The Directorate of Forensic Science Laboratories, State of Maharashtra, Home Department, Mumbai

*** Guidelines to the Investigation Agency for Identification, Seizure of Digital Storage Evidence and its Submission to the Cyber Forensics Division ***

1. **INTRODUCTION**:
   The CYBER CRIME is an unlawful act wherein any digital storage media is either used as a tool or made a target or both. It covers every single digital storage media.
   The different types of cyber crimes are referred as hacking, software piracy, music piracy, movie piracy, child pornography, ATM credit/debit card related frauds, phishing, spoofing, threatening, cyber defamation (fake profile), cyber stalking, data theft, mail bombing, financial fraud etc. The cyber crimes also relate to the cases such as murder, rape, bomb blast, CCTV footage etc.
   The **CYBER CRIME FORENSICS** division of this directorate works to deal with such crimes to help the investigation agencies to create more concrete digital evidence, which is admissible in the court of law. The roles and responsibilities of this division include reconstruction and detailed analysis of the digital evidence extracted from the submitted digital storage media using forensic methods and tools; and presenting it in a meaningful format.

2. **IDENTIFICATION OF DIFFERENT TYPES OF DIGITAL STORAGE MEDIA**:
   The different types of digital storage media are received in this division for detailed Cyber Forensic analysis. The identification of these digital storage media is one of the crucial procedures to be followed at the crime scene. The below mentioned list of such different types of digital storage media will help to investigating team to identify the correct digital evidence for the case.
   a) Hard Disks - Internal type of IDE, SATA, SCSI, SSD interface and external type of USB 2.0, 3.0 port, Server hard disks etc.
   b) Mobile Phones - Standard Mobile Phones, China made Mobile Phones, Smartphones such as Android OS Based Mobile Phones, Windows OS Based Mobile Phones, iOS based Mobile Phones such as iPhones, iPads, Tablets etc.
   c) SIM Cards - Standard SIM Cards, Micro SIM Cards etc.
   d) Memory Cards - MSC, MS PRO, SMC, CFC, MD, XD, SDC and MMC type etc.
   e) USB Pen Drives, USB Internet Modems
   f) ATM Debit/Credit Cards
   g) Digital Cameras, Camcorders, Pen Cameras
   h) Compact Disks (CDs)/DVDs
   i) Floppy Disks

3. **SEIZURE OF DIFFERENT TYPES OF DIGITAL STORAGE MEDIA:**
   Once identified, the proper care should be taken while seizing the evidence to avoid it from getting tampered. The seized material should be packed and sealed properly. Some guidelines are given below depicting the care to be taken while handling digital evidence.
   CPU CABINETS AND/OR LAPTOPS:
   a) If CPU cabinet/s and/or laptop/s are seized from the crime scene, then kindly remove the hard disk/s (CD/DVD if any) from them and submit ONLY hard disk/s (CD/DVD if any) in this division.
   b) The description of these seized CPU cabinet/s and/or laptop/s can be mentioned in the forwarding letter.

c) Other accessories such as keyboard, mouse, monitor, scanner, printer, laptop power adapter etc. are not required to be submitted.

NOTE-If no technical assistance is provided at the crime scene for opening the CPU cabinets and/or laptops and removing the hard disk/s from them, then DO NOT TRY TO OPEN IT AND REMOVE THE HARD DISK. This may damage the evidence, if done inappropriately. In such cases, these CPU cabinets and/or laptops can be submitted here. At the case receiving time, the CPU cabinets and/or laptops will be opened and hard disk/s will be removed in front of police official and the said CPU cabinets and/or laptops will be returned in the FSL sealed parcel/s to the same police official at the same time.

CCTV FOOTAGE DIGITAL VIDEO RECORDER (DVR) SYSTEM:

The below mentioned points can be noted down, before shutting down and seizing the CCTV FOOTAGE DVR system from the crime scene.

a) Any USB device attached to the DVR system
b) No. of working channels
c) Description of DVR system

Also, take a copy of the Software-CD, containing the video file player, which is used to play the captured CCTV footage video files. It is most important, since every DVR system has its own unique player used. The CCTV footage video files can be played ONLY by using its respective software.

MOBILE PHONES:

a) Remove the battery from the mobile phone/s before sealing it.
b) Keep the battery separately in the same parcel that of mobile phone.
c) If SIM Card/s and/or memory card are removed from the mobile phone, then do keep them separately in the same parcel that of mobile phone.
d) Submit the USB Data Cable for the respective mobile phone, mainly for iPhone, iPad, if found. It should be sealed in the same parcel that of mobile phone.

NOTE-

It is always a good practice to remove the battery from the Mobile Phones to avoid it from getting switched on during travelling or sealing.

Remove the SIM Card/s and/or memory card from the seized mobile phone/s only, if possible.

4. TYPE OF MATERIAL TO BE USED FOR PACKAGING THE SEIZED EVIDENCE:

Some types of material that can be used to take good care of the seized evidence and protecting it from getting damaged are listed below.

a) Thick Cardboard Boxes
b) Plastic Bubble-Wraps
c) Small Polythene Bags

The Directorate of Forensic Science Laboratories, State of Maharashtra, Home Department, Mumbai

*** Guidelines to the Investigation Agency for Identification, Seizure of Digital Storage Evidence and its Submission to the Cyber Forensics Division ***

5. PROFORMA OF A LABEL ON PACKED EVIDENCE:

An appearance of a packed parcel of an evidence should be easy to understand and descriptive. It should depict the description of evidence inside the sealed parcel. The below mentioned information is required to be mentioned on the label that will be sticked on the sealed parcel.

a) Case Registration Number (C.R. No./ A.D.R. No./ MECR No. / L.A.C. No. etc.)
b) Sections of IPC Act, IT Act and others if any
c) Date of Seizure
d) Signatures of Investigating Officer (IO) and two Panchās
e) Description of exhibit inside the sealed parcel

6. PROFORMA OF FORWARDING LETTER:

The below mentioned detailed information is required through the "Forwarding Letter" to be submitted.

a) Letter Outward Number
b) Letter Date
c) Full Postal Address of Police Station
d) Subject
e) Case Registration Number (C.R. No./ A.D.R. No./ MECR No. / L.A.C. No. etc.)
f) List and description of the exhibit/s to be submitted
   E.g. In case of-
   - Mobile Phones - Do mention Make, Model No., Type, IMEI No. etc.
   - SIM Cards - Do mention Make, Card No., Colour etc.
   - Memory Cards - Do mention Make, Type, Capacity, any other printed number etc.
   - Hard Disks - Do mention Make, Model No., S/N (Serial Number), P/N (Part Number), Capacity etc.
g) Sample Seal - The copy of a seal used to seal the parcel/s of the exhibit/s at crime scene is required on the forwarding letter. Note: It must be clear and readable on both parcel/s of exhibit/s and forwarding letter.
h) Brief history of crime
i) Questionnaire - Must be specific and clear. They should depict what kinds of results are expected, which can help to gather more and more evidence from the digital storage media.
j) Reference Document/s - In some cases, such as document forgery, fake internet profile, threatening e-mails etc., the reference documents will be helpful to us. The photocopies of these reference documents MUST be attested by Investigating Officer and should also contain the seal of the police station.
   E.g. Copies of e-mail content, forged documents, original documents, photographs of victim/s and accused
k) List of attached and to be submitted material -
   - Total no. of sealed parcel/s or envelope/s of exhibit/s sent for submission
   - Total no. of blank hard disk/s provided
   - Total no. of pages attached attested photocopies of reference documents, if any
   - Copy of FIR, if any
   - Copy of Panchanama, if any

l) Name, Designation, Batch No. of Police Official who will bring the forwarding letter and sealed parcel/s of exhibit/s

m) Signature, designation stamp of senior official of the police station, name and contact number of Investigating Officer, contact number of the police station and police station stamp

7. REQUIREMENT OF MATERIAL NEEDED FOR ANALYSIS:

As per the cyber forensic procedures, the forensic analysis is not performed directly on the submitted digital evidence, mainly in the case of hard disk drive, to avoid tampering of evidence. The mirror image, i.e. a clone copy (exact bit-by-bit) of the submitted hard disk drive is created on a new blank (forensically cleaned) hard disk drive and then the entire cyber forensic analysis is performed on this newly created mirror image. For mirror image processing, we require blank new hard disk drive along with the exhibit (hard disk drive). Kindly provide the new blank hard disk drive as per the below given guidelines.

a) A new blank hard disk drive MUST be of double capacity that of the exhibit.
E.g. If the hard disk of capacity of 80 GB is to be submitted, then provide a new blank hard disk of capacity of 160 GB. If two hard disks of capacity of 500 GB each are to be submitted, then provide two new blank hard disks of capacity of 1000 GB (1 TB) each.

b) Do prefer a new blank hard disk drive of INTERNAL and SATA type interface since it makes the data transfer faster.

NOTE-
If the exhibit/s to be submitted is mobile phone, SIM card, memory card, CD, DVD then new blank hard disk is not required.

8. If any assistance/information is required about sealing or labelling the exhibits, finalizing the questionnaire, or any other queries, then you can contact us on number viz. "022-26670755/58" with "Cyber Forensic Division" extension number viz. "321", "323", "325", "339" and "345" during working hours during from 10:00 AM to 05:30 PM.