Lab 1: Digital Forensics Investigation of a USB Drive

Objective:

This lab aims to introduce you to the fundamentals of digital forensics through a practical investigation of a USB drive image. You will learn how to use Autopsy to recover files and analyse data, applying the steps of digital investigation to understand the significance of the recovered information.

Part 1: Understanding Digital Forensics

1**. What is Digital Forensics?**

- **Research and summarize the definition of digital forensics. Explain its importance in the context of investigations.**
- **Deliverable: Write a brief explanation (150-200 words) and include it in your lab report.**

Digital forensics is the scientific process of identifying, preserving, analysing, and presenting digital evidence in a way that is legally acceptable in court

it involves investigating digital devices (like computers, phones, network or servers) to uncover facts about cybercrimes, data breaches, or unauthorized activities.

Importance of Digital Forensics in context if investigations are:

Evidence Collection: Digital forensics begins with the collection of electronic evidence from various digital devices, such as computers, servers, mobile phones, server storage media, already etc. This phase requires meticulous documentation to maintain the integrity and chain of custody of the evidence.

Data Analysis: Investigators employ advanced tools and techniques to analyse the collected data. This includes examining file structures, recovering deleted files, and identifying patterns or anomalies that may be indicative of malicious activities.

Crime Reconstruction: Assists investigators in understanding how an incident occurred, who was responsible, and what actions were taken.

Preservation of Evidence: Ensuring the integrity and admissibility of evidence is paramount in digital forensics. Investigators use forensic procedures to preserve the original state of digital evidence, maintaining its authenticity and reliability for legal proceedings.

Reporting and Documentation: Investigators create detailed reports documenting their findings, methodologies, and the chain of custody. These reports are crucial for presenting evidence in legal proceedings and providing a clear understanding of the investigative process.

Prevention and Security Improvement: Helps strengthen systems by analysing vulnerabilities and preventing future attacks.

2. Steps of Digital Investigation:

- **Outline the essential steps involved in a digital investigation:**
  - **Identification**
  - **Preservation**
  - **Analysis**
  - **Presentation**
- **Deliverable: Create a flowchart or a list detailing each step and its significance. Include this in your lab report.**

Forensic investigators use advanced tools to unearth critical evidence, build timelines of illicit activities, and preserve evidence in a manner that is admissible in civil and criminal courts

To be able to do these digital forensic investigators conduct a structured and process-driven investigation to ensure the integrity of the data and its admissibility in a court of law. The core steps involved in digital forensics' investigation include:

- Identification
- Preservation
- Analysis
- Presentation

Step 1: Identification

The first step in a digital forensics investigation involves identifying all devices and resources that might hold relevant data.

This includes organizational devices such as desktops, laptops, servers, and network systems, as well as personal devices including smartphones, tablets, and external storage media. Each identified device is then carefully seized and isolated to prevent any possibility of data tampering.

In cases where data resides on servers or in cloud storage, strict access controls are implemented to ensure that only the authorized investigative team can access the data, thereby maintaining its integrity and security.

Step 2: Preservation

Once the devices involved in the investigation have been secured, the digital forensics investigator uses specialized forensic techniques to extract all potentially relevant data. This

process involves creating a "forensic image," which is an exact bit-by-bit digital copy of the original data.

The forensic image is then used for in-depth analysis, ensuring the original data remains untouched and stored securely in a safe location. This meticulous approach safeguards the integrity of the evidence, even if the investigation encounters unforeseen issues, preventing any tampering or data loss.

Step 3: Analysis

After securing and duplicating the data, digital forensic investigators employ a variety of advanced techniques to meticulously analyse the extracted data for evidence of wrongdoing. This process includes:

- Reverse Steganography: Extracting hidden data by examining the underlying hash or character string of an image or other data items.
- File or Data Carving: Identifying and recovering deleted files by locating and reconstructing file fragments.
- Keyword Searches: Using specific keywords to locate and analyze relevant information, including deleted data.

Investigators also use other sophisticated methods to uncover, piece together, and interpret evidence, ensuring a thorough examination of all potential digital clues. This comprehensive analysis helps build a clear and detailed understanding of the activities in question.

Step 4: Presentation

Upon completing the investigation, the findings are compiled and presented to the appropriate court, board, or group responsible for deciding the outcome of an allegation. Digital forensic investigators frequently function as expert witnesses, summarizing the evidence they have uncovered and explaining their analysis and conclusions.

They prepare comprehensive reports and visual aids to illustrate the findings clearly and effectively, ensuring that all relevant evidence is communicated in an understandable and persuasive manner, thereby supporting the judicial or administrative decision-making process.

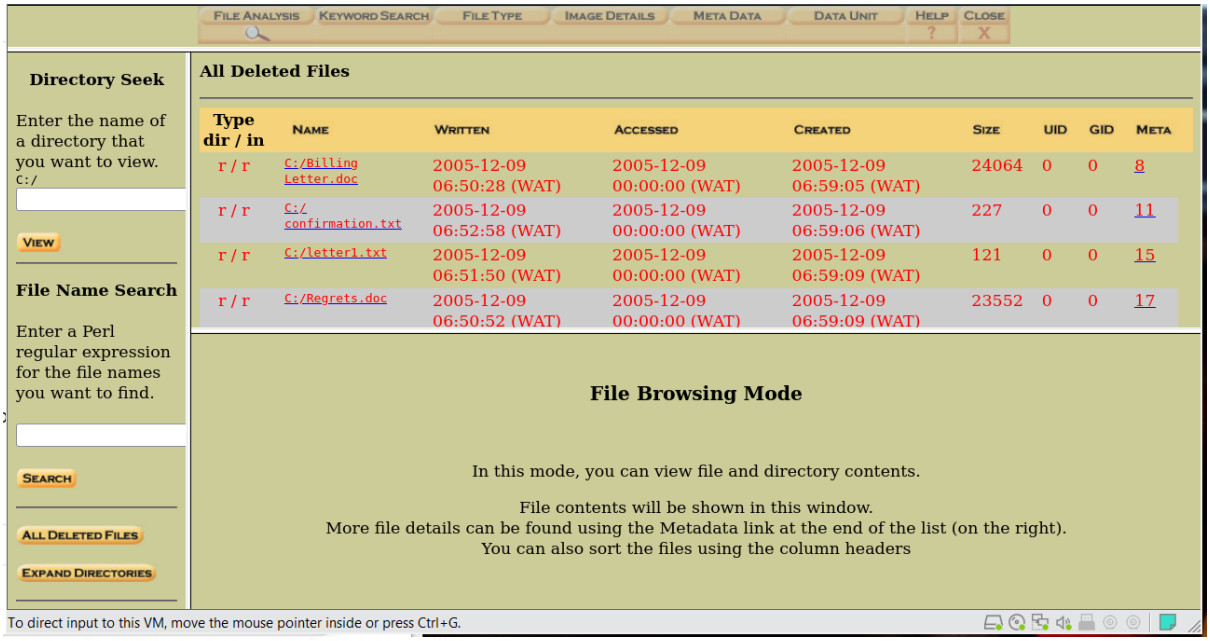
Part 2: Investigating the USB Drive with Autopsy

1. Setup Autopsy:

- Step 1: Download the USB drive image file from this link.
- Step 2: Install Autopsy if it is not already installed. Follow the instructions specific to your operating system.
- Step 3: Load the USB drive image into Autopsy.

2. File Recovery:

- Task: Use Autopsy to recover deleted Word files and images from the USB drive.
- Deliverable: Document the names and types of the recovered files in your lab report.



Listed below are what i recovered from the USB image:

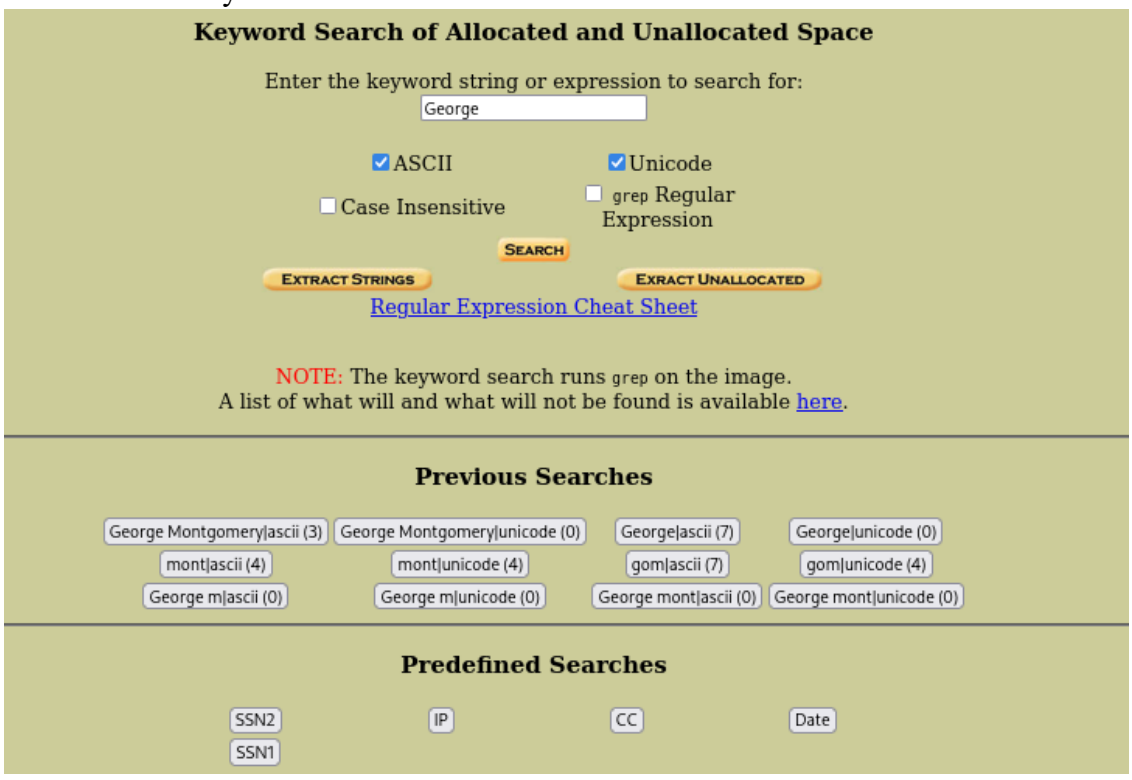
- two Microsoft Word documents
- two text files
- No image files were found.

Recovered Files Summary

File Name	File Type	Status	Written Time	Created Time	Size (bytes)	File Name
Billing Letter.doc	Microsoft Word Document	Deleted	2005-12-09 06:50:28 (WAT)	2005-12-09 06:59:05 (WAT)	24,064	Billing Letter.doc
Regrets.doc	Microsoft Word Document	Deleted	2005-12-09 06:50:52 (WAT)	2005-12-09 06:59:09 (WAT)	23,552	Regrets.doc
confirmation.txt	Text File	Deleted	2005-12-09 06:52:58 (WAT)	2005-12-09 06:59:06 (WAT)	227	confirmation.txt
letter1.txt	Text File	Deleted	2005-12-09 06:51:50 (WAT)	2005-12-09 06:59:09 (WAT)	121	letter1.txt

Part 3: Conducting Keyword Searches

1. Keyword Search: Task: Conduct a keyword search related to George Montgomery. Document the keywords used.



- Deliverable: Summarize your findings in your lab report, highlighting any significant documents or images recovered.

Keyword Used: George

Searching for ASCII: Done
Saving: Done
7 hits- link to results

Searching for Unicode: Done
Saving: Done
0 hits

New Search

7 occurrences of George were found
Search Options:
ASCII
Case Sensitive

Sector 184 (Hex - Ascii)
1: 236 (homasGeorge567 P)

Sector 240 (Hex - Ascii)
2: 460 (George Mont)

Sector 241 (Hex - Ascii)
3: 292 (George Mont)

Sector 284 (Hex - Ascii)
4: 221 (George)

Sector 289 (Hex - Ascii)
5: 141 (omas George)

Sector 312 (Hex - Ascii)
6: 115 (George)

Sector 316 (Hex - Ascii)
7: 390 (George Mont)

George was not found
Search Options:
Unicode
Case Sensitive

Part 3: Keyword Search Findings

Procedure:
A keyword search was performed in Autopsy using the ASCII search option for the keyword **"George"**. The Unicode search was also executed but returned no results.

Results:
The ASCII search found **7 occurrences** of the keyword "George" in different disk sectors..

Sector	Context (Extract)	Likely Source File
184	homasGeorge567 P	Possibly within a text fragment from a document or user reference
240	George Mont	Likely part of "George Montgomery" found in Billing Letter.doc
241	George Mont	Continuation of the previous hit, likely same document
284	George	Text fragment from deleted document
289	omas George	Possibly reference to "Thomas George" in same dataset
312	George	Document text reference
316	George Mont	Likely part of Regrets.doc referencing "George Montgomery"

Part 4: Analysis and Documentation

Analysis of Recovered Data (200–300 words)

The forensic analysis of the USB drive image using **Autopsy** led to the recovery of several deleted files that provide strong evidential value. The recovered items include:

- **Billing Letter.doc**: a deleted Microsoft Word document likely containing formal or financial correspondence.
- **Regrets.doc**: another deleted Word document possibly related to communication or personal matters.
- **confirmation.txt**: a deleted text file, likely used to record confirmations or short messages.
- **letter1.txt**: a simple text file that may contain informal notes or drafts.

A **keyword search** was conducted using the term **"George"**, associated with **George Montgomery**, the subject of the investigation. The results revealed:

- **7 occurrences** of "George" in the ASCII search.
- Partial matches such as *"George Mont"* and *"omas George"*, found across several disk sectors.
- No matches found in the Unicode search.

These results indicate that traces of data connected to George Montgomery remained within the deleted file space of the USB drive, showing remnants of previous activity.

Documentation of Findings

- case name INT313
- host name usb.
- USB Image Loaded: .dd file
- Keyword Search: showing "George".

Lab 2: Comparative Analysis of Autopsy and The Sleuth Kit (TSK)

Objective:

This lab aims to familiarize students with the differences between Autopsy and The Sleuth Kit (TSK), understand the architecture of TSK, and perform a practical examination of a USB drive image using TSK commands to recover deleted files.

Part 1: Overview of Autopsy and The Sleuth Kit

1. Autopsy vs. The Sleuth Kit:

- Provide a brief overview of the differences between Autopsy and TSK in terms of functionality and user interface.
- Deliverable: Write a comparison (150-200 words) to include in your lab report.

Autopsy and Sleuth Kit are integral components of digital forensics investigations, often used in tandem to analyse digital data effectively. They are particularly valuable in scenarios involving data recovery, system analysis following a security breach, or law enforcement investigations.

- Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It's primarily used for conducting end-to-end forensics investigations. While The Sleuth Kit (TSK) is a collection of command-line tools and a C library that allows you to analyze disk images and recover files from them. It forms the backbone of many forensic investigations and is used to conduct low-level analysis of filesystems.

- **Key Features of Autopsy:**
    - User-Friendly Interface: Autopsy provides a graphical user interface (GUI) that makes it easier for investigators to use, especially those who might be less comfortable with command-line tools.
    - Data Extraction and Analysis: It can analyze smartphones and hard drives, searching for various types of data, including keywords, internet history, geolocation, and more.
    - Timeline Analysis: Autopsy allows users to view system activities in a chronological order, which is crucial for understanding the sequence of events before and after a cyber incident.
    - Module-Based Architecture: Autopsy is extensible through modules, which means that users can add new functionalities according to their specific needs.
    - File System Analysis: It supports numerous file systems and can be used to recover deleted files and access hidden data.

- **Key Features of Sleuth Kit**
    - Broad Filesystem Support: TSK supports a wide range of file systems, including NTFS, FAT, ExFAT, HFS+, and ext2/3/4, which makes it applicable in various scenarios.
    - Recovery of Deleted Data: One of the strengths of TSK is its ability to recover deleted files and reveal unallocated space on a drive.
    - Detailed File Analysis: It can provide comprehensive details about files, such as timestamps, permissions, and modifications.
    - Command-Line Interface: TSK is operated via a command-line interface, offering powerful scripting capabilities for advanced users.

2. TSK Architecture:

- Research and summarize the layers of the TSK architecture.
- Deliverable: Create a diagram or list showing the layers of TSK and the tools provided at each layer.

Application Layer

(Autopsy, Custom Scripts, Forensic Tools)

File Layer

(icat, ifind, blkcat – Extract file data)

File System Layer

(fls, fsstat, istat – Analyze file systems)

Volume System Layer

(mmls, mmstat – Analyze partitions)

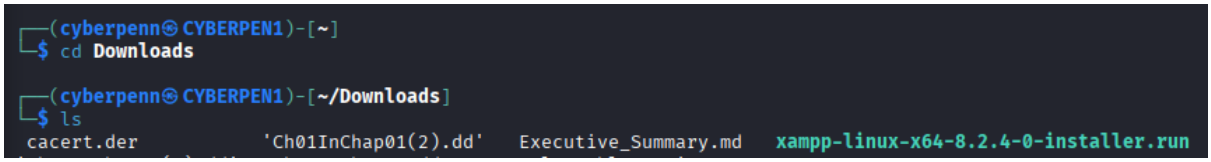
Physical Layer

(Reads raw disk sectors / devices)

Part 2: Examining a USB File Using TSK

1. Setup TSK:

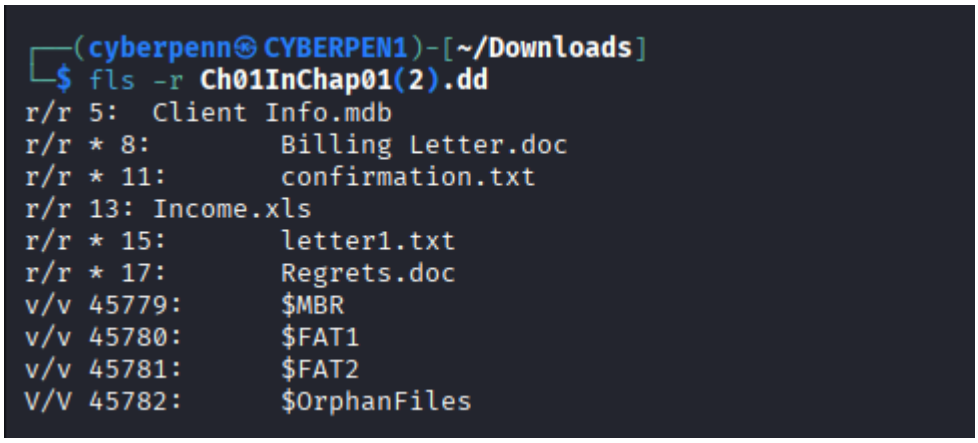
- Download the USB drive image from this link.



2. Using TSK Commands:

- Follow the PowerPoint presentations provided in class to practice all Linux commands related to The Sleuth Kit.
- Task: Determine how many deleted files are in the disk image.
  - Use the command:

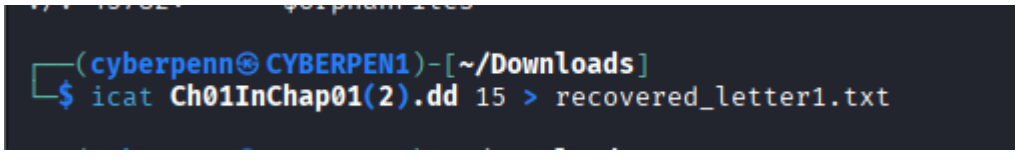
    fls -r Ch01InChap01(2).dd



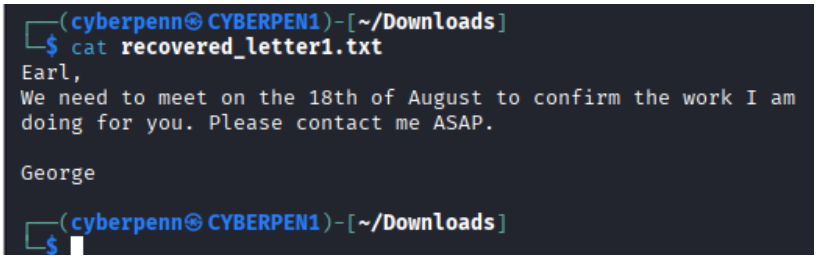
3. Recovering Deleted Files:

- Task: Recover the deleted file letter1.txt using TSK commands.
- Command Example:

    icat Ch01InChap01(2).dd 15 > recovered_letter1.txt



- Deliverable: Document the command used and any relevant outputs.



Part 3: Demonstrating Recovery Tools

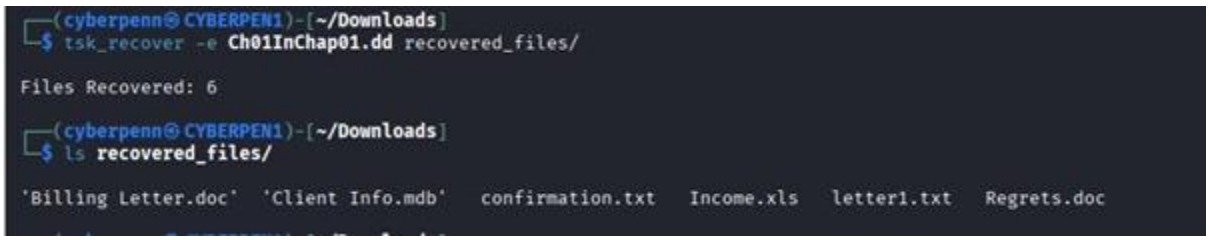
Student ID: 8475

8475 mod 4 =3

Selected Tools: TSK_RECOVERY

1. Recovering Deleted Files:

- Demonstrate the recovery of all deleted files using three different tools introduced in class using (tsk_recover).
- Deliverable: For each tool, provide:
  - The command used:
    - tsk_recover -e Ch01InChap01.dd recovered_files/
    - ls recovered_files/
  - The inputs required (e.g., URL or custom inputs):
    - Disk image: Ch01InChap01.dd
    - Flag: -e → recovers only deleted files
    - Output folder: recovered_files/
  - The expected outputs: Files Recovered: 6



An explanation of how each command works and how its parameters influence the output.

- The tsk_recover command extracts files from a disk image by reading the file system structures stored within the image.
- The -e parameter specifically filters the output to include only deleted files, ensuring that active files are ignored.
- The command scans the image (Ch01InChap01.dd), reconstructs the deleted file entries from the metadata, and saves them in the recovered_files/ directory
- ls: list the content of the recovered_files/

Lab 3: Disk Imaging Techniques: Acquisition Methods for USB Drives

Objective:

This lab aims to provide students with a comprehensive understanding of disk images and the techniques used to acquire USB drives in both Windows and Linux environments. By the end of this lab, students will have hands-on experience using FTK Imager and the dd command for forensic imaging.

Part 1: Understanding Disk Images

1. What is a Disk Image?

- Define a disk image and its importance in digital forensics.
- Deliverable: Write a brief explanation (100-150 words) discussing the purpose and benefits of creating disk images in forensic investigations.

Part 2: Acquisition of USB Drives

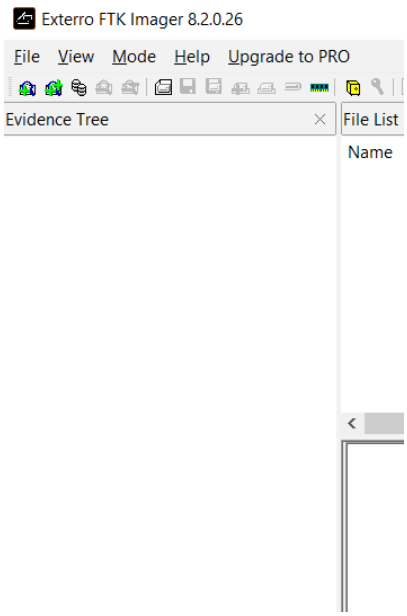
Task 1: Acquisition Using FTK Imager (Windows)

1. Setup FTK Imager:

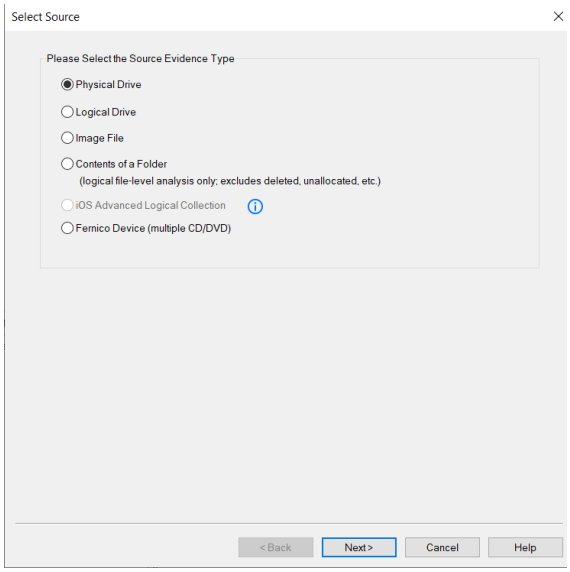
- Download and install FTK Imager from the official website.

2. Create a Disk Image:

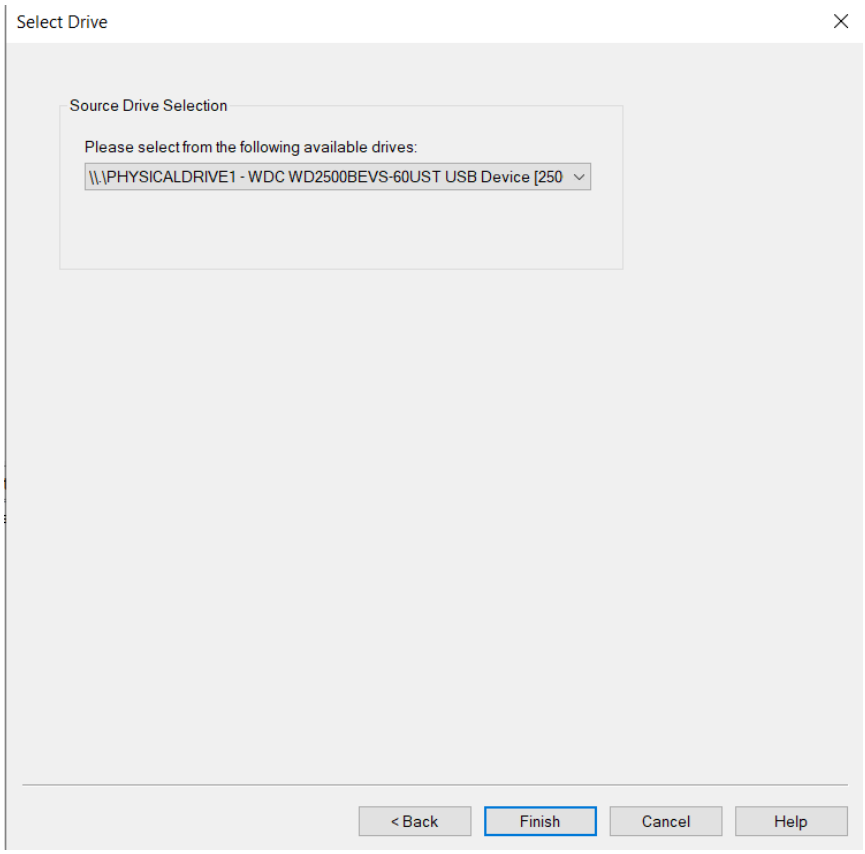
- Step 1: Connect your USB flash drive to the Windows machine.



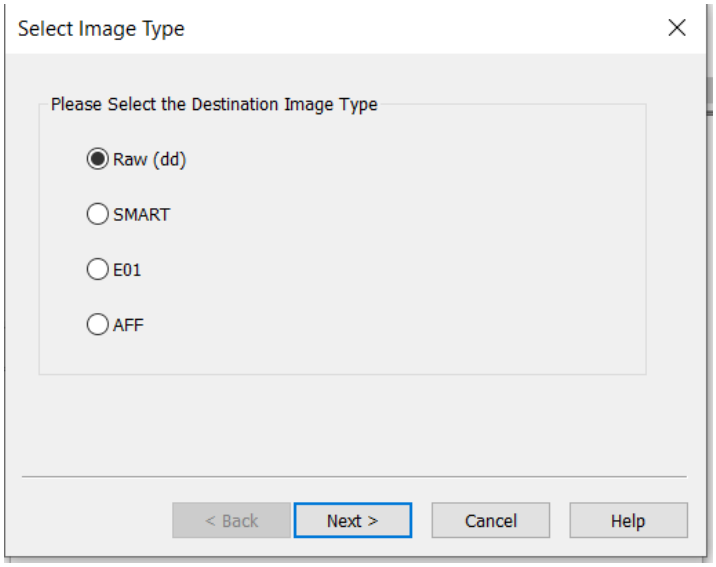
- Step 2: Open FTK Imager and select File > Create Disk Image.



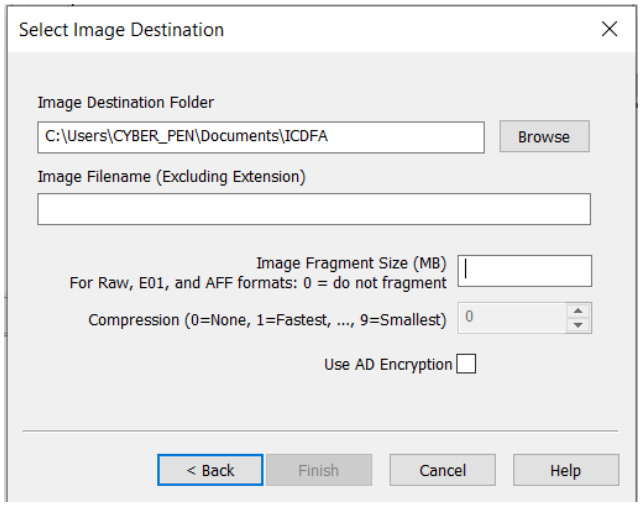
- Step 3: Choose the connected USB drive from the list of available drives.



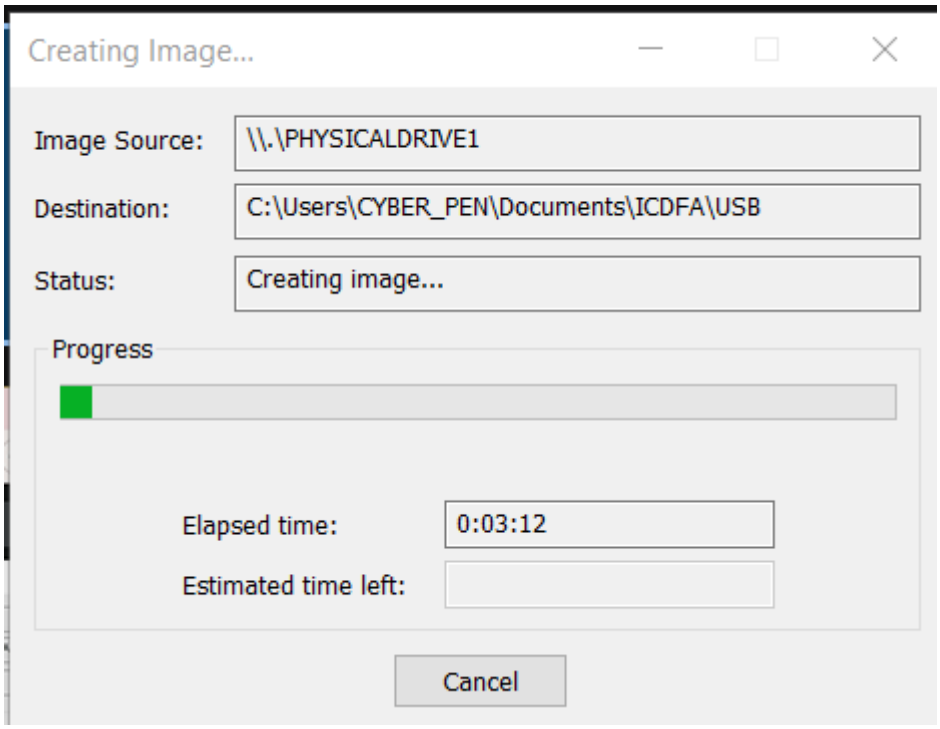
- Step 4: Select the output format (e.g., E01 or RAW) and specify a destination for the image file.

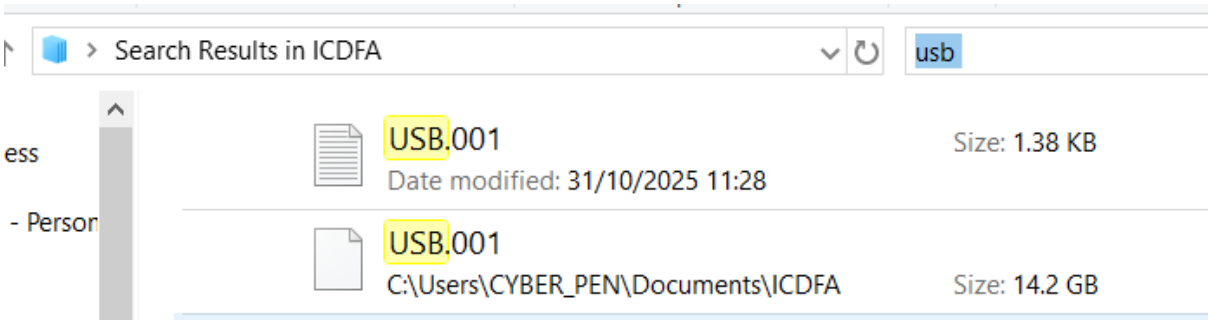


- Step 5: Click Finish to create the disk image.



3. Deliverable: Capture screenshots of each step in FTK Imager, including the final mage file location.





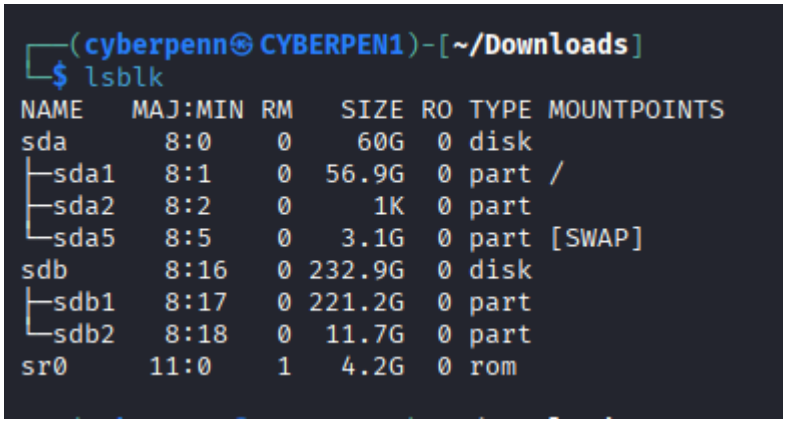
Task 2: Acquisition Using dd Command (Linux)

1. Setup Linux Environment:

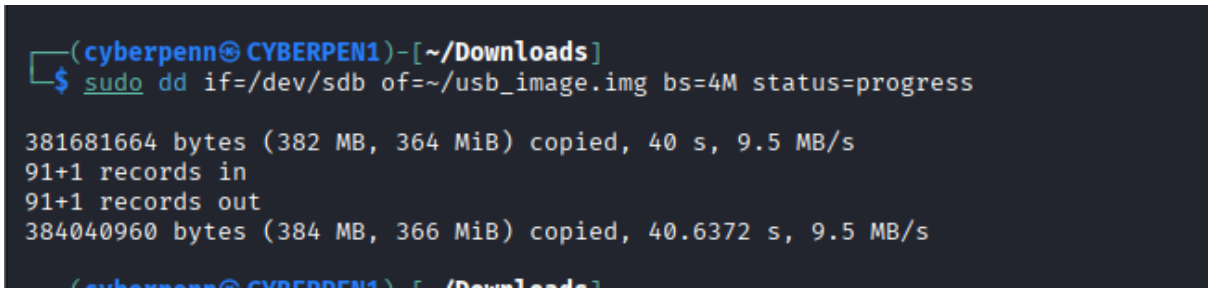
- Use a Linux distribution (e.g., Ubuntu) and connect your USB flash drive.

2. Create a Disk Image:

- Step 1: Identify the USB drive using the lsblk command.



- Step 2: Use the dd command to create a disk image. Replace /dev/sdX with the correct identifier for your USB drive.



sudo dd if=/dev/sdX of=~/usb_image.img bs=4M status=progress

- Step 3: Wait for the process to complete. This may take some time depending on the size of the USB drive.

3. Deliverable: Document the command used and capture a screenshot of the

terminal output showing the image creation progress.

Task 3: Acquisition via Network

1. Network Imaging:

- Discuss the concept of acquiring disk images over a network.
- Note: In this lab, students will not perform network acquisition, but will learn about tools like FTK Imager and dd used in conjunction with network protocols (e.g., FTP, SCP) for remote imaging.
- Deliverable: Write a short paragraph (100 words) on the advantages and challenges of acquiring disk images via network methods.

The concept of acquiring disk images over a network.

The fundamental idea is to perform disk imaging, a process that captures all data including visible files, boot sectors, operating systems, applications, unallocated space, and even deleted files, without requiring physical access to directly connect the source drive to the destination storage device. This allows for efficient, centralized management of backups, system deployments, and data collection for remote systems.

Advantages of acquiring disk images via network methods.

- Remote Acquisition: Evidence can be collected from devices in different locations without physical travel.
- Reduced Downtime: network acquisition can happen alongside normal operations (live analysis) or with limited interruption
- Speed: In environments with high-speed networks and powerful processing servers, network acquisition can be significantly faster than traditional methods.
- Centralized Management: Network methods allow for the centralized management and collection of evidence from multiple endpoints simultaneously

Challenges of acquiring disk images via network methods.

- Data Integrity and Admissibility: The original evidence can be unintentionally altered or tampered with during a live acquisition, which may render it inadmissible in court unless strict, verifiable procedures are followed.
- Network Performance and Volume: Modern networks generate vast amounts of data, and the sheer volume can be overwhelming to store and analyse.
- Encryption: Widespread use of encryption makes it difficult to analyse network traffic or data on the target drive
- Technical Complexity and Expertise: Network acquisition requires a high level of technical skill to implement and manage correctly

REFERENCE

1. Sveinsson, R. L. (2023). What are the 5 stages of a digital forensics investigation?
2. Forensic Focus. Retrieved from https://www.forensicfocus.com/
3. RandyLee.com. (2024). Forensics Tools: Autopsy and Sleuth Kit. Retrieved from https://www.randylee.com/