LAB MANUAL
DIGITAL FORENSICS

CY-334L

AIR UNIVERSITY

DEPARTMENT OF
CYBER
SECURITY

Air University Islamabad

Prepared by: Ms. Memoona Sadaf

Instructor: Memoona Sadaf

Lab/teaching Assistant:

Muhammad Ahmad Ali Qureshi

Semester: Spring 2025

Class: Fall 22 A, Fall 22 B

Lab Schedule

Week	Lab Topics
Week 1	Intro To Digital Forensics And Lab Environment Window File Structure / Linux Structure

Intro to Digital Forensics and Lab Environment

Definition and Importance of Digital Forensics:

Digital forensics is the branch of forensic science that involves the recovery and investigation of digital devices and data to aid legal proceedings. It encompasses the collection, preservation, analysis, and presentation of digital evidence. This field has become increasingly critical due to the growing reliance on digital devices and technologies in various aspects of life. Digital forensics helps in uncovering evidence related to cybercrime, data breaches, fraud, intellectual property theft, and more.

Real-world Applications and Examples:

Digital forensics finds applications in a wide range of scenarios, including:

Cybersecurity Incidents: Investigating cyberattacks, identifying intrusion points, and tracking down responsible individuals or groups.

Criminal Cases: Recovering evidence from digital devices such as computers, smartphones, and IoT devices to solve crimes.

Corporate Investigations: Uncovering insider threats, data leaks, and policy violations within organizations.

Civil Litigation: Extracting digital evidence for use in civil disputes, such as intellectual property theft or contractual disagreements.

Legal and Ethical Considerations:

Admissibility: Ensuring that digital evidence is collected and handled in a way that makes it admissible in court. Following proper protocols is crucial to prevent evidence from being deemed inadmissible due to mishandling.

Chain of Custody: Maintaining a documented trail that tracks the possession and handling of evidence. This ensures the integrity of the evidence and demonstrates that it hasn't been tampered with.

Privacy: Respecting the privacy rights of individuals while conducting digital investigations. Investigators must follow legal procedures and obtain appropriate permissions to access private data.

Ethics: Practicing ethical behaviour, including honesty, transparency, and professionalism. Balancing the pursuit of justice with respecting the rights of individuals is vital.

Digital Forensics Process

Digital forensics involves a systematic process that ensures the proper handling of digital evidence while maintaining its integrity and admissibility. The process typically consists of the following stages:

1. Identification:

Purpose: Identify potential sources of digital evidence relevant to the investigation.

Actions:

Determine the scope and goals of the investigation.

Identify the devices, systems, or networks that might contain relevant data.

Establish a clear understanding of what needs to be examined and why.

2. Preservation:

Purpose: Prevent any alterations or tampering with the original evidence.

Actions:

Create a bit-for-bit copy (forensic image) of the original evidence. This copy is used for analysis while preserving the original intact.

Use write-blocking techniques to ensure that the original evidence remains unaltered during the copying process.

Properly document and maintain the chain of custody for the evidence.

3. Collection:

Purpose: Gather the forensic images and other relevant data for examination.

Actions:

Collect data from various sources, including hard drives, external devices, cloud storage, and network traffic.

Document the sources, dates, times, and locations of collected evidence.

Maintain the integrity of the evidence during transportation.

4. Examination:

Purpose: Analyze the collected data to identify relevant information and potential leads.

Actions:

Use specialized forensic tools to extract and analyze data from the forensic image.

Identify files, documents, communications, metadata, and other relevant artifacts.

Look for patterns, anomalies, and evidence that align with the investigation's objectives.

5. Analysis:

Purpose: Interpret the findings from the examination stage and draw conclusions.

Actions:

Correlate and cross-reference evidence to reconstruct events and timelines.

Identify potential relationships between various pieces of evidence.

Apply forensic techniques to recover deleted files, hidden data, and encrypted information.

6. Presentation:

Purpose: Present the findings in a clear and organized manner that supports the investigation.

Actions:

Document the analysis process, methodologies, and tools used.

Create reports, summaries, and visual aids that present the evidence and its significance.

Prepare for legal proceedings by ensuring that the findings are well-documented and can be presented in court if necessary.

Setting up Lab Environment

1. Accounts on Cyber Defender and Tryhackme.

Purpose: Practice

Features: Best Recourses to Practice ☺

2. Kali Linux VM:

Purpose: Kali Linux is a powerful Linux distribution specifically designed for penetration testing and digital forensics. The virtual machine version allows students to explore various forensics tools in a controlled environment.

Features: Kali Linux comes with a wide range of pre-installed tools for digital forensics, network analysis, and more.

3. Autopsy:

Purpose: Autopsy is an open-source digital forensics platform that offers a user-friendly graphical interface for conducting investigations.

Features: Autopsy provides features for data analysis, keyword searching, timeline analysis, and reporting. It's suitable for both beginners and experienced forensic analysts.

4. FTK Imager:

Purpose: FTK Imager is a widely used tool for creating forensic images and working with various image formats.

Features: FTK Imager allows users to create images of storage devices, verify their integrity through hashing, and explore the contents of forensic images.

5. dd (Linux Command-line Tool):

Purpose: dd is a fundamental command-line tool used for low-level copying and converting data.

Features: dd can be used to create disk images, clone drives, and perform other data manipulation tasks. It's versatile and valuable for understanding the core concepts of data manipulation.

6. WinHex:

Purpose: WinHex is a hexadecimal editor and disk editor that can be used for data recovery, forensics, and analysis.

Features: WinHex allows users to view and edit binary data, recover deleted files, analyze disk structures, and perform data carving.

Window File Structure / Linux Structure

Introduction to File Systems and Directory Structures

File Systems:

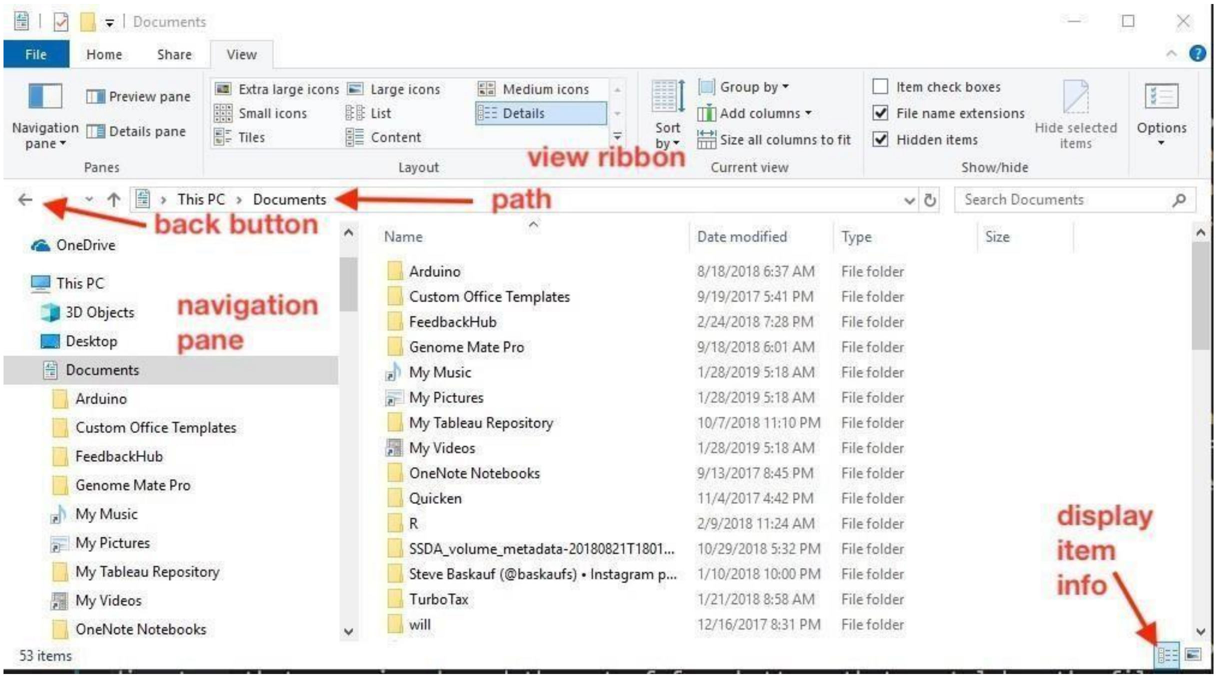
A file system is a method that an operating system uses to organize and store files on a storage device, such as a hard drive or a solid-state drive. It defines how data is stored, retrieved, and managed on the device. File systems manage not only the data itself but also metadata like file names, attributes, permissions, and directory structures.

Directory Structures:

A directory structure, also known as a file hierarchy or folder structure, is the way in which files are organized within an operating system. It involves creating directories (folders) and subdirectories to group and categorize files in a logical manner. The arrangement of directories and files forms a tree-like structure, with the top-level directory often referred to as the root directory.

Windows File Structure

In Windows operating systems, the file structure is organized hierarchically, starting with drive letters (e.g., C:, D:, etc.) that represent different storage devices. Each drive contains directories (folders) and files that are organized in a tree-like structure. The primary storage device is often associated with the C: drive, where the operating system and critical system files are located.

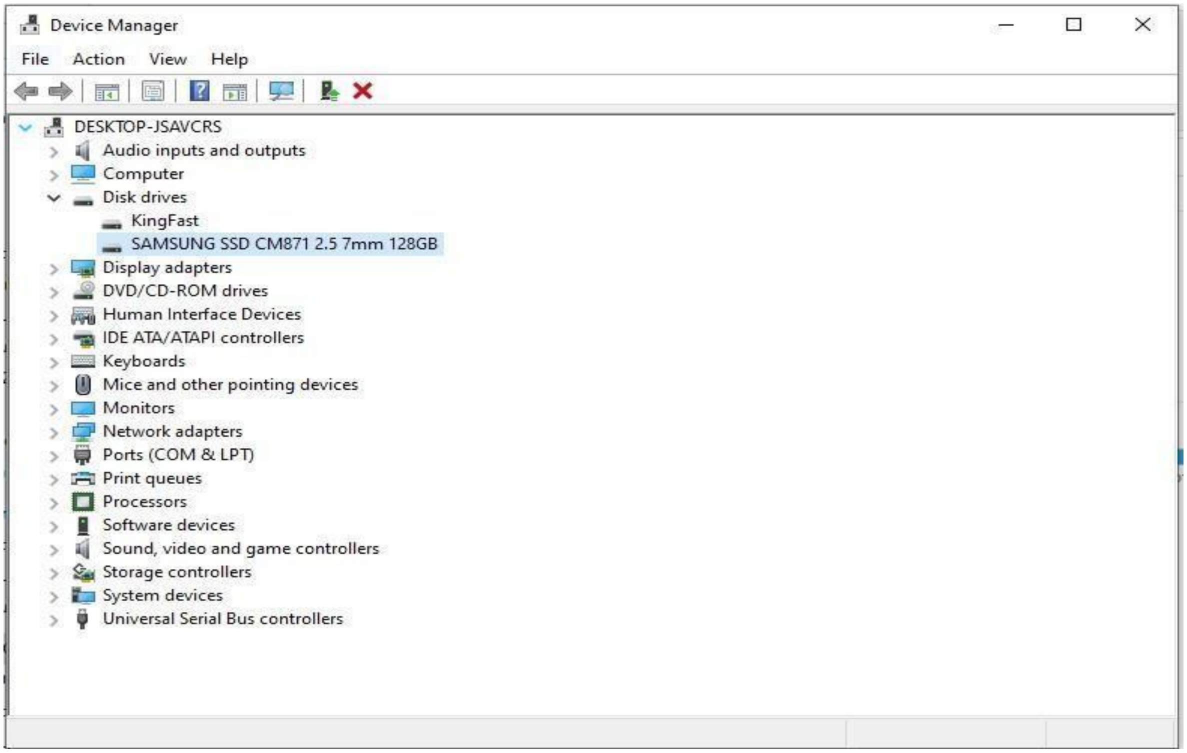


☐ Item check boxes
☑ File name extensions
☑ Hidden items

Name	Date modified	Type	Size
Arduino	8/18/2018 6:37 AM	File folder	
Custom Office Templates	9/19/2017 5:41 PM	File folder	
FeedbackHub	2/24/2018 7:28 PM	File folder	
Genome Mate Pro	9/18/2018 6:01 AM	File folder	
My Music	1/28/2019 5:18 AM	File folder	
My Pictures	1/28/2019 5:18 AM	File folder	
My Tableau Repository	10/7/2018 11:10 PM	File folder	
My Videos	1/28/2019 5:18 AM	File folder	
OneNote Notebooks	9/13/2017 8:45 PM	File folder	
Quicken	11/4/2017 4:42 PM	File folder	
R	2/9/2018 11:24 AM	File folder	
SSDA_volume_metadata-20180821T1801...	10/29/2018 5:32 PM	File folder	
Steve Baskauf (@baskaufs) • Instagram p...	1/10/2018 10:00 PM	File folder	
TurboTax	1/21/2018 8:58 AM	File folder	
will	12/16/2017 8:31 PM	File folder	

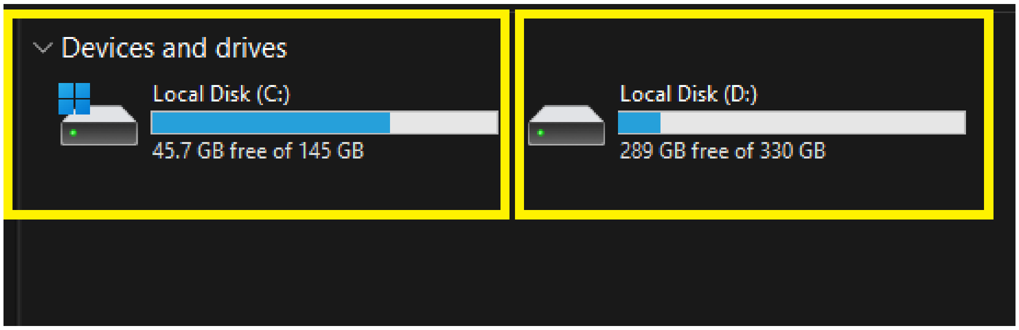
Check attached drives (Hardisk/SSD/NVME’s):

This PC →Left Click →Properties →Device Manager →Disk Drives



```
DESKTOP-JSAVCRS
    Audio inputs and outputs
    Computer
    Disk drives
        KingFast
        SAMSUNG SSD CM871 2.5 7mm 128GB
    Display adapters
    DVD/CD-ROM drives
    Human Interface Devices
    IDE ATA/ATAPI controllers
    Keyboards
    Mice and other pointing devices
    Monitors
    Network adapters
    Ports (COM & LPT)
    Print queues
    Processors
    Software devices
    Sound, video and game controllers
    Storage controllers
    System devices
    Universal Serial Bus controllers
```

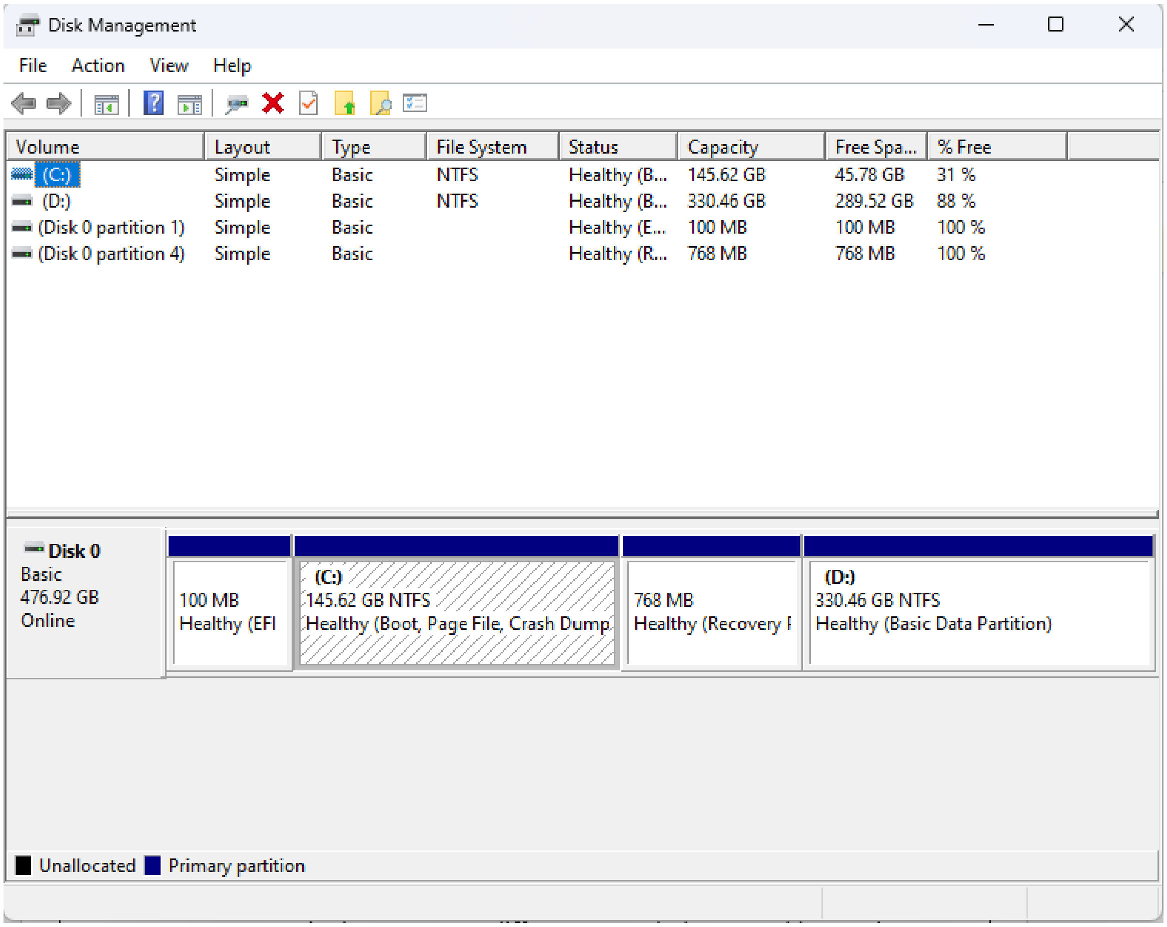
Check Partitions:



```
Devices and drives
Local Disk (C:)
45.7 GB free of 145 GB
Local Disk (D:)
289 GB free of 330 GB
```

Play with Partitions:

Search for Disk Management or Partitions →Disk Management



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	145.62 GB	45.78 GB	31 %
(D:)	Simple	Basic	NTFS	Healthy (B...	330.46 GB	289.52 GB	88 %
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	100 MB	100 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	768 MB	768 MB	100 %

Disk 0 Basic 476.92 GB Online	100 MB Healthy (EFI	(C:) 145.62 GB NTFS Healthy (Boot, Page File, Crash Dump	768 MB Healthy (Recovery I	(D:) 330.46 GB NTFS Healthy (Basic Data Partition)

■ Unallocated ■ Primary partition

Drive Letters, Paths, and Directory Hierarchy:

Drive Letters: Drive letters represent different storage devices or partitions on the computer. For example, C: is commonly used for the system drive, D: for additional partitions, and so on.

Paths: A path is a string that specifies the location of a file or directory in the file structure. It consists of the drive letter (or root), followed by the sequence of directories leading to the target file or directory. For instance, C:\Users\Username\Documents\file.txt.

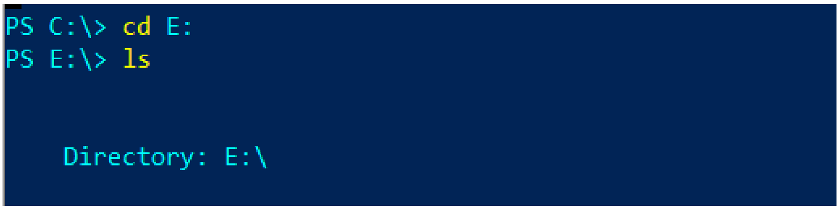
Directory Hierarchy: Directories contain files and other subdirectories. The top-level directory on a drive is often used for system and operating system files, while subsequent directories organize user files, applications, and settings.

Key Directories in Windows:

C:\Windows: This directory contains the operating system files, including system executables, libraries, and configuration files.

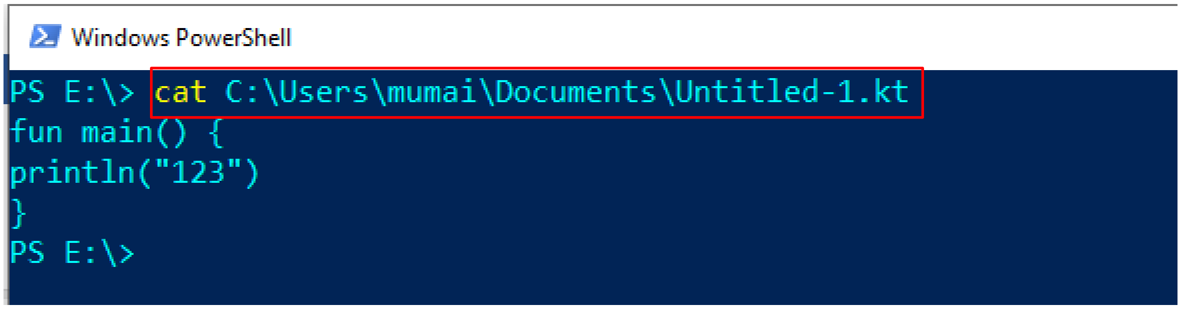
C:\Program Files: This directory hosts installed applications and software. Each application is typically contained within its own subdirectory.

C:\Users: This directory contains user-specific data, including user profiles, documents, downloads, and settings.



```
PS C:\> cd E:
PS E:\> ls


    Directory: E:\
```



```
PS E:\> cat C:\Users\mumai\Documents\Untitled-1.kt
fun main() {
println("123")
}
PS E:\>
```

From E: we are accessing the file in C: by giving complete of file.

Linux Directory Structure

In Linux, the file structure is organized as a single unified hierarchy, starting from the root directory ("/"). All files and directories are located within this hierarchy, regardless of the storage devices or partitions they reside on.

Root Directory and Subdirectories:

Root ("/"): The root directory is the highest level of the Linux file system. Everything in Linux is a descendant of the root directory. It's represented by a single forward slash ("/").

/bin: Contains essential binary executable files (commands) that are required for basic system functionality.

/etc: Hosts system-wide configuration files and settings that affect the behavior of various applications and services.

/home: This is where user home directories are located. Each user has their own subdirectory within /home.

/var: Holds variable data, such as log files, temporary files, and system databases.