DIGITAL CRIME SCENE INVESTIGATION

Search, Seizure, and Evidence Handling

WHAT IS A DIGITAL CRIME SCENE ?

A **digital crime scene** refers to the location, whether physical or virtual, where **digital evidence** related to a crime resides.

Unlike a traditional physical crime scene, a digital crime scene can be spread across **multiple devices, systems, and geographical locations**. It is the environment from which digital forensic investigators must identify, preserve, and collect data in a forensically sound manner.

WHAT IS A DIGITAL EVIDENCE ?

A digital evidence (or electronic evidence) is any information or data of value that is stored, received, or transmitted in binary form (0s and 1s) and can be relied upon in a court of law.

It is information retrieved from any electronic device that is relevant to an investigation, whether criminal or civil, and helps establish a fact.

The "Scene of Crime" is no longer just a physical room; it is a global network.

The Three Dimensions of Digital Evidence:

- **1. Volatility (The "Vanishing" Act):**
  - Unlike a knife or pistol, data in RAM (Random Access Memory) disappears the moment power is cut.
  - *Indian Context:* A suspect deleting a WhatsApp chat or a UPI transaction history remotely.
- **2. Invisibility:**
  - Evidence exists as magnetic charges, not visible to the naked eye. It requires "specialized eyes" (Forensic Tools) to see.
- **3. Boundlessness (Jurisdiction Challenges):**
  - **Local:** The mobile phone in the suspect's pocket.
  - **Networked:** The Wi-Fi router at the suspect's home.
  - **Cloud (The greatest challenge):** Data stored in Google Drive (USA) or Telegram servers (Dubai).
  - *Legal Note:* **Section 75 of the IT Act** applies to offenses committed outside India if they

The Paradigm Shift in Policing

⚠️ The Challenge

Digital devices are now the primary repository of criminal evidence. Traditional investigation methods are insufficient. Mishandling digital evidence at the crime scene can render it inadmissible in court.

⚖️ Legal Mandate

The transition from CrPC/IEA to **BNSS** and **BSA 2023** mandates strict adherence to electronic evidence integrity. Hash value generation and proper chain of custody are now non-negotiable legal requirements.

1. Search & Seizure: Preparation

The Team

Assemble the Investigating Officer (IO), a Digital Forensic Expert (mandatory for major crimes), and an official photographer/videographer.

The Kit

Ensure you have Faraday bags, write-blockers, anti-static bags, seizure memos, and labels. Do not enter a digital crime scene unprepared.

Legal Authority

Secure a Search Warrant under **Section 96 BNSS** (formerly 93 CrPC). Ensure compliance with Section 105 BNSS regarding videography of the seizure.

Search & Seizure: Legal Authority

Part A: The Legal Shield (BNSS & IT Act)

- **Search Authority:**
  - **Section 185 BNSS:** Empowering police officers to search for material/documents.

    Section 185 of the Bharatiya Nagarik Suraksha Sanhita (BNSS) allows police officers to conduct **warrantless searches** when they have reasonable grounds to believe that evidence related to an investigation may be found in a specific location. The section mandates that officers must record their reasons for the search in writing and follow specific procedures to ensure accountability, including the use of audio-video recording during the search. This provision aims to balance the need for effective law enforcement with the protection of individual rights

  - **Section 186 BNSS**

    This section enables a police officer to request another police station to conduct a search within their jurisdiction if they have reasonable grounds. It also provides for exceptions where a direct search may be conducted without involving another station.

THROUGH A SEARCH WARRANT

- **Digital Specifics:**
  - **Section 69 IT Act:** Power to issue directions for interception or monitoring or decryption of any information.

On-Scene Protocol

Part B: The "Do No Harm" Protocol

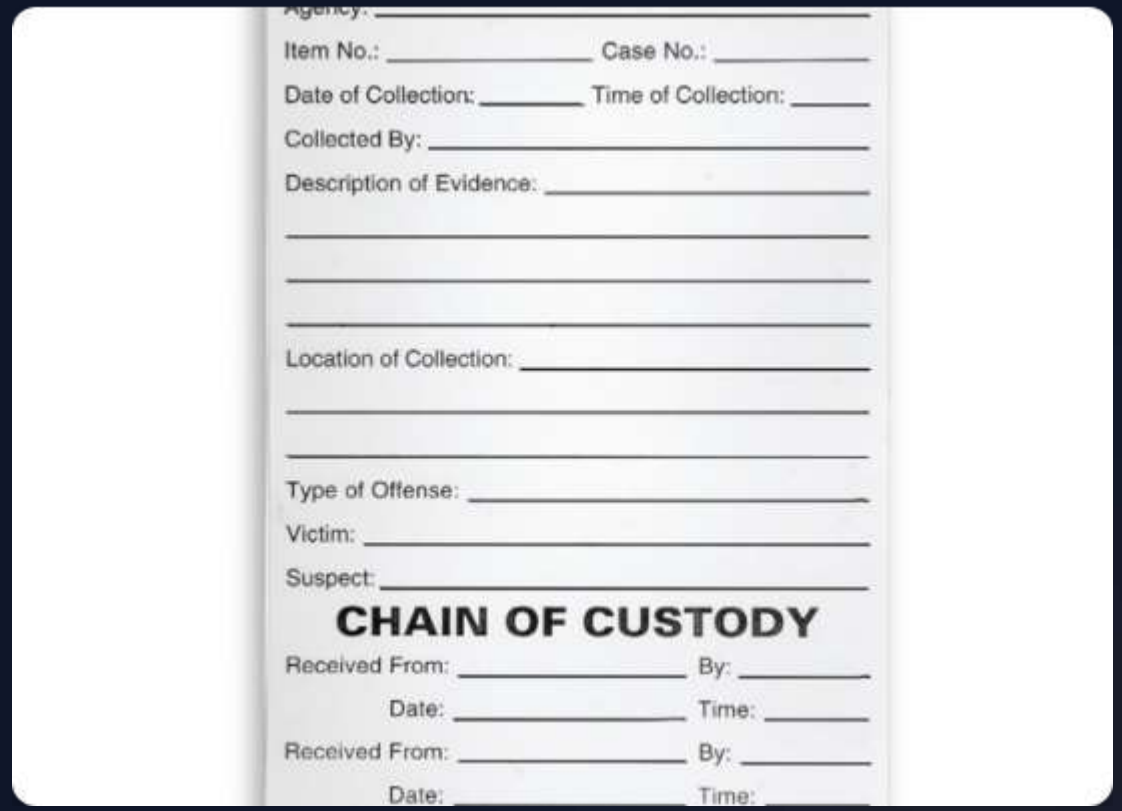
- **1. Secure the Area:** Isolate the device from the suspect.
- **2. Network Isolation (The "Faraday" Rule):**
  - **Mobile Phones:** Immediately place in a **Faraday Bag** (Signal Blocking Bag).
  - *Why?* To prevent "Remote Wiping" (Factory reset command sent via 'Find My Device').
  - *No Bag?* Wrap in multiple layers of heavy-duty aluminum foil (Emergency Field Hack) and turn on Airplane Mode *if* accessible without password.
- **3. The Power Decision:**
  - **If OFF:** Leave it OFF. Never turn it on to "just check."
  - **If ON: STOP.** Do not pull the plug immediately.
  - *Critical:* Photograph the screen. If trained, use a "Live Response Tool" to capture RAM. If untrained, document running processes, then pull the power (for desktops) or isolate (for mobiles).

2. Chain of Custody

Definition & Importance

The "Chain of Custody" is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.

- **Objective:** To prove that the evidence presented in court is the *same* evidence seized at the scene.
- **Requirement:** No time gaps. Every transfer must be signed by both giver and receiver.



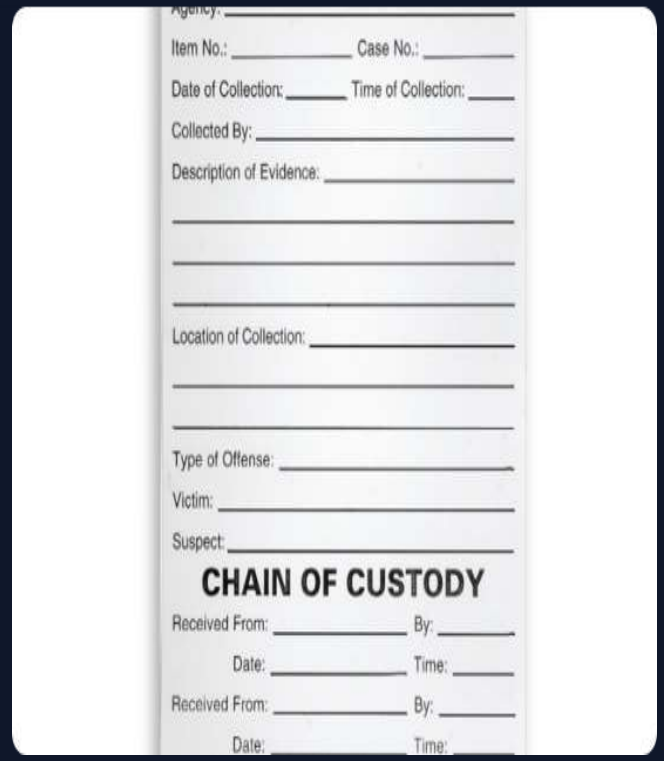
Chain of Custody

The Backbone of Admissibility

Concept: If you cannot prove *who* held the device, the defense will claim "Tampering."

The Golden Rules:

1. **Chronological Documentation:** A paper trail from the spot of seizure to the FSL (Forensic Science Lab) and finally to the Court.
2. **Seizure Memo (Panchnama):**
    - Must include **Hash Value** (Digital Fingerprint) if possible on-site (using hash blockers/write blockers).
    - Record: Make, Model, Serial Number (IMEI for phones), physical condition (scratches/damage).
    - *Legal Note:* **Section 105 BNSS** covers the process of seizure.


Agency: _____
Item No.: _____ Case No.: _____
Date of Collection: _____ Time of Collection: _____
Collected By: _____
Description of Evidence: _____
_____
_____
_____
Location of Collection: _____
_____
_____
Type of Offense: _____
Victim: _____
Suspect: _____
CHAIN OF CUSTODY
Received From: _____ By: _____
Date: _____ Time: _____
Received From: _____ By: _____
Date: _____ Time: _____

Digital Evidence Collection Form

Mandatory Fields

- **Case Reference:** FIR No., Police Station, Date.
- **Device ID:** Make, Model, Serial Number (IMEI for phones).
- **Condition:** Powered On/Off, Screen Cracked, Password protected?
- **Location:** Specific room/desk where found.

Integrity Data

- **Hash Value:** (MD5/SHA-256) captured at scene (if feasible) or immediately at lab.
- **Sealing Officer:** Name, Rank, and Signature.
- **Witnesses:** Signatures of two independent witnesses ().

3. Tools: Memory & Mobile

Memory (RAM) Forensics

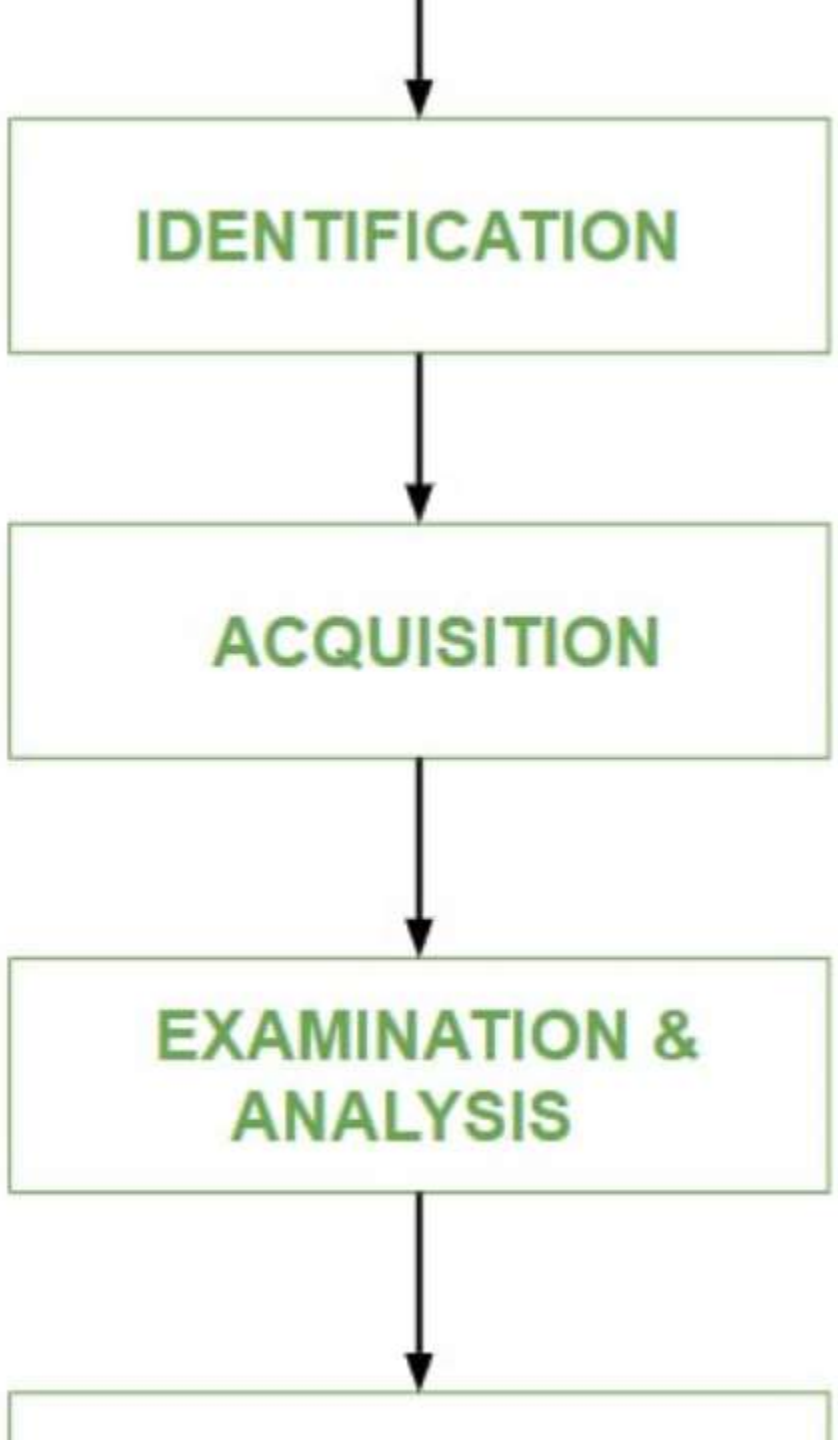
Tools: FTK Imager, DumpIt, Volatility.

Critical for capturing volatile data like passwords, running processes, and unencrypted keys before the device loses power.

Mobile Forensics

Tools: Cellebrite UFED, MSAB XRY, Oxygen Detective.

Used for physical and logical extraction of data from smartphones, bypassing locks, and decoding app data (WhatsApp, Telegram).



3. Tools: Specialized Forensics

Cloud Forensics

Magnet AXIOM, Elcomsoft.
Used to extract data from cloud backups (Google Drive, iCloud) using tokens found on seized devices.

Audio/Visual

Amped FIVE, Adobe Audition.
Essential for enhancing CCTV footage, authenticating voice recordings, and noise reduction.

Data Recovery

Autopsy, EnCase, Recuva.
Used to recover deleted files, formatted drives, and carve data from unallocated space.

4. Packaging & Labeling

Packaging Protocols

- **Hard Drives/Laptops:** Use Anti-Static Bags to prevent electrostatic discharge (ESD) damage.
- **Mobile Phones:** Use Faraday Bags to block network signals and prevent remote wiping.
- **Sealing:** Use tamper-evident tape. The seal must be signed by the IO and witnesses.(Although our local way of putting ink on tape over the seal is ok for now)

Labeling

Label must include: **"Exhibit A"**, FIR No, Date, Time, and WITNESS/IO signatures.A label "Warning: Electronic Evidence".

5. Post-Seizure Legal Procedure

Section 63 BSA 2023

This section replaces Section 65B of IEA. It is **mandatory** to furnish a certificate for the admissibility of any electronic record (secondary evidence). Without this, printouts/copies are inadmissible.

Expert Opinion

Section 39 BSA: (Formerly 45A IEA). Expert opinion is required for the examination of electronic evidence. The integrity of the Hash Value generated at the time of seizure is verified here.

Key Takeaways

- **1. Law Guides Tech:** Always back your technical seizure with **BNSS Sections** and **IT Act** provisions.
- **2. Hash is King:** The Hash Value is your defense against claims of planting evidence.
- **3. Don't be "Click-Happy":** If you don't know what to do, **Photograph everything** and wait for the Cyber Cell expert.
- **4. The Chain is Sacred:** A break in the Chain of Custody (Malkhana register) breaks the case in court.

"Digital Evidence is Fragile, but when handled right, it is the most powerful witness in the room."

DIGITAL EVIDENCE SEIZURE CHECKLIST

Objective: Secure evidence integrity & ensure admissibility

PHASE 1: SECURE & ISOLATE (The First 5 Minutes)

[ ] **Secure the Scene:** Remove all persons from the vicinity of digital devices.

[ ] **Network Isolation (CRITICAL):**

- **Mobile Phones:**
  - If **ON**: Do **NOT** switch off. Immediately enable **Airplane Mode** (if accessible).
  - Disconnect WiFi/Bluetooth/Data.
  - Place in **Faraday Bag**.
  - *Field Hack:* If no Faraday bag is available, wrap the phone in **3-4 layers of heavy-duty aluminum foil** or place inside a microwave oven (do not turn it on!) until a bag is found.
- **Computers/Laptops:**
  - **Wired:** Unplug the Ethernet (LAN) cable immediately.
  - **Wireless:** If you can disable Wi-Fi via a physical switch, do it.

[ ] **Power State Decision:**

- **If OFF: LEAVE IT OFF.** Never power on to "check."
- **If ON (Desktop):** Photograph screen. Pull the power plug from the *back of the CPU* (not the wall) to freeze the state.
- **If ON (Laptop):** Photograph screen. Disconnect battery if removable. If not, pack in Faraday bag and transport immediately to FSL.

PHASE 2: DOCUMENTATION (Section 105 BNSS)

] Mandatory Videography:

Record the entire seizure process using an official device/mobile.

Requirement: Ensure the video shows the device condition, the serial number/IMEI, and the sealing process.

[ ] Photograph the "Context":

Take photos of where the device was found (on a table, under a bed, etc.).

Take close-ups of the screen (if on) and any connected cables/drives.

[ ] Seizure Memo (Panchnama):

Must Record: Make, Model, Color, Serial Number, IMEI (dial *#06# if unlocked), Condition (scratches, screen cracks).

Hash Value: (If FSL expert is present) Record the MD5/SHA-256 hash of the seized data.

PHASE 3: PACKAGING & LABELLING

[ ] Prevents Static: Place Hard Drives/Circuit Boards in Anti-Static Bags.

[ ] Prevent Signals: Place Mobiles/Tablets/Smartwatches in Faraday Bags.

[ ] Sealing:

Seal with official tape.

Sign across the seal (IO + Witnesses).

Affix the Lak (Wax) Seal.

[ ] Labeling: EXHIBIT A

Case/FIR No: _____

Date/Time: _____

IO Name: _____

WARNING: "DIGITAL EVIDENCE – DO NOT X-RAY / DO NOT USE MAGNETS"

PHASE 4: LEGAL COMPLIANCE

[ ] Certificate under Section 63(4) BSA:

Formerly Sec 65B IEA. Ensure you identify the person in "lawful control" of the device to sign Part A of the certificate.

[ ] Chain of Custody Form:

Log every person who touches the evidence.

Entry: Scene -> IO -> Malkhana -> Constable (Transit) -> FSL.

QUICK REFERENCE: BSA SECTION 63 CERTIFICATE

Who Signs?

Part A: The owner/user of the device (The person who "regularly" uses it).

Part B: The Expert (FSL/Cyber Consultant) who validates the hash/integrity.

Why? Without this, the electronic record is inadmissible as primary evidence.

BEFORE SHOWING SOME PRACTICAL DEMO,

ANY Questions?

Thank you