MIT World Peace University

Attack Research and Documentation
Fourth Year B. Tech, Semester 8

Hands on Exercise on Preserving Digital Evidence for Legal purposes

Lab Assignment 6

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 15

April 5, 2025

Contents

1 Introduction

- This report documents the use of two digital forensics tools — **FTK Imager** and **Autopsy**.
- The aim is to simulate data deletion scenarios and analyze the ability to recover data.
- Screenshots are attached as visual evidence for each step.

2 Tools Used

2.1 FTK Imager

FTK Imager is a lightweight, freeware imaging tool developed by Exterro. It is widely used in digital forensics for creating forensic images of storage devices. The tool is designed to ensure data integrity and is capable of generating MD5 and SHA1 hash values for verification. Key features of FTK Imager include:

- **Forensic Imaging:** Allows users to create bit-by-bit copies of storage devices, ensuring no data is altered during the process.
- **Hash Verification:** Generates hash values (MD5 and SHA1) to confirm the integrity of the forensic image.
- **Preview Functionality:** Enables users to preview files and folders on the storage device before imaging.
- **Support for Multiple Formats:** Supports imaging in various formats, including E01, DD, and raw image formats.
- **Logical and Physical Imaging:** Provides options to create logical images (specific files or folders) or physical images (entire storage devices).

FTK Imager is an essential tool for forensic investigators, ensuring that evidence is preserved in a reliable and verifiable manner.

2.2 Autopsy

Autopsy is an open-source, graphical digital forensics platform designed for analyzing disk images and recovering data. It is built on top of The Sleuth Kit (TSK) and provides an intuitive interface for investigators. Key functionalities of Autopsy include:

- **File System Analysis:** Supports analysis of various file systems, including NTFS, FAT, exFAT, and EXT.
- **Deleted File Recovery:** Attempts to recover deleted files and directories from disk images.
- **Keyword Search:** Allows users to search for specific keywords within files and metadata.
- **Timeline Analysis:** Generates a timeline of file activities, helping investigators understand the sequence of events.
- **Artifact Extraction:** Extracts artifacts such as browser history, email data, and registry information.

- **Hash Set Matching:** Compares file hashes against known hash sets to identify suspicious or known files.
- **Modular Architecture:** Supports plugins and modules for extending functionality, such as analyzing mobile devices or network traffic.

Autopsy is a powerful tool for forensic analysis, enabling investigators to uncover critical evidence and reconstruct events effectively.

3 Environment Setup

3.1 Installation of FTK Imager

- FTK Imager was downloaded from the official Exterro website.
- Terms and conditions were reviewed before installation.

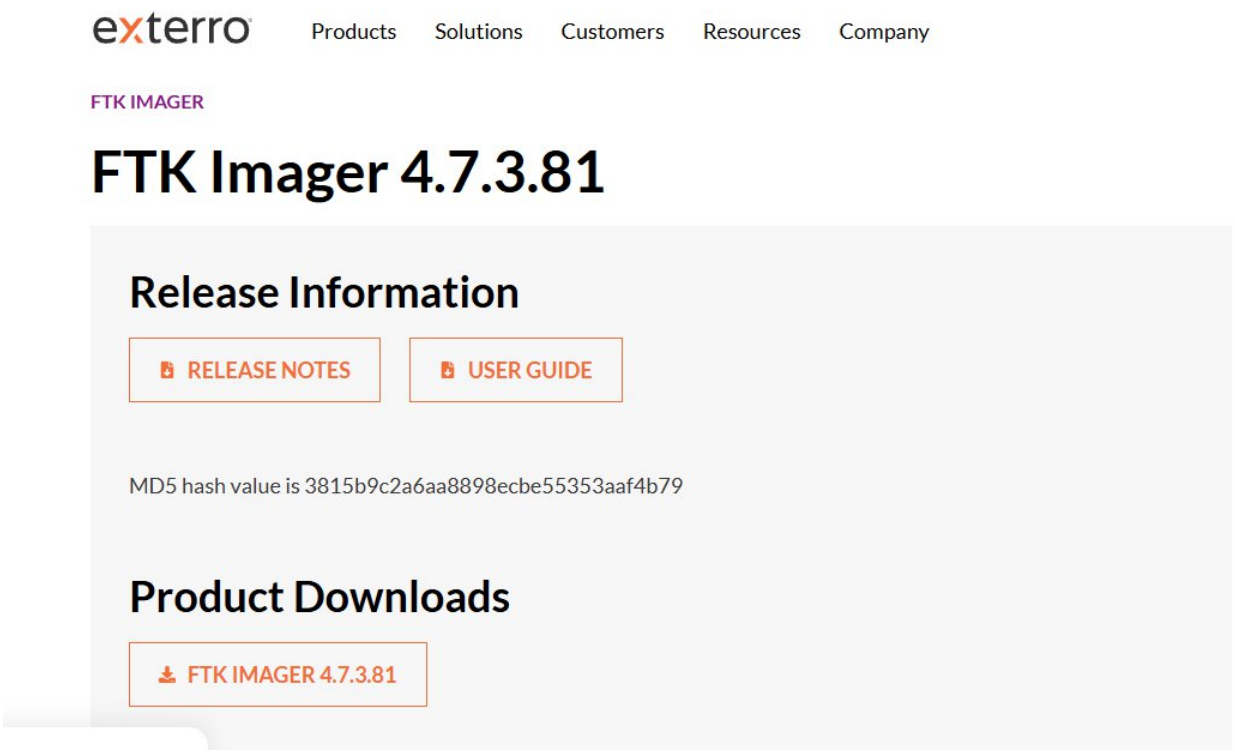


Figure 1: Downloading FTK Imager

3.2 Installation of Autopsy

- Autopsy was downloaded from https://www.autopsy.com.
- The tool was installed and verified for functionality.

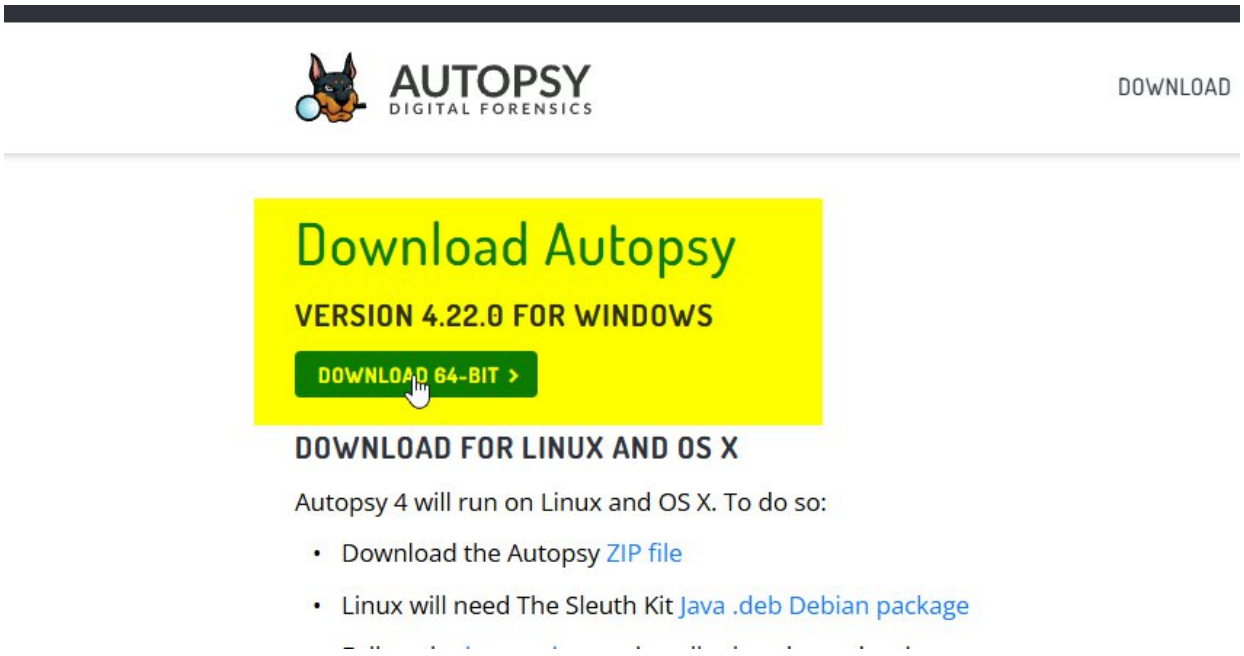


Figure 2: Downloading Autopsy

4 Creating Logical Partition and Files

4.1 Partition Creation

- A 20MB logical partition was created using the built-in disk management utility.

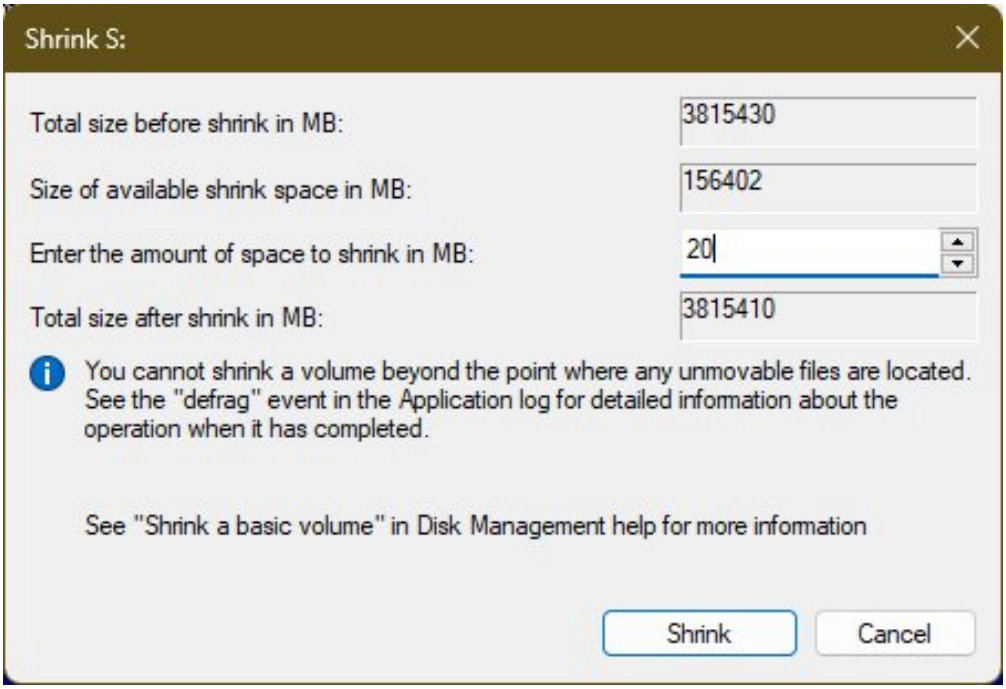


Figure 3: Shrinking Volume to then create a new one.

4.2 File Creation and Deletion

4.2.1 Images

- Multiple files were created in the partition.
- A few files were then deleted to simulate data loss.

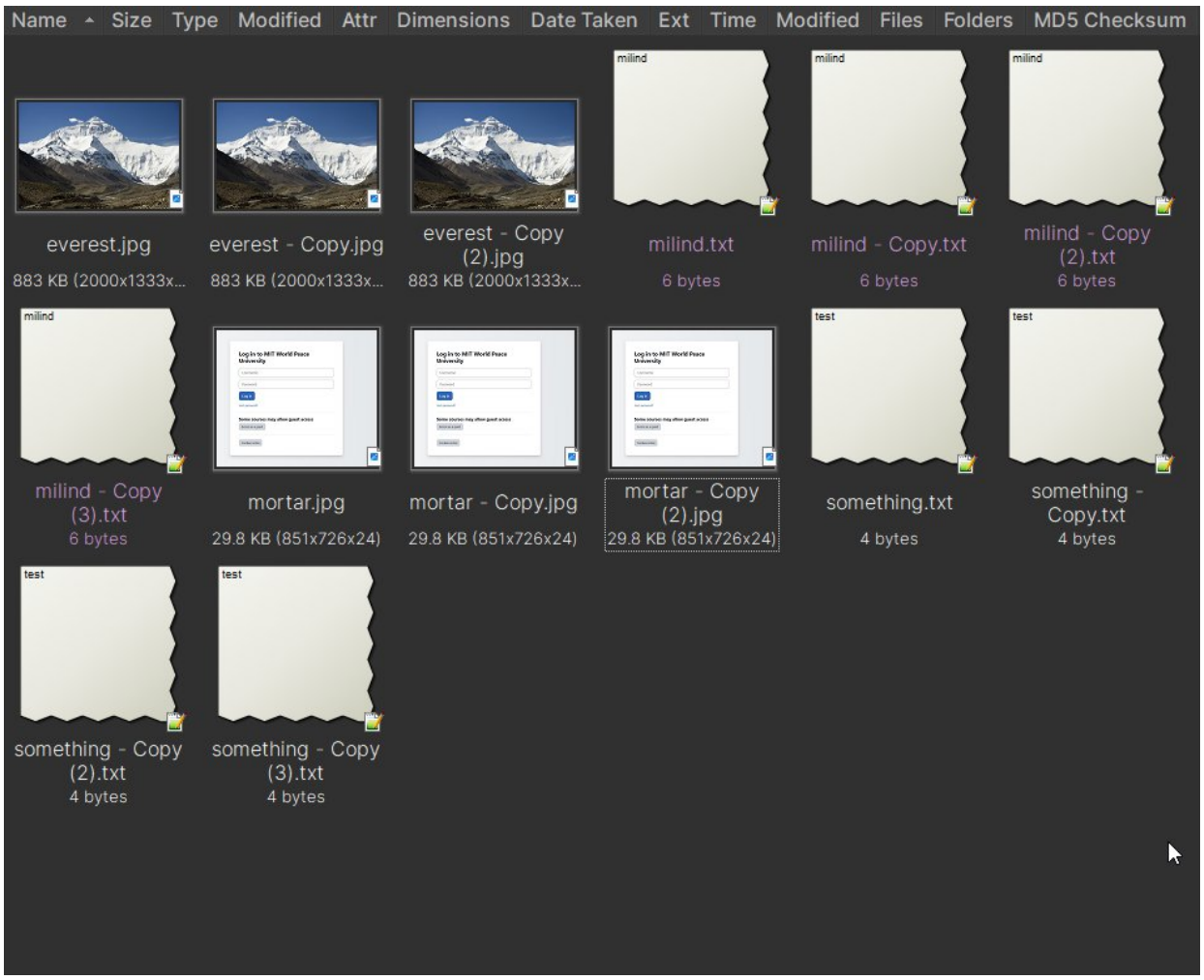


Figure 4: Screenshot

Figure 5: JPEG Downloaded from Internet

4.2.2 Text

Name	Size	Type
something2.txt	9 bytes	TXT File
something - Copy (3).txt	4 bytes	TXT File
something - Copy (2).txt	4 bytes	TXT File
something.txt	4 bytes	TXT File
mortar - Copy (2).jpg	29.8 KB	JPEG image
mortar - Copy.jpg	29.8 KB	JPEG image
mortar.jpg	29.8 KB	JPEG image
milind - Copy (3).txt	6 bytes	TXT File
milind - Copy (2).txt	6 bytes	TXT File
milind - Copy.txt	6 bytes	TXT File
milind.txt	6 bytes	TXT File
everest - Copy (2).jpg	883 KB	JPEG image
everest - Copy.jpg	883 KB	JPEG image
everest.jpg	883 KB	JPEG image

Figure 6: Contents

something.txt was created and deleted. The file contained the following text:

```
test
```

something.txt was created and deleted. The file contained the following text:

```
test test
```

This was done to check if the file was recoverable after deletion. The file was created using Notepad and saved in the logical partition.

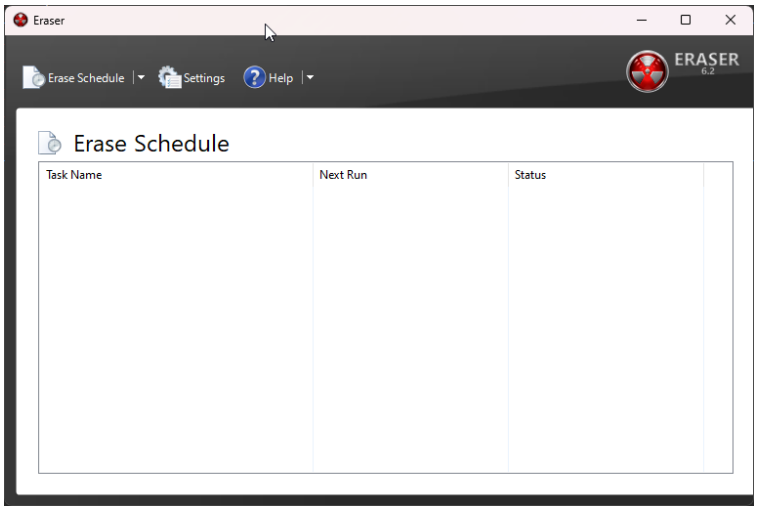


Figure 7: Deletion using Eraser

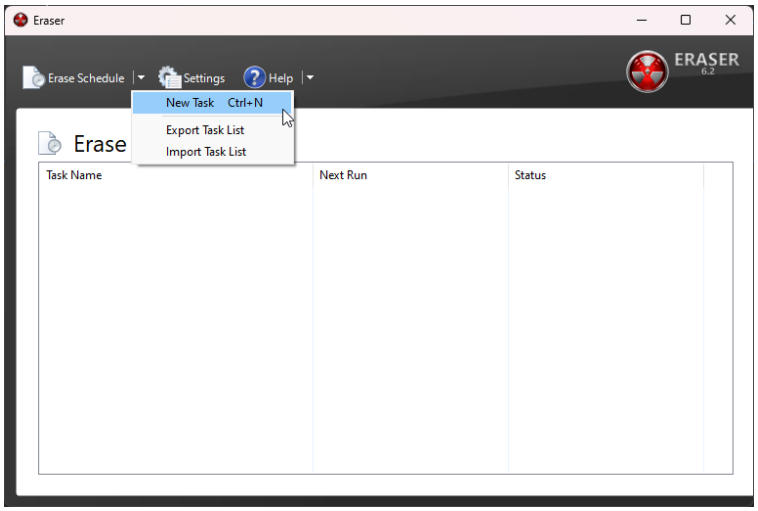


Figure 8: Deletion using Eraser

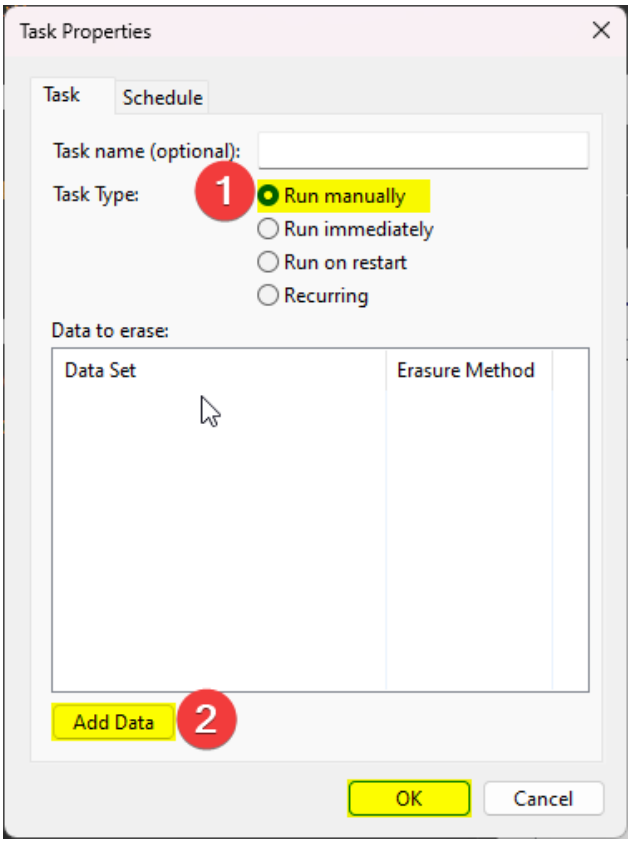


Figure 9: Deletion using Eraser

5 Imaging and Hash Verification

5.1 SHA256 Hash for something.txt

`9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08`

5.2 SHA256 Hash for something.txt after modifying

`7e443c809e8ff0a43b9e53074098ffb5524be525e81b3bee0d37cf6ea9730011`

5.3 SHA256 Hash for mortar.png

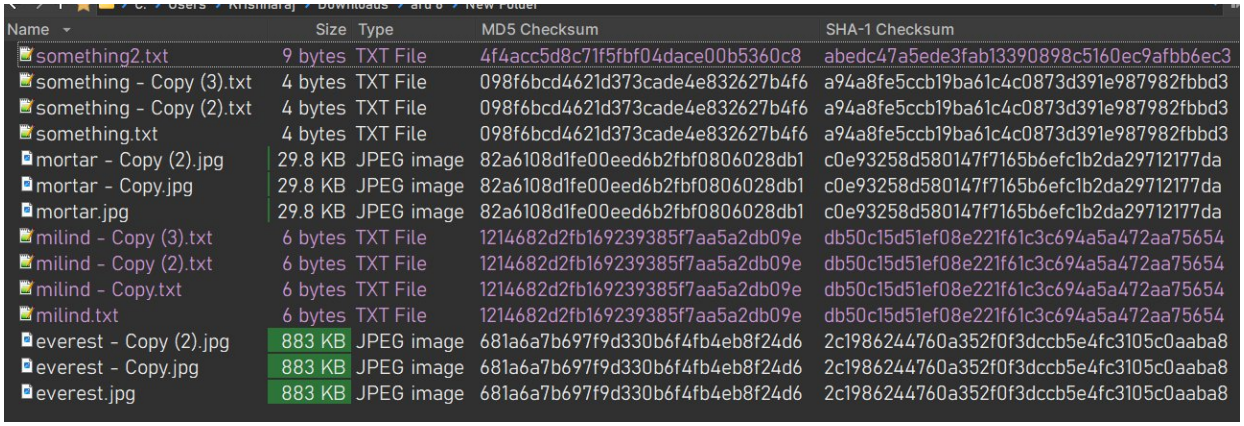
`8c4345bda41f90d9693395383b99fcd14940c6629e4a218cb5a7cce6c0910fad`

5.4 SHA256 Hash for everest.jpg

`17912ca3fd92f220d331d80e799c1194c79ff2e7af453d05c261544c3bafecea`

5.5 Hash Value Documentation

- The MD5 and SHA1 hashes were recorded at the time of image creation.



Name	Size	Type	MD5 Checksum	SHA-1 Checksum
something2.txt	9 bytes	TXT File	4f4acc5d8c71f5fbf04dace00b5360c8	abedc47a5ede3fab13390898c5160ec9afbb6ec3
something - Copy (3).txt	4 bytes	TXT File	098f6bcd4621d373cade4e832627b4f6	a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
something - Copy (2).txt	4 bytes	TXT File	098f6bcd4621d373cade4e832627b4f6	a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
something.txt	4 bytes	TXT File	098f6bcd4621d373cade4e832627b4f6	a94a8fe5ccb19ba61c4c0873d391e987982fbbd3
mortar - Copy (2).jpg	29.8 KB	JPEG image	82a6108d1fe00eed6b2fbf0806028db1	c0e93258d580147f7165b6efc1b2da29712177da
mortar - Copy.jpg	29.8 KB	JPEG image	82a6108d1fe00eed6b2fbf0806028db1	c0e93258d580147f7165b6efc1b2da29712177da
mortar.jpg	29.8 KB	JPEG image	82a6108d1fe00eed6b2fbf0806028db1	c0e93258d580147f7165b6efc1b2da29712177da
milind - Copy (3).txt	6 bytes	TXT File	1214682d2fb169239385f7aa5a2db09e	db50c15d51ef08e221f61c3c694a5a472aa75654
milind - Copy (2).txt	6 bytes	TXT File	1214682d2fb169239385f7aa5a2db09e	db50c15d51ef08e221f61c3c694a5a472aa75654
milind - Copy.txt	6 bytes	TXT File	1214682d2fb169239385f7aa5a2db09e	db50c15d51ef08e221f61c3c694a5a472aa75654
milind.txt	6 bytes	TXT File	1214682d2fb169239385f7aa5a2db09e	db50c15d51ef08e221f61c3c694a5a472aa75654
everest - Copy (2).jpg	883 KB	JPEG image	681a6a7b697f9d330b6f4fb4eb8f24d6	2c1986244760a352f0f3dccb5e4fc3105c0aaba8
everest - Copy.jpg	883 KB	JPEG image	681a6a7b697f9d330b6f4fb4eb8f24d6	2c1986244760a352f0f3dccb5e4fc3105c0aaba8
everest.jpg	883 KB	JPEG image	681a6a7b697f9d330b6f4fb4eb8f24d6	2c1986244760a352f0f3dccb5e4fc3105c0aaba8

Figure 10: MD5 and SHA1 Checksums

6 Image Creation with FTK Imager

- The logical partition was imaged using FTK Imager.

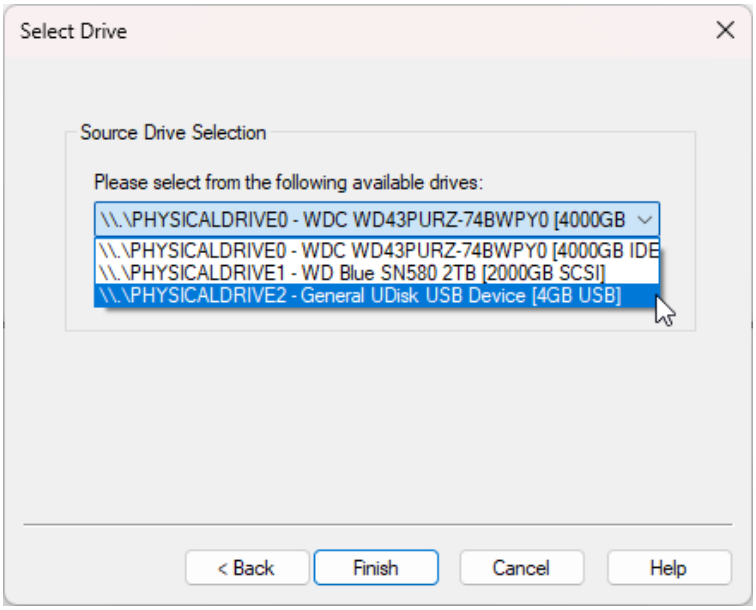


Figure 11: Selecting partition in FTK

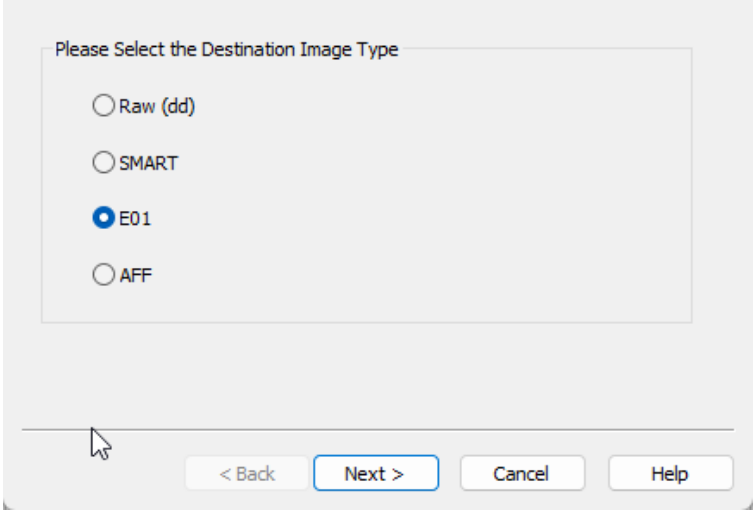


Figure 12: Selecting Format for image

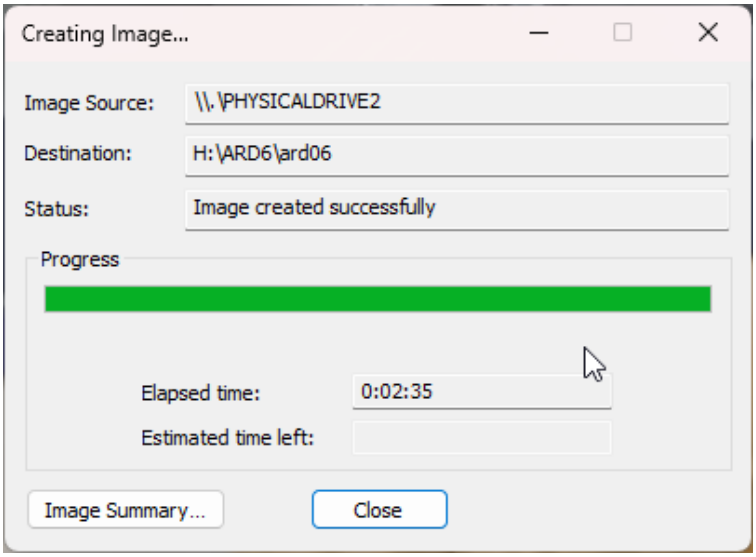


Figure 13: Creating Image

7 Analysis in Autopsy

- Autopsy was used to attempt recovery of deleted files.
- The results varied based on the deletion scenario.

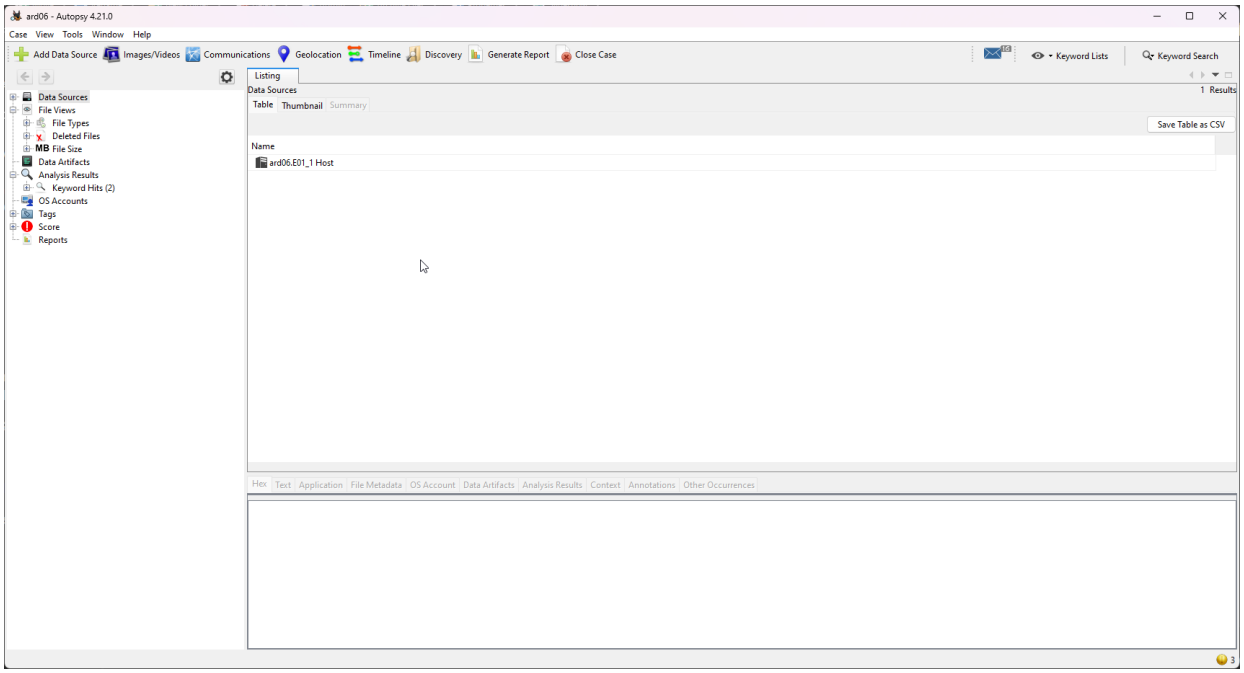


Figure 14: Importing Image as a new case

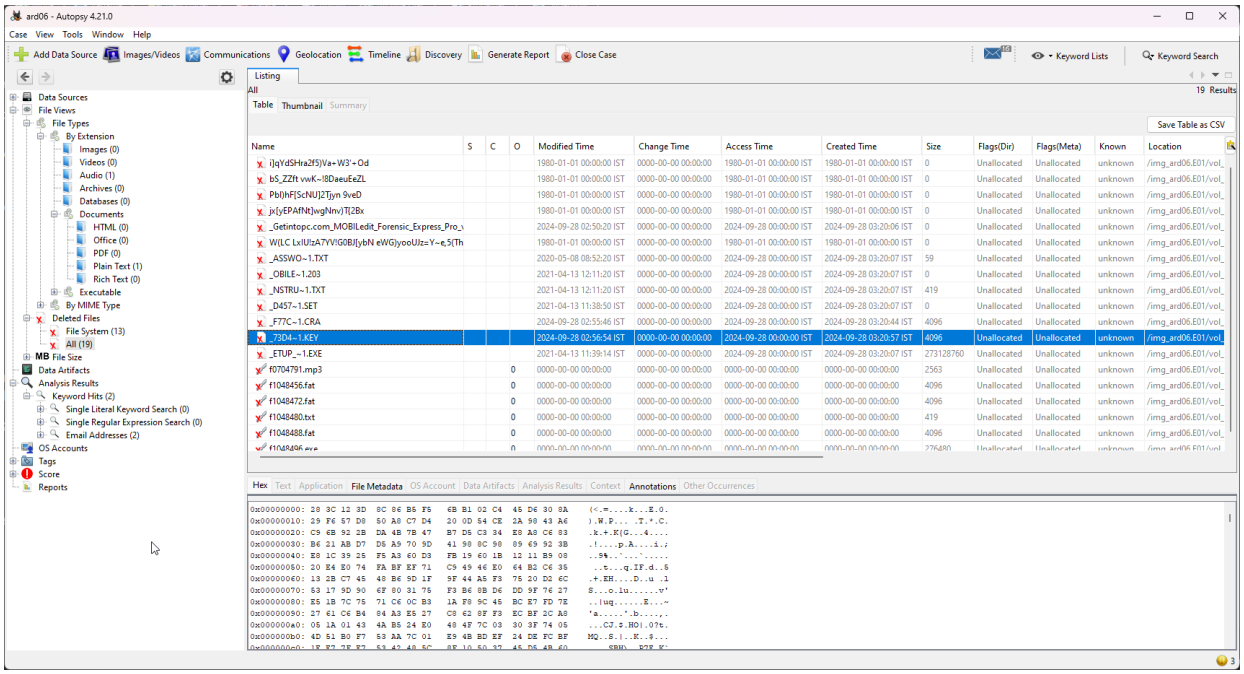


Figure 15: Looking at Recovered files

7.1 Autopsy Text Reports

```
Created By Exterro® FTK® Imager 4.7.3.81

Case Information:
```

```
Acquired using: ADI4.7.3.81
Case Number: 1
Evidence Number: 11
Unique description: 1
Examiner: 1
Notes: 1

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

Information for C:\Users\Computer\Downloads\ard:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Logical
[Drive Geometry]
 Bytes per Sector: 512
 Sector Count: 38,912
[Physical Drive Information]
 Removable drive: False
 Source data size: 19 MB
 Sector count:    38912
[Computed Hashes]
 MD5 checksum:    9ea725c870a83043ea15b591d16abdd8
 SHA1 checksum:   2495b0f0da571ec75453f9000690528af61aefd6

Image Information:
 Acquisition started:   Tue Mar 25 09:49:46 2025
 Acquisition finished:  Tue Mar 25 09:49:47 2025
 Segment list:
  C:\Users\Computer\Downloads\ard.E01
```

8 Use Case Experiments and Results

8.1 Case 1: File Deleted and Removed from Trash

- The file was deleted and permanently removed.
- Recovery was possible using Autopsy.

8.2 Case 2: File Deleted Using Erase Tools

- A secure delete tool (e.g., Eraser) was used.
- File recovery was not possible as data blocks were overwritten.

8.3 Case 3: File Deleted and New File with Same Name Created

- The new file partially overwrote the original.

- Only the latest deleted file with the same name was recoverable.

9 Conclusion

- FTK Imager successfully captured forensic images and verified their integrity.
- Autopsy enabled effective analysis and partial recovery depending on the deletion method.
- Overwriting or secure deletion significantly reduced recovery success.

References

[1] FTK Imager.
Website: https://accessdata.com/products-services/ftk-imager

[2] Autopsy.
Website: https://www.autopsy.com/

[3] Hashing Algorithms (MD5, SHA1, SHA256).
Website: https://en.wikipedia.org/wiki/Cryptographic_hash_function

[4] The Sleuth Kit (TSK).
Website: https://www.sleuthkit.org/

[5] Disk Management Utility (Windows).
Website: https://support.microsoft.com/en-us/windows/create-and-format-a-hard-disk-partition-

[6] Eraser - Secure Data Deletion Tool.
Website: https://eraser.heidi.ie/