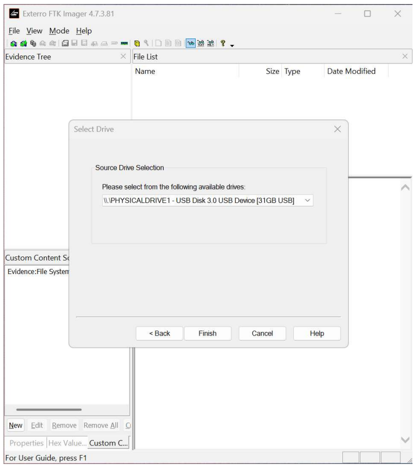
Digital Forensics Assignment 2

Task 1: Physical Drive Acquisition

Objective: Use FTK Imager to acquire an image of an entire physical drive (e.g., a USB drive).

Evidence:

- Screenshot of the drive selection screen



Select Drive

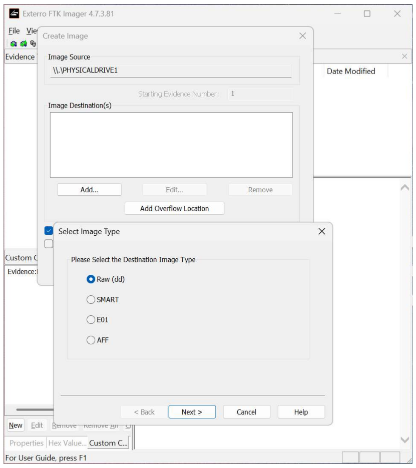
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - USB Disk 3.0 USB Device [31GB USB]

< Back | Finish | Cancel | Help

- Screenshot of the imaging progress or summary



Create Image

Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

Add... | Edit... | Remove

Add Overflow Location

Select Image Type

Please Select the Destination Image Type

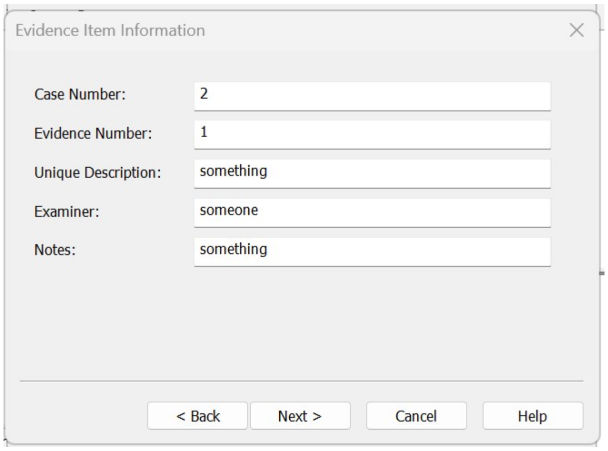
● Raw (dd)

○ SMART

○ E01

○ AFF

< Back | Next > | Cancel | Help



Evidence Item Information

Case Number: 2

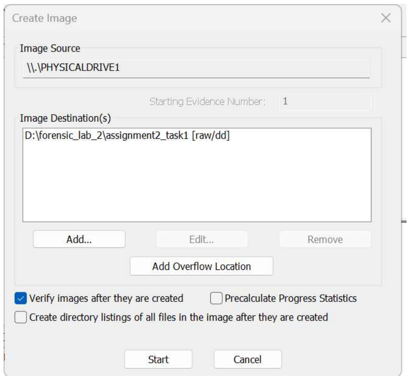
Evidence Number: 1

Unique Description: something

Examiner: someone

Notes: something

< Back | Next > | Cancel | Help



Create Image

Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 1

Image Destination(s)

D:\forensic_lab_2\assignment2_task1 [raw/dd]

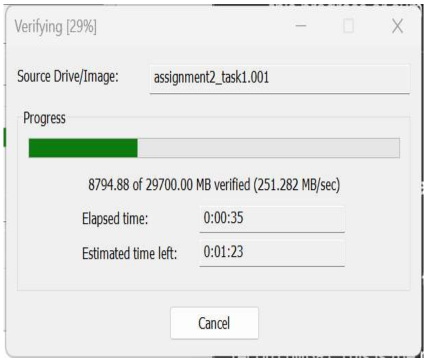
Add... | Edit... | Remove

Add Overflow Location

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Start | Cancel



Verifying [29%]

Source Drive/Image: assignment2_task1.001

Progress

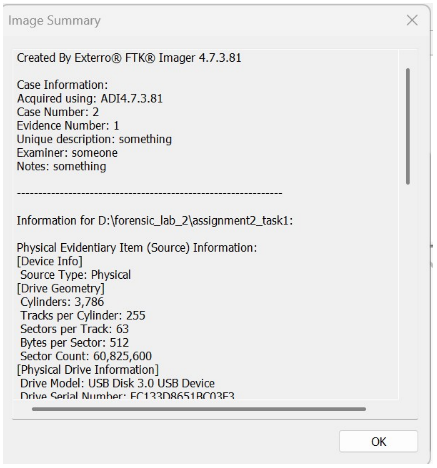
8794.88 of 29700.00 MB verified (251.282 MB/sec)

Elapsed time: 0:00:35

Estimated time left: 0:01:23

Cancel

Digital Forensics Assignment 2



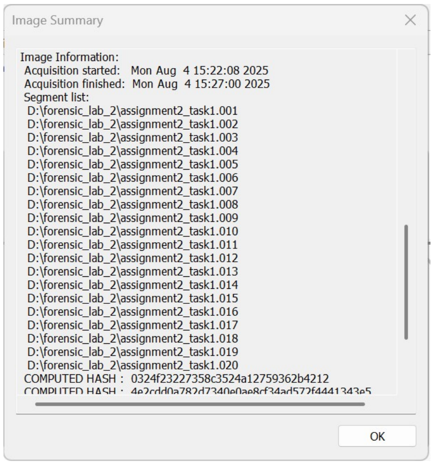
```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
Acquired using: ADI4.7.3.81
Case Number: 2
Evidence Number: 1
Unique description: something
Examiner: someone
Notes: something

------------------------------------------------------------

Information for D:\forensic_lab_2\assignment2_task1:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 3,786
 Tracks per Cylinder: 255
 Sectors per Track: 63
 Bytes per Sector: 512
 Sector Count: 60,825,600
[Physical Drive Information]
 Drive Model: USB Disk 3.0 USB Device
 Drive Serial Number: FC133D8651BC03E3
```



```
Image Information:
 Acquisition started:   Mon Aug  4 15:22:08 2025
 Acquisition finished:  Mon Aug  4 15:27:00 2025
 Segment list:
  D:\forensic_lab_2\assignment2_task1.001
  D:\forensic_lab_2\assignment2_task1.002
  D:\forensic_lab_2\assignment2_task1.003
  D:\forensic_lab_2\assignment2_task1.004
  D:\forensic_lab_2\assignment2_task1.005
  D:\forensic_lab_2\assignment2_task1.006
  D:\forensic_lab_2\assignment2_task1.007
  D:\forensic_lab_2\assignment2_task1.008
  D:\forensic_lab_2\assignment2_task1.009
  D:\forensic_lab_2\assignment2_task1.010
  D:\forensic_lab_2\assignment2_task1.011
  D:\forensic_lab_2\assignment2_task1.012
  D:\forensic_lab_2\assignment2_task1.013
  D:\forensic_lab_2\assignment2_task1.014
  D:\forensic_lab_2\assignment2_task1.015
  D:\forensic_lab_2\assignment2_task1.016
  D:\forensic_lab_2\assignment2_task1.017
  D:\forensic_lab_2\assignment2_task1.018
  D:\forensic_lab_2\assignment2_task1.019
  D:\forensic_lab_2\assignment2_task1.020
 COMPUTED HASH :  0324f23227358c3524a12759362b4212
 COMPUTED HASH :  4e2cdd0a782d7340e0ae8cf34ad572f4441343e5
```

Evaluation Questions

1. What is the difference between imaging a physical drive vs. a logical drive?

A **physical drive acquisition** captures a bit-for-bit copy of the entire physical storage device, including all partitions, unallocated space, and the master boot record (MBR). This is the most comprehensive type of acquisition. A **logical drive acquisition**, on the other hand, only captures the data within a specific file system or partition, excluding the unallocated space and other partition structures.

2. Why might you choose the Raw (dd) format over others like E01?

The **Raw (dd)** format creates a bit-for-bit copy of the drive without any additional metadata, compression, or error checking capabilities. It's universally compatible with most forensic tools and operating systems, making it highly interoperable. While formats like E01 offer features like compression, metadata (case number, examiner's name), and error checking, the Raw format is often chosen for its simplicity and broad compatibility.

3. How can this image be validated for forensic integrity?

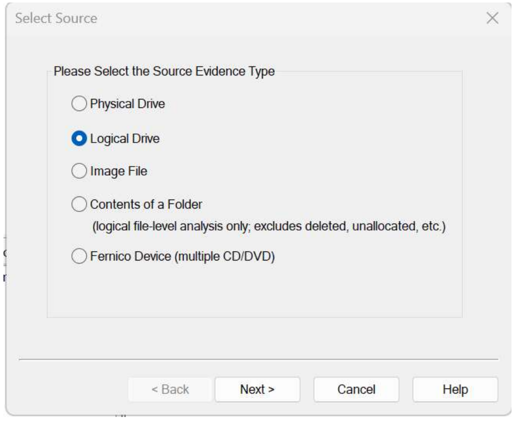
Forensic integrity is validated by using **cryptographic hashing**. During the imaging process, FTK Imager calculates a hash value (e.g., MD5 and SHA1) of the source drive's data. This hash value is recorded in the acquisition summary. After the image is created, the same hash value is calculated for the destination image file. If the two hash values match, it confirms that the data in the image is an exact, unaltered replica of the original drive's data. You'll need to check the hash value of the newly created image using a tool like **Autopsy** or FTK Imager to confirm it matches the hash value recorded during acquisition.

Digital Forensics Assignment 2

Task 2: Logical Drive Acquisition

Objective: Use FTK Imager to acquire the logical contents (file system) of a partition or drive. **Evidence**:

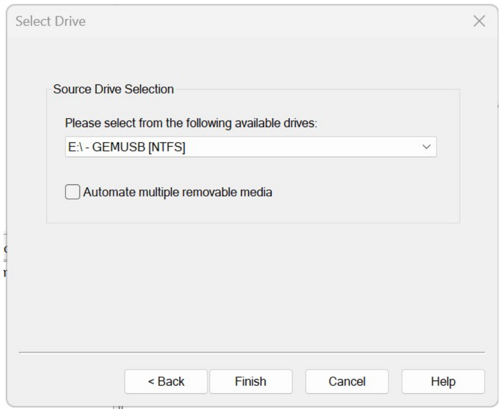
• Screenshot of the logical drive selection screen



Select Source

Please Select the Source Evidence Type

○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Fernico Device (multiple CD/DVD)



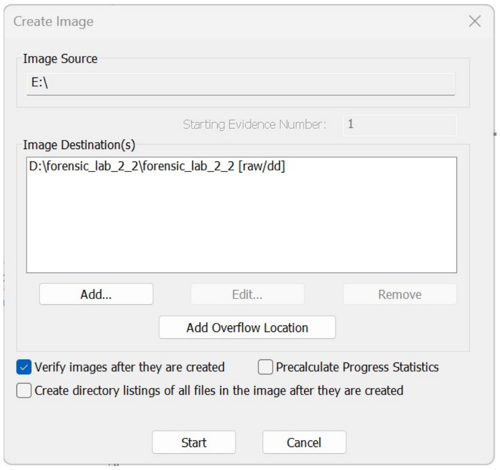
Select Drive

Source Drive Selection

Please select from the following available drives:
E:\ - GEMUSB [NTFS]

□ Automate multiple removable media

• Screenshot of destination and format setting



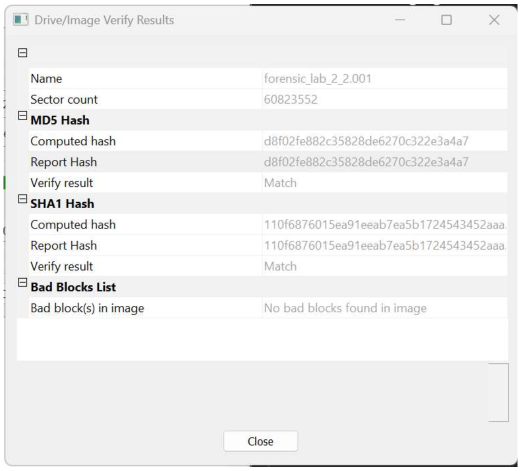
Create Image

Image Source
E:\

Starting Evidence Number: 1

Image Destination(s)
D:\forensic_lab_2_2\forensic_lab_2_2 [raw/dd]

☑ Verify images after they are created
□ Precalculate Progress Statistics
□ Create directory listings of all files in the image after they are created



Drive/Image Verify Results

Name	forensic_lab_2_2.001
Sector count	60823552
MD5 Hash	
Computed hash	d8f02fe882c35828de6270c322e3a4a7
Report Hash	d8f02fe882c35828de6270c322e3a4a7
Verify result	Match
SHA1 Hash	
Computed hash	110f6876015ea91eeab7ea5b1724543452aaa
Report Hash	110f6876015ea91eeab7ea5b1724543452aaa
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Evaluation Questions

1. What is the advantage of performing a logical drive acquisition?

The main advantage is **speed and efficiency**. A logical acquisition is much faster than a physical acquisition because it only copies the files and folders that are part of the file system. It doesn't waste time copying unallocated space, slack space, or other hidden areas of the disk. This method is ideal when you're certain that the evidence resides within the active file system and you need to get the data quickly.

2. What types of data might not be captured in a logical acquisition?

A logical acquisition will **not capture** data from:

- **Unallocated space:** This is the free space on a disk where deleted files and other data fragments may still exist.

- **Slack space:** The unused space at the end of a cluster that may contain remnants of previously stored files.
- **Page file or hibernation file:** These are system files that exist outside of the typical file system structure and contain volatile memory data.
- **Hidden partitions:** Any partitions that are not mounted or recognized by the operating system will be missed.
- **Master Boot Record (MBR):** The MBR, which contains the partition table, is not included.

3. In what scenarios would this type of acquisition be preferred?

Logical acquisition is preferred in scenarios where:

- **Time is a critical factor:** When you need to quickly preserve files from a live system and can't afford a full physical acquisition.
- **The evidence is clearly defined:** If you know exactly which files or folders are relevant to your investigation and they are all within the active file system.
- **Storage space is limited:** The resulting image file is much smaller than a physical image, which is helpful if you have limited storage capacity for your evidence.
- **Initial Triage:** It can be used for a preliminary investigation to quickly verify if certain files exist before committing to a full, time-consuming physical image.

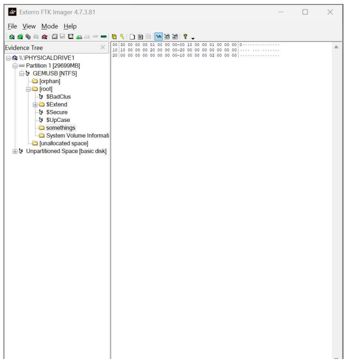
Digital Forensics Assignment 2

Task 3: Folder or File-Level Acquisition

Objective: Acquire only specific folders or files from a storage device.

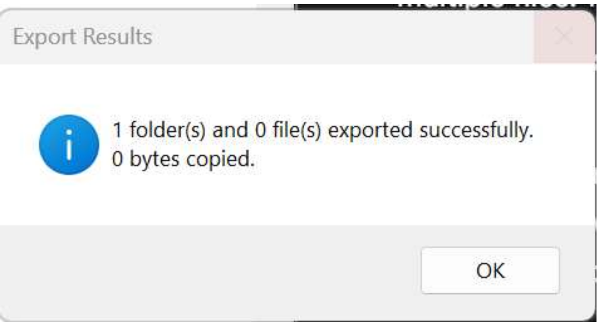
Evidence:

- Screenshot of selected folder or files



```
00 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 0···············
10 10 00 00 00 20 00 00 00-20 00 00 00 00 00 00 00 ················
20 00 00 00 00 00 00 00 00-10 00 00 00 02 00 00 00 ················
```

- Screenshot of the export operation



1 folder(s) and 0 file(s) exported successfully.
0 bytes copied.

Evaluation Questions

1. Why would an investigator choose file-level acquisition instead of full disk imaging?

An investigator would choose **file-level acquisition** to save time and storage space. It's the fastest method of data collection because it only copies the required files, which is ideal for a **targeted investigation** where you know exactly which files are relevant. This method is also useful for a **quick preview** or **triage** to determine if a full disk image is even necessary.

2. How can you ensure the authenticity of exported files?

To ensure the authenticity of exported files, you must create a **hash value** (e.g., MD5 or SHA1) of each file **before** and **after** the export. FTK Imager can calculate the hash of a file on the source disk. After exporting the file, you would use a separate tool or FTK Imager itself to calculate the hash of the exported copy. If the hash values match, it confirms the file was copied without alteration.

3. What are the limitations of this method?

The primary limitation of file-level acquisition is that it **only captures the active files**. It does not collect any data from:

Digital Forensics Assignment 2

- **Unallocated space** (deleted files)
- **File slack**
- **Hidden files or folders**
- **File system metadata** that is not directly tied to the file itself

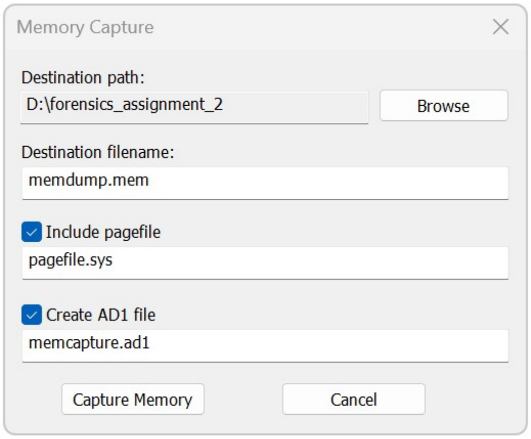
Digital Forensics Assignment 2

Task 4: RAM (Memory) Acquisition

Objective: Capture the live system memory (RAM) for volatile data analysis.

Evidence:

• Screenshot of memory capture settings



Memory Capture

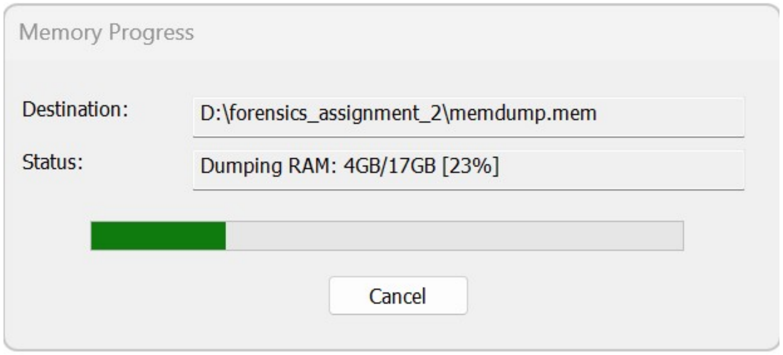
Destination path: D:\forensics_assignment_2

Destination filename: memdump.mem

☑ Include pagefile
pagefile.sys

☑ Create AD1 file
memcapture.ad1

• Screenshot showing successful capture



Memory Progress

Destination: D:\forensics_assignment_2\memdump.mem

Status: Dumping RAM: 4GB/17GB [23%]

Evaluation Questions

1. What kind of evidence can be recovered from RAM?

RAM contains **volatile data**—information that is lost when the power is turned off. Recoverable evidence from a RAM dump can include:

- **Running processes** and open network connections.
- **Active user sessions** and cached passwords.
- **Decryption keys** for encrypted files.
- **Malicious code or rootkits** that reside only in memory.
- **Clipboard data** and recently typed commands.

2. Why is timing critical when performing memory acquisition?

Timing is critical because RAM is **constantly changing**. The longer you wait, the more likely the evidence you're looking for will be overwritten by other processes or data. Malicious actors or malware can also detect that they are being investigated and attempt to delete or hide evidence. Therefore, memory acquisition should be one of the first steps in a live system investigation.

3. How can you analyze a memory dump after acquisition?

After a memory dump is acquired, you can analyze it using specialized forensic tools like **Volatility Framework**. Volatility is an open-source tool that can parse the raw memory image and extract valuable information. For example, it can identify active processes, find hidden network connections, or locate decryption keys from the memory dump. Other commercial tools, such as FTK and Autopsy, also have modules for memory analysis.