LECTURE 10

DIGITAL FORENSIC INVESTIGATION METHODOLOGY

1. What are the three types of Analysis and Explain?

Media Analysis

* Examining physical media for evidence. Require understanding of file types and file signature

Network Analysis

* Examine network traffic and logs to identify and locate relevant activity

Malware Analysis

* Review of software for malicious signature

1. What are the four phases of DFIM?

* Acquisition and Preservation
* Discovery and Extraction
* Analysis and Validation
* Reconstruction and Presentation

Digital materials are collected and stored

Search for the data needed and extract it

The extracted data is examined for accuracy and reliability

Display the data found

1. What is Chain of custody?

* Every individual that is involved in the collection and transportation of evidence must be recorded.
* Label copies with data, time, metadata.

1. What are Features of software tools that help the forensic analyst maintain the chain of evidence when working with storage devices?

* **Static Acquisition: making a copy of the original drive**
* **Live Acquisition: required for full-disk encryption, capturing contents of RAM**
* **Preservation: creating original hash values to verify data integrity**
* **Validation: ensuring the integrity of data by comparing hash values of copies**
* **Extraction: copying files to an organized evidence repository**