CONTENTS :-

- Definitions
- Branches of Digital Forensics
- Digital Evidence
- Types of Cybercrime
- Crime Scene Management

DEFINITION :-

Cyber Crime :-

“Any Crime Committed By Using Computer, Internet Or Any Other Digital Medium As A Tool Or Target.”

Cyber Forensics :-

“Cyber Forensics is the process of Identifying, Collecting, preserving, analyzing and presenting the digital evidence in such a manner that the evidence are legally accepted.”

BRANCHES OF DIGITAL FORENISCS :-

- Computer Forensics
- Mobile Device Forensics
- Network Forensics
- E-mail and Social Media Forensics
- Database Forensics

DIGITAL EVIDENCE :-

What Is Digital Evidence :-

- "Digital Evidence Is Any Information Or Data Related To The Case, That Is Stored On, Received By, Or Transmitted By An Electronic Device That May Be Relied In The Court Of Law."

Properties of Digital Evidence :-

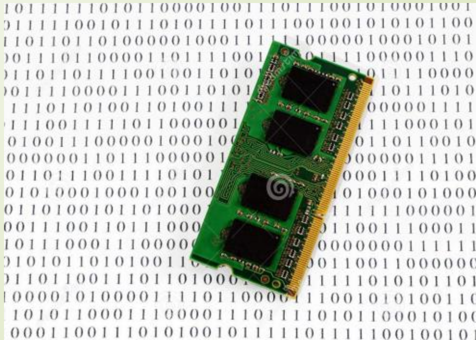
- It can be duplicated exactly and a copy can be examined as if it were the original.
  - Examining a copy will avoid the risk of damaging the original.
- With the right tools it is very easy to determine if digital evidence has been modified or tampered with by comparing it with the original.
- It is relatively difficult to destroy.
  - Even if it is "deleted," digital evidence can be recovered.
- When criminals attempt to destroy digital evidence, copies can remain in places they were not aware of.

Types Of Digital Evidence :-

1. **Persistent (Non-volatile) Data :-**
   - ➢ It Means Data That Remains Intact When The Computer Is Turned Off.

   - ➢ E.G. Hard-disk, Flash-drives

2. **Volatile Data :-**
   - ➢ It Means Would Be Lost When The Computer Is Turned Off.
   - ➢ E.G. Temp. Files, Unsaved Open Files Etc.



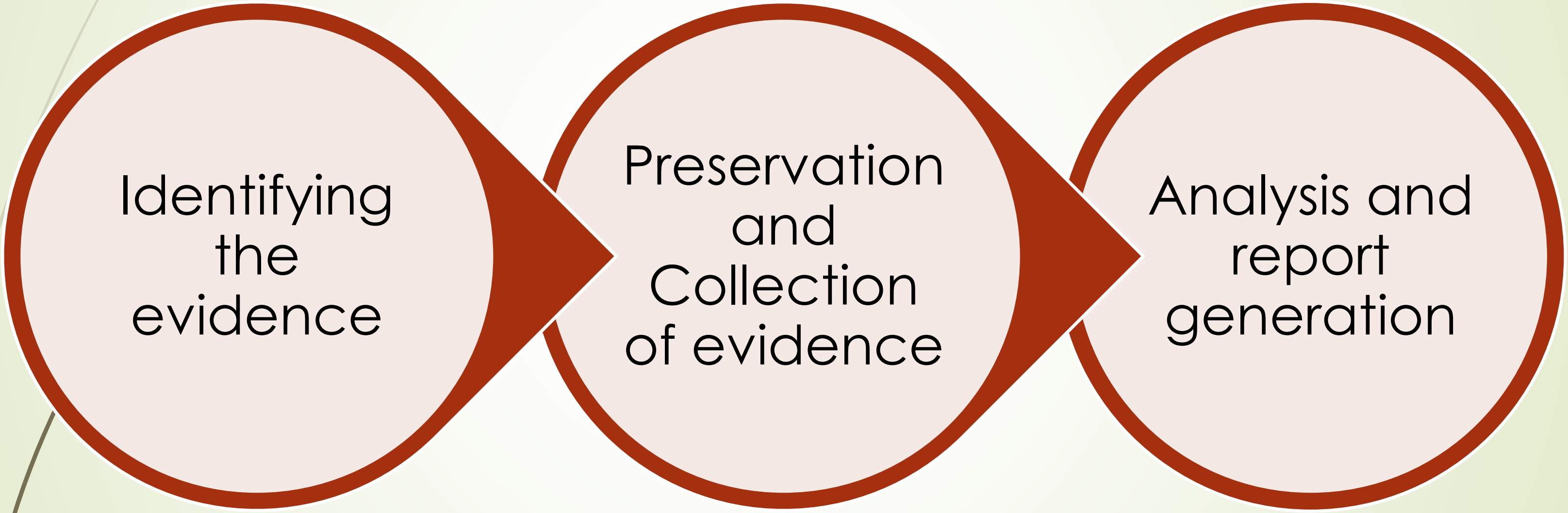
- **Source Of Digital Evidence :-**

- Hard-Drive (Desktop, Laptop, External, Server)
- Flash Drive
- SD Cards
- Floppy Disks
- RAIDs
- Optical Media (CD, DVD)
- CCTV/DVR
- Internal Storage of Mobile Device
- GPS (Mobile/Car)
- Call Site Track (Towers)
- RAM

Types Of Cyber Crime :-

- Hacking
- Phishing
- Spoofing
- Cyber Stalking
- Cyber Terrorism
- Data Theft
- Social Engineering
- Morphing
- Skimming
- Identity Theft
- Malware Attack
- Drug Trafficking
- Spamming
- Web Jacking
- Child Pornography
- Piracy
- Piggy Banking
- Online Fraud

DIGITAL FORENSIC PROCESS



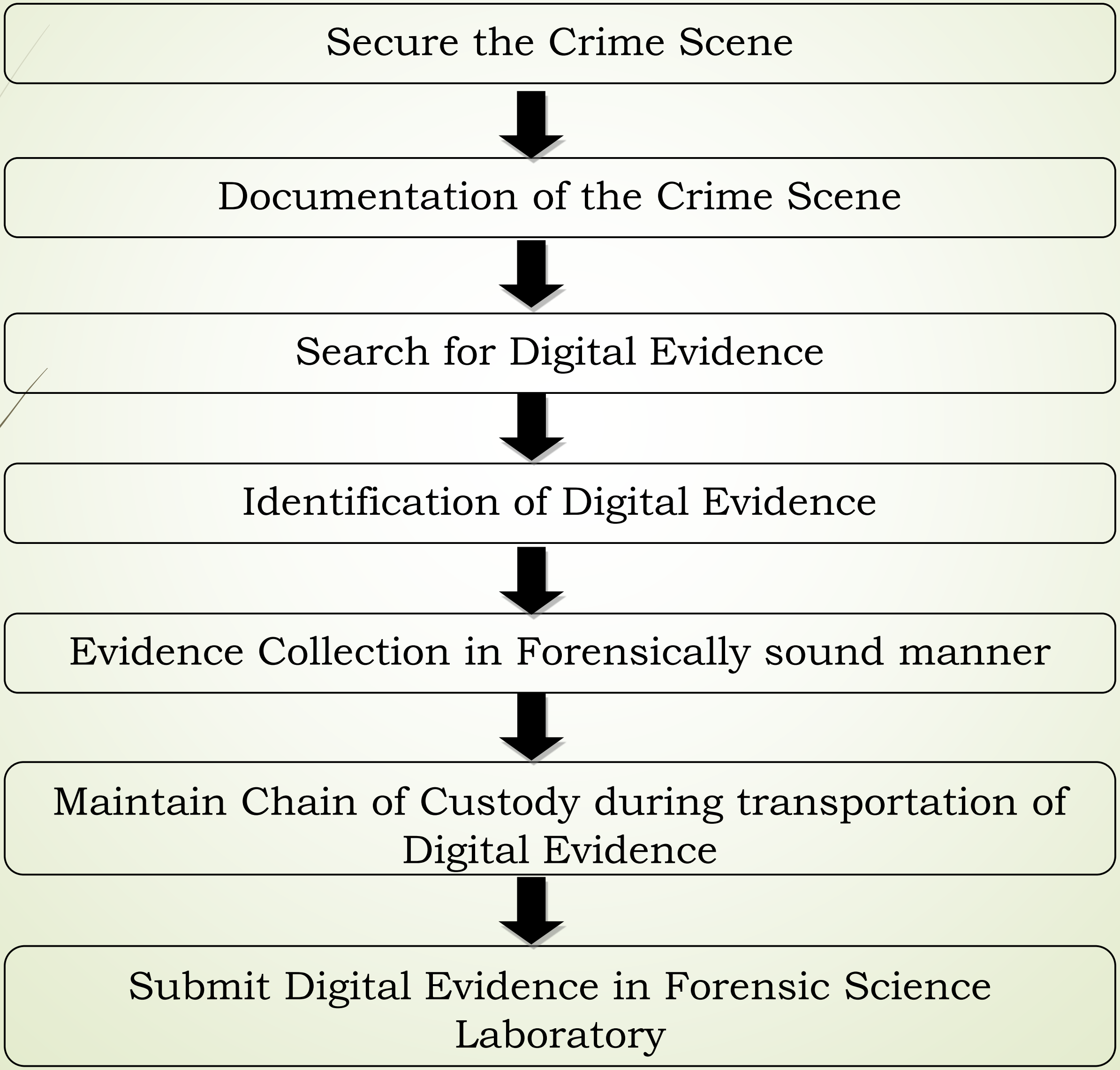
Identifying the evidence

Preservation and Collection of evidence

Analysis and report generation

CRIME SCENE MANAGEMENT

Important steps at crime scene



Secure the Crime Scene

Documentation of the Crime Scene

Search for Digital Evidence

Identification of Digital Evidence

Evidence Collection in Forensically sound manner

Maintain Chain of Custody during transportation of Digital Evidence

Submit Digital Evidence in Forensic Science Laboratory

Investigative Tools and Equipment

- Crime scene securing tapes
- Digital Camera
- Extra batteries
- Video cameras
- Note/sketch pads
- Blank sterile storage media: Portable USB hard disks and pen drives
- Write-Blocker device
- Labels
- Pens, permanent markers
- Storage containers
- Anti-static bags
- Faraday bags
- Toolkit containing screwdrivers (nonmagnetic), pliers, forceps, scissors, clips, pins, cutters etc.
- Rubber gloves
- Incident response toolkit (Software)
- Converter / Adapter: USB, SATA, IDE, SCSI
- Forensic Imaging software
- Tools to collect volatile data (FTK Imager, Magnet Forensics Ram Capture)

TABLEAU
FireWire800+USB2.0 SATA Bridge
Maxtor
OLD MAIL SERVER

1
Nikon
EVIDENCE

SATA/IDE
USB 2.0 to SATA/IDE cable
USB2.0
2.5" HDD
3.5" HDD
CD-ROM
CD-RW
COMBO
DVD-ROM
DVD-RW

Non-electronic Evidence Collection

- Recovery of non-electronic evidence can be crucial in the investigation of electronic crimes. Take proper care to ensure that such evidence is recovered and preserved. Items relevant to subsequent examination of electronic evidence may exist in other forms (**written passwords and other handwritten notes, blank pads of paper with indented writing, hardware and software manuals, calendars, literature, text or graphical computer printouts, and photographs**) and should be secured and preserved for future analysis.

- These items are frequently in close proximity to the computer or related hardware items. All evidence should be identified, secured, and preserved in compliance with departmental procedures.

Digital Evidence Collection process from computer

Situation 1: The Monitor Is On And The Work Product and/or Desktop is Visible

Digital Evidence Collection process from computer

Situation 1: The Monitor Is On And The Work Product and/or Desktop are Visible

- Photograph the screen and record the information displayed.
- Collect volatile data using memory capturing tools.
- Check for virtual drives. If yes, collect logical copies of mounted data.
- Label all connections and ports.
- Photograph them.
- Disable network connectivity to prevent remote access.
- Disconnect the power/shutdown.
- Open CPU chassis to locate Hard disk and disconnect it.
- Seize and package all evidence in Anti magnetic (Faraday) bags.
- Transport evidence to forensic laboratory.
- Maintain chain of custody.

Digital Evidence Collection process from computer

Situation 2: The Monitor Is On and The Screen Is Blank (Sleep Mode) Or The Screensaver (Picture) Is Visible

Digital Evidence Collection process from computer

Situation 2: The Monitor Is On and The Screen Is Blank (Sleep Mode) Or The Screensaver (Picture) Is Visible

- Move the mouse slightly (without pushing buttons). The screen should change and show the work product or request a password.
- Do not perform any other keystrokes or mouse operations if mouse movement does not cause a change in the screen.
- Photograph the screen and record the information displayed.
- Collect volatile data using memory capturing tools (Mind that always use write blocker to prevent any kind of manipulation during data collection).
- Follow further steps as per situation 1.

Digital Evidence Collection process from computer

Situation 3: The Monitor Is Off

- Make a note of the "off" status.
- Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.
- Check for outside connectivity (telephone modem, cable, integrated services digital network [ISDN], and digital subscriber line [DSL]). If a telephone connection is present, attempt to identify the telephone number.
- Avoid damage to potential evidence by removing any floppy disks that are present, packaging the disk separately, and labeling the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive.
- Place tape over all the drive slots and over the power connector.
- Record the make, model, and serial numbers.

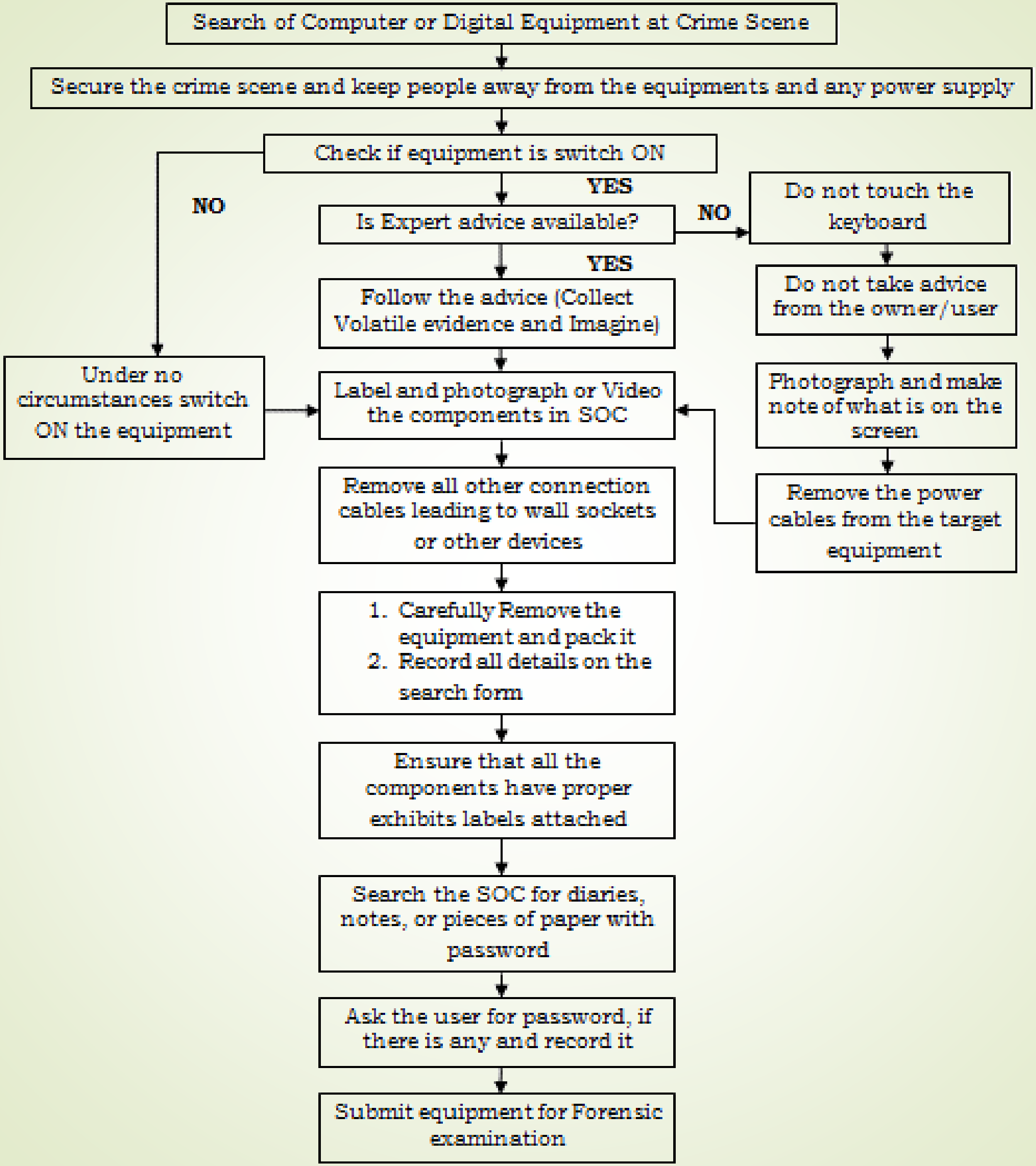
Digital Evidence Collection process from computer

Situation 3: The Monitor Is Off

- Photograph and diagram the connections of the computer and the corresponding cables.
- Label all connectors and cable ends (including connections to peripheral devices) to allow for exact reassembly at a later time. Label unused connection ports as “unused.” Identify laptop computer docking stations in an effort to identify other storage media.
- Collect non-volatile data, i.e. storage media (Hard Disk, Pen drives, Optical Disks, Mobile phones, Memory card etc.)
- Seize and package all evidence in anti-magnetic (Faraday) bags.
- Tag/label each bag.
- Transport evidence to forensic laboratory.
- Maintain chain of custody.

Digital Evidence Collection process from computer

Situation 3: The Monitor Is Off



Search of Computer or Digital Equipment at Crime Scene

Secure the crime scene and keep people away from the equipments and any power supply

Check if equipment is switch ON

YES

Is Expert advice available?

YES

Follow the advice (Collect Volatile evidence and Imagine)

NO

Under no circumstances switch ON the equipment

NO

Do not touch the keyboard

Do not take advice from the owner/user

Photograph and make note of what is on the screen

Remove the power cables from the target equipment

Label and photograph or Video the components in SOC

Remove all other connection cables leading to wall sockets or other devices

1. Carefully Remove the equipment and pack it
2. Record all details on the search form

Ensure that all the components have proper exhibits labels attached

Search the SOC for diaries, notes, or pieces of paper with password

Ask the user for password, if there is any and record it

Submit equipment for Forensic examination

Evidence Packaging, Transporting, and Storing

Packaging

- If multiple computer systems are collected, label each system so that it can be reassembled as found (system A: mouse, keyboard, monitor, and main base unit; system B: mouse, keyboard, monitor, and main base unit).

When packaging evidence at a crime scene—

- Ensure that all collected electronic evidence is properly documented, labeled, and inventoried before packing.
- Pay special attention to latent or trace evidence and take action to preserve it.
- Pack magnetic media in antistatic packaging (paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags (Faraday bags).
- Avoid folding, bending, or scratching computer media, such as a diskette, compact disk-read only memory (CD-ROM), or tape.
- Ensure that all containers used to hold evidence are properly labeled.

Evidence Packaging, Transporting, and Storing

Transporting

- Ensure that computers and other components that are not packaged in containers are secured in the vehicle to avoid shock and excessive vibrations. For example, computers may be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt. When transporting evidence—

- Keep all electronic evidence away from magnetic sources. Radio transmitters, speaker magnets, and heated seats are examples of items that can damage electronic evidence.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Conditions of excessive heat, cold, or humidity can damage electronic evidence.
- Maintain the chain of custody on all evidence transported.

Evidence Packaging, Transporting, and Storing

Storing

- Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust, and other harmful particles or contaminants. Be aware that potential evidence, such as dates, times, and system configurations may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel (such as the evidence custodian, laboratory chief and forensic examiner) should be informed that a device powered by batteries is in need of immediate attention.