Overview of Cyber Forensics

What is Cybersecurity?

- **What?** Cybersecurity tends to focus on how malicious actors use electronic assets (Internet, WAN, LAN, routers, printers, network appliances) to attack information.

- **Why?** To prevent individuals, organizations, financial institutions and universities from cyber attacks including, ransomware, malware etc.

- **How?** Running the assets safely with security implementations of databases, networks, hardware, firewalls and encryption.

What is Cyber Forensics?

- **What**? The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
- **How?** Through the digital forensics investigation process including: **I**dentification, **P**reservation, **A**nalysis, and **P**resentation (IPAP).
- **Why?** Used in criminal investigations to identify what happened, how it happened, when it happened and the people involved.

Relationship between Cybersecurity and Cyber Forensics

- Cybersecurity aims to protect electronic assets from breaches; whereas, cyber forensics explains how a policy became violated and who was responsible for it.

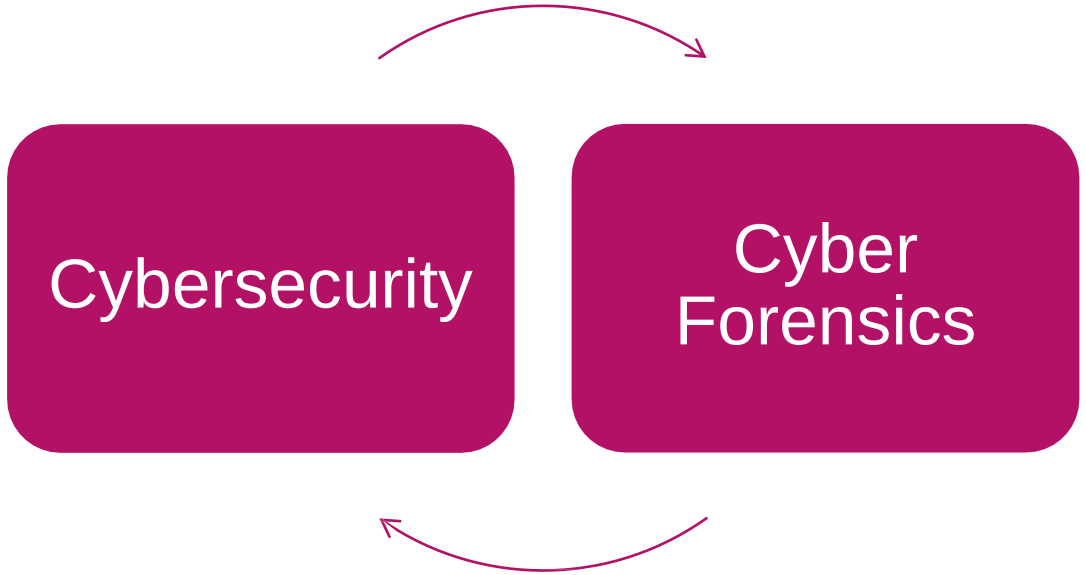


Fig. 1 Feedback cycle of Cybersecurity and Cyber Forensics

Edmond Locard's Principle

Locard's Principle - Perpetrator of a crime will bring something into the crime scene and leave with something from it, and that can be used as forensic evidence; thus, every Cyber Fraud or Cyber Crime will have evidence.

Don’t Touch the Suspect Drive

The first, and perhaps most important, is to touch the system as little as possible. You do not want to make changes to the system in the process of examining it. Look at one possible way to make a forensically valid copy of a drive.

Document Trail

Beyond not touching the actual drive, the next issue is documentation. If you have never worked in any investigative capacity, the level of documentation may seem onerous to you. But the rule is simple: *Document everything.*

Secure the Evidence

- First and foremost, the computer must be taken offline to prevent further tampering. There are some limited circumstances in which a machine would be left online to trace down an active, ongoing attack. But the general rule is to take it offline immediately.
- Limit access
- Document person who had access

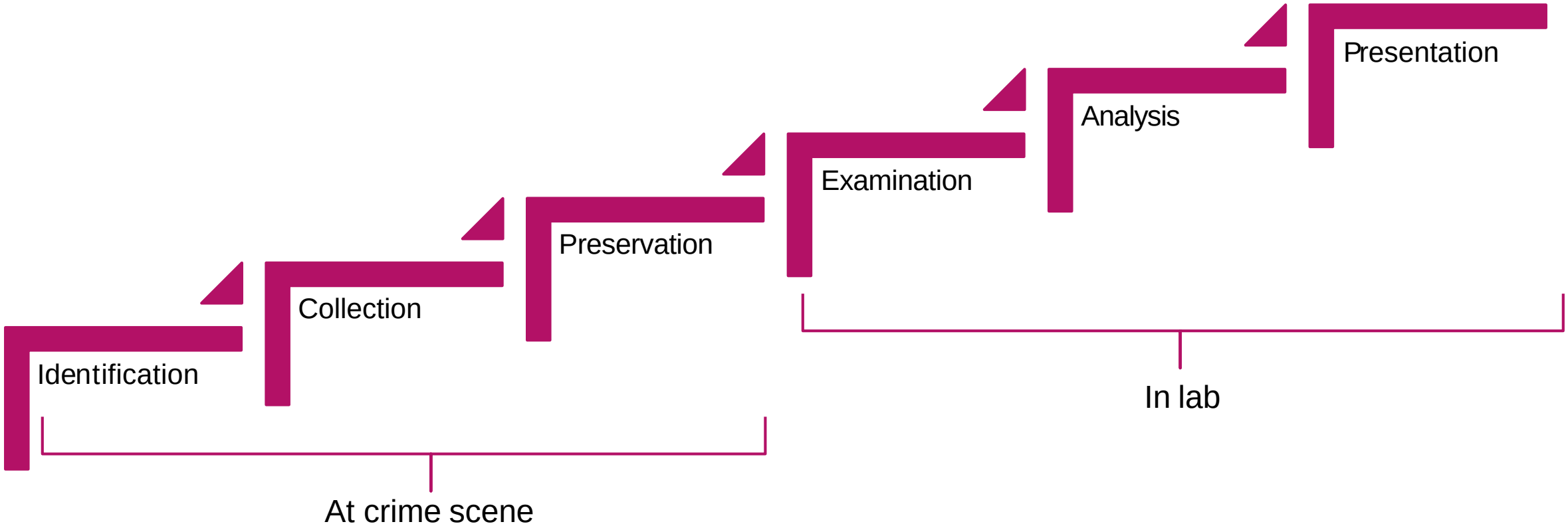
Document Losses

- Labor cost spent in response and recovery. (Multiply the number of participating staff by their hourly rates.)
- If equipment were damaged, the cost of that equipment.
- If data were lost or stolen, what was the value of that data? How much did it cost to obtain that data and how much will it cost to reconstruct it?
- Any lost revenue, including losses due to down time, having to give customers credit due to inconvenience, or any other way in which revenue was lost.

Finding Evidence in the Browser

The browser can be a source of both direct evidence and circumstantial or supporting evidence. Obviously in cases of child pornography, the browser might contain direct evidence of the specific crime. You may also find direct evidence in the case of cyber stalking. However, if you suspect someone of creating a virus that infected a network, you would probably find only indirect evidence such as the person having searched virus creation/programming-related topics.

Digital Forensics Investigation Process Model



Stage 1: Identification

In this stage, potential sources of relevant evidence and/or information (devices) as well as key custodians and location of data are identified.

- determine the scope of the incident
- assess the case,
- nature of case : internal, criminal

Stage 2: Collection

Collecting digital information that may be relevant to the investigation.

Collection may involve removing the electronic device(s) from the crime or incident scene and then taking photos, imaging, copying or printing out its (their) content.

Important Note: As collection begins, those persons doing the collecting should keep the **Chain of Custody** in mind.

Step 2: Collection: Chain of Custody (CoC)

The CoC is a printed or electronic document in which the acquisition, custody and transfers of any piece of evidence are recorded. It must include all basic information regarding:

1. **Acquisition:** Who, when, where and how. Who acquired the evidence, when and where the evidence was acquired, and what method was used.
2. **Custody:** Who, where, how and how long. Who had possession of the evidence, where it was kept, what method was used to store it, and how long it was kept.
3. **Processing:** What was done to the evidence (cloning, analysis, etc.)
4. **Transfer:** Transfer of the evidence from one possessor to another, recorded along with the signature of the new keeper.
5. **Final Fate:** Destruction, secure deletion of evidence, return of evidence to owner, etc.

Collecting Evidence: What is the most important thing?

- Document, document, document
- Lawfully capture evidence
- Make cryptographically verifiable copies
- Setup secure storage of collected evidence
- Establish chain of custody
- Analyze copies only
- Use legally obtained, reputable tools
- Document every step

Stage 3: Preservation

The process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.

It’s an important step because information may be lost upon lack of care on volatile electronic devices.

Stage 4: Examination

The purpose of the examination process is to extract and analyze digital evidence.

Extraction refers to the recovery of data from its media.

Stage 5: Analysis

An in-depth systematic search of evidence relating to the incident being investigated.

The outputs of examination are data objects found in the collected information; this may include system- and user-generated files.

.

Stage 6: Presentation

Begins with reports based on proven techniques and methodologies.

Also includes the aspect that other competent forensic examiners should be able to duplicate and reproduce the same results.

Event Log Analysis and Sources

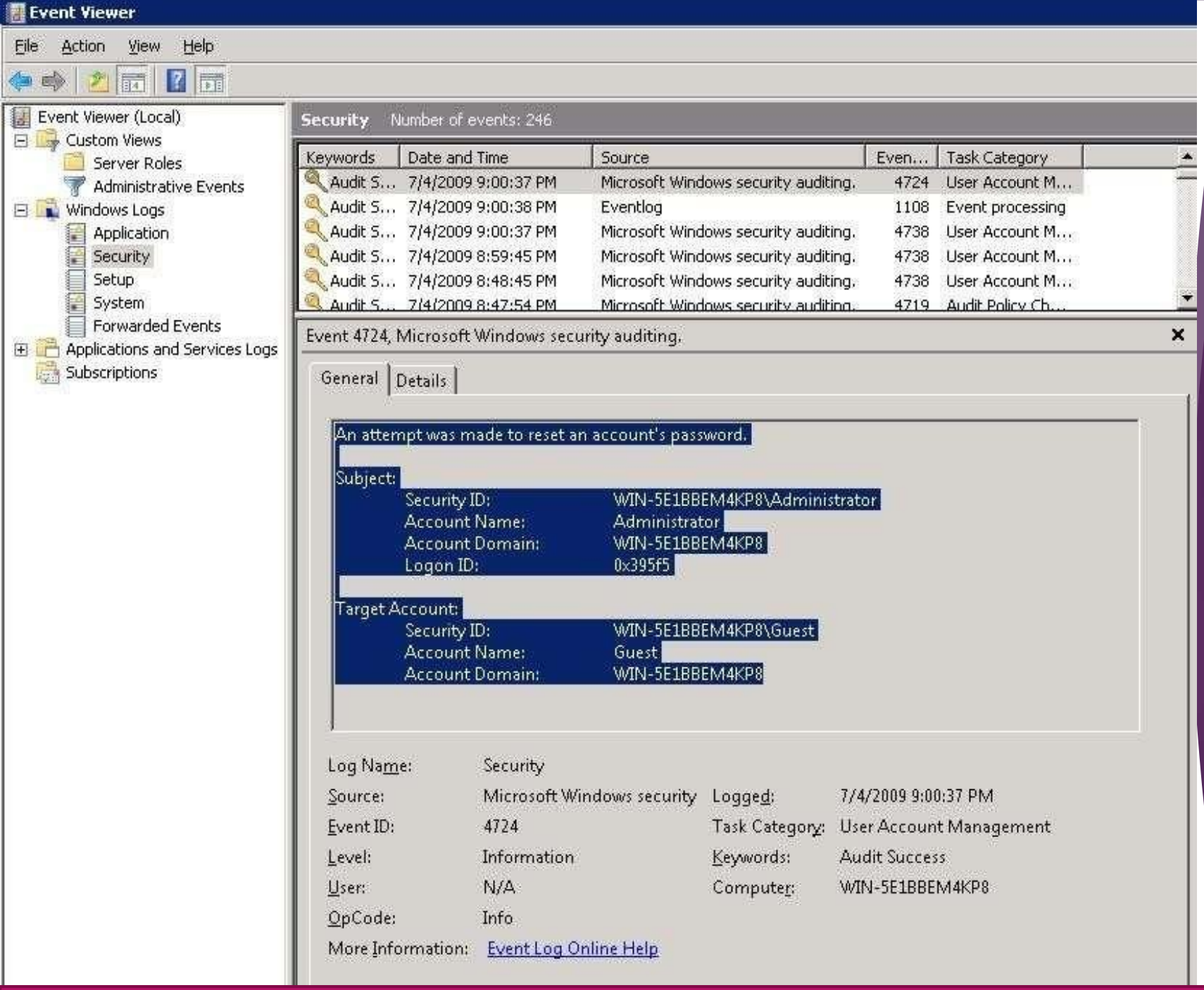
Event Log Analysis

What? On any OS platform (Windows/Linux/MacOS) event logs contains a lot of useful information about the system and its users.

How? Through log manager and analyzer tools all the event data can be captured automatically.

Why? Event logs can provide investigators with details about applications, login timestamps for users and system events of interest.

Event Viewer in Windows



prodiscover®
COMPUTER FORENSICS

WinFE

MAGNET
FORENSICS®

MALTEGO

splunk> Products Solutions Why Splunk? Resources

Benefits Features Integrations Resources Get Started

AUTOPSY
DIGITAL FORENSICS

EnCase®

What is windows event viewer? and how it can be used in cyber forensics?