Investigation in Digital Era

Presented By
Dr. Harold D'Costa
CEO - Intelligent Quotient Security System,
President - Cyber Security Corporation,
Advisor (Law Enforcement Agencies - Cyber Crime),
Sr. Trainer (Judges & Public Prosecutors),

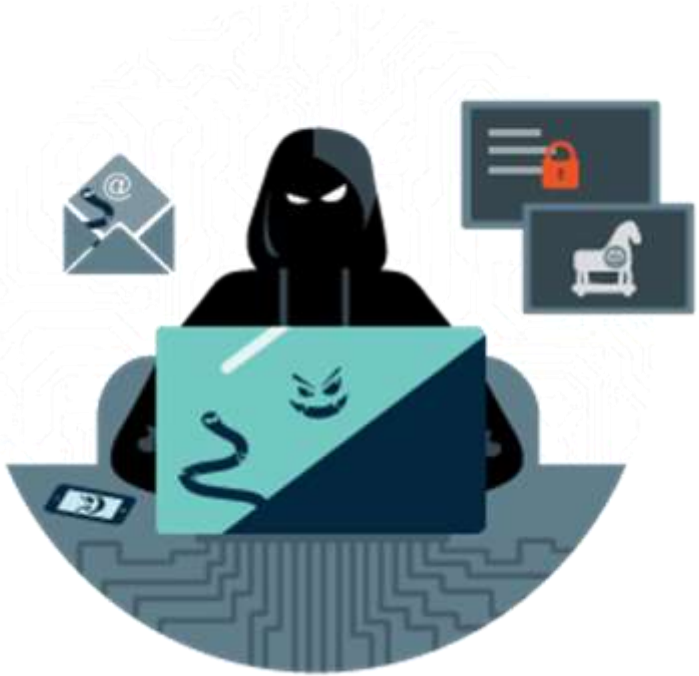
Office No 5, 3rd Floor, Anandi Gopal Building,
Fergusson College Road, Pune - 411005, India
Email: hld@rediffmail.com
Cell: +91-9637612097
Website: https://cybersecuritycorp.in

Who Owns the Internet?

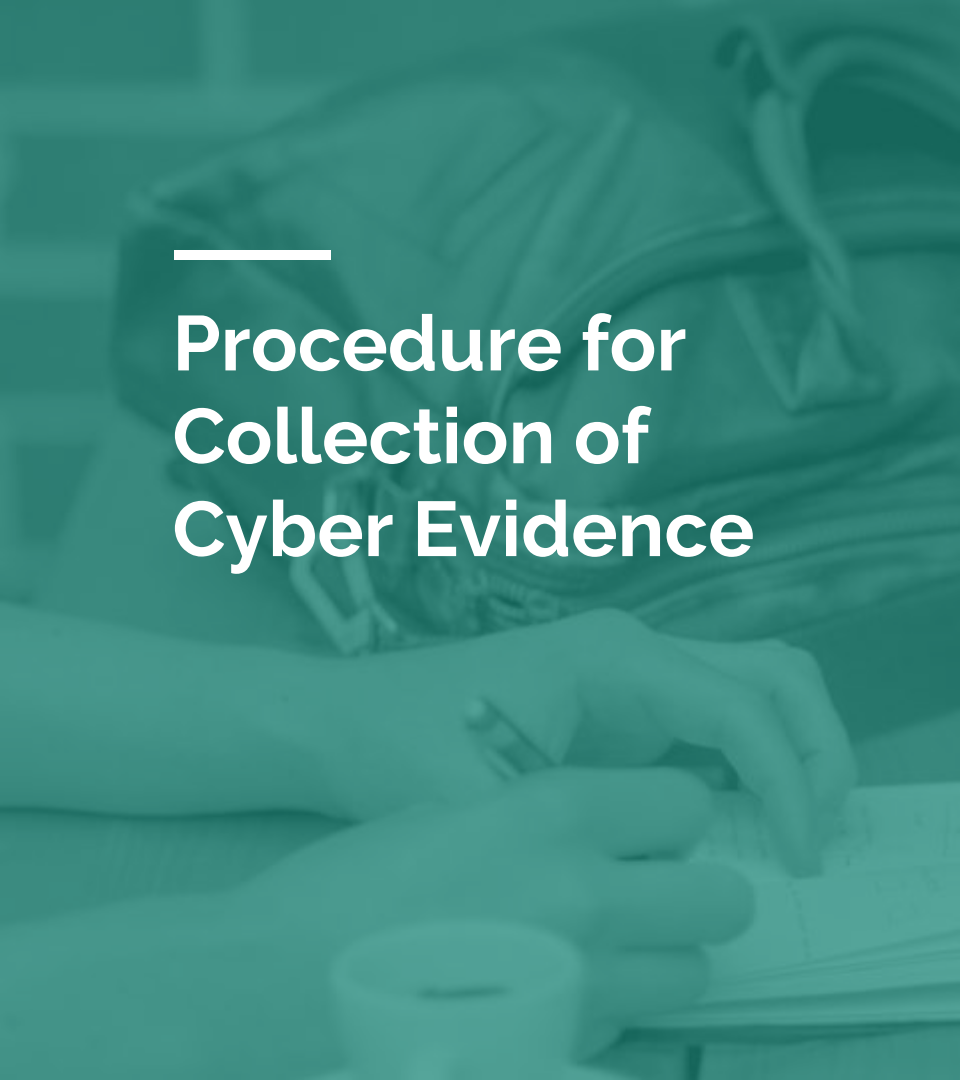
No one actually owns the Internet, and no single person or organization controls the Internet in its entirety. The Internet is more of a concept than an actual tangible entity and it relies on a physical infrastructure that connects networks to other networks.

Cyber Crime

Use of technology to do any illegal activities is known as cybercrime.



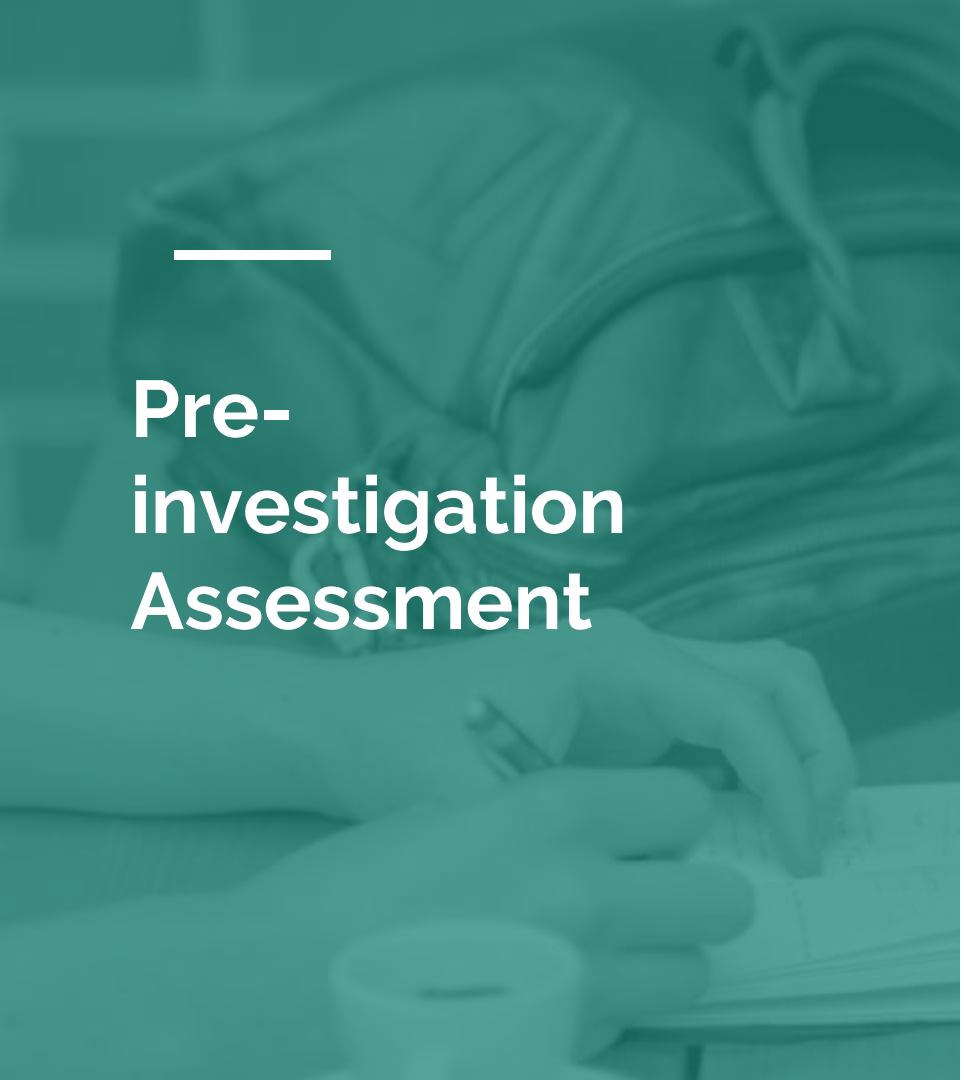
Types of Cyber Crimes



Procedure for Collection of Cyber Evidence

Steps for Cyber Investigation:-

I. Pre-investigation Assessment
II. Evaluation of Scene of Crime
III. Collection of Physical Evidences
IV. Precaution for collecting digital evidences
V. Collection of Digital Evidences
VI. Forensic duplication
VII. Seizure of Digital Evidence
VIII. Packaging, Labelling and transportation
IX. Legal procedure after seizure
X. Gathering information from various agencies



Pre-investigation Assessment

I. Collection of all necessary information like:
   i) profiles of the suspect,
   ii) location,
   iii) circumstances,
   iv) computer system

II. Collection should be done by In-charge/cyber cell (Investigating Officer)

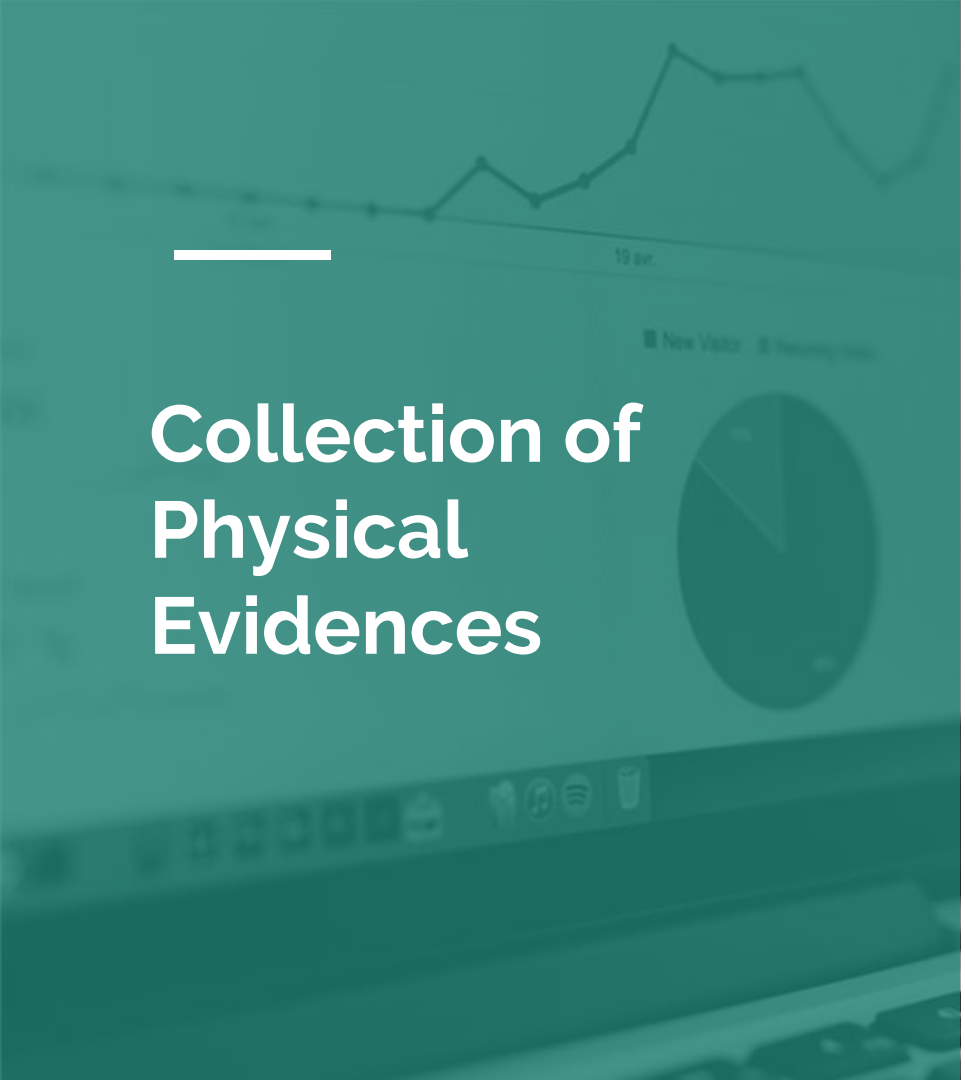
III. Analyzing scope of the offence and its possible outcomes.

Evaluation of the Scene of Crime

I. Crime scene should be evaluated properly before collection of evidences.
II. Digital evidences are very volatile in nature and could be available in number of devices, locations and formats.
III. Evidences like number of computer system, type of connection (Wi-Fi, Ethernet), personal appliances and computer peripherals should be noted and photographed.

Categories of Crime Scene:

I. House of an individual having one or more computer network.
II. Office or coffee shop of an individual or company.
III. Public place.



Collection of Physical Evidences

- Identification and collection of potential evidences from crime scene.
- Evidences include receipts of cyber appliances, left behind diaries, notes/password on slip, e-mail IDs, contact numbers or bank account number.
- Nothing and sketching position of various equipment's at crime scene. For e.g. a mouse at left hand side of keyboard may indicate the user being dexterous.

Precaution To Be Taken While Collecting Digital Evidences

- Minor mishandling may corrupt or vanish the evidence.
- Without proper documentation evidence may not be admissible in court of law.
- Special skills are required for leveling and preserving of digital evidence.
- Chain of custody should be prepared to identify who handled the evidence.
- A proper documentation like the Digital evidence form should be done separately for every device.
- Serial number of devices should be properly documented.

Collection of Digital Evidence

Switched off system

- Disconnect all network connections. Allow printers to finish printing (if any).
- Label and photograph all components.
- Ask users for passwords, Operating Systems, details of other users and off-site data storage.
- The suspected drive should be connected using wire block device only for investigation.

Switched on System

- Disconnect all network connection.
- Label and photograph all components.
- Ask users for passwords, Operating Systems, details of other users and off-site data storage.
- Use live forensic tools to collect evidence present in the RAM.

Cellphone

- If device is switched off, do not turn it on and if it is on put it on flight mode.
- Photograph, label the device and screen display.
- Use Faraday bags for storing of evidence.
- Keep the device charged, record every activity with photograph and time.

Forensic Duplication

In forensics duplication, the data should be copied accurately without making any change to it.
It can be done by following ways:

Logical backup

In this method, deleted files and residual data present in the device is not captured, it only capture and copies the directory and files of a logical volume.

Bit stream imaging

It is also known as imaging or cloning
It is a bit-by-bit copy of an original media.

Write blocker

It is a hardware or software tool which forbids computer writing on a storage media.

PRECAUTIONS:

- **The copied data should be exact copy of the original data so that the integrity of the data is maintained.**
- **To ensure integrity, hash value of the copied data should be calculated.**

Seizure of Digital Evidences

It involves the following:

- Calculating hash value of the suspect storage media.
- Creating a digital fingerprint (image / clone) of the same.
- Calculating hash value of forensic image.

PRECAUTIONS

- Professional approach and guidelines should be followed by I.O to maintain reliability, integrity and legal relevance of the evidence.
- Write blockers should be used to avoid change in time stampings.
- Permanent sterile new physical media should be used.
- New media should be fire proof and tamper proof.
- If already used hard disk is used, existing data should be wiped off.
- After imaging data into media, it should be marked with unique exhibit number related to case which is computed through hash algorithm.
- This number should be, mentioned in panchnama.
- Hash valued of copied image and the original data should be exactly same.
- The seizure memo should be prepared .
- Digital evidences collected should be preserved in anti-static cover.

Packaging, Labelling and Transportation

I. The collected evidences should be numbered and labelled properly for future use.
II. A tag should be attached to evidence which will display all the details about the evidence.
III. For packaging of evidence, proper material of suitable size should be used.
IV. Good quality evidence envelopes, faraday bags should be used instead of common plastic/gunny bags.
V. Each evidence should be packed separately to avoid damage to the evidence.
VI. During Transportation, the evidences should be kept away from the place of frequent mechanical shocks or with drastic temperature change.
VII. The evidence should be carried by only trained and authorized messenger and not by courier/post.

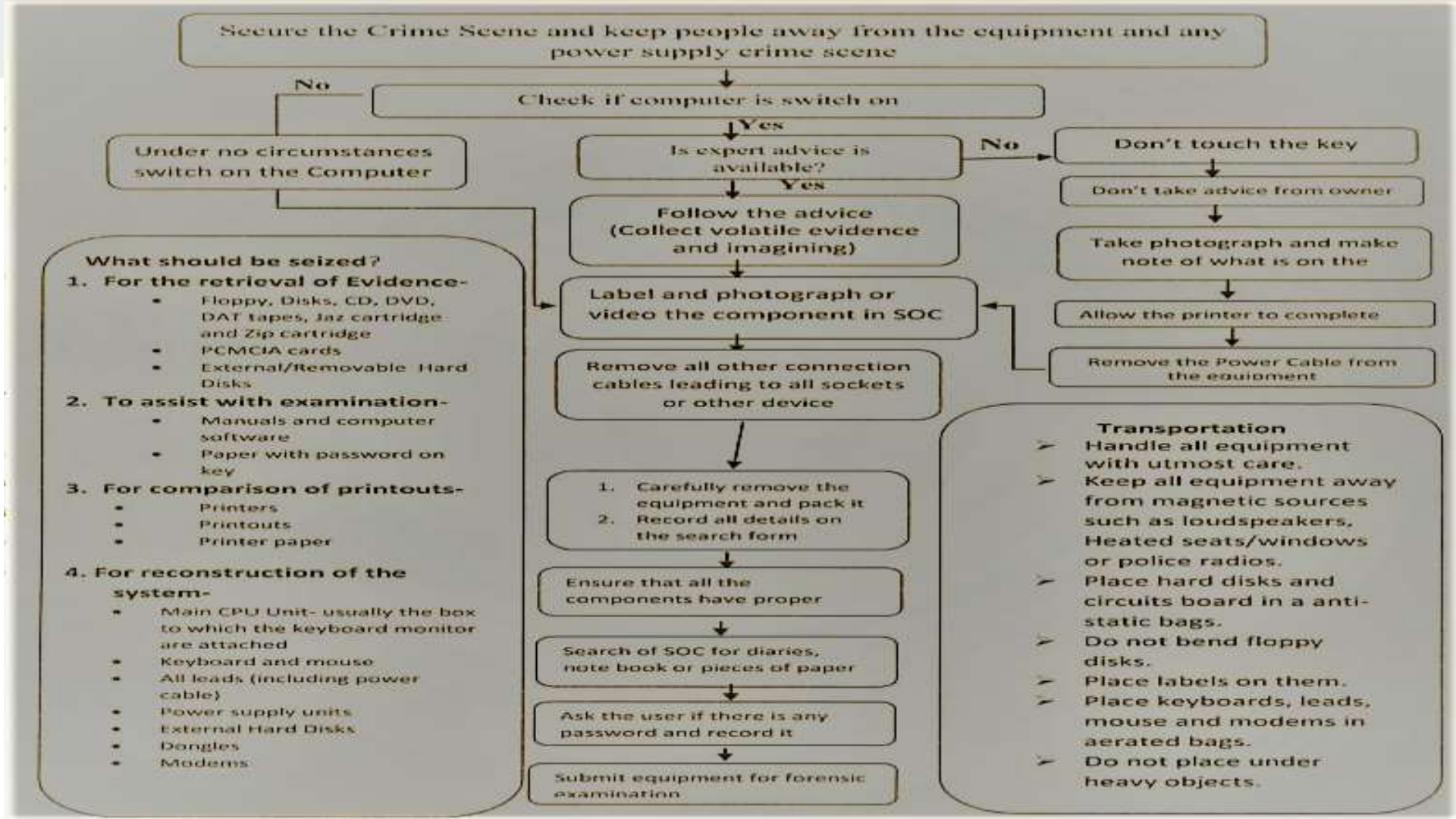
Legal procedure after seizure

I. After seizure, documentation and transportation of digital evidence, permission from court should be obtained to keep evidence in custody.

II. Ensure that no original evidence related to case are returned to owner.

III. Even if court instructs to return the original evidence, try to impress upon that only an authentically imaged copy of evidence is provided to owner.

Flowchart for Collection of Digital Evidence


Seeure the Crime Seene and keep people away from the equipment and any power supply crime seene
No
Cheek if computer is switch on
Yes
Under no circumstances switch on the Computer
Is expert advice is available?
No
Don't touch the key
Don't take advice from owner
Yes
Follow the advice (Collect volatile evidence and imagining)
Take photograph and make note of what is on the
Label and photograph or video the component in SOC
Allow the printer to complete
Remove all other connection cables leading to all sockets or other device
Remove the Power Cable from the equipment
What should be seized?
1. For the retrieval of Evidence-
• Floppy, Disks, CD, DVD, DAT tapes, Jaz cartridge and Zip cartridge
• PCMCIA cards
• External/Removable Hard Disks
2. To assist with examination-
• Manuals and computer software
• Paper with password on key
3. For comparison of printouts-
• Printers
• Printouts
• Printer paper
4. For reconstruction of the system-
• Main CPU Unit- usually the box to which the keyboard monitor are attached
• Keyboard and mouse
• All leads (including power cable)
• Power supply units
• External Hard Disks
• Dongles
• Modems
1. Carefully remove the equipment and pack it
2. Record all details on the search form
Ensure that all the components have proper
Search of SOC for diaries, note book or pieces of paper
Ask the user if there is any password and record it
Submit equipment for forensic examinatinn
Transportation
➢ Handle all equipment with utmost care.
➢ Keep all equipment away from magnetic sources such as loudspeakers, Heated seats/windows or police radios.
➢ Place hard disks and circuits board in a anti-static bags.
➢ Do not bend floppy disks.
➢ Place labels on them.
➢ Place keyboards, leads, mouse and modems in aerated bags.
➢ Do not place under heavy objects.

Gathering Information From Various Agencies

Information preserved by internet service providers and other firms can be obtained by legal request.

The officer can acquire such information as given below:

Telecom service provider(TSP)/ Internet service provider(ISP):

- Username
- Telephone number in case of DSL/CDMA/3G,4G and dial up
- Personal details like name, email ID, address etc. mentioned in CAF form.
- Day-wise activity i.e. when and how long used etc.
- Physical address of the IP address.

E-mail service provider:

- Username, user activity i.e. date and time of logged in and time it is active, etc.
- Details of all incoming and outgoing e-mails along with mails stored in draft folder.
- The IP address from where the email ID is accessed.
- Registered details (IP address, date and time, other services availed) etc.

Gathering Information From Various Agencies

Mobile service provider

- Customer acquisition forms- personal details like name and address.
- Calling number, caller number, time, type of call (ISD/STD/Local/SMS etc.)
- Roaming to other cities, Tower Location and tower data.

Social networking sites

- Username.
- Personal details updated in the profile.
- The IP address from where the profile is accessed.
- User activity i.e. date and time of logged in and duration of the active sessions etc.
- Friends and group with which the user is associated.
- Email –IDs updated in the personal information.

Gathering Information From Various Agencies

Financial Institutions/ Internet Banking Institutions

1. Personal details updated in the profile of the account holder
2. Transactional details
3. Supporting documents submitted by the customer along with the introducer details.
4. IP address in case of Internet Banking.

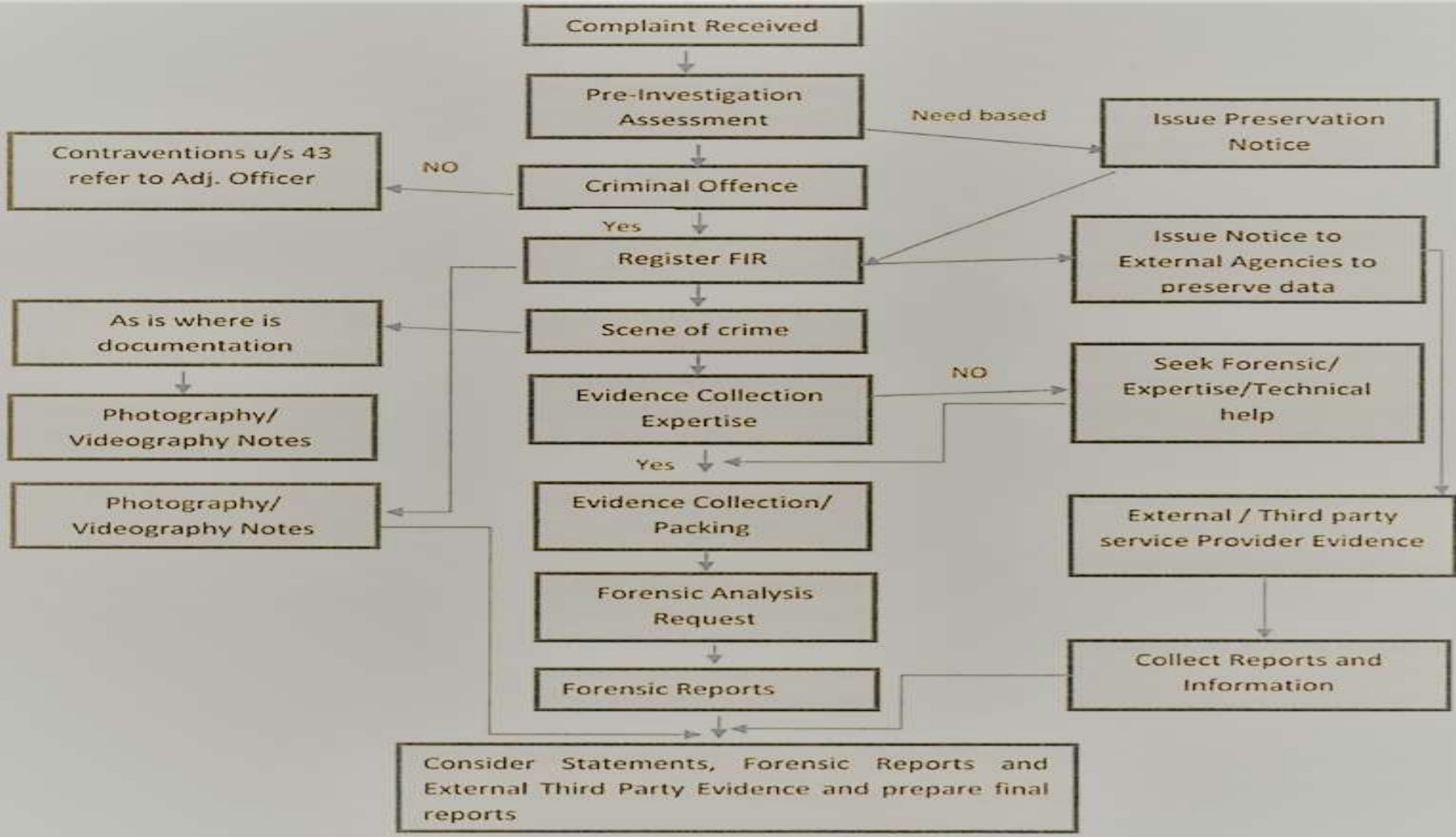
Website domain/ Hosting providers

1. Registration details, Access details, FTP logs
2. Payment details
3. Technical/administrative/owner of the domain
4. Details of website developer

VoIP service providers

1. Registration details, Access details,
2. IP addresses, Payment details,
3. Calling/Called numbers.

Flowchart / Cyber Investigation Diagram


Complaint Received
Pre-Investigation Assessment
Need based
Issue Preservation Notice
Contraventions u/s 43 refer to Adj. Officer
NO
Criminal Offence
Yes
Register FIR
Issue Notice to External Agencies to preserve data
As is where is documentation
Scene of crime
Photography/ Videography Notes
Evidence Collection Expertise
NO
Seek Forensic/ Expertise/Technical help
Yes
Photography/ Videography Notes
Evidence Collection/ Packing
External / Third party service Provider Evidence
Forensic Analysis Request
Collect Reports and Information
Forensic Reports
Consider Statements, Forensic Reports and External Third Party Evidence and prepare final reports

Admissibility Of Digital Evidence

Admissibility Of Electronic Evidence

Evidence Act provides that evidence can be given regarding only facts in issue or of relevance. Whereas section 65A provides that the contents of electronic records may be proved in accordance with the provisions of Section 65B.

Section 65B provides that not withstanding that anything contained in the Evidence Act, any information contained in an electronic record, i.e. the contents of a document or communication printed on a paper that has been stored recorded and copied in optical or magnetic media produced by a computer output, is deemed to be a document admissible as evidence without further proof of the original’s production, provided that the conditions in section 65B(2) to (5) are satisfied.

Conditions For Admissibility of Electronic Evidence

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried over that period by person having lawful control over the use of the computer;

(b) During the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in ordinary course of the said activities;

(c) Throughout the material part of the said period the computer was operating properly, or if not, then in respect of any period, in which it was not operating properly or was out of operation during that part of time, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in ordinary course of the said activities.

Evidence Recorded on CD

Anvar P.V. v P.K Basheer and others.

(a) CDs which are made after recording the speeches, songs and announcements using other instruments and by feeding them in the computer. It was held that since the CD's produced were not certified , the same were not admissible as secondary evidence.

Admissibility of Intercepted Telephone Calls

- **Ravi Kant Sharma and Others v. State**

It was held that call detail records is not a direct computer printout of the data available on the data available in the computers/servers of the telephone company. As the telephone data has been tampered with it cannot be relied upon to base conviction of the accused.

- **State(NCT of Delhi) vs Navjot Sandhu (overruled)**

A submission was made on behalf of the accused that no reliance can be made on the mobile phone call records because prosecution has failed to take on record the relevant certificate under section 65(B) of Indian Evidence Act.

The Supreme Court concluded that a cross examination of the competent witnesses aquatinted with the functioning of the computer during relevant time and manner in which printouts of the call records were taken was sufficient to prove the call records.

Deleted Files on Hard Disk

Dharambir vs Central Bureau of Investigation

The judgment states that even if the hard disk is restored to its original position of blank hard disk by erasing what was recorded on it, it would still retain information which indicates that some text or file in any form was recorded on it at one time and subsequently removed.

By use of software programs it is possible to find out the precise time when such changes occurred in the hard disk.

To that extent even a blank hard disk which has once been used in any manner, for any purpose will contain some information and will therefore be an electronic record.

Admissibility of SMS

- **Rohit Ved Paul Kaushal v State of Maharashtra,** the Bombay High Court after examining the SMS sent by the accused held, “that some of the SMS sent by the accused certainly fall within the scope of Section 67 of the IT Act.

Email as E-Evidence

Nidhi Kakkar v Munish Kakkar

It was held by the Hon. Court that if the person produced text of information generated through computer, it should be admissible as evidence provided proof was tendered in a manner brought through Evidence Act.

IP Address as E- Evidence

Sanjay Kumar Kedia v Narcotics Control Bureau

It was held by the court that “ the Xponse Technologies Limited and Xponse IT Services Pvt. Ltd. Were not acting merely as a network service provider but ere actually running internet pharmacy and dealing with prescription drugs like Phentermine and Butalbital. In this case Section 79 will not grant immunity to an accused who has violated the provisions of the Act.

Pornography and Intermediary's Liability

Avnish Baja v State

It was held by the court that by not having appropriate filters that could have detected the words in the listing or the pornographic content of what was being offered for sale, the website ran a risk of having imputed to it the knowledge that such an object was in fact obscene.

The proliferation of the internet and the possibility of a widespread use through instant transmission of pornographic material calls for a strict standard having to be insisted upon.

Expert Opinion

A new section 79A of the IT Act 2000, which provides that the Central Government may, for the purpose of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Pramod Mahajan Murder Trial

The learned trial Court of Bombay, dismissed the submission that the SMS is inadmissible as valid evidence, as the practical demonstration was conducted by the defense witness who was “not a cyber expert” as per law.

Thank You

DR. HAROLD D'COSTA

+91-96376 12097