Day 157

Topic: Digital Forensics

Objective: To recover deleted data and investigate digital evidence.

Theoretical Concepts:
We introduced the "Chain of Custody." We explained that "deleted" files are often just marked as free space but remain on the disk. We discussed disk imaging (bit-by-bit copy).

Practical Work:
We used **FTK Imager** to create a forensic image of a USB drive. We then used **Autopsy** (or PhotoRec) to analyze the image and recover "deleted" photos and documents. We analyzed file metadata to establish a timeline of events.

Tools Used: Autopsy, FTK Imager.

Outcome: Ability to recover lost data and perform basic forensic investigations.