Just to recap…

Objectives

- Determine **what data to analyze** in a digital forensics investigation
- Explain **tools used to validate data**
- Explain **common data-hiding techniques**

Determining What Data to Collect and Analyze

- Examining and analyzing digital evidence depend on the **nature of the investigation** And
  - The amount of data to process
  - Corporate investigators often locating and recovering a few specific items, such as emails, which simplifies and speeds processing

- **Scope creep** - when an investigation expands beyond the original description
  - Because of unexpected evidence found
  - Attorneys may ask investigators to examine other areas to recover more evidence
  - Increases the time and resources needed to extract, analyze, and present evidence
  - *Need to document additional time spend on recovering additional evidences!!*

Validating Forensic Data

- Ensuring the integrity of data collected is essential for presenting evidence in court

- Most forensic tools offer **hashing** of image files
  - Example - when ProDiscover loads an image file:
    - It runs a hash and compares the value with the original hash calculated when the image was first acquired

Addressing Data-Hiding Techniques

- **Data hiding** - changing or manipulating a file to conceal information
- Techniques:
  - Hiding entire partitions
    - *Use Disk Management*
  - Changing file extensions
  - Setting file attributes to hidden
    - *Change file signature*
  - Bit-shifting
    - *Shift 1 bit to left*
  - Using encryption
  - Setting up password protection

Week 6 - Digital Forensics Analysis and Validation

- A sample "Chain of Custody" form is uploaded in week 6 folder for reference.
- An article "An Overview of Steganography for the Computer Forensics Examiner" for more info on steganography

Assignment 1 Submission -- Reminder

- Presentation : 27th Nov 23 – 1st Dec 23
- Rerport : 8th Dec 2023, Friday, 2359
- Submit to BrightSpace. One submission per group. Please submit both presentation slides and report.
- Do note Similarity Rerpot Checker "**Turnitin**" will be applied to your written report