FTK Imager & Autopsy Forensic Lab Report - Loksharan Saravanan

Objective

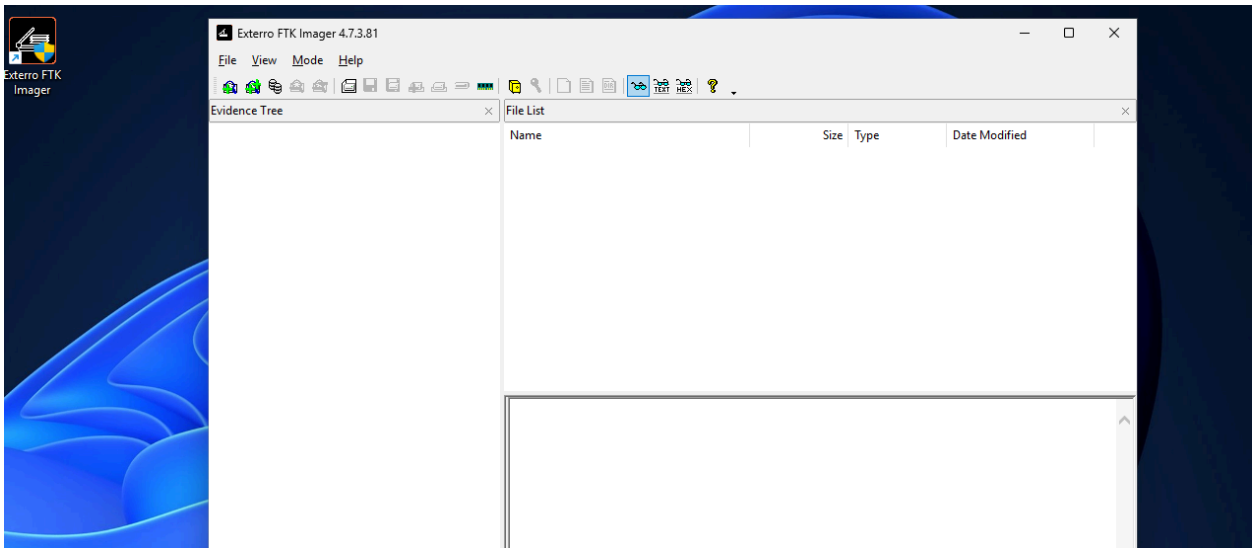
This lab documents a complete forensic acquisition and analysis workflow using FTK Imager and Autopsy/Sleuth Kit. I captured a disk image from a Windows 10 victim VM and performed analysis on an Ubuntu analysis system.

---

1. **FTK Imager Installation**

Steps taken

1. Downloaded FTK Imager 4.7 from Exterro using a .edu email.
2. Installed FTK Imager on the Windows 10 victim VM using default settings.
3. Verified successful launch of the FTK Imager GUI.



(Figure 1 – FTK Imager main window)

Metadata entered during image capture

- Case Number: 001
- Evidence Number: WIN10-VM-01

- Unique Description: Windows 10 Victim VM
- Examiner: Loksharan Saravanan
- Notes: Test forensic acquisition for lab project

---

2. **Disk image acquisition**

Objective
Capture a complete forensic disk image of the Windows 10 victim VM using FTK Imager, preserving data integrity for later analysis.

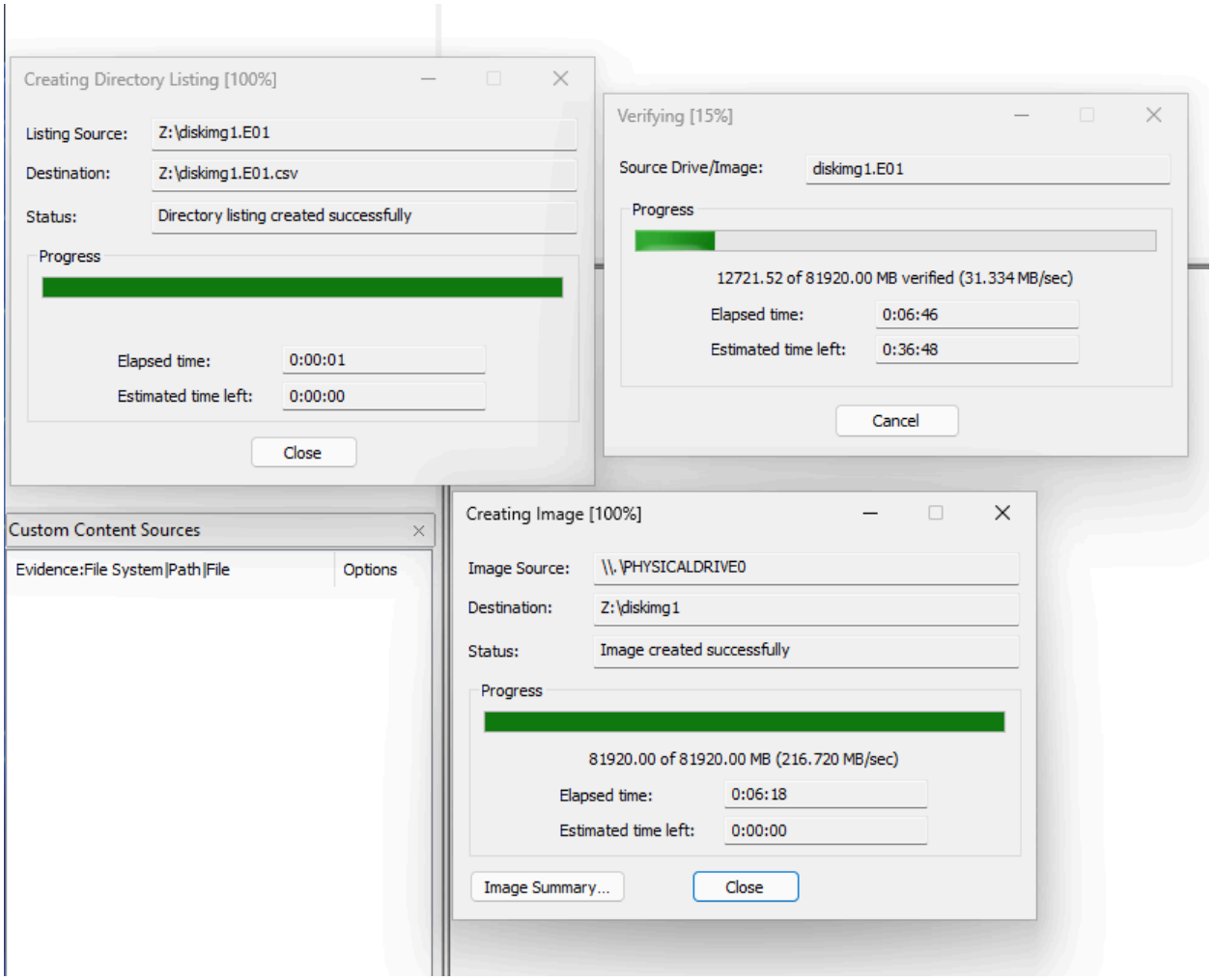
Tools and settings

- FTK Imager 4.7 (Windows)
- Disk type: Physical Drive (C:)
- Image format: E01 (EnCase Evidence File)
- Hashing: MD5 and SHA1

Procedure

1. Opened FTK Imager → File → Create Disk Image.
2. Selected Physical Drive (C: drive of Windows 10 victim VM).
3. Chose E01 format to preserve metadata and enable segmenting.
4. Entered metadata fields
5. Set the destination folder on a separate disk / shared folder (not the source disk).
6. Enabled MD5 and SHA1 hashing for integrity verification.
7. Started the acquisition and waited for completion.

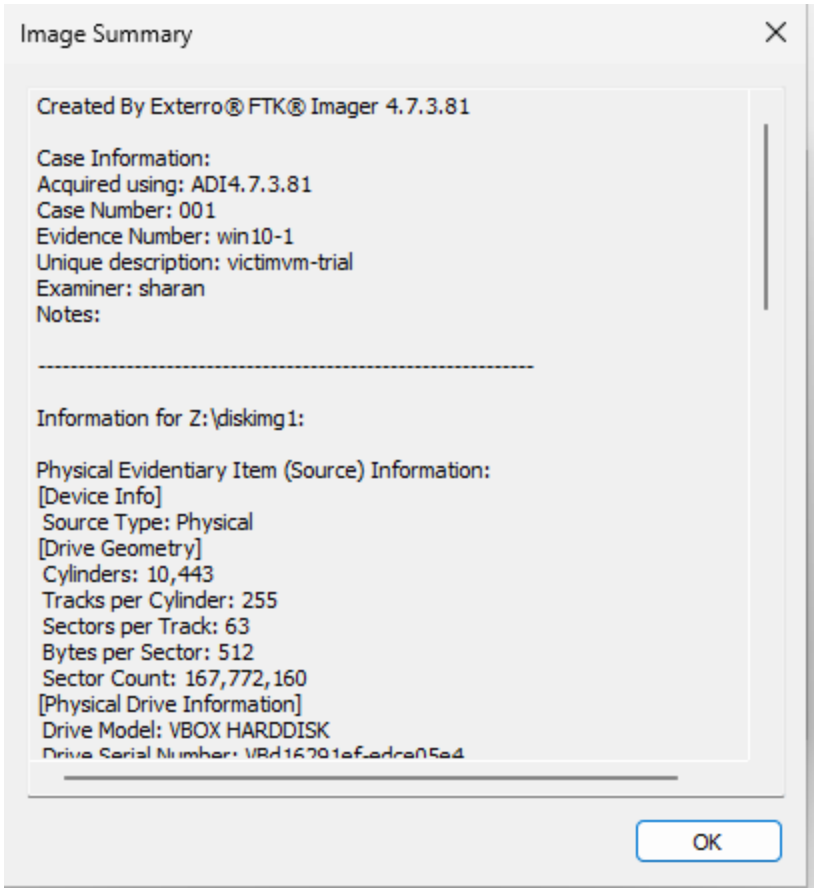
Important: The destination folder must not reside on the disk being imaged.



(Figure 2 – Creating a disk image in FTK Imager)

Image details

- Total size: 49 GB
- Number of segments: 34 (win10-victim.E01 → win10-victim.E34)
- Storage location: Shared folder on host machine
- Hashes: MD5 & SHA1 values recorded from the FTK Imager log



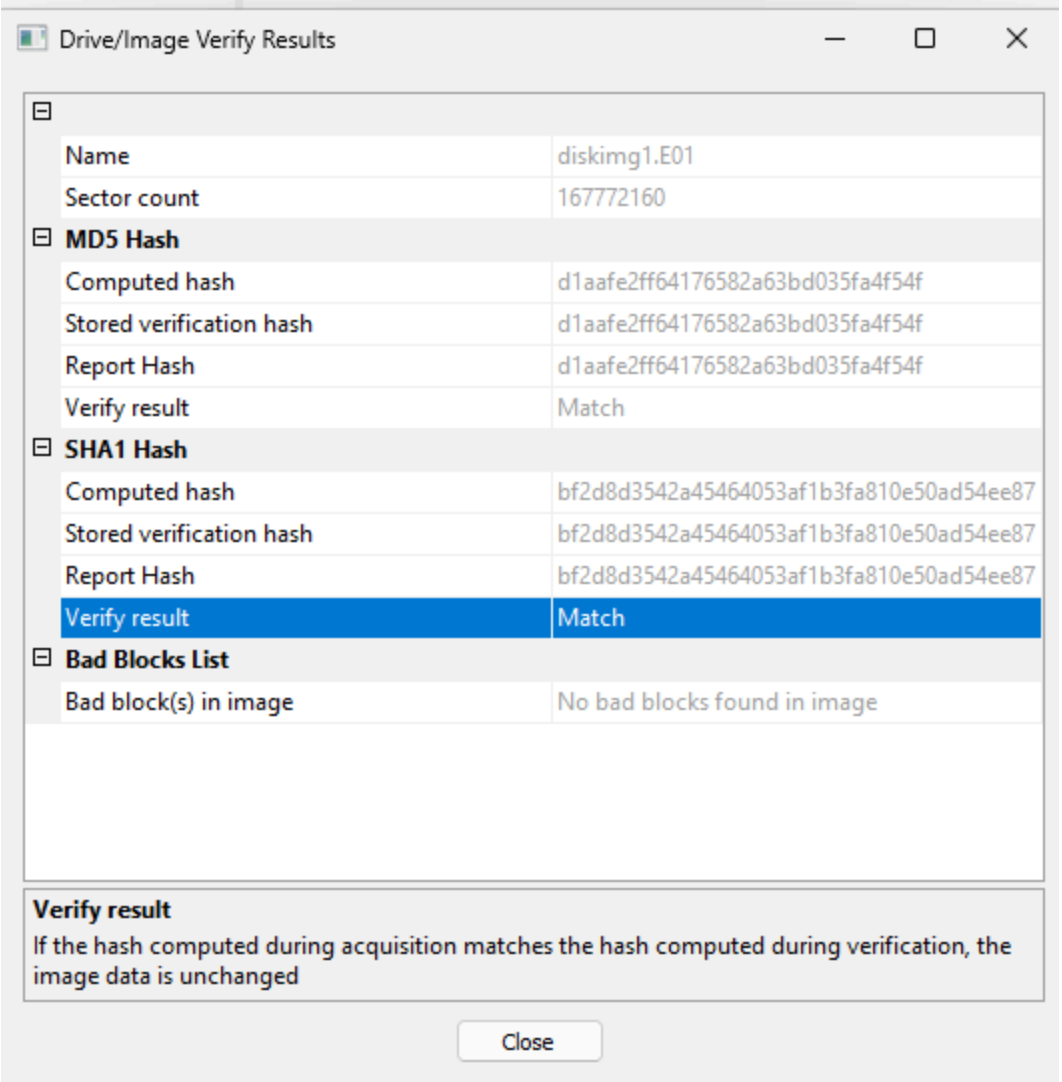
(Figure 3 – Disk image summary and segment list)

Verification

After acquisition, I verified the integrity of the image on the Ubuntu analysis machine using standard hashing tools:

md5sum win10-victim.E01
sha1sum win10-victim.E01

I confirmed that the calculated hashes matched the values recorded by FTK Imager and that all 34 segments were present in the same folder.



(Figure 4 – Hash verification output)

Observations

- All E01 segments must be kept together for successful analysis.
- E01 preserves metadata and supports hash verification, which is essential for maintaining chain of custody.
- Storing the image on a shared host folder avoided storage limits on the Ubuntu VM.

3. **Ubuntu setup for analysis**

Environment preparation
I used an Ubuntu VM for analysis and installed Sleuth Kit and Autopsy.

Commands used

sudo apt update && sudo apt upgrade -y
sudo apt install sleuthkit openjdk-11-jdk unzip wget -y
wget https://github.com/sleuthkit/autopsy/releases/download/autopsy-4.21.0/autopsy-4.21.0.zip
sudo unzip autopsy-4.21.0.zip -d /opt/
sudo chmod +x /opt/autopsy-4.21.0/bin/autopsy
sudo /opt/autopsy-4.21.0/bin/autopsy

Notes

- Autopsy runs a web interface at http://localhost:9999.
- Sleuth Kit CLI tools (mmls, fls, icat, tsk_recover, istat) are available for manual analysis.

---

4. **Sleuth Kit (TSK) CLI basics**

Common commands used

- List partitions:

mmls win10-victim.E01

- List files recursively:

fls -r -m / win10-victim.E01

- Extract a single file:

icat win10-victim.E01 <inode> > recovered_file.txt

- Recover entire partition:

```
tsk_recover -a win10-victim.E01 /recovered_files/
```

- Inspect metadata for an inode:

```
istat win10-victim.E01 <inode>
```

I verified these commands to ensure the image was readable and consistent.

---

5. **Autopsy analysis**

Case setup

1. Created a new case named WIN10_Forensics in Autopsy.
2. Added the acquired image (win10-victim.E01) as the data source.
3. Allowed Autopsy to parse and index the image.

Modules analyzed and findings

- File metadata viewer: Reviewed timestamps, file types, and sizes. Found typical system files and user documents.
- Deleted files recovery: Recovered several deleted text and image files.
- Web artifacts: Extracted browser history, cookies, and download records; found recent browsing activity consistent with user behavior.
- Keyword search: Searched for terms of interest; the keyword "password" appeared in a recovered configuration file.
- Recent documents: Reviewed recently accessed .docx and .xlsx files.
- Timeline analysis: Correlated file creation and access times; identified a cluster of activity around 21:00 prior to imaging.

Observations

- Web artifacts and timeline views were useful to reconstruct user activity before imaging.
- Recovered deleted files were validated using both Autopsy GUI and Sleuth Kit CLI methods.

Conclusion

This report documents a full forensic workflow from disk acquisition with FTK Imager to artifact analysis with Autopsy and Sleuth Kit. The exercise reinforced core forensic practices: preserving data integrity, recording metadata, verifying hashes, and performing structured analysis.