This week lecture is about **Data Acquisition**...

Forensic Data Acquisition

- Before we can analyse data, we have to **secure** it.
- Also to ensure the **integrity** of original evidence is not compromised.
- The goal of forensic **data acquisition** is to create a **forensic copy** of a piece of media that is suitable for use as evidence in a court of law.

Understanding **Storage Formats** for Digital Evidence

- **Data** in a forensics acquisition tool is stored as an **image file**
  - *Basically, the **image file** can be in one of* the three formats
    - **Raw format**
    - **Proprietary formats**
    - **Advanced Forensics Format (AFF) – Open source : *Newer***

Determining the **Best Acquisition Method**

- Acquisition can be mainly divided into **2** categories. **Static** or **Dynamic**.
  - Need to determine which is the best to use for each investigation. Case by case…

- There are **4 methods** of collecting data:-
  - Creating a **disk-to-image** file
  - Creating a **disk-to-disk**
  - Creating a **logical disk-to-disk**
  - Creating a **sparse data copy** of a file or folder – *Same as Logical acquisition but also collects **fragments of unallocated (deleted) data***

- **Determining the best method depends on the circumstances of the investigation!!**

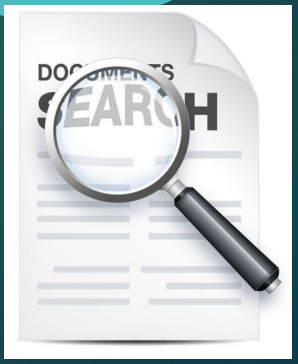
Using **Acquisition Tools**

Examples of Acquisition Tools :-

1) ProDiscover Basic
2) AccessData FTK Image Lite
3) OS Forensic
4) Encase
5) **Magnet Axiom**
6) Others…

Validating Data Acquired

- **Validating evidence** may be the most **critical** aspect of computer forensics. Why?
- Requires using a **hashing algorithm utility**
- Validation techniques. May DFI tools come with hashing functions. For example:-
  - **CRC-32, MD5, and SHA-1 to SHA-512**



https://eforensicsmag.com

Quiz – Revision…

1

1 of 1

1. What are the three storage formats for digital evidence?

- ○ Raw Format, Proprietary format, Windows format
- ○ Raw Format, Advanced Forensics Format, Windows format
- ○ Raw Format, Proprietary format, Advanced Forensics Format
- ○ Raw Format, Linux Format, Advanced Forensics Format

2

1 of 1

1. Are the methods of data collection listed here correct ? Creating a disk-to-image file, Creating a disk-to-disk, Creating a logical disk-to-disk, Creating a sparse data copy of a file or folder

- ○ True
- ○ False

Submit Answers

3

1 of 1

1. What are challenges investigators face when dealing with encrypted data?

- ○ Transmission speed is too fast, evidence cannot be captured
- ○ Unable to decrypt data due to lack of encryption key
- ○ Too many encrypted data formats used
- ○ Not able to validate an encrypted data

4

1 of 1

1. What is the possible drawback for investigator when doing remote access acquisition?

- ○ Not enough disk space to copy data
- ○ Acquisition tool interface is not user friendly
- ○ Too expensive in cost to do remote access acquisition
- ○ Antivirus, antispyware, and firewall tools can be configured to ignore remote access programs

Week 3 Lab

- Work on Lab 3 - submit lab exercise individually
  - **Practical 3A** – Learn how to **search documents** and metadata via the filters bar with keywords as well as understand build in help, artefact reference in AXIOM.
  - **Practical 3B** – Learn different **types of media** that can be parsed by Magnet AXIOM and what view are available in post-processing.
- Continue to work on your Assignment 1 when have time