Evidence Handling and Forensic Reporting

Digital evidence:

- Today digital evidence collection is used in the investigation of a wide variety of crimes such as fraud, espionage, cyberstalking, etc.
- The knowledge of forensic experts and techniques are used to explain the contemporaneous state of the digital artifacts from the seized evidence such as computer systems, storage devices (like SSDs, hard disks, CD-ROM, USB flash drives, etc.), or electronic documents such as emails, images, documents, chat logs, phone logs, etc.

Characteristics of digital evidence:

The rule of digital evidence refers to the set of guidelines and principles that govern the collection, preservation, analysis, and presentation of digital evidence in legal proceedings. It is important to follow these rules to ensure that the evidence is admissible in court and that the integrity of the evidence is preserved.

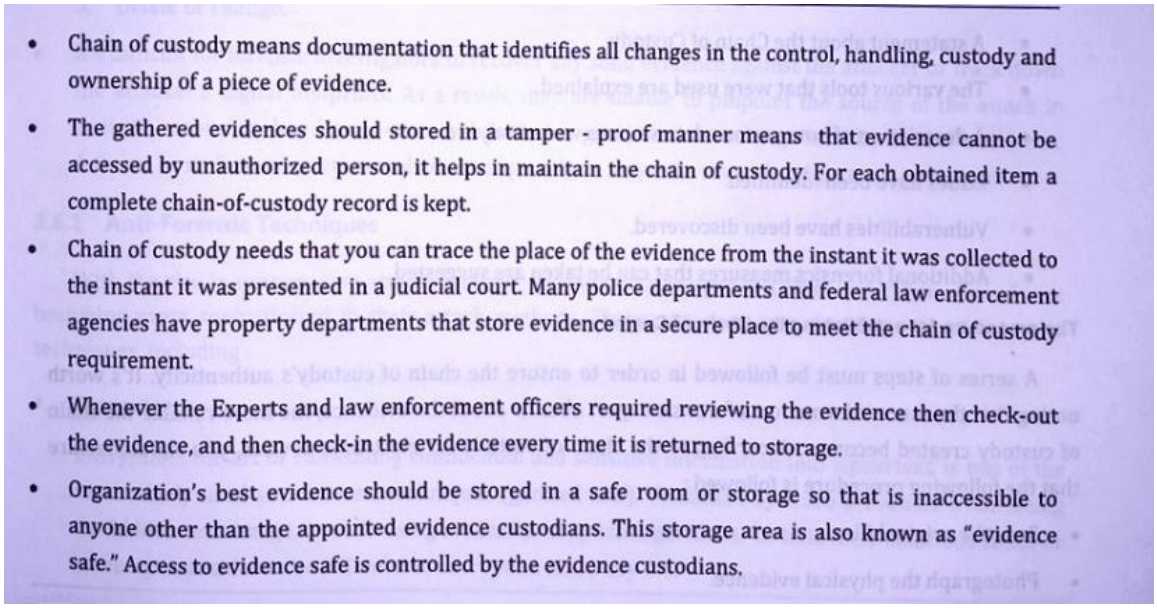
✅ Some of the key characteristics of digital evidence include:

1. Volatility: Digital evidence can be easily lost or modified if it is not properly preserved and protected.
2. Complexity: Digital evidence can be difficult to analyze and interpret due to the vast amount of data that may be involved.
3. Ubiquity: Digital evidence is found in nearly all aspects of modern life, from personal computers to smartphones to internet-connected devices.
4. Fragility: Digital evidence can be easily damaged or corrupted if not handled properly.
5. Persistence: Digital evidence can remain on a device or network even after it has been deleted or erased.

✅ Evidence Handling Methodology

- **Identification of evidence**: It includes of identifying evidences related to the digital crime in storage media, hardware, operating system, network and/or applications. It is the most important and basic step.
- **Collection**: It includes preserving the digital evidences identified in the first step so that they doesn't degrade to vanish with time. Preserving the digital evidences is very important and crucial.
- **Analysis**: It includes analyzing the collected digital evidences of the committed computer crime in order to trace the criminal and possible path used to breach into the system.
- **Documentation**: It includes the proper documentation of the whole digital investigation, digital evidences, loop holes of the attacked system etc. so that the case can be studied and analysed in future also and can be presented in the court in a proper format.
- **Presentation**: It includes the presentation of all the digital evidences and documentation in the court in order to prove the digital crime committed and identify the criminal.

Chain of Custody/ Digital Evidence Collection Process:



- Chain of custody means documentation that identifies all changes in the control, handling, custody and ownership of a piece of evidence.
- The gathered evidences should stored in a tamper - proof manner means that evidence cannot be accessed by unauthorized person, it helps in maintain the chain of custody. For each obtained item a complete chain-of-custody record is kept.
- Chain of custody needs that you can trace the place of the evidence from the instant it was collected to the instant it was presented in a judicial court. Many police departments and federal law enforcement agencies have property departments that store evidence in a secure place to meet the chain of custody requirement.
- Whenever the Experts and law enforcement officers required reviewing the evidence then check-out the evidence, and then check-in the evidence every time it is returned to storage.
- Organization's best evidence should be stored in a safe room or storage so that is inaccessible to anyone other than the appointed evidence custodians. This storage area is also known as "evidence safe." Access to evidence safe is controlled by the evidence custodians.

Chain of Custody Process

The chain of custody should extend from the first step of data collection to examination, analysis, reporting, and the time of presentation to the courts in order to preserve digital evidence. This is critical in order to avoid any suggestion that the evidence has been tampered with in any way.

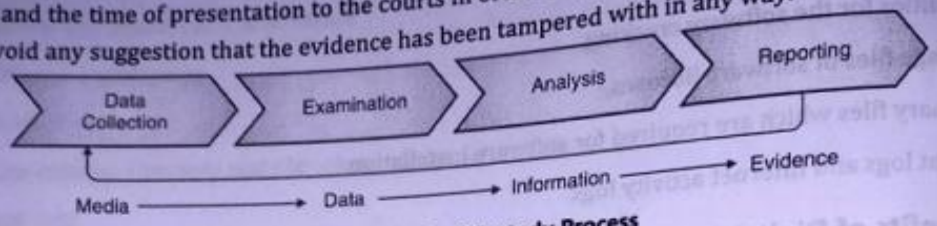


Fig. 2.5.1 : Chain of Custody Process

1. **Data collection :** It is the first step in the chain of custody process. It entails the identification, labelling, recording, and acquisition of data from all relevant sources while maintaining the data and evidence's integrity.
2. **Examination :** During this step, the chain of custody information is documented, as well as the forensic procedure that was followed. It's critical to take screenshots throughout the process to demonstrate the tasks that have been completed and the evidence that has been discovered.
3. **Analysis :** The result of the examination stage is the analysis stage. In the Analysis stage, legally justifiable methods and techniques are used to gather useful information in order to respond to the questions posed in the case.
4. **Reporting :** In the Examination and Analysis stage, this is the documentation phase. The following items are included in reporting :
   - A statement about the Chain of Custody.
   - The various tools that were used are explained.
   - A description of how various data sources were analysed.

📍Types of Evidence:

Collecting the shreds of evidence is really important in any investigation to support the claims in court. Below are some major types of evidence.

1. **Real Evidence**: These pieces of evidence involve physical or tangible evidence such as flash drives, hard drives, documents, etc. an eyewitness can also be considered as a shred of tangible evidence.
2. **Hearsay Evidence**: These pieces of evidence are referred to as out-of-court statements. These are made in courts to prove the truth of the matter.
3. **Original Evidence**: These are the pieces of evidence of a statement that is made by a person who is not a testifying witness. It is done in order to prove that the statement was made rather than to prove its truth.
4. **Testimony**: Testimony is when a witness takes oath in a court of law and gives their statement in court. The shreds of evidence presented should be authentic, accurate, reliable, and admissible as they can be challenged in court.

Demonstrate the challenges in evidence handling

Challenges:

Risk of Data Breach, Tampering, and Cyber Attacks

Collecting digital evidence is easy in most cases. The tricky part is securing and protecting it from data breaches, cyber-attacks, and tampering. It is very challenging to prevent these attacks and detect tampering as it is done discreetly to make it seems like it is still intact.

Diversity of Digital Devices, Data Type, and Volume

Digital evidence now exists in multiple formats ingested from different devices like CCTV, body cams, drone cams, home security cameras etc. For agencies, the problem is that the volume of digital evidence is increasing at an exponential rate.

Access Management

CJIS Security Policy clearly states that agencies need to store digital evidence in a controlled environment or secure physical location and restrict access to authorized individuals only.

Errors and Mishaps

No human is perfect, and errors are bound to happen due to causes like unintentional biases,excessive workload, technology usage error, random mishaps, etc.

Transfer of Data

Evidence is most at-risk during transfer as data could be breached, exposed, or tampered with. Protecting digital evidence during transit is very difficult.

Presenting in Court Finally, if the digital evidence is made inadmissible in court due to problems in handling it

appropriately. Agencies should also be aware of how the evidence can be presented based on the court's technology setup and internet connectivity. Based on that, evidence should be transported and presented securely.

📍Types of Collectible Data:

The computer investigator and experts who investigate the seized devices have to understand what kind of potential shreds of evidence could there be and what type of shreds of evidence they are looking for. So, that they could structure their search pattern. Crimes and criminal activities that involve computers can range across a wide spectrum; they could go from trading illegal things such as rare and endangered animals, damaging intellectual property, to personal data theft, etc.There are two types of data, that can be collected in a computer forensics investigation:

1. **Persistent data**: It is the data that is stored on a non-volatile memory type storage device such as a local hard drive, external storage devices like SSDs, HDDs, pen drives, CDs, etc. the data on these devices is preserved even when the computer is turned off.
2. **Volatile data**: It is the data that is stored on a volatile memory type storage such as memory, registers, cache, RAM, or it exists in transit, that will be lost once the computer is turned off or it loses power. Since volatile data is evanescent, it is crucial that an investigator knows how to reliably capture it.

Faraday Bags:.

- Faraday Bags much like the Faraday cage is an enclosed, sealed unit which prevents signals from being sent and received thanks to the material the bag is made from.
- Faraday Bags, named after the inventor of the Faraday cage block RF signals from both being sent and received to an electronic device such as a mobile phone, car key or laptop
- This is important in cases of seized devices where the data contained in it is used as evidence in court as the faraday bag will ensure this has not been tampered with.
- Faraday bags can be made up of a wide range of materials but the most common are multiple layers of various metallic layers
- one of the main uses for Faraday Bags is protecting the integrity of information usually by law enforcement and government agencies.
- Other common uses can be from people known as “Preppers” that store devices in Faraday bags to protect themselves from hackers and unauthorised access but also from electromagnetic pulses from a man-made device or astrological event that can damage electronic equipment.
- Faraday Bags much like the Faraday cage is an enclosed, sealed unit which prevents signals from being sent and received thanks to the material the bag is made from.