

Lab-Manual

Digital Forensics

CY-334L



Prepared By: Ms.Memoona Sadaf

Instructor: Ms.Memoona Sadaf

Lab/Teaching Assistant: Muhammad Ahmad Ali Qureshi

Semester: Spring 2025

Class: Fall 22 A, Fall 22 B

Air University Islamabad

CY-334L Digital Forensics

AIR UNIVERSITY
Department of Cyber Security

Lab Schedule

Week	Lab Topics
Week 2	Crime Scenes and Data Acquisition

Crime Scenes and Data Acquisition

Introduction

Purpose and Scope of the Lab Manual

The "Crime Scenes and Data Acquisition Lab Manual" serves as a comprehensive guide for students, professionals, and anyone interested in the field of digital forensics. This manual aims to provide a structured and hands-on approach to understanding the critical role of digital evidence in criminal investigations, focusing on data acquisition techniques using Autopsy and FTK Imager.

Scope of the Lab Manual:

- Explore the fundamental concepts of digital forensics.
- Learn to use Autopsy and FTK Imager for data acquisition and analysis.
- Understand the legal and ethical considerations in digital forensics.
- Develop practical skills through hands-on exercises and case studies.
- Importance of Digital Evidence in Criminal Investigations

In today's digital age, digital evidence plays a pivotal role in criminal investigations. Digital devices such as computers, smartphones, and servers store vast amounts of information, often containing valuable clues and evidence related to crimes. The importance of digital evidence can be summarized as follows:

Ubiquity: Digital devices are ubiquitous in modern life, making them potential sources of evidence in various types of crimes.

Unalterable Records: Digital data is often difficult to alter or delete completely, making it a reliable source of information.

Digital Footprints: Criminals often leave digital footprints when engaging in illicit activities, providing investigators with valuable leads.

Corroboration: Digital evidence can corroborate or refute statements made by suspects or witnesses.

Timeliness: Rapid access to digital evidence can expedite investigations and potentially prevent further criminal activity.

FTK Imager

Overview of FTK Imager:

FTK Imager, developed by AccessData, is a powerful digital forensics tool designed for imaging and analyzing digital media. It provides a user-friendly interface and a range of features for data acquisition.

Functions and Use Cases:

- Creating forensic images of storage devices
- Viewing and analyzing disk contents
- Password recovery
- Logical and physical acquisitions

Installation and Configuration:

FTK Imager is available for download from the official website. Instructions for installation and basic configuration are provided in the user manual.

Understanding Crime Scenes

Types of Crime Scenes

Crime scenes can be classified into several types based on the nature of the evidence and the location of the incident. Understanding these types is crucial for forensic investigators to properly approach and process evidence:

Physical Crime Scenes: These are locations where physical evidence, such as weapons, bloodstains, or fingerprints, is present. Physical crime scenes can include murder scenes, burglary sites, or accident scenes.

Digital Crime Scenes: In the digital age, crime scenes also encompass digital environments where electronic evidence is relevant. This includes crime scenes involving cybercrimes, data breaches, or digital devices containing evidence.

Hybrid Crime Scenes: Some cases involve a combination of physical and digital evidence. For example, a homicide may involve both a physical crime scene and digital evidence on a suspect's computer or smartphone.

Preserving Evidence Integrity

Preserving evidence integrity is a fundamental principle in forensic investigations. It involves maintaining the authenticity, reliability, and admissibility of evidence throughout the entire investigative process. Key considerations include:

Chain of Custody: Properly documenting the possession and handling of evidence to ensure it is not tampered with or contaminated.

Evidence Packaging: Using appropriate containers and labels to prevent contamination or degradation of physical evidence.

Digital Evidence Handling: Safeguarding digital evidence from alteration, ensuring it remains unchanged during acquisition and analysis.

Documentation: Thoroughly documenting all actions taken with respect to evidence, including photographs, notes, and logs.

Legal Considerations: Adhering to legal standards and procedures for evidence handling to ensure its admissibility in court.

Preserving evidence integrity is essential for building a solid case and maintaining the credibility of the forensic investigator.

Data Acquisition Types

Bit-stream disk-to-image files

This is the most common data acquisition method in the event of a cybercrime. It involves cloning a disk drive, which allows for the complete preservation of all necessary evidence. Programs used to create bit-stream disk-to-image files include FTK, SMART, and ProDiscover, among others.

Bit-stream disk-to-disk files

When it is not possible to create an exact copy of a hard drive or network, different tools can be used to create a disk-to-disk copy. While certain parameters of the hard drive may be changed, the files will remain the same.

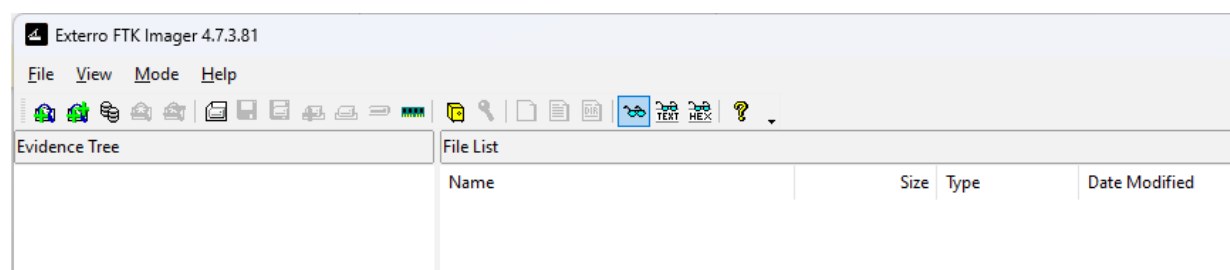
Logical acquisition

Logical acquisition involves collecting files that are specifically related to the case under investigation. This technique is typically used when an entire drive or network is too large to be copied.

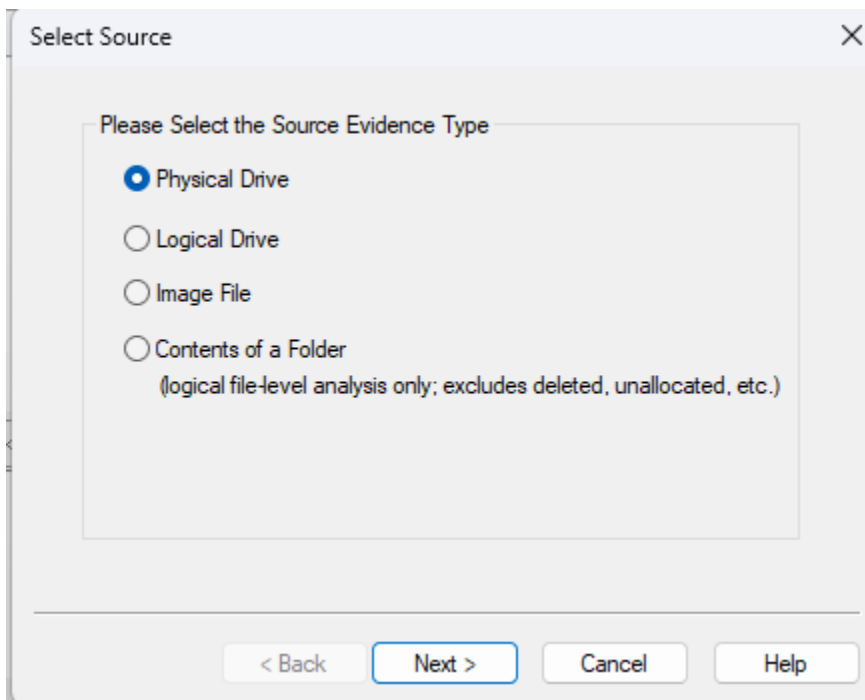
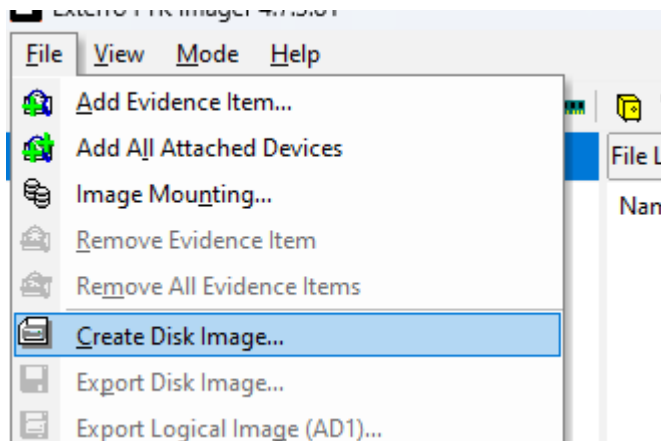
Acquiring non-volatile memory (Disk Image) using FTK Imager

As previously stated, this same tool can be used to collect a disk image as well.

Open FTK Imager and navigate to “Create Disk Image”.



Now select the create disk image that you need to acquire.

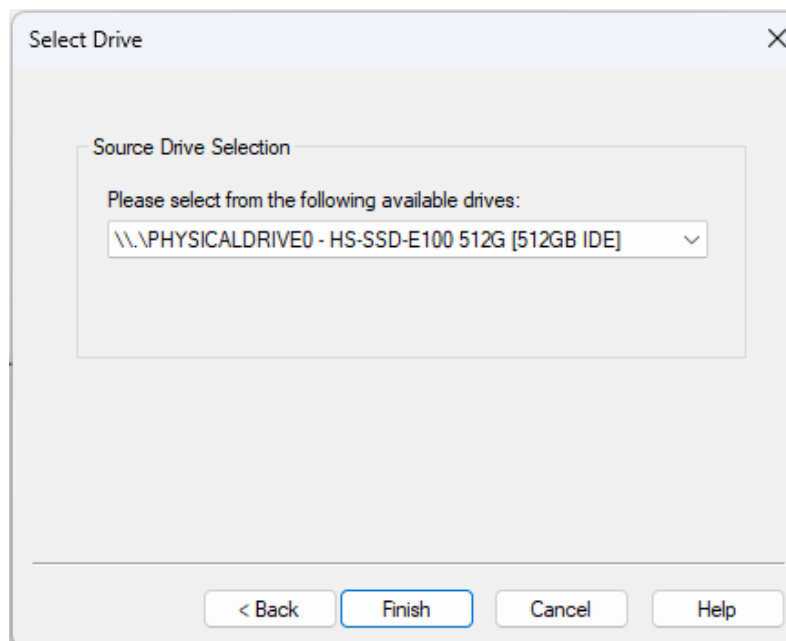


NOTE: FTK Imager is capable of acquiring physical drives (physical hard drives), logical drives (partitions), image files, contents of a folder, or CDs/DVDs. Investigators can connect external HDDs into the collection computer via write blocker and use the “logical drive” option to select the mounted HDD as a partition.

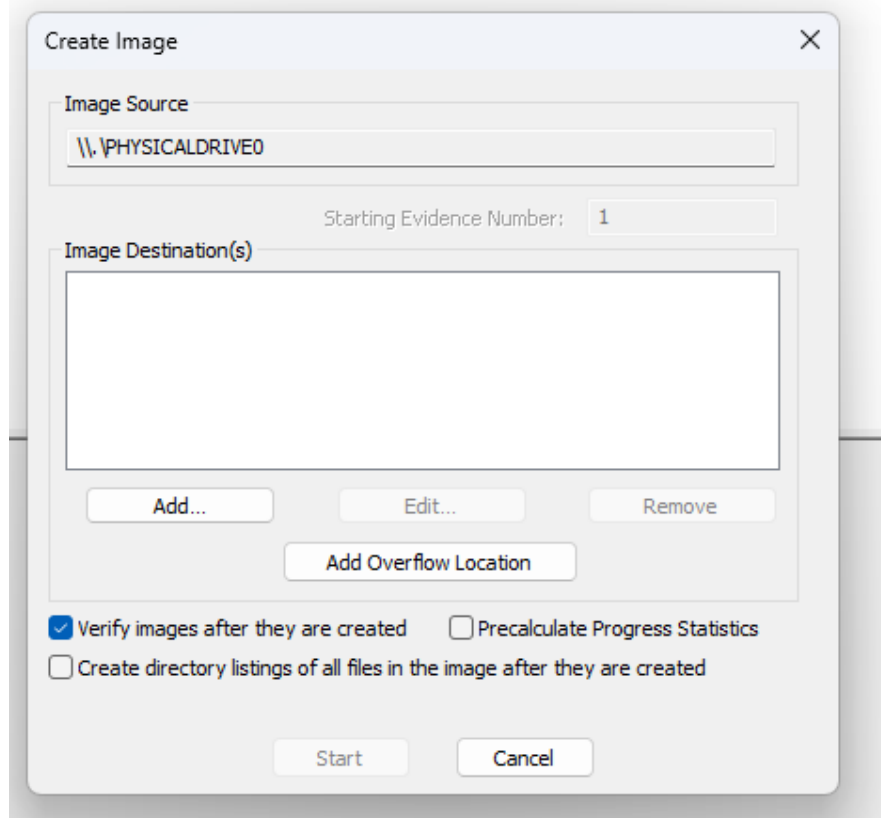
Collecting Physical Drives

Select the “Physical Drive” option.

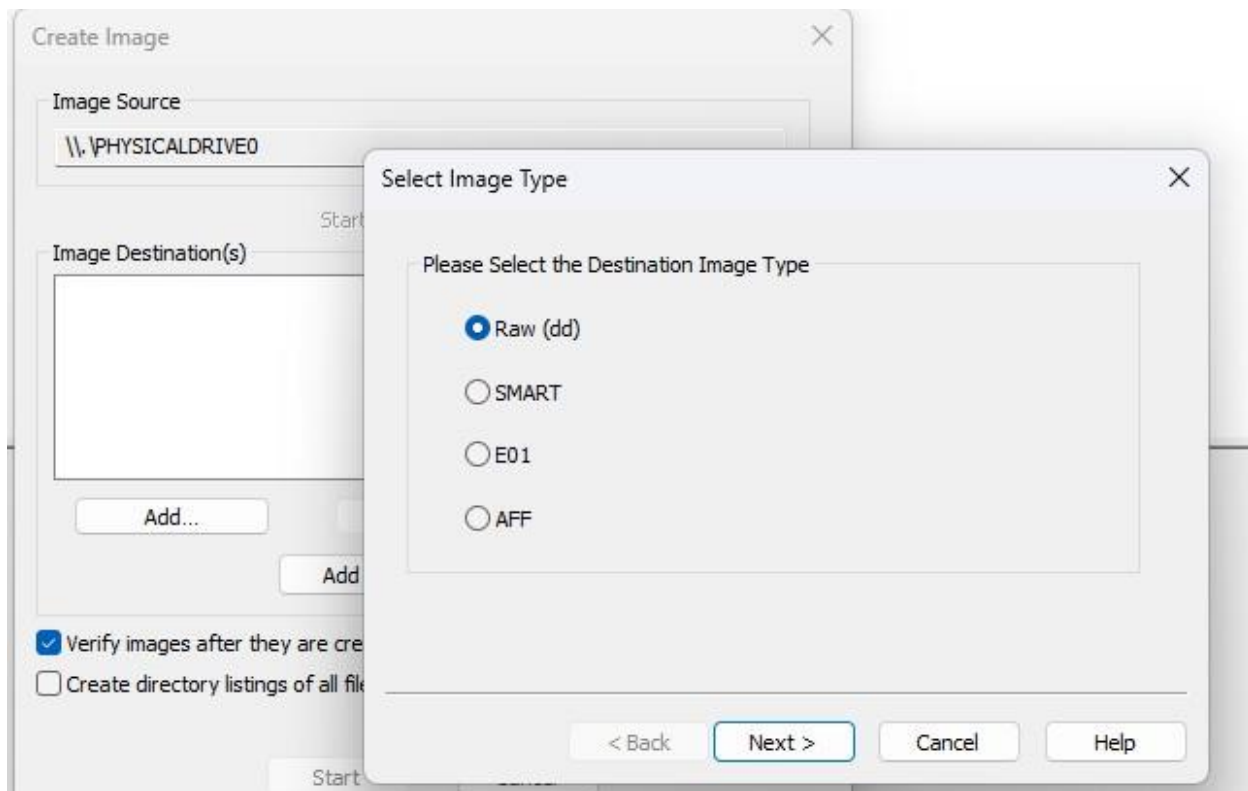
Select the drive you need to acquire and click “Finish”.



Now add a destination. (Click “Add...” to choose your destination.)



Now click on the add button to select the image format.



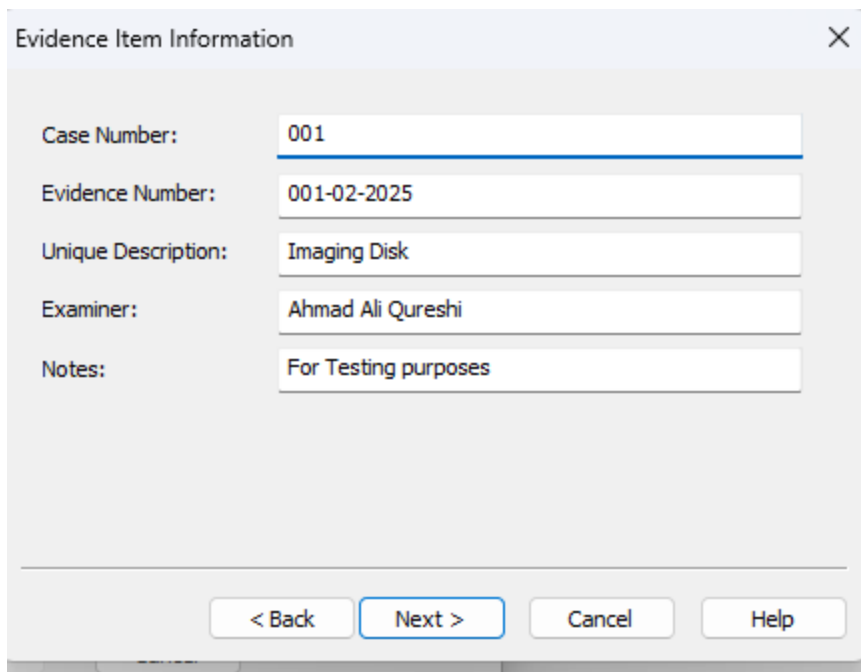
Raw (dd): This is the image format most commonly used by modern analysis tools. These raw file formatted images do not contain headers, metadata, or magic values. The raw format typically includes padding for any memory ranges that were intentionally skipped (i.e., device memory) or that could not be read by the acquisition tool, which helps maintain spatial integrity (relative offsets among data).

SMART: This file format is designed for Linux file systems. This format keeps the disk images as pure bitstreams with optional compression. The file consists of a standard 13-byte header followed by a series of sections. Each section includes its type string, a 64-bit offset to the next section, its 64-bit size, padding, and a CRC, in addition to actual data or comments, if applicable.

E01: this format is a proprietary format developed by Guidance Software's EnCase. This format compresses the image file. An image with this format starts with case information in the header and footer, which contains an MD5 hash of the entire bit stream. This case information contains the date and time of acquisition, examiner's name, special notes and an optional password.

AFF: Advance Forensic Format (AFF) was developed by Simson Garfinkel and Basis Technology. Its latest implementation is AFF4. The goal is to create a disk image format that does not lock the user into a proprietary format that may prevent them from being able to properly analyze it.

Now enter the case details.



Evidence Item Information

Case Number: 001

Evidence Number: 001-02-2025

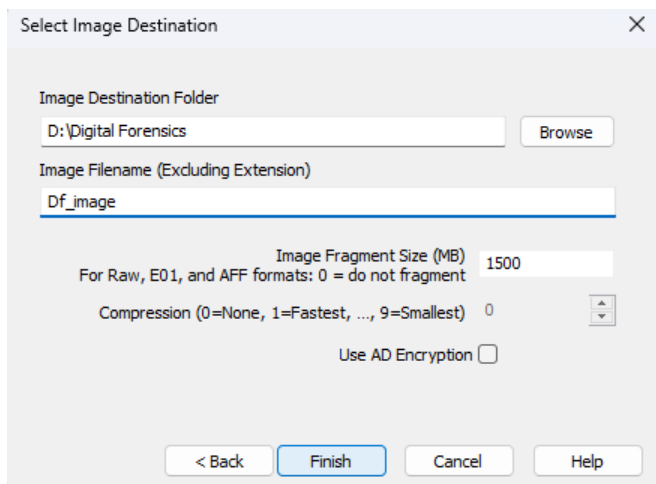
Unique Description: Imaging Disk

Examiner: Ahmad Ali Qureshi

Notes: For Testing purposes

< Back Next > Cancel Help

Add an image destination (where the image file will be saved), image file name and fragment size.



Select Image Destination

Image Destination Folder
D:\Digital Forensics Browse

Image Filename (Excluding Extension)
Df_image

Image Fragment Size (MB) 1500
For Raw, E01, and AFF formats: 0 = do not fragment

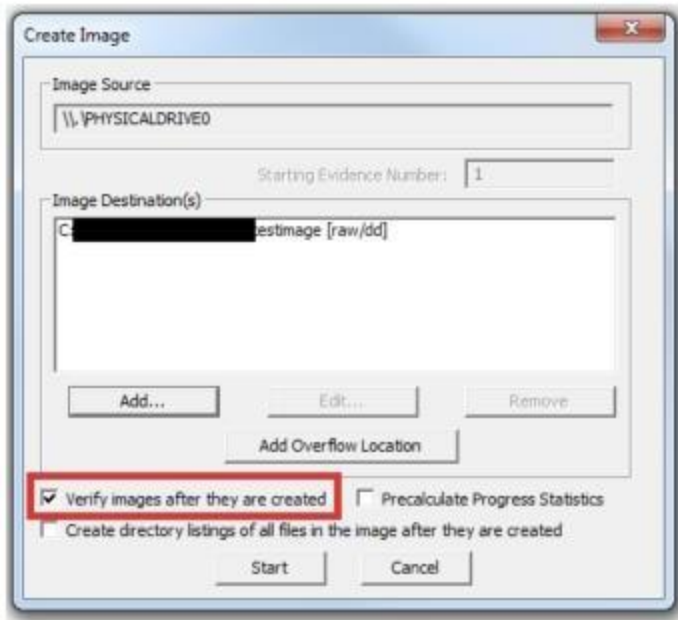
Compression (0=None, 1=Fastest, ..., 9=Smallest) 0

Use AD Encryption ☐

< Back Finish Cancel Help

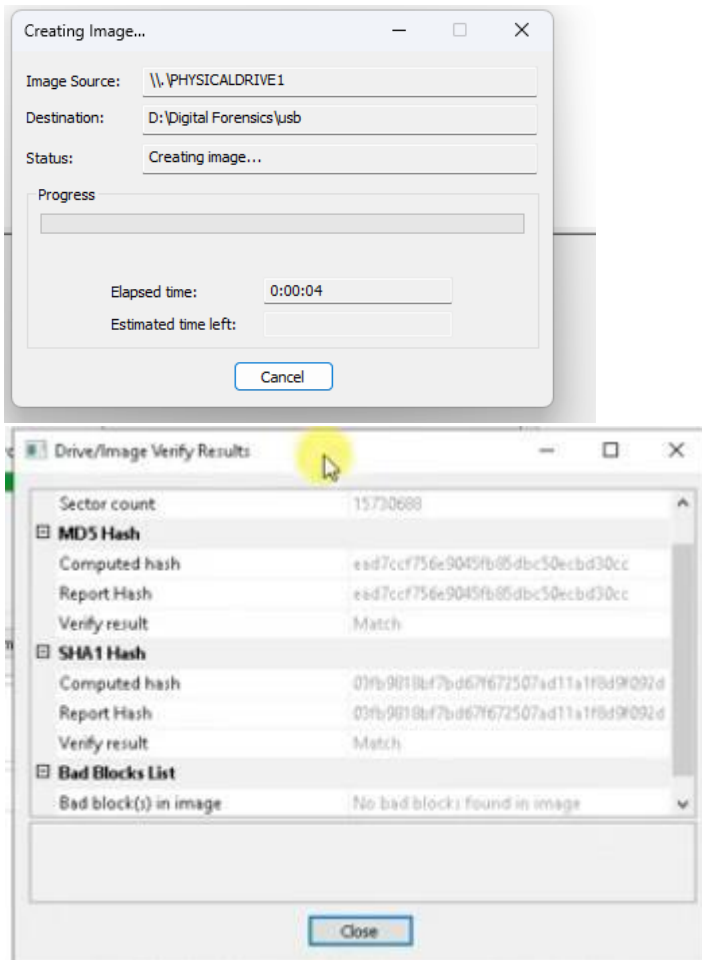
Image Fragment Size (MB): this option will separate the image file into multiple images and save them in the same destination. If you need only one file instead of creating multiple fragmented images, you must set the image fragment size to “0”.

Select the “verify images after they are created” option. This will verify the hash values once the image has created. In order to ensure integrity, it is recommended to use this option. However this will increase the time taken to acquire your evidence, especially if you’re dealing with a large disk image size.

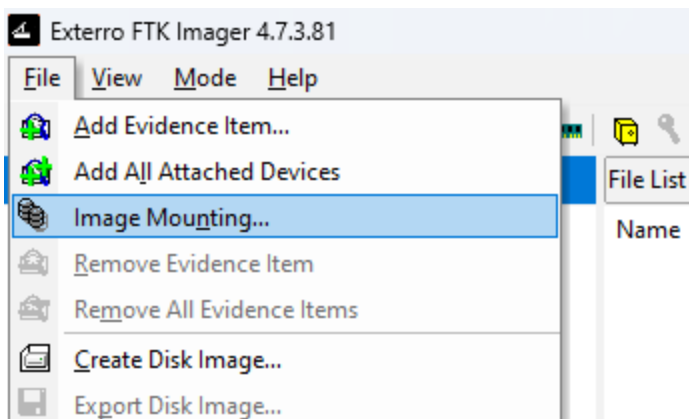


Click “start” to start acquiring.

Once acquiring is complete, it will create a text file including all the information it has acquired.



When to open this image or mount this created image click on the open image



Select the image created:

usb.002	2/6/2025 1:53 PM
usb.003	2/6/2025 1:54 PM
usb.004	2/6/2025 1:55 PM

Mount Image To Drive

Add Image

Image File:
D:\Digital Forensics\usb.002

Mount Type: Physical & Logical

Drive Letter: Next Available (F:)

Mount Method: Block Device / Read Only

Write Cache Folder:
D:\Digital Forensics

Mount

Mapped Image List

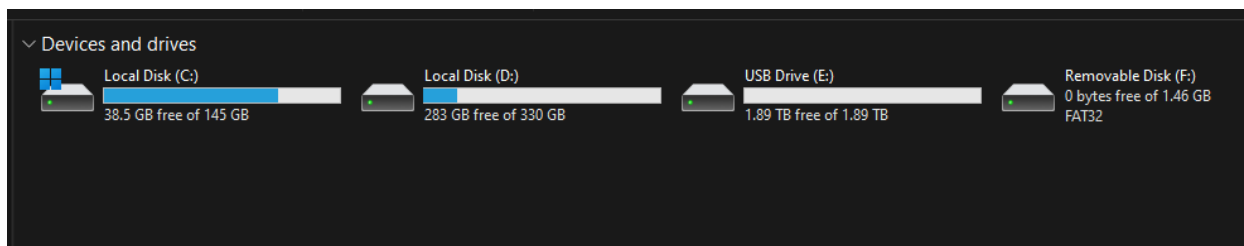
Mapped Images:

Drive	Method	Partition	Image

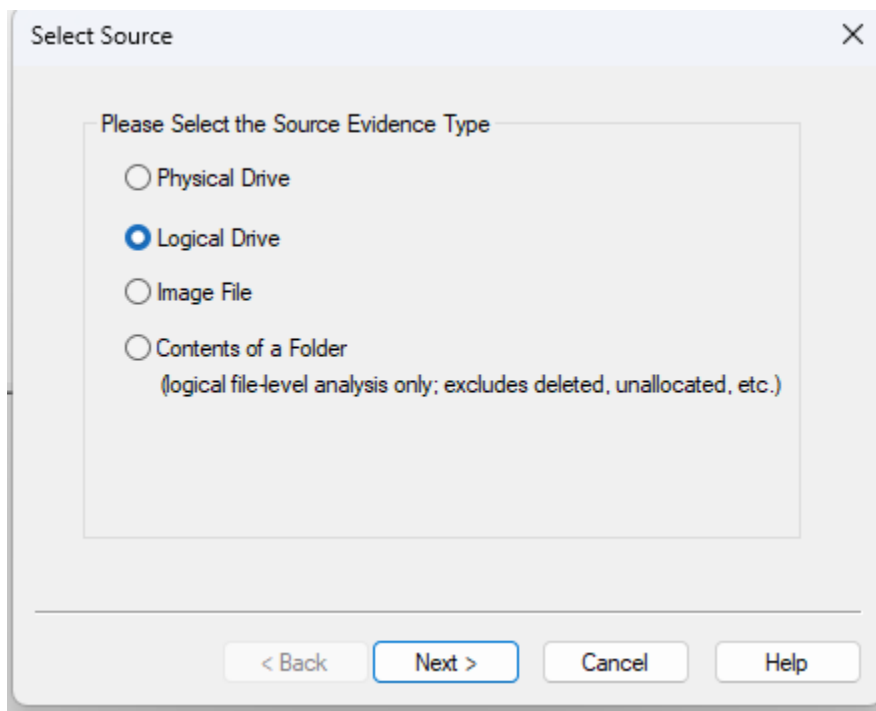
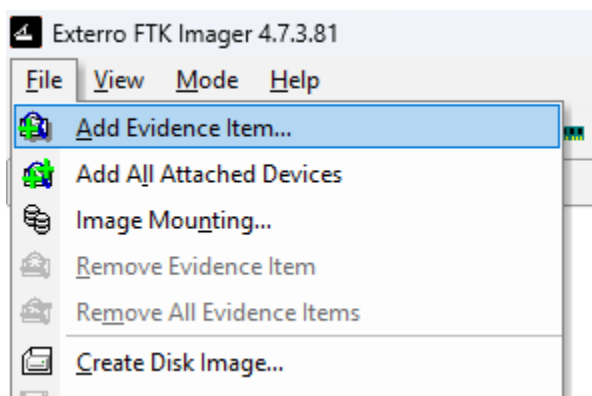
Unmount

Close

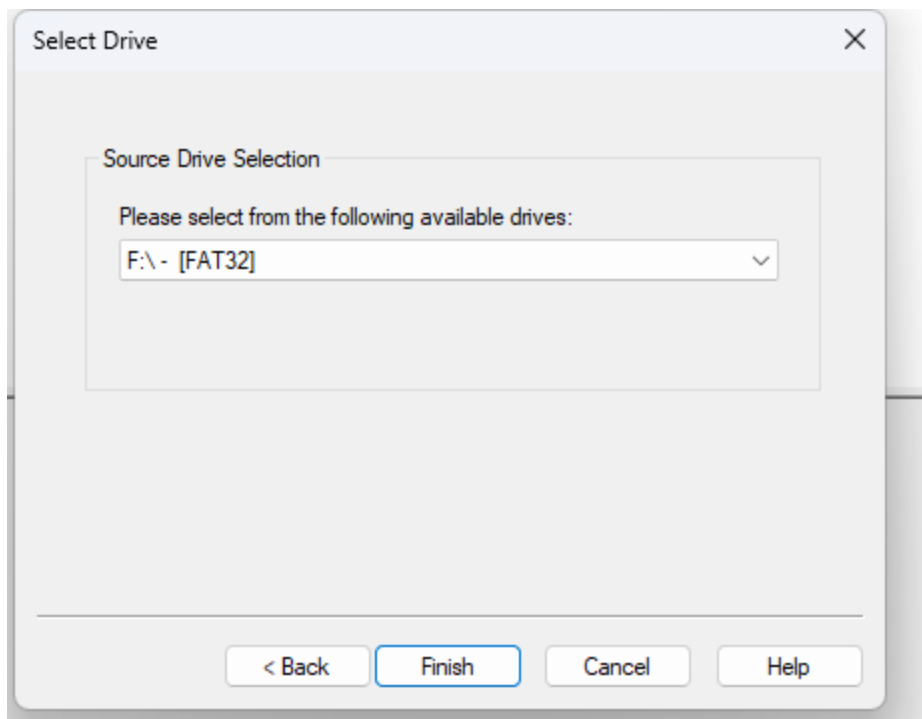
Click on the mount and the image will be mounted and also appeared as another physical disk in the computer



In order to see the contents of the image we will add the evidence as logical drive because we already mounted the drive



Select the drive that was mounted



Click on the finish and you will see the contents of the mounted drive

Extorero FTK Imager 4.7.3.81

File View Mode Help

Evidence Tree

- F:\
 - Unpartitioned Space [basic disk]
 - [unallocated space]

File List

Name	Size	Type	Date Modified
0000001	104,857,600 (10...	Unallocated Sp...	
0204801	104,857,600 (10...	Unallocated Sp...	
0409601	104,857,600 (10...	Unallocated Sp...	
0614401	104,857,600 (10...	Unallocated Sp...	
0819201	104,857,600 (10...	Unallocated Sp...	
1024001	104,857,600 (10...	Unallocated Sp...	
1228801	104,857,600 (10...	Unallocated Sp...	
1433601	104,857,600 (10...	Unallocated Sp...	
1638401	104,857,600 (10...	Unallocated Sp...	
1843201	104,857,600 (10...	Unallocated Sp...	
2048001	104,857,600 (10...	Unallocated Sp...	
2252801	104,857,600 (10...	Unallocated Sp...	
2457601	104,857,600 (10...	Unallocated Sp...	

Custom Content Sources

Evidence:File System|Path|File Options

New Edit Remove Remove All Create Image

Properties Hex Value Inter... Custom Conte...

Cursor pos = 0; log sec = 819201

Listed: 15 Selected: 1 F:\Unpartitioned Space [basic disk]/[unallocated space]/0819201