MODULE II

INTRODUCTION TO COMPUTER FORENSICS INVESTIGATION AND ELECTRONIC EVIDENCE

COMPUTER FORENSICS

❑Computer forensics involves the **preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.**

❑Evidence might be required for a wide range of computer crimes and misuses.

❑It involves:

1. **Discovering data on computer system**
2. **Recovering deleted, encrypted, or damaged file information**
3. **Monitoring live activity**
4. **Detecting violations of corporate policy**

❑Information collected assists in arrests, prosecution, termination of employment, and preventing future illegal activity.

EXAMPLES

❑Recovering thousands of **deleted emails.**

❑Performing **investigation after multiple users** had taken over the system.

❑ **Performing termination investigation post employment.**

❑ Recovering **evidence post formatting hard drive.**

WHO USES COMPUTER FORENSICS

Criminal Prosecutors :Rely on evidence obtained from a computer to prosecute suspects and use as evidence.

Civil Litigations : Personal and business data discovered on a computer can be used in fraud, divorce, harassment, or discrimination cases.

Insurance Companies : Evidence discovered on computer can be used to mollify costs, worker's compensation, arson, etc.

Private Corporations : Obtained evidence from employee computers can be used as evidence in harassment, fraud, and embezzlement cases.

Law Enforcement Officials : Rely on computer forensics to backup search warrants and post seizure handling.

Individual/Private Citizens :Obtain the services of professional computer forensic specialists to support claims of harassment, abuse, or wrongful termination from employment.

TYPES OF DIGITAL FORENSICS

Disk Forensics: It deals with extracting data from storage media by searching active, modified, or deleted files.

Network Forensics: It is a sub branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

Wireless Forensics: It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.

Malware Forensics: This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Email Forensics: Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

Memory Forensics: It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

Mobile Phone Forensics: It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Database Forensics: It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

IoT Forensics: IoT forensics is the practice of analyzing IoT devices to investigate crimes. Fitness trackers, smart appliances, connected vehicles, would form part of IoT Forensics.

Cloud Forensics: Cloud forensic is the amalgamation of all the different forensics(i e digital forensics, network forensics, hardware forensics etc.

DIGITAL EVIDENCE

- ❑Any **information being subject to human intervention or not, that can be extracted from a computer.**
- ❑Must be in **human-readable format or capable of being interpreted by a person with expertise in the subject**.

REASONS FOR EVIDENCE GATHERING

Evidence collected by Federal, State and local authorities for crimes relating to:

- Theft of trade secrets
- Fraud
- Extortion
- Industrial espionage
- Position of pornography
- SPAM investigations
- Virus/Trojan distribution

- Homicide investigations
- Intellectual property breaches
- Unauthorized use of personal information
- Unauthorized activity
- Tracking internet browsing habits
- Reconstructing Events
- Inferring intentions
- Selling company bandwidth
- Wrongful dismissal claims
- Sexual harassment
- Software Piracy

LOCARD’S PRINCIPLE OF EXCHANGE

- Locard’s exchange principle is an important part of forensic science investigation.

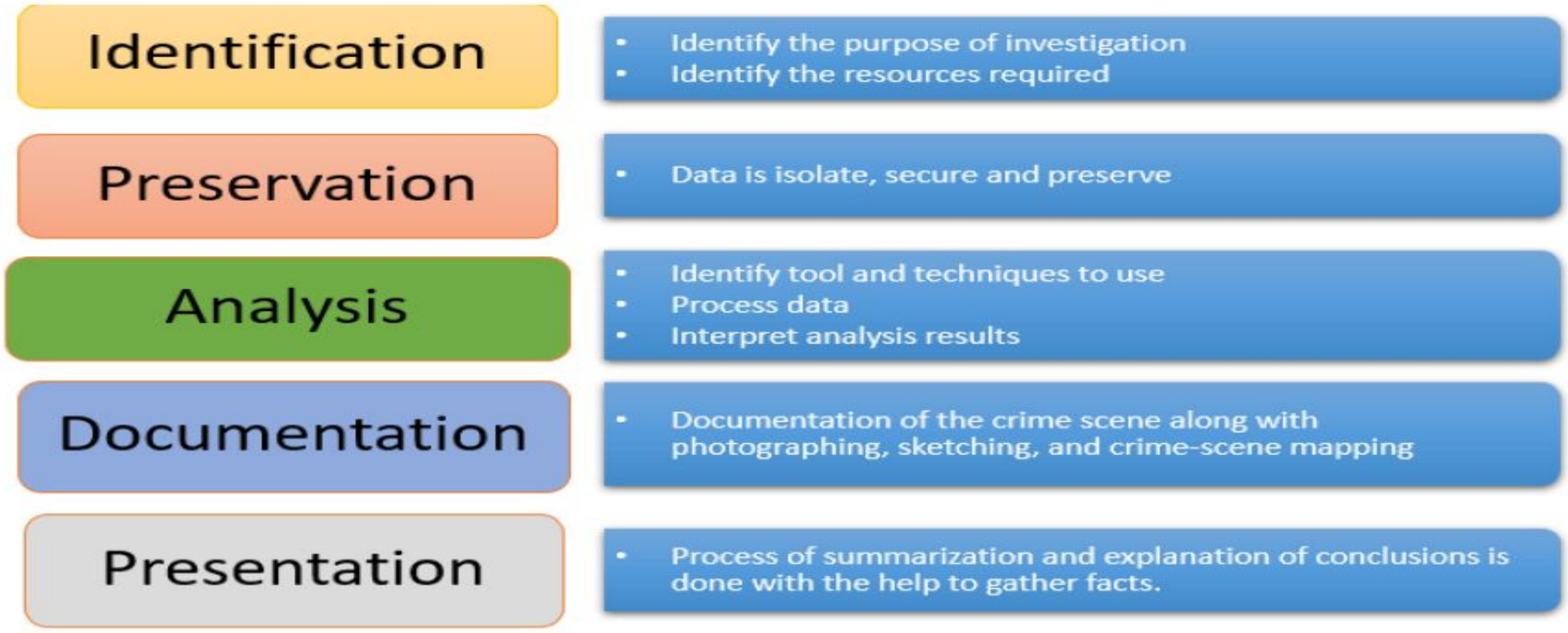
- **It states that any criminal leaves behind a trace when committing a violent crime.**

- It is the investigator’s duty to find this trace evidence and reconstruct the events of the crime.

- In other words, **the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence.**

STEPS OF COMPUTER FORENSICS

- Digital forensics entails the following steps:



Identification	• Identify the purpose of investigation • Identify the resources required
Preservation	• Data is isolate, secure and preserve
Analysis	• Identify tool and techniques to use • Process data • Interpret analysis results
Documentation	• Documentation of the crime scene along with photographing, sketching, and crime-scene mapping
Presentation	• Process of summarization and explanation of conclusions is done with the help to gather facts.

PROCESS OF DIGITAL FORENSICS

Identification: It is the **first step in the forensic process**. The identification process mainly includes things like **what evidence is present, where it is stored, and lastly, how it is stored (in which format).** Electronic storage media can be personal computers, mobile phones, PDAs, etc.

Preservation: In this phase, data is **isolated, secured, and preserved**. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis: In this step, **investigation agents reconstruct fragments of data and draw conclusions based on evidence found.**

Documentation

- In this process, a record of all the visible data must be created.
- It helps in recreating the crime scene and reviewing it.
- It Involves **proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.**

Presentation

- In this last step, the **process of summarization and explanation of conclusions is done.**

DIGITAL CRIME SCENE INVESTIGATION PROCESS

- A **digital investigation** is a **process where hypotheses that answer questions about digital events is developed and tested.**
- A digital forensic investigation is a **process that uses science and technology to analyze digital objects and that develops and tests theories.**
- It **should be admissible in a court of law, to answer questions about events that occurred.**
- In other words, **a digital forensic investigation is a more restricted form of digital investigation.**

Digital crime scene includes digital environment created by hardware and software.

Digital Crime Investigation process has three major phases:

1. **System Preservation Phase**
2. **Evidence Searching Phase**
3. **Event Reconstruction Phase**

TYPES OF ANALYSIS:

Live Analysis

Dead Analysis

INITIATING A INVESTIGATION

1. **Do not begin by exploring files on system randomly.**
2. Establish evidence custodian - start a detailed journal with the date and time and date/information discovered.
3. If possible, **designate suspected equipment as “off- limits” to normal activity.** This includes back-ups and configuration changes.
4. Collect email, DNS, and other network service logs.
5. Capture exhaustive external TCP and UDP port scans of the host.
6. Contact security personnel [CERT], management, State and local enforcement, as well as affected sites or persons.

PRESERVATION PHASE

- Involves **preservation of state of digital crime scene**.
- Action taken is based on legal or operational requirements.
- **Unplug the system to create a image.**
- **Purpose –** To reduce the amount of evidence that could be overwritten.
- **Write blocker can be used to prevent overwriting of data.**
- Creating a cryptographic hash of the data like MD5, SHA1, etc.

HANDLING EVIDENCE

- **Admissibility of Evidence**
  - Legal rules which determine **whether potential evidence can be considered by a court.**
  - **Must be obtained in a manner which ensures the authenticity and validity and that no tampering had taken place.**

- Preventing viruses from being introduced to a computer during the analysis process.
- Extracted/relevant evidence is properly handled and protected from mechanical or electromagnetic damage.

- No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to search the computer.
- Establishing and maintaining a continuing chain of custody.
- Limiting the amount of time business operations are affected.
- **Not divulging andrespecting any ethically [and legally] client-attorney information that is inadvertently acquired during a forensic exploration.**

HANDLING INFORMATION

- **Information and data being sought after and collected in the investigation must be properly handled.**

✔ **Volatile Information**

- **Network Information**
  - Communication between system and the network.
- **Active Processes**
  - Programs currently active on the system.
- **Logged-on Users**
  - Users/employees currently using system.
- **Open Files**
  - Libraries in use; hidden files; Trojans (rootkit) loaded in system.

✔ **Non-Volatile Information**

- This includes information, **configuration settings, system files and registry settings that are available after reboot.**
- Accessed through drive mappings from system.
- This information should investigated and reviewed from a backup copy.

EVIDENCE GATHERING PHASE

- After data is preserved, **evidence needs to be searched.**
- Depending the evidence type **various locations are searched.**
- The hypothesis **created based on the case details need to be refuted or supported to ensure appropriateness of evidence collected.**
- General characteristics of the object being searched needs to be defined and then searched in the data gathered.
- Evidence can be **searched based on name, pattern, comparing hash, keyword based or searching for IP address, specific port/source address**.

EVENT RECONSTRUCTION PHASE

- Based on the evidence found reconstruction of the digital event is done in this phase.

- Once digital event reconstruction is done**, it can be compared with physical events**.

- **Event reconstruction requires adequate knowledge of OS and the installed applications.**

GENERAL GUIDELINES

PICL should be followed in all investigations to ensure no evidence is left out

- **P – Preservation**
- **I – Isolation**
- **C - Correlation**
- **L – Logging**

Preservation

- Original data should be kept in safe custody and investigation should be on the copy of the original data.
- Write blocker should be used.
- Calculate hash of the original evidence.
- Live analysis should be done carefully to prevent overwriting of existing data.

ISOLATION

- The analysis environment **should be isolated from all possible threats.**
- The analysis should be done in a **virtual environment to prevent any data loss.**
- **Connection to the outside world should be avoided to prevent any tampering of evidence.**
- Isolation is implemented using an analysis network that has limited connectivity.
- Implementing isolation during a live analysis is difficult and hence should be done with caution.

CORRELATION

- Data should be correlated with other independent sources to prevent any forgery/planting of evidence.
- **Timestamps can be easily manipulated and preventing correlation in such instances.**
- **File activity timeline should be correlated with log entries, network traffic or other events.**

LOGGING

- All the actions being taken should be logged and documented.
- This will prevent missing important actions and activities.
- **Data changes during live analysis should be well documented.**

STANDARD OPERATING PROCEDURES

- **First responders may follow the steps listed below to guide their handling of digital evidence at an electronic crime scene:**
  - Recognize, identify, seize, and secure all digital evidence at the scene.
  - Document the entire scene and the specific location of the evidence found.
  - Collect, label, and preserve the digital evidence.
  - Package and transport digital evidence in a secure manner.

Before collecting evidence at a crime scene, first responders should ensure that:

- Legal authority exists to seize evidence.
- The scene has been secured and documented.
- Appropriate personal protective equipment is used.

First responders without the proper training and skills should not attempt to explore the contents of or to recover information from a computer or other electronic device other than to record what is visible on the display screen.

- **For proper evidence preservation, follow these procedures in order:**
    - Photograph the computer and scene.
    - If the computer is off , do not turn it on.
    - If the computer is on, photograph the screen.
    - **Collect live data - start with RAM image** and then collect other live data "as required" such as network connection state, logged on users, currently executing processes etc.
    - **Unplug the power cord from the back of the tower** - If the computer is a laptop and does not shut down when the cord is removed then remove the battery.

- **Document all device model numbers and serial numbers.**
- Disconnect all cords and devices.
- Image hard drives using a write blocker.
- Package all components(using anti-static evidence bags).
- **Seize all additional storage media** (create respective images and place original devices in anti-static evidence bags).
- **Keep all media away from magnets, radio transmitters and other potentially damaging elements.**
- Collect instruction manuals, documentation and note.
- Document all steps used in the seizure and **maintain proper Chain of Custody.**

CHAIN OF CUSTODY

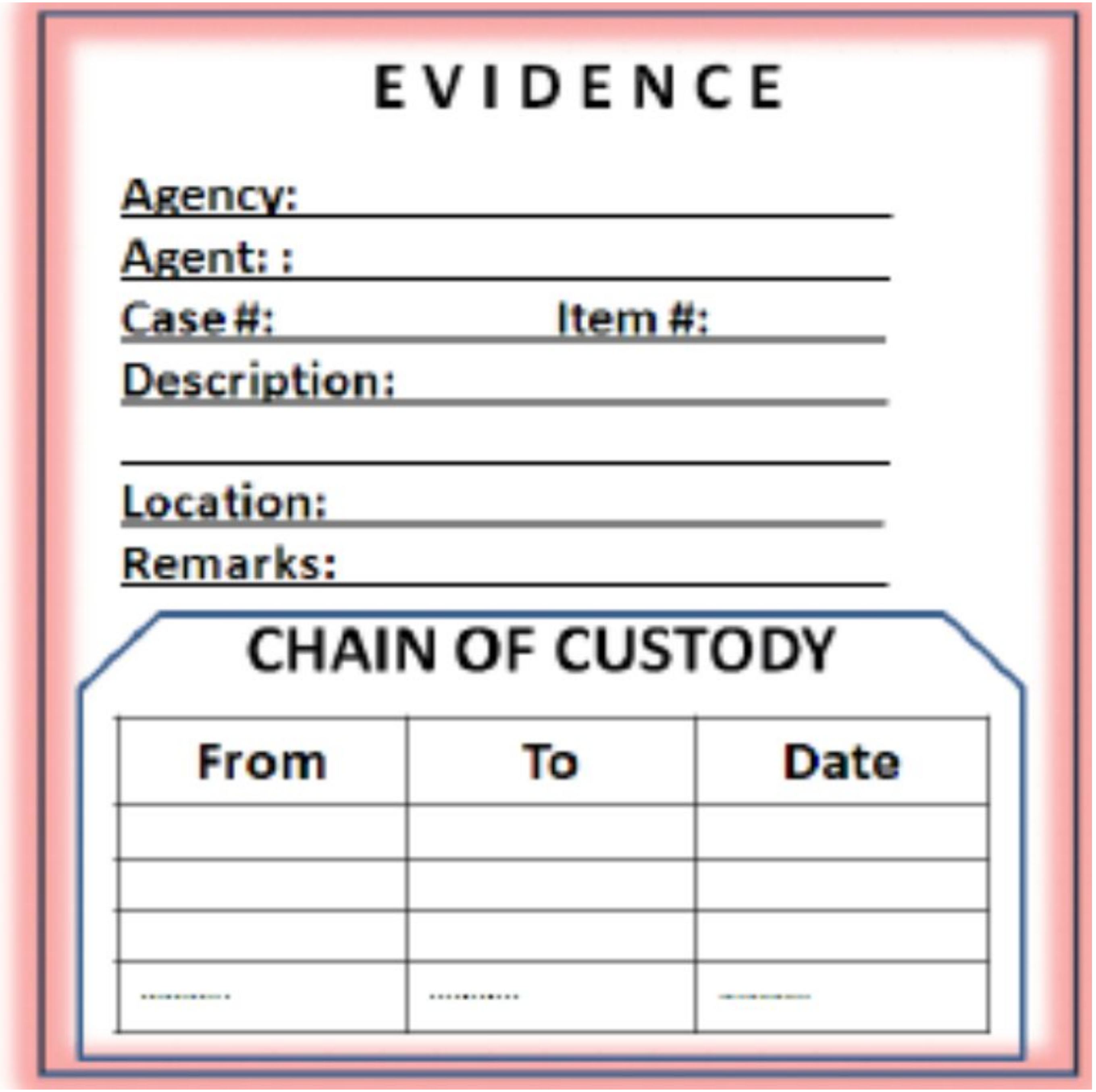
- **The movement and location of physical evidence from the time it is obtained until the time it is presented in court.**

- As is the case with all evidence, it's important to maintain a chain of custody for computer evidence.

- The term "chain of custody" refers to **documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence (physical or electronic).**

- It is required to **trace the route that evidence takes from the moment it is collected until the time it is presented in Court of Law.**

- Chain of Custody refers to the **logical sequence that records the sequence of custody, control, transfer, analysis and disposition of physical or electronic evidence in legal cases.**
- Each **step in the chain is essential and if there is a break, the evidence may be rendered inadmissible.**



EVIDENCE

Agency: ______________________________

Agent: : ______________________________

Case #: ______________ Item #: ______________

Description: ______________________________

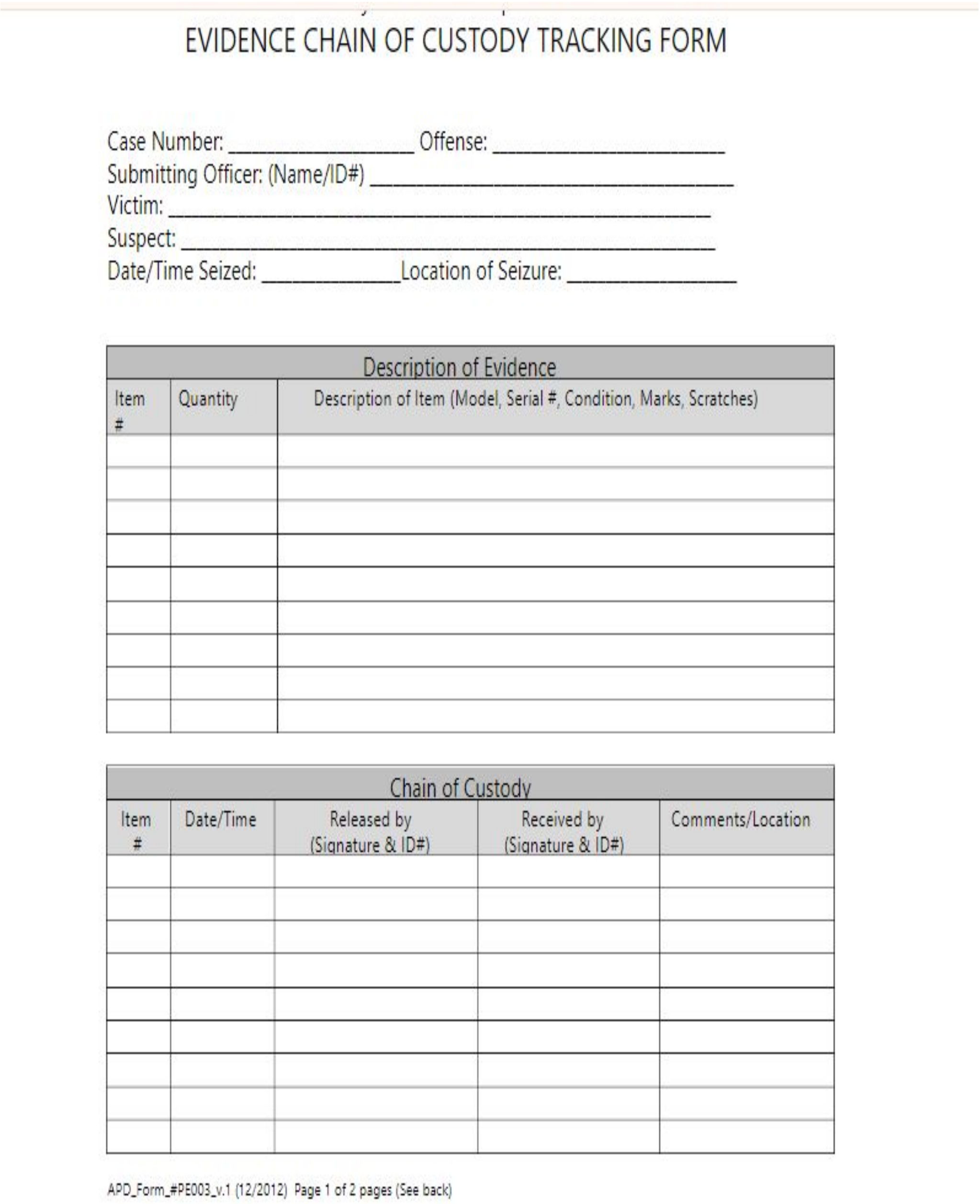
____

Location: ______________________________

Remarks: ______________________________

CHAIN OF CUSTODY

From	To	Date
....	....	....



EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: ________________ Offense: ____________________

Submitting Officer: (Name/ID#) ________________________________

Victim: ____

Suspect: ____

Date/Time Seized: ____________Location of Seizure: ______________

Description of Evidence

Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody

Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

IMPORTANCE OF CHAIN OF CUSTODY

- Maintaining the chain of custody is critical in forensic practice **to avert tampering**.

- The goal is to establish that the evidence is related to the alleged crime, was collected from the scene, and was in **its original/unaltered condition rather than having been tampered with or " deceitfully to make someone seem guilty.**

- The chain of **custody maintains the integrity of the sample.**

- **The traceability of the record of the control, transfer, and analysis of samples indicates the transparency to the procedure.**

WRITE BLOCKERS

A write blocker is any **tool that permits read only access to data storage devices without compromising the integrity of the data.**

It prevents any write access to the hard disk.

Write blockers are devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents. **They do this by allowing read commands to pass but by blocking write commands.**

As per NIST general guidelines:

- ❖The write blocker tool shall not **allow a protected drive to be changed.**
- ❖The write blocker tool shall not prevent **any operations to a drive.**
- ❖The write blocker tool shall not **prevent obtaining any information from or about any drive.**

TYPES OF WRITE BLOCKERS

Write Blockers are basically of 2 types: Hardware Write Blocker and Software Write Blocker

- **Hardware write blocker—**The hardware blocker is a device that is installed that runs software internally to itself and will block the write capability of the computer to the device attached to the write blocker.
- **Software write blocker—**The software blocker is an application that is run on the operating system that implements a software control to turn off the write capability of the operating system.

TABLEAU
FireWire800+USB2.0 SATA Bridge
A On B On
DC IN B
DC IN A
USB 2.0
800
800
400
SATA
Power
SATA Detect
Host Detect
Write Block
Activity
DC OUT
Maxtor
OLD MAIL SERVER

TABLEAU
Forensic USB Bridge
DC IN
DC IN
Host Detect
Power
Write Block
Activity
ON
OFF
FireWire — Host — USB 2.0
Menu
Enter
Mfg name
SanDisk
Device Detect
USB 2.0