on capturing the entire search process, including a detailed walkthrough of the area being searched. It should capture close-ups of seized items, showing their condition and any identifying marks.

8. The Police Officers shall not talk unnecessarily while recording the video unless the same is required for procedural compliance, as applicable. He shall clearly narrate the discovery and seizure of items, ensuring they are visible in the recording.

9. The documentation and signing of the seizure list, Panchanama etc. by witnesses, owner of the place etc. shall be recorded so as to ensure that recording continues from the point of initiation of search till the completion including the documentation, packing, and sealing.

10. On completion of recording, the Police Officer shall narrate the conclusion as follows: "*The search and seizure procedure completed on 1st July 2024 at 1630 hrs.*"

Procedure for preservation of Audio-Video (AV) Recording

11. The AV recording file gets stored on either the internal memory of the device concerned or an external memory in the form of SD Card etc. In either case, the recorded file has to be acquired and preserved properly. The acquisition of electronic evidence is relatively easier if the recording is done on external SD Card or microSD Card which can be taken out, seized as per procedure, and used as a primary evidence.

12. For the sake of understanding, the procedure for acquisition of data in each possible scenario is illustrated herein and the IOs must follow the procedure diligently, as far as practicable. The actual steps may vary if the Police Officer uses a different software application or an upgraded version of the application illustrated herein. The Police Officer shall consult the documentation of the application used before initiating the acquisition process.

Panchanama & Photography

13. In each of the following scenarios, the Police Officer shall initiate a Panchanama in the presence of independent witnesses to record all the steps taken and take photographs at each step. These photographs shall be printed, signed by the independent witnesses, and enclosed with the Panchanama.

Scenario 1 (Original Storage Media available for seizure)

14. The following procedure shall be followed in the scenario in which the storage media like SD Card, Pen Drive etc. in which the original AV recording file was stored can be taken out and seized.

(a) Remove the storage media from the recording device and obtain the signature of independent witnesses on the body of the storage media using a permanent marker. If

the storage media is too small in size and it is not possible to put signature on it, the signature may not be taken. However, the reason for not obtaining signature shall be recorded in the Panchanama.

(b) Connect the storage media to a Laptop, Desktop PC or Forensic Workstation using a Write Blocker Device and calculate the hash value of the storage media using a forensic application like AccessData FTK Imager, etc. The procedure to calculate the hash value using AccessData FTK Imager has been explained in Illustration 1 appended with this circular.

(c) Print the Hash report generated by the application and obtain the signature of independent witnesses on it.

(d) Fill Part A, Part B, Part C, Part D, and Part E of the Audio-Video Electronic Evidence Collection Form (Annexure-1). If it is not possible to calculate hash value at crime scene due to unavailability of Write Blocker Device or Hashing Tool, skip the hashing procedure and leave Part E blank.

(e) Fill Part-A of the certificate u/s 63(4)(c) BSA (Annexure-2).

(f) Fill Chain of Custody Form for Electronic Evidence (Annexure-3).

(g) Pack & Seal the exhibit. Obtain signature of independent witnesses on the package or container, as applicable. Mark Exhibit No. and put your signature. Use permanent marker only.

(h) Handover the seized exhibits along with Annexure-1, Annexure-2, and Annexure-3 to the Officer in Charge. Enclose other documents in the Case Diary.

(i) Make first entry in the Chain of Custody for Electronic Evidence Form (Annexure - 3) at the time of handing over as follows:

Column 1: Date of Handing Over;

Column 2: Time of Handing Over;

Column 3: Name & Signature of Police Officer handing over exhibit;

Column 4: Name & Signature of Police Officer receiving exhibit;

Column 5: Reason for transaction;

Scenario 2 (Original Storage Media not available for seizure and a CD-R/DVD-R is used for storing AV Recording)

15. The following procedure shall be followed in the scenario in which the storage media like SD Card, Pen Drive etc. in which the original audio-video recording file was stored cannot be taken out and the electronic evidence is required to be transferred to another storage media i.e., a CD-R or DVD-R drive in this scenario.

(a) Remove the storage media or connect the recording device to a Laptop, Desktop PC or Forensic Workstation using a Write Blocker Device.

- (b) Connect a CD/DVD Writer Device to the same Laptop, Desktop PC or Forensic Workstation. Insert a new CD-R/DVD-R in the writer.
- (c) Using the writer application, burn/copy the AV recording file from the storage media to the CD-R/DVD-R (Destination Drive).
- (d) Calculate the hash value of the CD-R/DVD-R using a forensic application like AccessData FTK Imager, etc. as explained above.
- (e) Print the Hash report generated by the application and obtain the signature of independent witnesses on it.
- (f) Fill Part A, Part B, Part C, Part D, and Part E of the Audio-Video Electronic Evidence Collection Form (Annexure-1).
- (g) Fill Part-A of the certificate u/s 63(4)(c) BSA (Annexure-2).
- (h) Fill Chain of Custody Form for Electronic Evidence (Annexure-3).
- (i) Remove the CD-R/DVD-R and obtain the signature of independent witnesses. Mark Exhibit No. and put your signature. Use permanent marker only.
- (j) Pack & Seal the exhibit and obtain signature of independent witnesses. Mark Exhibit No. on the on the package or container and put your signature. Use permanent marker only.
- (k) Handover the seized exhibits along with Annexure-1, Annexure-2, and Annexure-3 to the Officer in Charge. Enclose other documents in the Case Diary.
- (l) Make first entry in the Chain of Custody for Electronic Evidence Form (Annexure - 3) at the time of handing over.

Scenario 3 (Original Storage Media not available for seizure and a Pen Drive, SD Card, Hard Disk Drive etc. is used for storing AV Recording)

16. The following procedure shall be followed in the scenario in which the storage media like SD Card, Pen Drive etc. in which the original audio-video recording file was stored cannot be taken out and the electronic evidence is required to be transferred to another storage media i.e., a Pen Drive, SD Card, or Hard Disk Drive in this scenario.

- (a) Remove the storage media or connect the recording device to a Laptop, Desktop PC or Forensic Workstation using a Write Blocker Device.
- (b) Connect a new freshly formatted or forensically wiped Pen Drive, SD Card, or Hard Disk Drive (Destination Drive) to the same Laptop or Desktop PC or Forensic Workstation directly (without Write Blocker Device) and transfer the files from the storage media to the Destination Drive.
- (c) Disconnect the Destination Drive and again, reconnect it to the same Laptop, Desktop PC or Forensic Workstation using the Write Blocker Device.
- (m) Calculate the hash value of the Destination Drive using a forensic application like AccessData FTK Imager, etc. as explained above.

- (d) Print the Hash report generated by the application and obtain the signature of independent witnesses on it.
- (e) Fill Part A, Part B, Part C, Part D, and Part E of the Audio-Video Electronic Evidence Collection Form (Annexure-1).
- (f) Fill Part-A of the certificate u/s 63(4)(c) BSA (Annexure-2).
- (g) Fill Chain of Custody Form for Electronic Evidence (Annexure-3).
- (n) Remove the Destination Drive and obtain the signature of independent witnesses. Mark Exhibit No. and put your signature. Use permanent marker only.
- (o) Pack & Seal the exhibit and obtain signature of independent witnesses on the package or container. Mark Exhibit No. and put your signature. Use permanent marker only.
- (h) Handover the seized exhibits along with Annexure-1, Annexure-2, and Annexure-3 to the Officer in Charge. Enclose other documents in the Case Diary.
- (i) Make first entry in the Chain of Custody for Electronic Evidence Form (Annexure - 3) at the time of handing over.

Procedure for creating Forensic Image

17. There might be scenarios in which the Investigation Officer may require an image of the primary evidence for analysis purpose. The forensic image may be created at the crime scene itself and stored in a Hard Disk Drive or any other storage media. The following procedure shall be followed in such cases:

- (a) Perform all steps as outlined above for Scenario 3 and disconnect the Destination Drive in which AV recording has been transferred. The recording device shall remain connected to the Laptop, Desktop PC or Forensic Workstation.
- (b) Now, connect another new freshly formatted or forensically wiped Pen Drive, SD Card, or Hard Disk Drive (Destination Drive) to the same Laptop, Desktop PC or Forensic Workstation directly (without Write Blocker Device).
- (c) Obtain the forensic image using a forensic application like AccessData FTK Imager, etc. as explained above. The procedure to create the forensic image using AccessData FTK Imager has been explained in Illustration 2 appended with this circular.
- (d) The application shall create a report containing hash value of the forensic image. Print the report generated by the application, and obtain the signature of independent witnesses.
- (e) Disconnect the Destination Drive and again, reconnect it to the same Laptop, Desktop PC or Forensic Workstation using the Write Blocker Device.
- (f) Calculate the hash value of the Destination Drive using a forensic application like AccessData FTK Imager, etc. as explained above.

- (g) Print the Hash report generated by the application and obtain the signature of independent witnesses on it.
- (h) Fill Part F, and Part G of the Audio-Video Electronic Evidence Collection Form.
- (i) Fill Part-A of the certificate u/s 63(4)(c) BSA (Annexure-2).
- (j) Fill Chain of Custody Form for Electronic Evidence (Annexure-3).
- (k) Remove the Destination Drive and obtain the signature of independent witnesses. Mark Exhibit No. and put your signature. Use permanent marker only.
- (l) If the forensic image is required to be sent to the FSL, pack & seal the exhibit, and obtain signature of independent witnesses on the package or container. Mark Exhibit No. and put your signature. Use permanent marker only.
- (m) Handover the seized exhibit along with Annexure-1, Annexure-2, and Annexure-3 to the Officer in Charge.
- (n) Make first entry in the Chain of Custody for Electronic Evidence Form (Annexure - 3) at the time of handing over.

Action to be taken by Officer in Charge at Police Station

18. After handing over of the exhibits and other document as mentioned above, the Officer in Charge shall take following steps:

- (a) Check all the documents, exhibits, packing, sealing etc. If satisfied, make entry in Malkhana Register. Mark the MR No. on Annexure-1 and Annexure-3.
- (b) Handover the seized exhibit to Malkhana in Charge and make entry in the Chain of Custody Form accordingly.
- (c) Return the Audio-Video Electronic Evidence Collection Form and the Certificate u/s 63(4)(c) BSA (Annexure - 2) after signing Part B to the Police Officer or Investigation Officer, as applicable.

Action to be taken by Officer in Charge at Police Station if Hash Value of Secondary Evidence not calculated at Crime Scene

19. If due to any reason the Police Officer conducting the search and seizure is unable to calculate hash value of electronic evidence at the crime scene, the Officer in Charge shall take following steps:

- (a) Requisition two independent witnesses, and obtain the possession of seized exhibits from the Malkhana in Charge in their presence. Update Chain of Custody Form accordingly.
- (b) Draw another Panchanama for this procedure.
- (c) Open the seal of the packed exhibits and calculate the hash value as per procedure explained above.

(d) Prepare fresh Audio-Video Electronic Evidence Collection Form duly filling in Part A, Part B, Part C, Part D, and Part E. In this form, the exhibit shall be shown as seized from the Malkhana In Charge.

(e) Prepare another certificate u/s 63(4)(c) BSA. The Police Officer calculating the hash value shall sign part-A of the certificate and thereafter, the Officer in Charge shall sign Part-B of the Certificate.

(f) Once the process is completed, pack & Seal the seized exhibits, and deposited in Malkhana. Make entry in the Chain of Custody for Electronic Evidence Form and handover the form to Malkhana in Charge.

(g) Hand over the Panchanama, Certificate, and Audio-Video Electronic Evidence Collection Form to the Investigation Officer.

Subsequent Action

20. Subsequent steps to be taken by the Officer in Charge, Investigation Officer, and other concerned Police Officers are as follows:

(a) The seized exhibit and all documents shall be forwarded to the court at the earliest for seen and note.

(b) The investigating Officer shall forward the seized exhibits to FSL for expert opinion regarding integrity of the AC Recording file and other questionnaires in connection with the facts of the case, as applicable.

(c) The chain of custody form shall also be forwarded along with the seized exhibits after proper entries both before forwarding and after seen and note.

(d) When the forwarding letter and exhibits are brought from PS Malkhana to SP Office, Malkhana in Charge and the SP or any other Police Officer under his direction shall sign on the chain of custody form with date and time. Similarly, when the seized exhibits and forwarding letter is handed over by the SPs Office to the duly authorized messenger, the SP or any other Police Officer under his direction as well as the messenger shall sign on the chain of custody form.

(e) The messenger, while depositing the seized exhibits to FSL for examination and at the time of receiving it from the FSL, shall again update the Chain of Custody Form. Similarly, the messenger and the Malkhana In Charge shall sign the chain of custody form at the time of deposition of seized exhibits to PS Malkhana.

(f) The chain of custody form shall be updated every time the seized exhibit is taken out from PS Malkhana for any purpose.

General Instructions

21. The following general instructions shall be followed by the Police Officers:

(a) Always use a new formatted or forensically wiped storage media for storing electronic evidence. The method of formatting and forensic wiping is explained in Illustration 3 and Illustration 4 appended with this circular.

(b) The storage media containing electronic evidence must not be plugged into any computer system or any electronic device without using Write Blocker Device.

(c) Separate Chain of Custody Form should be used for different exhibits and must be updated whenever the electronic evidence changes hands. For example – at the time of submission to PS Malkhana, at the time of sending to FSL for expert opinion, at the time of receipt of the evidence from FSL, while forwarding the evidence to court, etc.

22. This circular deals with the procedure to maintain authenticity and accuracy of electronic evidence generated by the Police Officer during investigation. Other procedures related to search & seizure as enumerated in the Bharatiya Nagarik Suraksha Sanhita, 2023, and other Special & Local Laws shall also be complied with. Separate order shall be issued once any other cloud server based application is implemented in the State of Meghalaya for storage of AV Recording files.

23. The Training & Armed Police Branch, Range Deputy Inspector General of Police, and Superintendents of Police are hereby directed to conduct training courses for subordinate officers regarding the procedure and supervise the actions taken on the field regularly for strict compliance.

24. This circular shall come into effect w.e.f. 1st July, 2024 and remain in operation until further orders. Any circular, order etc. related to similar matter issued earlier by this officer, Law & Order Branch, Range Deputy Inspector General of Police, Superintendents of Police, or any other competent authority within the Meghalaya Police Force shall stand repealed once this circular comes into operation.

Sd/-

(Smti. I. Nongrang, IPS)

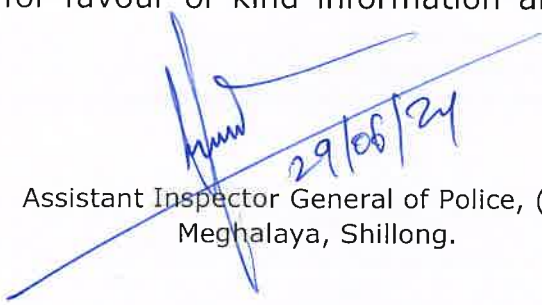
Director General of Police
Meghalaya, Shillong

Memo No. MG/DGP Circular/2024/2

Dated Shillong, the 29th June 2024

1. The Director General of Police, Meghalaya, Shillong for favour of kind information.
2. The Inspectors General of Police (Police Welfare / Comm.) / (R/PR/F&ES) / (SB/Border), Meghalaya, Shillong for favour of kind information.
3. The Dy. Inspectors General of Police (CID) / (ER) / (WR) / (TAP), Meghalaya, Shillong / Tura for favour of kind information.
4. The Principal, PTS, Umran for favour of kind information and necessary action.

5. The Asstt. Inspectors General of Police (A) / (L&O) / (E) / (R), Meghalaya, Shillong for favour of kind information and necessary action.
6. The Spl. Superintendents of Police (SB-I) / (SB-II), Meghalaya, Shillong for favour of kind information and necessary action.
7. The Superintendents of Police (AID), Shillong / (AID), Tura / (City), Shillong / (Traffic), Shillong / (Sadar), Shillong / (SCRB), Shillong / (F&ES), Shillong / (F&ES), Tura / (VIS), Shillong / (Border), Shillong / (EOW), Shillong / (R/PR), Shillong / (Security), Shillong / (ER), Shillong / MPRO, Shillong / MPRO, Tura for favour of kind information and necessary.
8. The Superintendents of Police East Khasi Hills D.E.F, Shillong / West Khasi Hills D.E.F, Nongstoin / South West Khasi Hills D.E.F, Mawkyrwat / Eastern West Khasi Hills D.E.F, Mairang / Ri-Bhoi D.E.F, Nongpoh / East Jaintia Hills D.E.F, Khliehriat / West Jaintia Hills D.E.F, Jowai / West Garo Hills D.E.F, Tura / South West Garo Hills D.E.F, Ampati / North Garo Hills D.E.F, Resubelpara / East Garo Hills D.E.F, Williamnagar / South Garo Hills D.E.F, Baghmara for favour of kind information and necessary action.
9. The Commandant, 1st MLP Bn, Mawiong / 2nd MLP Bn, Goeragre / 3rd MLP Bn, Sahbsein / 4th MLP Bn, Sohpiam / 5th MLP Bn, Samanda / 6th MLP Bn, Umran / SF-10, Shillong for favour of kind information and necessary action.


Assistant Inspector General of Police, (A)
Meghalaya, Shillong.

ANNEXURE – 1
(AUDIO-VIDEO ELECTRONIC EVIDENCE COLLECTION FORM)

A. Basic Details			
FIR/GDE No.			
Date of Seizure:		Place of Seizure:	
Time of Seizure:		MR No.	
Police Officer who seized:			
Person from whom seized:			
Details of Forensic Expert, if any:			
Particulars of Independent Witness (1):			
Particulars of Independent Witness (2):			
Evidence Collection Procedure started at:			
B. Details of Recording Device			
Manufacturer:		Model Number:	
Serial Number:		Type:	
C. Details of Storage Media used in Recording Device, if any			
Manufacturer:		Model Number:	
Serial Number:		Capacity:	
Type:		Exhibit No.	
D. Checklist for Forensic Activities undertaken, if applicable			
Whether Write Blocker Device is available at crime scene?	<input type="checkbox"/>	Yes	<input type="checkbox"/> No
Whether Hash Value was calculated at crime scene?	<input type="checkbox"/>	Yes	<input type="checkbox"/> No
Whether Forensic Image was created?	<input type="checkbox"/>	Yes	<input type="checkbox"/> No
Details of Write Blocker used, if applicable:			
Forensic Tool used for Hashing:			
Forensic Tool used for Forensic Imaging:			
E. Details of Destination Drive used for storing AV Recording File			
Manufacturer:		Model Number:	
Serial Number:		Capacity:	
Type:		Exhibit No.	
Hash Value of Destination Drive (Minimum two algorithms to be used)	<input type="checkbox"/>	MD5	
	<input type="checkbox"/>	SHA1	
	<input type="checkbox"/>	SHA256	
F. Details of Forensic Image in Destination Drive			
Size of Forensic Image:			
Name/Path of Forensic Image File:			

Hash Value of AV Recording File (Minimum two algorithms to be used)	<input type="checkbox"/> MD5	
	<input type="checkbox"/> SHA1	
	<input type="checkbox"/> SHA256	
G. Details of Destination Drive used for Forensic Image		
Manufacturer:		Model Number:
Serial Number:		Capacity:
Type:		Exhibit No.
Hash Value of Destination Drive (Minimum two algorithms to be used)	<input type="checkbox"/> MD5	
	<input type="checkbox"/> SHA1	
	<input type="checkbox"/> SHA256	
Evidence Collection Procedure completed at:		
Signature of Independent Witness (1):		
Signature of Independent Witness (2) :		
Signature of person from whom seized		
Signature of Forensic Expert:		
Signature of Police Officer:		

ANNEXURE – 2

(CERTIFICATE U/S 63(4)(c) OF THE BSA, 2023)

PART A (To be filled by the Party)

I,, S/D/o, 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):

<input type="checkbox"/> Computer	<input type="checkbox"/> Storage Media	<input type="checkbox"/> DVR	<input type="checkbox"/> Mobile Phone
<input type="checkbox"/> Server	<input type="checkbox"/> Flash Drive	<input type="checkbox"/> CD/DVD	<input type="checkbox"/> Cloud
<input type="checkbox"/> Other	Other:		
Make & Model:		Colour:	
IMEI/ UIN/ UID/ MAC/ Cloud ID		Serial Number:	
Any other relevant information, if any, about the device/digital record			

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:

<input type="checkbox"/> Owned	<input type="checkbox"/> Maintained	<input type="checkbox"/> Managed	<input type="checkbox"/> Operated
--------------------------------	-------------------------------------	----------------------------------	-----------------------------------

by me. I state that the HASH value of the electronic/digital record/s is , obtained through the following algorithm:

MD5	
SHA1	
SHA256	
Other	

(Hash report to be enclosed with the certificate)

Date (DDMMYYYY):

Time (IST): hrs

Place:

(Name and signature)

PART B (To be filled by the expert)

I,, S/D/o, 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):

<input type="checkbox"/> Computer	<input type="checkbox"/> Storage Media	<input type="checkbox"/> DVR	<input type="checkbox"/> Mobile Phone
<input type="checkbox"/> Server	<input type="checkbox"/> Flash Drive	<input type="checkbox"/> CD/DVD	<input type="checkbox"/> Cloud
<input type="checkbox"/> Other	Other:		
Make & Model:		Colour:	
IMEI/ UIN/ UID/ MAC/ Cloud ID		Serial Number:	
Any other relevant information, if any, about the device/digital record			

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

MD5	
SHA1	
SHA256	
Other	

(Hash report to be enclosed with the certificate)

Date (DDMMYYYY):

Time (IST): hrs

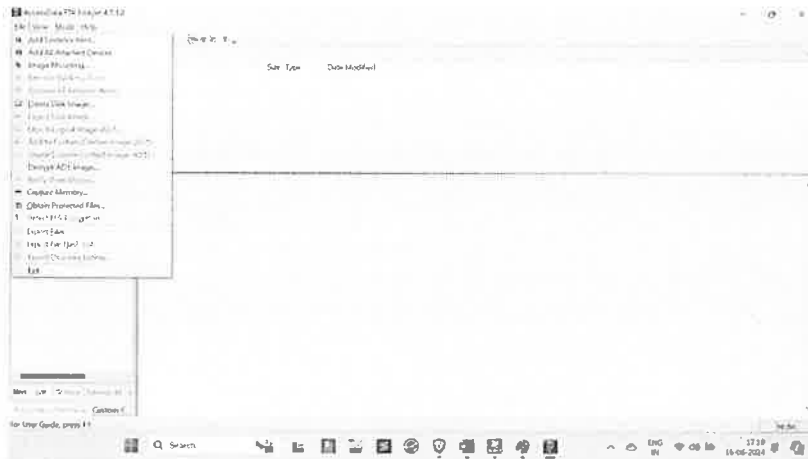
Place:

(Name, Designation, and signature)

ILLUSTRATION – 1

(Calculation of Hash Value using AccessData FTK Imager)

- (a) Plug in the Storage Media into Forensic Workstation/Laptop/Desktop PC using a USB Write Blocker Device. Run the "FTK Imager" application file as Administrator.
- (b) Click **File** and then click **Add Evidence Item**.



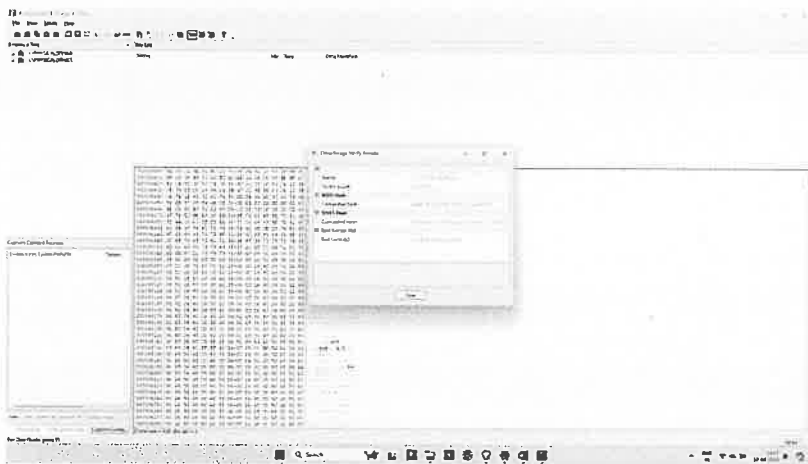
- (c) In the **Select Source** dialog box, select **Physical Drive** and click **Next**.



- (d) Select the **Source Drive** which is the Pen Drive or SD Card, and then click **Finish**. If the IO is not sure about which is the correct drive, he should compare the name of manufacturer and size of drive to select the correct drive.



(h) Once the process is complete, the hash value is displayed as shown below.



(i) Take the screenshot of this page, take signature of independent witnesses, and enclose with the Electronic evidence Collection Form. Mention the hash values in appropriate column in this form.

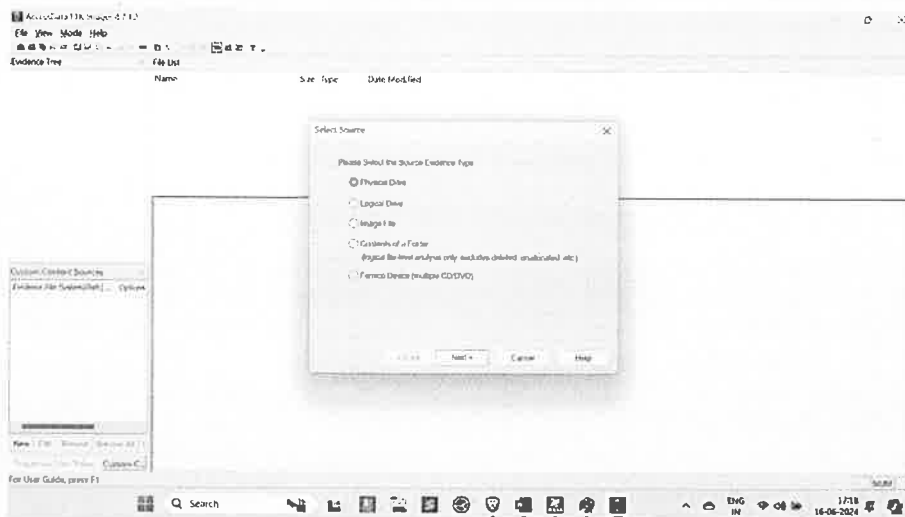
ILLUSTRATION – 2

(Creating Forensic Image of HDD using AccessData FTK Imager)

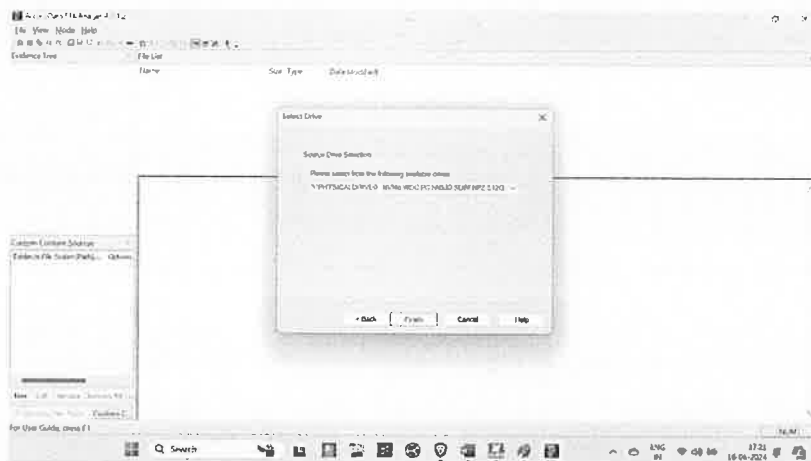
- (a) Plugin the Hard Disk Drive into Forensic Workstation/Laptop/Desktop PC using a USB Write Blocker Device. Run the "FTK Imager" application file as Administrator.
- (b) Click **File** and then click **Create Disk Image**.
- (c) Click the **Create Disk Image button** on the Toolbar.



- (d) In the **Select Source Evidence Type** dialog box, select the source you want to make an image of and click **Next**.
- (e) In case of a hard Disk Drive, select **Physical Drive**.



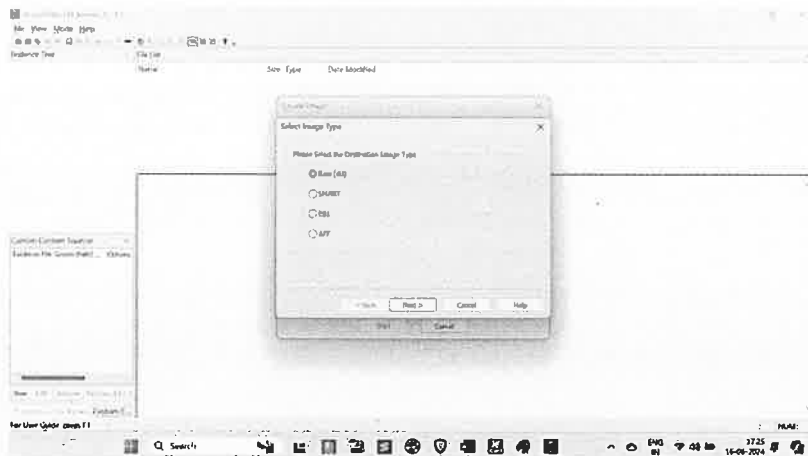
- (f) Select the **Source Drive** or browse to the source of the image you want, and then click **Finish**.



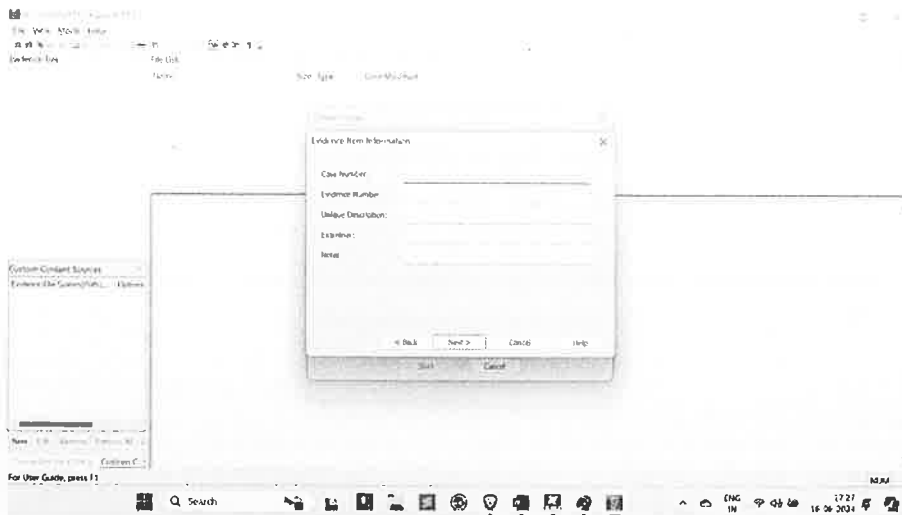
- (g) In the **Create Image** dialog, click **Add**.



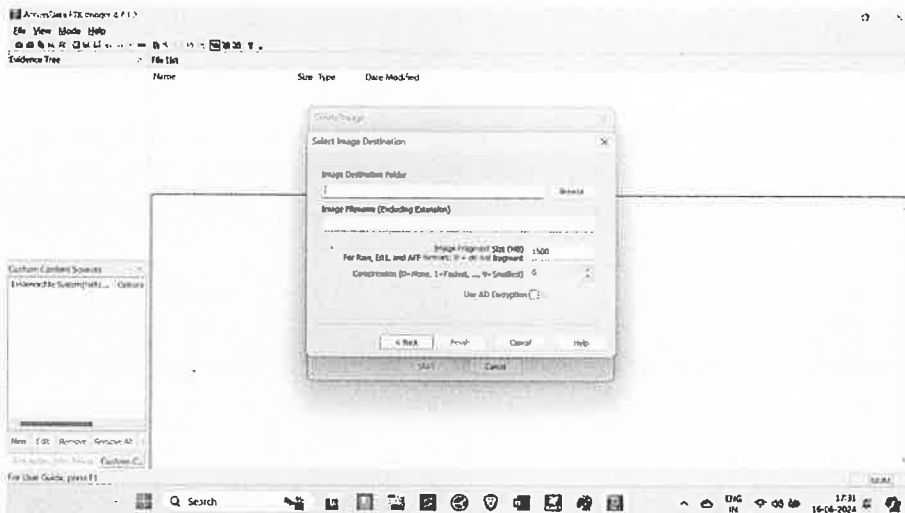
- (h) Check the **Verify images after they are created** box. This option will generate a hash value after creating the image.
- (i) Select the type of image you want to create i.e., **Destination Image Type** and click **Next**. The **Raw(dd)** image type is mostly used. Be sure to have adequate available drive space for the resulting image.



- (j) Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation
- (k) Complete the fields in the **Evidence Item Information** dialog. Enter the FIR/GDE No. in the **Case Number** Field, Exhibit No. in the **Evidence Number** field, **Unique Description**, if any, Name of IO or Forensic Expert in **Examiner** field, and Observation Notes, if any, in **Notes** field, and click Next.



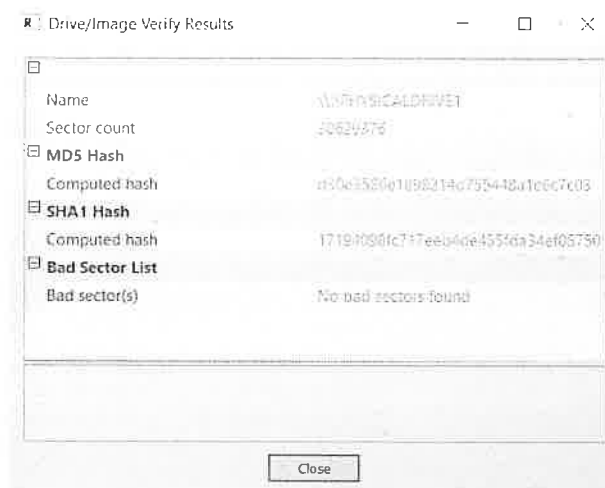
- (l) In the **Image Destination** dialogue box, in **Image Destination Folder** field, either type the location path where you want to save the image file, or click **Browse** to find and select the desired location. If the destination folder you select is on a drive that does not have sufficient free space to store the entire image file, FTK Imager prompts for a new destination folder when all available space has been used in the first location. However, all related image files must be saved together in the same folder prior to being added to a case.



- (m) In the **Image Filename** field, specify a name for the image file but do not specify a file extension.
- (n) Specify the **Image fragment** Size and click **Finish**.

Default Image Fragment Size	1500 MB
To save images segments that can be burned to a CD	650 MB
To save image segments that can be burned to a DVD	4000 MB

- (o) A progress dialog appears showing various details. After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 hash values, and bad sectors.



- (p) Take the screenshot of this page, take signature of independent witnesses, and enclose with the Electronic evidence Collection Form. Mention the hash values in appropriate column in this form.

ILLUSTRATION – 3

(Formatting using Windows OS)

- Connect the storage media to your computer.
- Open File Explorer.
- Right-click on the storage media and select "Format".
- Select the file system. Choose the file system you want to use for the pen drive. Common options include FAT32, exFAT, and NTFS.
- Choose the allocation unit size. Select the allocation unit size, which determines how the drive is divided into smaller blocks for storage.
- Format the storage media by clicking "Start" to begin the formatting process. This may take a few minutes to complete.

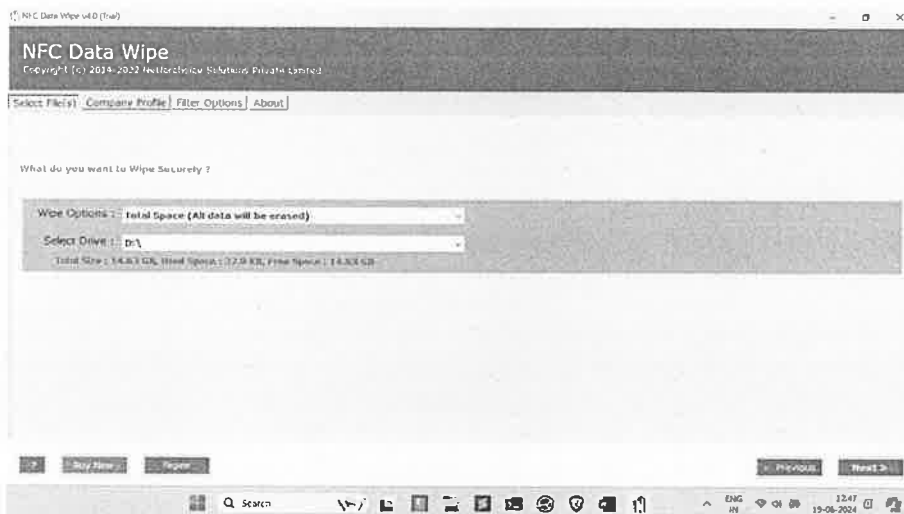
ILLUSTRATION – 4

(Forensically Wiping using NFC Data Wipe Software)

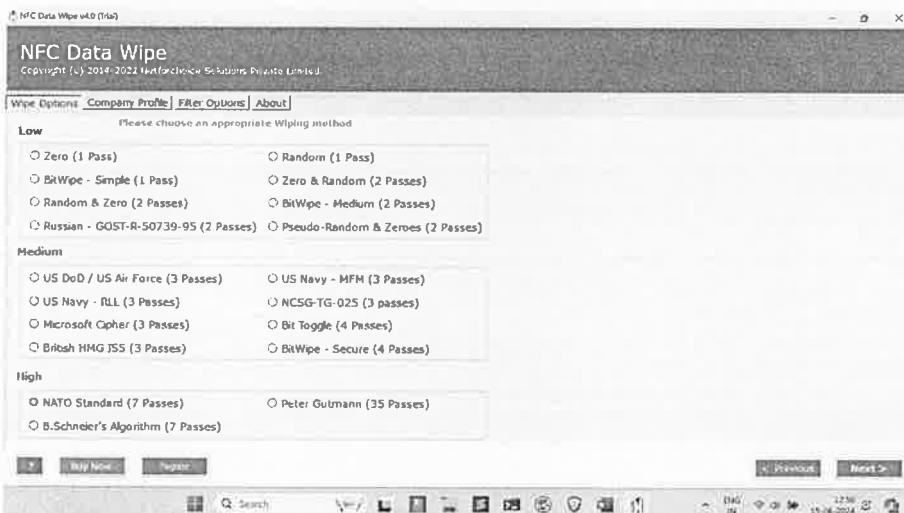
- Plugin the storage media to a computer or laptop in which the NFC Data Wipe Application is installed.
- Run the **NFC Data Wipe** application files as Administrator.
- Once the application window opens, Select **Wipe Logical Drives**.



- (d) On the next screen, select **Wipe Options: Total Space (All data will be erased)**, and in **Select Drive**, select the storage media to be wiped and click **Next**.



- (e) Select **NATO Standard (7 passes)** and click **Next**.



- (f) Select Wipe.

