KERALA POLICE

STANDARD OPERATING PROCEDURE

DIGITAL EVIDENCE RELATED TO CRIMES AGAINST WOMEN AND CHILDREN

PREFACE

Justice C.N. Ramachandran Nair Commission on Police and Prisons Reforms has recommended that *the digital evidence, especially that which related to crimes against women and children, are to be collected immediately (or as early as possible) and then, preserved scientifically because any delay or lapse in the collection and preservation of these digital materials can result in the unavailability of some valuable digital evidence of the perpetrator's criminal activities and so, can be ultimately unhelpful to the victims.*

In this connection we have issued, time and again, various instructions and those have to be complied with. However, we don't have a consolidated SOP.

Therefore, I directed to prepare a Standard Operating Procedure (SOP) which will help the investigators to follow proper procedure in collection of digital evidence, to collate them and present them before Courts. Sri. S.Sreejith IPS, ADGP Crimes; Sri. Kori Sanjaykumar Gurudin IPS, DIG TVPM Range and Sri. E.S.Bijumon, Addl. SP, Hi-Tech Cell, PHQ have done excellent work in comprehensively preparing the SOP. I compliment the Officers for their work of diligence, sincerity, skill and knowledge.

I am sure this SOP will be very useful to one and all and these procedures are to be followed by the concerned Police Officer. As the technology is changing, there will be a requirement to change the SOP over the period of time. Therefore, the Nodal Officer of the Cyberdome, ADGP of the Crime Branch and the Chief of the Kerala Police Hi-Tech Cell, PHQ must issue timely amendments and make necessary changes as per requirement.

LOKNATH BEHERA IPS
DGP & State Police Chief
Kerala

Thiruvananthapuram
29-04-2021

STANDARD OPERATING PROCEDURE FOR DIGITAL EVIDENCE RELATED TO CRIMES AGAINST WOMEN AND CHILDREN

GENERAL CONTENT

CHAPTER 1

INTRODUCTION

Section 79A Information Technology (Amendment) Act 2008 defines electronic form of evidence as "**any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cellphones and digital fax machines".**

The main feature of digital evidence is that it can be transmitted beyond borders with ease and speed, highly fragile and can be easily altered, damaged, destroyed and also time sensitive. Owing to this reason special precaution should be taken while documenting, collecting, preserving and examining digital evidence.

Digital evidence especially that which related to crime against women and children are to be collected immediately as early as possible and should be preserved scientifically because digital evidence are highly volatile. Any delay or laps in collection and preservation of digital evidence will result in unavailability or deterioration of valuable evidences. So ultimate care and diligence should be used for collection of digital evidences so that all available evidences are collected and the victim does not suffer any miscarriage of justice.

Conventional crimes against women and children

- Rape (sexual assault)
- Kidnapping/abduction
- Molestation
- Eve teasing
- Dowry homicide
- Dowry suicide
- Acid attack

Cyber harassment against women and children

- Cyber Bullying
- Cyber Teasing
- Cyber Stalking

- Cyber Defamation
- Identity Theft
- Catfishing
- Doxing
- Swatting
- Trolling
- Revenge Porn

WHAT ARE DIGITAL EVIDENCE & THE NATURE OF DIGITAL EVIDENCE?

Digital evidence or electronic evidence is "any probative information stored or transmitted in digital form that a party to a court case may use at trial". Section 79A of IT (Amendment) Act, 2008 defines electronic form evidence as "any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, and digital fax machines".

The main characteristics of digital evidence are, it is latent as fingerprints and DNA, can transcend national borders with ease and speed, highly fragile and can be easily altered, damaged, or destroyed and also time sensitive. For this reason,special precautions should be taken to document, collect, preserve, and examine this type of evidence. When dealing with digital evidence, the principles that should be applied are, actions taken to secure and collect digital evidence should not change that evidence; persons conducting the examination of digital evidence should be trained for this purpose and activity relating to the seizure, examination, storage, or transfer of digital evidence should be fully documented, preserved, and available for review.

ADVANTAGES OF DIGITAL EVIDENCE

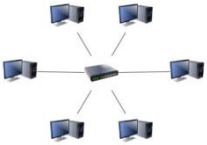
In addition to the advantages of recovering deleted files, digital evidence contains a wealth of critical data and "embedded" information for both intact files as well as deleted files. For example, forensic software can view the contents of a Excel file to reveal, (depending on how it was configured by the user), information such as: the creation date and original author; dates the file was last accessed, modified and printed; when the file was last saved and by

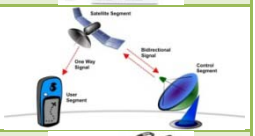
whom; the number of times the file was edited, for how long and by whom; the number of revisions; client name, ID and reference number; hidden key words and comments that identify who edited or collaborated on the file; and the original file location.

DIGITAL DEVICES – SOURCES FOR DIGITAL EVIDENCES

Throughout this SOP is an attempt has been made to provide the investigators an understanding of the investigation of cybercrimes or crimes involving computer resources. Towards this primary understanding and knowledge of the digital devices and their uses is assumed.

Sl. No.	Digital Device	Potential Evidence	
1	**CPU**	The device itself may be evidence of component theft, counterfeiting etc. The device contains digital devices with all the files and folders stored including deleted files and information, which may not be seen normally. Cyber Forensic is used to image, retrieve and analyze the data.	
2	**Display Monitor (CRT/LCD/TFT etc.) screens of Mobile Phones, if switched on**	All the graphics and files that are open and visible on the screen in switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and through description in seizure memo.	
3	**Smart Cards, Dongles and biometric scanners etc.**	The device itself, along with the identification/authentication information of the card and the user, level of access, configurations and permissions.	
4	**Answering Machines**	The device can store voice messages and sometimes, the time and date information about when the message was left. It may have details such as last number called, memos, phone numbers & names, caller identification information, deleted messages.	

5	**Digital Cameras**	The device can be looked for images, videos, sounds, removable cartridges, time& date stamps.	
6	**Handled Devices (Personal Digital Assistants [PDAs], Electronic Organizers, Smart Phones)**	Much information can be obtained from these devices like address book, appointment calendars/information, documents, emails, phone book, messages (text & voice), emails passwords etc.	
7	**Hard Drives**	The device in itself, as it stores all the information.	
8	**Local Area Network (LAN) Card or Network Interface Card (NIC)**	The device itself and also MAC (Media Access Control) address can be obtained.	
9	**Modems, Routers, Hubs and Switches**	The device itself. In routers, configuration files contain information related to IP addresses etc.	
10	**Servers**	Information like last logins, mails exchanged, contents downloaded, pages accessed etc. can be obtained.	
11	**Network cables and connectors**	Network cables are used to trace back to their respective computers. Connectors help in identifying the types of devices that are connected to the computers.	
12	**Pagers**	The device can be looked for address information, text messages and phone numbers.	
13	**Printers**	The device has data like number of prints last printed and some maintain usage logs, time & date information. If attached to a network, they may store network identity information. In addition, it can also be examined for figure prints	

14	**Removable storage media and devices**	All New generation mobile phones, cameras etc., use these. These devices store files, in which evidence can be found.	
15	**Scanners**	The device itself, having the capability to scan may help prove illegal activity.	
16	**Telephones**	Many telephones can store names, messages (text, voice), memos, passwords, phone numbers, and caller identification information. Additionally, some cellular telephones can store appointment information, and may act as a voice recorder.	
17	**Copiers**	Copies may contain some documents both physical and electronic, user usage logos, time and data stamps.	
18	**CD & DVD Drives**	These devices store files/data in which evidence can be found.	
19	**Credit Card Skimmers**	Tracks of magnetic stripe contain Cardholders information which may include: Card expiration date, User's address, Credit card numbers, and User's name.	
20	**Digital Watches**	Some latest digital watches contain information like address book, notes, appointment calendars, phone numbers, emails etc.	
21	**Fax machine**	These devices contain some documents, phone numbers, send/receive logs, film cartridges that can be considered.	
22	**Global Positioning System (GPS)**	The device may provide travel logs, home location, previous destinations, way point coordinators, way point name etc.	
23	**Keyboard & Mouse**	These devices can be examined for fingerprints.	

CHAPTER 2

STANDARD OPERATING PROCEDURE (SOP)

IMPORTANCE OF SOP IN THE INVESTIGATION

Standard Operating Procedures (SOPs) are agency unique documents describing themethods and procedures to be followed in performing routine operations. SOPs areessential to improve the quality and to implement uniform processes for conductingdigital & multimedia evidence forensic tasks in a precise, accurate manner. SOPsshould be task-based and written for each procedure conducted. They should bereviewed at least annually. The previously approved versions of an SOP should beretained for reference.

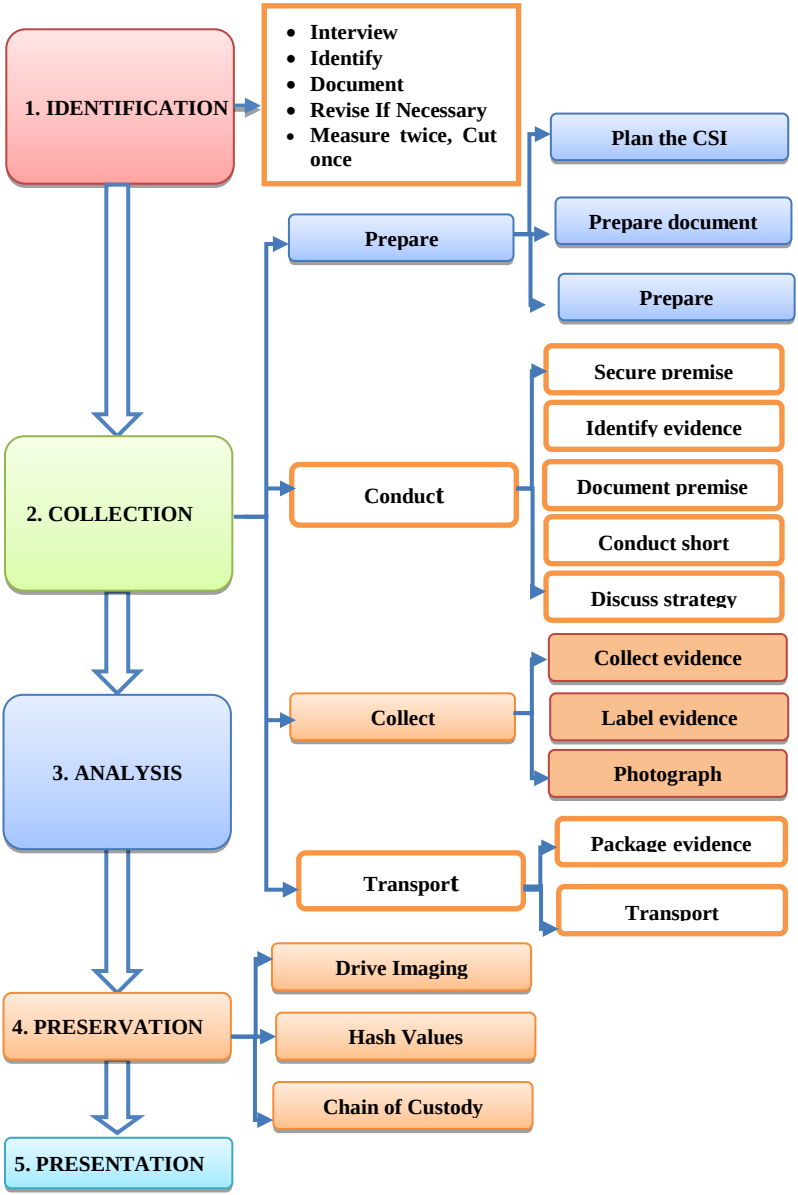
The SOPs guide us to develop every process in the investigation right from securing the scene and identifying media to be collected, etc., till the time charge sheet is filed and evidence is adduced in the court of law. Due to the nature and legality of digital evidence, it is clear that an investigation in an automated environment requires standard methods and procedures for the following main reasons:

Evidence has to be gathered in a way that will be accepted by a court of law. This will be easier if standard procedures are formulated and followed. This will also facilitate the exchange of evidences in cases having interdepartmental and international ramifications, especially, if investigators from all departments and countries collect evidence in a similar manner.

Every care must be taken to avoid anything which might corrupt the data or cause any other form of damage, even accidentally. The use of standard methods and procedures minimizes this risk of damage. In some cases, it is inevitable that some data will be changed or over written during the examination process. Thus there is a need for a thorough understanding of technology, which is being used for examination and also need for its documentation so that it would be possible to explain the causes/ effects later on in a court of law.

Some of the most important reasons for improper evidence collection are poorly written policies, lack of an established incident response plan, incident response training. This may result in a broken chain of custody.

DIGITAL EVIDENCE COLLECTION WORKFLOW



The methodology involves with 5 basic phases; Identification, Collection, Analysis, Presentation and Preservation. Most of the time, Police Officer shall involve with only three (3) phases of the Digital Forensics Methodology; which are the Identification, Collection and Preservation phase. The next topic shall describe the process involves in handling the digital evidence.

Step No. 1.

IDENTIFICATION

Before any digital forensic examination begins, the scope of actions must be identified. Who are the key players and custodians? What are the best sources of potential electronic evidence that will need to be accessed for collection? This information is needed for many reasons, including:

- So that no essential evidence is missed that might affect a case
- So costs can be estimated in advance and the scope of the case can be adjusted to fit actual needs
- So potential sources of evidence identified later will have smaller impact in cost increases

a. Interview

Conducting interviews is a very important early step in a successful digital forensic examination. When determining relevant devices from which to collect data for a case, these individuals must be interviewed at a minimum:

- Custodians
- Site administrators
- Users-when available

b. Identify

- Look at the range of variables and determine what factors are at play in the case, including:
- To what extent does legal authority exist to make a search?
- Is there an administrator who can identify devices and custodians?
- How many and what type of devices may be involved?

- Are any peripheral devices involved, such as flash drives, printers, scanners or memory cards?
- What types of electronically stored information (ESI) are potentially involved? It could be photographs, documents, spreadsheets, emails, text messages, databases and many other types of ESI.
- How was ESI communicated and who was communicating? We may be looking for email addresses, text numbers, IP addresses and other similar information.
- Has information been stored in an offsite location? On backup media? In the cloud? In remote locations?
- Are there devices involved that have potential remote login capabilities?
- What different operating systems may be involved?
- Do any devices require continuous electric power to operate?
- Other variables?

c. Document

- Interviews, including:
- Names and titles of interviewees
- The number and types of primary and peripheral devices to be included in the collection and search
- Any locations from which peripheral devices may have been removed or where they were found
- Whether or not any kind of network is present
- File types involved
- Any off-site storage that is used
- What different types of software are present, including any proprietary software

d. Revise If Necessary

If it is determined that additional electronic evidence (not included in the original plan) needs to be gathered, it's important to determine if there is a need for a legal warrant, amended consent form or any other changes to the original scope of work.

e. Measure Twice, Cut Once

Digital evidence needs to be thoroughly assessed with respect to the scope of the case. The scope of a forensic examination cannot include "everything." At least, not unless there is unlimited time and budget involved.

It is important to spend time at the very beginning to more accurately determine the true scope of the examination, narrow down what digital evidence is needed for a case and where to find it. Otherwise, costs will grow and grow as the investigation moves forward, as will the amount of time required for the investigation.

Taking the extra time and attention to accurately determine necessary devices and custodians prior to proceeding with the next steps in the forensic process will dramatically impact the investigation as a whole and, therefore the outcome of the case.

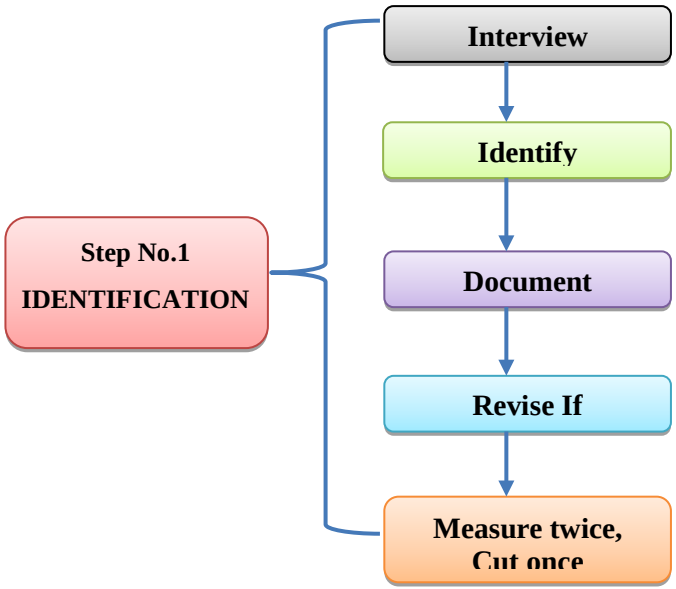
This phase, the Identification, is a phase where Police Officer collects some preliminary information prior to collecting the evidence. Preliminary information may help Police Officer to strategize the process of collecting the evidence, especially if the incidents happen at several locations.In most cases; evidence that need to be collected varies from one case to another. For example, a web related case may involve with collection of the web server and the database server, whereas a document counterfeiting case may involve with the collection of a personal computer.

The following lists some of the questions that may guide Police Officer in establishing the facts of the case:

Sample of Questions for Preliminary Information Gathering

WHAT	• What types of crime is it? (Financial fraud, harassment, cyber terrorism, bribery) • What are the resources needed? (People, equipment, budget) • What are the needed documents? (Warrant, Seizure list, Chain of custody form) • What is the IP address? • Who owns the IP address?
WHO	• Who are the people involve? • Who are the IT personnel of the premise? • Who are the top management of the company?
WHERE	• Where is the location of the crime? India or cross border? • Where is the database server?
WHEN	• When did the crime happen? • When did the investigating team first detect the crime?
HOW	• How did the crime happen?

The following flow chart detailed out the process involves in Identification phase.

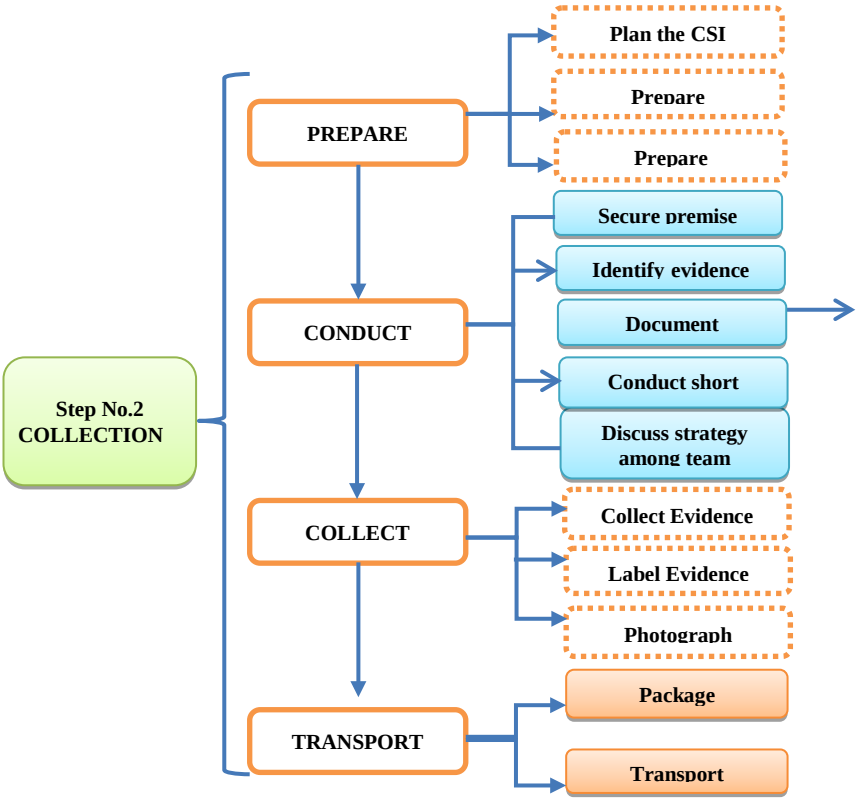


Police Officer must be aware that some of the information gathered during this phase might be tendered into court. Thus, it is necessary that all information gathered during this phase be documented or preserved. Preserving the information is also important in order to conduct a smooth storyline to stakeholders. The preserved information or the written document is best to be printed out, signed and dated by the person who produces it.

Step No. 2

COLLECTION

The next phase is to set off to the premise to collect the evidence. During collection phase, there are several steps that a Police Officer may follow. The process of collection is summarized in the following flow chart:



❖ **Steps in Prepare phase are**

1. **Plan the CSI (Crime scene investigation)**

1. During this phase, Team Leader shall conduct a briefing session and brainstorming session.
2. Items to be briefed:
    - Introduce team members;
    - Purpose of raid;
    - Explain the committed offense, the related Act, the location of the premise, the expected total numbers of occupier and IT literacy of the suspect;
    - The strategy of the Crime Scene Investigation (CSI);
    - Evidence transportation & lodging;
    - Team member's transportation & lodging.
3. Ensure competent personnel are available during the CSI.

2. Prepare document

- Ensure that related documents are readily available.
- Example: Investigation Diary or journal, seizure list, and chain of custody form.

3. Prepare equipment

List of possible equipment's to be brought:

- Camera
- Evidence labeling tool (markers, stickers, tie-on tagging)
- Evidence packaging (anti-static bag, aluminum foil, bubble wrapper, cardboard box)
- Imaging tool
- Pre-Analysis tool (Encase, FTK)
- Storage device to store acquired data
- Power bank for your mobile phone
- Tools, small pliers, wire cutters
- Torch

Synchronize your watch/computer/mobile phone with atomic clock.

❖ **Steps in Conduct phase are**

1. Secure premise

- Once you have arrived at the premise, identify wireless connections around the premise and the security features.
- Identify yourself and the purpose of the raid.
- Identify person-in-charge of the premise and everyone else in the premise.
- Check all rooms in the premise and identify available digital devices.
- Check as well the occupier's vehicles.
- Move people away from the digital devices and power source.

2. Identify evidence

- Identify technical person and interview him.
- Identify potential evidence based on the facts of the case.

3. Document premise

- Sketch these items in diary/journal for the purpose recreating/conveying details of the scene to stakeholders:
  - The plan of the premise.
  - Location of the evidence

4. Conduct short interview

- The purpose is to gather and verify information.
- Information to be gathered:
  - Purpose of evidence
  - Users of the evidence
  - Type of internet access & ISP
  - Any offsite storage
  - Username & password of the digital device, email, webmail, blogs, social media or instant messaging.

5. Discuss strategy among team members

- Police Officer may then need to make decision of these matters:
  - Do we need to collect all digital evidence?
  - Do we need to collect; or just forensically copy them?
  - Do we need to forensically copy them bit by bit, or just copy the related folder/file?
  - Is our storage media able to store all acquired data?

- Ensure that each decision is justifiable.

❖ **Steps in Collect phase are**

1. Collect Evidence

The 'Collect' process depends on types of digital evidence.

2. Label Evidence

- Label must be UNIQUE.
- Label at appropriate place.
- Label parent device together with its sub devices.
- If you decide to seize the cables, ensure that the cables are properly labeled for future reconstruction.
- Write down complete serial number OR unique identification of the evidence in diary.

3. Photograph Evidence

- While documenting the evidence's details are important, Police Officer can always choose the option of photographing the evidence.
- Take photograph of the device and its labeling, overall view and close up view.
- Items to be captured; device setting, serial number, manufacturer, model, any unique features, etc.
- Photos can facilitate understanding in court, especially when presenting information of items that was not seized at the premise.

❖ **Steps in Transport phase are**

1. Package

- This process takes place after the evidence has been properly labeled.
- The evidence must then be packaged with anti- static bag, or other materials such as bubble wrapper or plastic bag.
- Police Officer must ensure that the packaging:
  - Able to detect any attempt to gain access to the evidence.
  - Does not damage the evidence; ie. Water resistant
- Both party, Police Officer and the occupier, sign the Seizure List.
- The chain of custody now starts here.

- Any transfer from one officer to another shall be recorded in Chain of Custody Form.

2. Transport

- During transportation, the evidence in the vehicle must not be left unattended.
- At least one personnel must be in the vehicle at all time

Critical Steps in Preserving Digital Evidence while collecting digital evidence

o As a general rule, make sure you do not turn ON a device if it is turned OFF. For computers, make sure you do not change the current status of the device at all. If the device is OFF, it must be kept OFF. If the device is ON, call a forensics expert before turning it off or doing anything.

o If it is not charged, do not charge it; for mobile phones, if the device is ON, power it down to prevent remote wiping or data from being overwritten.

o Ensure that you do not leave the device in an open area or other unsecured space. Document where the device is, who has access, and when it is moved.

o Do not plug 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.

o Do not open any applications, files, or pictures on the device. You could accidentally lose data or overwrite it.

o Do not copy anything to or from the device.

o Preserve any and all digital evidence that you think could be useful for your case.

o Take a picture of the piece of evidence (front, back, etc.) to prove its condition.

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

- Last but not least, do not trust anybody without forensics training to investigate or view files on the original device. They might cause the deletion of data or the corruption of important information.

Step No. 3

ANALYSIS

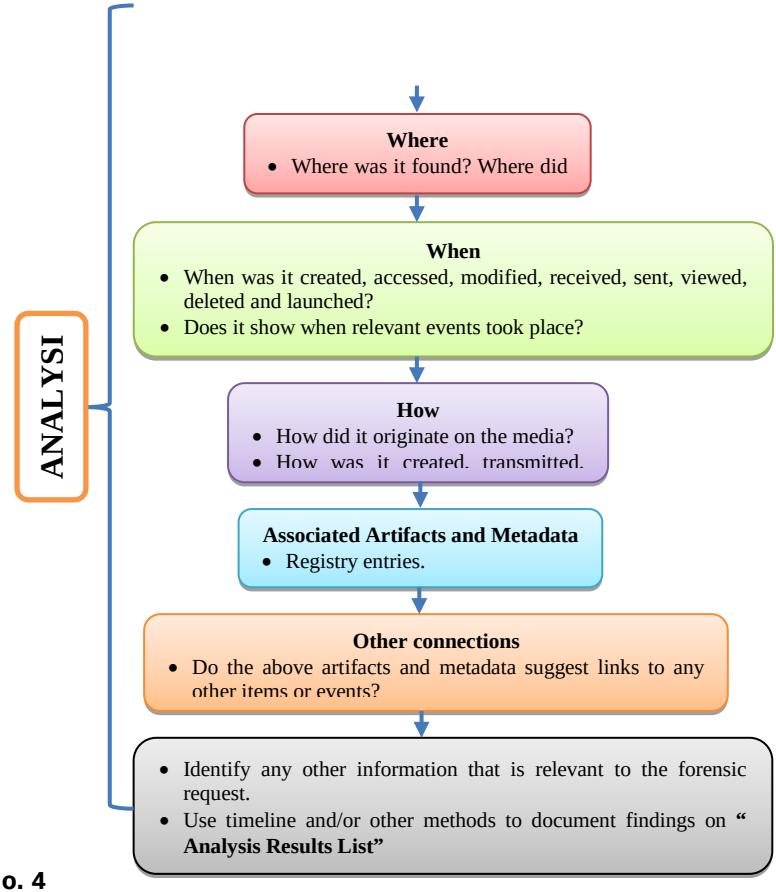
In the analysis phase, examiners connect all the dots and paint a complete picture for the requester. For every item on the Relevant Data List, examiners answer questions like who, what, when, where, and how. They try to explain which user or application created, edited, received, or sent each item, and how it originally came into existence. Examiners also explain where they found it. Most importantly, they explain why all this information is significant and what it means to the case.

Often examiners can produce the most valuable analysis by looking at when things happened and producing a timeline that tells a coherent story. For each relevant item, examiners try to explain when it was created, accessed, modified, received, sent, viewed, deleted, and launched. They observe and explain a sequence of events and note which events happened at the same time.

Examiners document all their analysis, and other information relevant to the forensic request, and add it all to a fifth and final list, the "Analysis Results List." This is a list of all the meaningful data that answers who, what, when, where, how, and other questions. The information on this list satisfies the forensic request. Even at this late stage of the process, something might generate new data search leads or a source of data leads. If this happens, examiners add them to the appropriate lists and consider going back to examine them fully.

Finally, after examiners cycle through these steps enough times, they can respond to the forensic request. They move to the Forensic Reporting phase. This is the step where examiners document findings so that the requester can understand them and use them in the case. Forensic reporting is outside the scope of this article, but its importance cannot be overemphasized.

The final report is the best way for examiners to communicate findings to the requester. Forensic reporting is important because the entire forensic process is only worth as much as the information examiners convey to the requester. After the reporting, the requester does case-level analysis where he or she (possibly with examiners) interprets the findings in the context of the whole case.



Step No. 4

PRESERVATION

Preservation is process where evidence is taken care to ensure that it is not tampered, chain of custody is not broken and integrity is intact. Police Officer must ensure that evidence is properly preserved from the point of taken, to the point of it is handed over to other authorized personnel. Police Officer must

also be able to demonstrate that evidence is properly preserved to stakeholders.

The methods of Evidence Preservation are:

a. Document evidence's variables

- Items to be documented:
  - o Evidence's Serial number
  - o Manufacturer & Model
  - o Storage size (if applicable)
  - o Any defects from normal condition, example: keyboard missing 'k' letter
  - o MAC address (if applicable)
  - o Hash value (if applicable)
  - o This can all be written down in the Seizure List, which is signed by the occupier and the Police Officer.

b. Label and seal

- Label or tag the evidence. It must be unique.
- Label must be able to stay throughout the lifetime of the evidence.
- Label sub device as well, for example, memory card of a mobile phone.
- Label of sub device must be able to be tracked to parent device.
- Label at appropriate place. (Not on the display screen or at the opening of battery).
- Seal properly (anti-shock, water-resistant, anti-static charge). Seal must be able to detect any attempt to gain access to the evidence.

c. Document the chain of custody

As investigators collect media from their client and transfer it when needed, they should document all transfers of media and evidence on Chain of Custody (CoC) forms and capture signatures and dates upon media handoff.

It is essential to remember chain-of-custody paperwork. This artifact demonstrates that the image has been under known possession since

the time the image was created. Any lapse in chain of custody nullifies the legal value of the image, and thus the analysis.

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. These would be people who have seized the equipment, people who are in charge of transferring the evidence from the crime scene to the forensic labs, people in charge of analyzing the evidence, and so on. As electronic evidence is easy to tamper or to get damaged, it is necessary for us to know exactly who, when, what, where, and why was the evidence transferred to the concerned person. It is possible that defense may level charges of tampering and fabrication of evidence and, it would be difficult to prove the integrity of the evidence, if the chain of custody is not properly maintained. Lack of integrity in the process of custody and, absence of appropriate documentation in this regard, will not only be detrimental to the cyber-crime investigation, during trial but also, expose the IOs to criminal liability under Section 72 of the ITAA2008.

Important Points to remember for Foolproof Chain of Custody:

- Physically inspect the storage medium-take photographs and systematically record observations.
- Guard against hazards like theft and mechanical failure. Use good physical security and data encryption. House multiple copies in different locations.
- Protect digital magnetic media from external electric and magnetic fields. Ensure protection of digital media particularly optical media from scratches.
- Account for all people with physical or electronic access to the data.
- Keep the number of people involved in collecting and handling the devices and data to a minimum.
- Always accompany evidence with their chain-of-custody forms.
- Give the evidence positive identification at all times that is legible and written with permanent ink.

- Establishing the integrity of the seized evidence through forensically proven procedure by a technically trained investigating officer or with the help of a technical expert will enhance the quality of the evidence when the case is taken forward for prosecution. The integrity of the evidence available on a digital media can be established by using a process called as “Hashing”.
- Establish a baseline of contents for authentication and proof of integrity by calculating hash value for the contents. An identical hash value of the original evidence seized under panchanama (Seizure Memo) and, the forensically imaged copy, helps the IO to prove the integrity of the evidence. Similarly, the seized original evidence can be continued to be checked for its integrity by comparing its hash value, to identify any changes to it.

d. Drive Imaging

Before investigators can begin analyzing evidence from a source, they need to image it first. Imaging a drive is a forensic process in which an analyst creates a bit-for-bit duplicate of a drive. This forensic image of all digital media helps retain evidence for the investigation. When analyzing the image, investigators should keep in mind that even wiped drives can retain important recoverable data to identify and catalogue. In the best cases, they can recover all deleted files using forensic techniques.

As a rule, investigators should exclusively operate on the duplicate image and never perform forensic analysis on the original media. In fact, once a system has been compromised, it is important to do as little as possible – and ideally nothing-to the system itself other than isolating it to prevent connections into or out of the system and capturing the contents of live memory (RAM), if needed. Limiting actions on the original computer is important, especially if evidence needs to be taken to court, because forensic investigators must be able to demonstrate that they have not altered the evidence whatsoever by presenting cryptographic hash values, digital time stamps, and legal procedures

followed, etc. A piece of hardware that helps facilitate the legal defensibility of a forensic image is a "write blocker", which investigators should use to create the image for analysis whenever one is available.

e. Hash Values

When an investigator images a machine for analysis, the process generates cryptographic hash values (MD5, SHA-1). The purpose of a hash value is to verify the authenticity and integrity of the image as an exact duplicate of the original media.

Hash values are critical, especially when admitting evidence into court, because altering even the smallest bit of data will generate a completely new hash value. When you create a new file or edit an existing file on your computer, it generates a new hash value for that file. This hash value and other file metadata are not visible in a normal file explorer window but analysts can access it using special software. If the hash values do not match the expected values, it may raise concerns in court that the evidence has been tampered with.

Step No. 5

PRESENTATION

Tips To Prepare For Deposition of Evidence in Court

The Investigating Officer should prepare well to depose the evidence in the court of law like any other case. All the digital evidences will be presented as exhibits and introduced as evidence to establish the process used to identify, collect, preserve, transport, store, analyze, interpret, attribute, and/or reconstruct the information.

Re-constructing the scene of offence and the cyber-crime with the sequence of actions by each system and user is very important in the deposition.

To depose the evidence, Investigating Officers are requested to prepare their notes in the below order.

- Complaint received
- Collected relevant information

- Crime Scene visit
- Evidence Identification
- Collection
- Preservation
- Transport to FSL
- Request for Analysis
- Interpret the reports received from FSL
- Reconstruct the case
- Prepared the charge sheet

CHAPTER 3

COLLECTION OF DIGITAL EVIDENCE

A. Procedure for gathering evidences from switched-off systems

- Secure and take control the scene of crime both physically and electronically. Physically means sending away all persons from scene of crime and electronically means, disabling the modems, network connections etc.
- Make sure that the computer is switched OFF- some screen savers may give the appearance that the computer is switched OFF, but hard drive and monitor activity lights may indicate that the machine is switched ON. Be aware that some laptop computers may power ON by opening the lid. Remove the battery from laptop computers.
- Unplug the power and other devices from sockets.
- Never switch ON the computer, in any circumstances.
- Label and photograph (or video) all the components in-situ and if no camera is available, draw a sketch plan of the sys- tem.
- Label the ports and (in and out) cables so that the computer may be reconstructed at a later date, if necessary.
- Carefully open the side casing of CPU or laptop and identify the Hard disk. Detach the hard disk from mother board by disconnecting the data transfer cable and power cable.
- Take out the storage device (Hard disk) carefully and record unique identifiers like make, model, and serial number. If, entire CPU is seized, also note down the any unique identifiers.
- Get the signature of the accused and witness on Hard disk, by using permanent marker. Ensure that all items have signed and completed exhibit labels.
- Search scene of crime for Non-electronic evidences like diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer. Ask the user if there are any passwords and if any off-site

data storage. Also ask, for the operating system in the suspected system, the application packages, the various users of the computer etc.,

- After the Hard disk is removed from the suspected system. Switch on the system and go to BIOS. Note down the date and time shown in BIOS.
- Prepare detailed notes giving "when, where, what, why & who" and overall actions taken in relation to the computer equipment.
- Allow any printers to finish printing.
- Connect the suspected hard drive to the investigator computer through write-block device for forensically previewing/ copying/ printing or for duplication. Never Connect Directly Without The Blocker Device.

(Make detailed notes of all actions taken in relation to the computer equipment)

B. Procedure for gathering evidences from live systems (Switched-On Systems)

- Secure the area containing the equipment.
- Move people away from computer and power supply.
- Disconnect the modem if attached.
- If the computer is believed to be networked, seek advice from the technically trained officer, in-house forensic analyst or external specialist.
- Do not take advice from the owner / user of the computer.
- Label and photograph or video all the components including the leads in-situ. If no camera is available, draw a sketch plan of the system and label the ports and cables so that the computer may be reconstructed at a later date.
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
- Carefully remove the equipment and record the unique identifiers – the main unit, screen, keyboards and other equipment will have different numbers.

- Ensure that all items have signed exhibit labels attached to them as failure to do so may cause difficulty with continuity and cause the equipment to be rejected by the forensic examiners
- Allow the equipment to cool down before removal
- Search area for diaries, notebooks or pieces of paper with passwords on which are often stuck to or close to the computer.
- Consider asking the user if there are any passwords and if these are given, record them accurately.
- Make detailed notes of all actions taken in relation to the computer equipment
- Record what is on the screen by photograph and by making a written note of the content of the screen?
- Do not touch the keyboard or click the mouse and if the screen is blank or a screen saver is present, the case officer should be asked to decide if they wish to restore the screen. If so, a short movement of the mouse will restore the screen or reveal that the screen saver is password protected. If the screen restores, photograph / video and note its content. If password protected is shown, continue as below without any further disturbing the mouse. Record the time and the activity of the use of the mouse in these circumstances.
- Take the help of technical expert to use live forensics tool to extract the information that is present in the temporary storage memory like RAM.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

C. Procedure for gathering evidences from Mobile Phones

- If the device is "OFF", do not turn "ON".
- With PDAs or cell phones, if device is ON, leave ON. Powering down device could enable password, thus preventing access to evidence.
- Photograph device and screen display (if available).

- Label and collect all cables (including power supply) and transport with device.
- Keep the device charged.
- If device cannot be kept charged, analysis by a specialist must be completed prior to battery discharge or data may be lost.
- Seize additional storage media (memory sticks, compact flash, etc).
- Document all steps involved in seizure of device and components.

CHAPTER 4

SEIZING CLOSED CIRCUIT TELEVISION (CCTV)

Digital CCTV installations vary greatly in terms of the recording methods used and picture export facilities provided. There are many manufacturers operating in the CCTV marketplace and each offers a slightly different solution with different capabilities and functionality. This makes the task of retrieving and replaying data increasingly complex for police technical staff, who have to develop a familiarity with a broad range of systems and export technologies.

Checklist:

The list of actions below should be followed when retrieving video data to ensure that all relevant video and information about the system is gathered. This is essential to permit future viewing and maintain evidential integrity, whilst minimising any potential disruption to the premises where the CCTV system is installed.

1. Timely notes should be kept, detailing the course of action taken, to provide an audit trail.

2. Note the make and model of the CCTV system, and the number of cameras. Take photographs of the system if possible, particularly if the recorder is unfamiliar or the manufacturer uncertain.

3. Note the basic system settings (e.g. current record settings and display settings), so that if changes have to be made to facilitate the retrieval, it is then possible to return the system to its original state. (Taking photographs of the system can assist, particularly if cable connections are changed during retrieval).

4. Time check – compare the time displayed by the CCTV system with that given by the speaking clock. Any error between the system time and real time should be recorded in the audit trail and compensated for when conducting the retrieval. This will ensure that the correct section of data is copied.

5. Determine time period required in conjunction with IO.

6. Determine which camera views are required, and whether they can be retrieved separately. It is good practice to draw a plan of the camera views to facilitate further decision making processes. Depending on the nature of the incident, there might, for example, be a requirement to retrieve all cameras with external views. Some systems permit video from individual cameras to be downloaded, but some do not, in which case data from all cameras will need to be taken. The decision taken and the reasons for it should be documented in the audit trail.

7. Replay Data. Check that the requested video exists on the system.

8. Check storage / overwrite time – to determine how long the relevant data will be retained on the system. This is particularly important if the retrieval cannot be carried out immediately, or needs to be prioritised against other tasks. A maximum time period can then be determined within which the retrieval must be carried out before data is lost.

9. Obtain system password, if necessary. Be aware that the standard user password may provide only limited functionality and an administrator password may be necessary in order to enable data retrieval.

10. The recording should not be stopped during the retrieval process unless

a. this is an unavoidable feature of the system or

b. there is an immediate risk that important data will be overwritten before it can be retrieved.

11. Protect data. Some systems allow write-protecting a selected video sequence to prevent it from being overwritten before it can be retrieved; however, it should not be assumed that this facility will be present.

12. It is preferable to extract the CCTV sequence in its native format in order to maintain image quality and provide best evidence, even where this file format is proprietary to the CCTV manufacturer. Some systems may provide an option to write the sequence to AVI file, which may seem to be an advantage in that the video will be replayable using standard software; however the generation of the AVI file often requires the video to be recompressed, resulting in a loss of quality, and so this method should be avoided. Metadata such as time and date information may also be lost, along with any stored bookmarks. (Note that when copying data files manually via Windows Explorer, the metadata and index files may be stored in a separate directory to the video files.)

13. The IO can seize the entire DVR/NVR (preferable due to propriety software), or can collect the relevant part of recording from the owner/operator/ technicianalong with a 65 B(4) Certificate.

NB: The person issuing the 65 B(4) Certificate must be aware of the details, file formats, installation details and specifications of the device.

CHAPTER 5

COLLECTION OF EVIDENCE FROM THIRD PARTY

A. Analyzing External / Third-party information

- **Time Zone Conversion**

  Time Zones and their conversions play a very important role in attributing acts / incidents to the accused. A time zone is a region of the earth that has uniform standard time, usually referred to as the local time. By convention, time zones compute their local time as an offset from UTC (Greenwich Mean Time). Local time is UTC, plus the current time zone offset for the considered location.

  For each computer system/server time zone set to its current location/local time. It is very important to know the time zone of that system to establish the exact time of offence and subsequent actions of the crime as supportive evidence.

  Since the time zone/difference may vary more than 12 hours for few locations for example United States of America, date of the occurrence of the crime may also change. This is very critical and important especially in crimes involved in sending e-mails from servers out of India. Time zone Conversion plays an important role in converting all the acts and incidents to one common time (usually the local time), so that the offences and the offender can be clearly linked. There are number of online Web sites/applications that are available to convert the time to Indian standard time (IST) and vice-versa.

- **E-mail Headers**

  In most of the cybercrime where e-mails are involved, analysis of e-mail headers plays a very important role. Each e-mail whether it is a company e-mail or Web-based e-mail like hotmail, yahoo, etc., carries lot of information about that e-mail. Information like sender IP address, e-mail address, time and date when the e-mail sent, through which server it passed, etc.

  E-mail header analysis can help an investigator to find out the IP address of the e-mail sender. E-mail message headers are digital histories

that are attached to every e-mail message that are sent and received. Headers record important information, including servers that the e-mail has traveled through, and the date and time that the message was received or forwarded.

E-mail messages

- Are attached automatically to every e-mail message that's sent and received.
- Comprise of 2 sections.
  - **Message Description:** Contains details of the sender and recipients, subject line, and sending date.
  - **Message Path:**
  - o Contains the server name and timestamp for every server the message travelled through.
  - o Displays entries in the message path in reverse chronological order.
  - o The header details can be copied and pasted into 'notepad' or similar program and, then the information is analyzed.
  - o Some free and popular tools on the internet, offer e-mail header analysis on-line.

B. Gathering Information From External Agencies/Companies

Various companies/Internet service providers (ISPs) are liable under various laws and regulations including ITAA 2008 to preserve and provide information to the law enforcement. The Investigating Officer can send Letter of Request to get this information from these agencies/providers.

i. Availability of information and format from ISPs:

It is very important for Investigating Officer to understand what information/evidence relevant to the investigation is avail- able with third-party companies/providers, which can be very useful and relevant to reconstruct the crime. All the service providers enable queries by e-mail from pre-registered e-mail ids of the IOs and, such e-mail have to be from their official e-mail id.

Information from ISP (Internet Service Provider): ISP will typically provide the following information, based on a law enforcement request.

- o User name
- o Telephone number in case of DSL/CDMA/3G, and Dial up
- o Personal details like name, e-mail ID, address, etc., mentioned in the CAF form
- o Day-wise activity i.e., when and how long used, etc.
- o Physical address of the IP address

ii. Information from e-mail service

- o User name
- o Details of all incoming and outgoing e-mails along with mails stored in Draft folder
- o The IP address from where the e-mail ID is accessed.
- o Registration details like IP address, date and time, other services availed, secondary e-mail ID etc
- o User activity, i.e., date and time of logged in and time it is active, etc.

The e-mail and other service providers have law enforcement designated nodal officers, who coordinate the requests from Police. Service providers do have laid down policies, in compliance with local laws and, laws of the country in which they are registered.

iii. Information from Mobile service providers

- o Customer Acquisition Forms (CAF) Forms-Personal details like name, address etc.
- o Calling number, called number, time, type of call (ISD/STD/Local/SMS, etc.)
- o Roaming to other cities, etc.
- o Tower locations - Latitude and Longitude of the tower
- o Tower data

iv. Information from Social networking sites like facebook, Orkutetc

- o User name
- o Personal details updated in the profile
- o The IP address from where the profile is accessed
- o User activity i.e. date, time of logged in and duration of the active sessions, etc.
- o Friends and groups with which the user is associated, etc.
- o E-mail IDs updated in the personal information.

v. Information from Financial institutions / Internet banking institutions

- o Personal details updated in the profile of the account holder
- o Transactional details
- o CAF and other supporting documents submitted by the customer along with the introducer details
- o IP address from where the transaction happened in case of Internet banking

CHAPTER 6

GUIDELINES TO PREPARE CHARGE SHEET

Inadequate skill in drafting the charge-sheet is one of the reasons which help the accused to get away with cybercrime committed by them. Many cases fail before the Courts of Law just because of the defective framing of charge-sheets. There are a number of incidents, where the Investigation Officer (IO) has failed to file the charge sheet with all required information/documentation in cyber-crimes and cases acquitted by courts of law.

Below are few guidelines for IO to include in the charge sheet.

- All the relevant information shared by the complainants during registering the FIR/course of investigation should be included in the charge sheet.
- Please make sure the sections mentioned in FIR are still applicable for the case OR it is advised to file a requisition to change of sections before the case including appropriate ITAA 2008 and other supportive IPC, special and local laws. (there are number of incidents, IO filing the charge sheet under wrong sections of IT Act)
- Make sure the search and seizure procedure along with Chain of custody and DEC form are included in the charge sheet.
- Make sure the nature of cybercrime and the necessary information / analysis requested from FSL or forensic examiner are incorporated properly in the charge sheet.
- Please provide the detailed information about the crime scene and the process IO followed to identify the systems used / affected in the crime.
- Please include all the technical persons who identified, produced and analyzed the digital in the case as witness.
- Please include the incidents occurred in the chronological order of time to establish the crime along with the findings.
- Time plays a very critical evidence in proving cyber-crimes, please mention the time stamps in a chronological order

- System Time: BIOS Time, Access Time, Log times, Physical Access Time etc.

CHAPTER 7

GUIDELINES TO PRESERVE THE SEIZED DIGITAL MEDIA

- After filing the charge sheet another important task for IO is to preserve the digital media till the end of the case.
- Please follow the below guidelines to preserve the digital evidence:
- Please keep the digital media always in an anti-static cover with all details and tag / barcode.
- Please create a separate inventory list for all the media seized with case number and other reference numbers (barcode)
- Please store in a dry and cool place.
- If possible, store in a good storage device which is fire proof and tamper proof.
- Please keep update the chain of custody, if the media is taken out for any reason.
- Last but not the least, the digital evidence may look simple to acquire or keep, but maintaining its legal relevance is not an easy task; professionalism has to take charge. Though digital evidence is more involving compared to real or 'hard' evidence, the point remains that both have to be reliable and accurate for them to be legally relevant.