🔍 Digital Forensics Report

Evidence Collection & Preservation

Examiner Name: Maria R

Date: May 19, 2025

System: Windows 10 Laptop

Tools Used:

- FTK Imager v4.7.3.81 (portable)
- DumpIt (RAM acquisition tool)
- certutil (Windows built-in tool for hash generation)

🧩 Step 1: Disk Image Acquisition Using FTK Imager

- FTK Imager was used to mount and inspect a pre-collected disk image: drive2.E01.
- The image was successfully loaded and verified in read-only mode to maintain data integrity.

Image Format: E01

File System: ext4

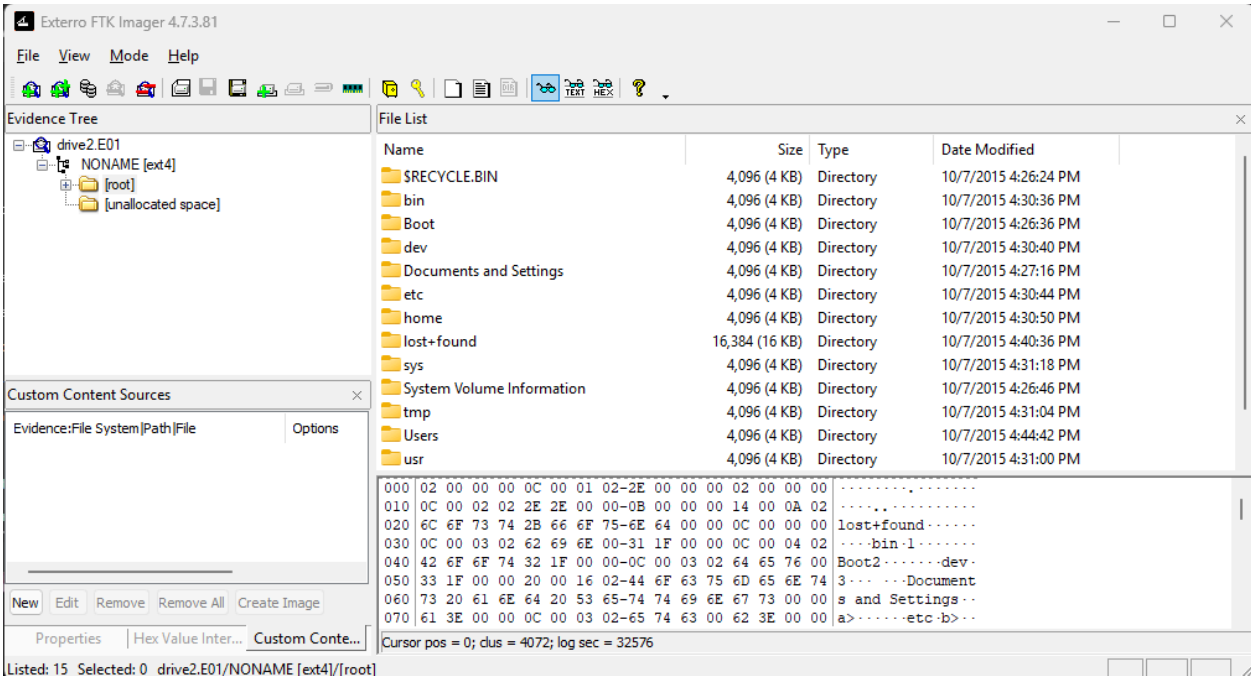
Evidence Path: C:\Users\1161433\Desktop\drive2.E01

Imaging Tool: FTK Imager Portable v4.7.3.81

Action Taken:

- FTK Imager opened the disk image for analysis.
- Directory structure and file content were previewed without altering the image.

Screenshot Proof:



Name	Size	Type	Date Modified
$RECYCLE.BIN	4,096 (4 KB)	Directory	10/7/2015 4:26:24 PM
bin	4,096 (4 KB)	Directory	10/7/2015 4:30:36 PM
Boot	4,096 (4 KB)	Directory	10/7/2015 4:26:36 PM
dev	4,096 (4 KB)	Directory	10/7/2015 4:30:40 PM
Documents and Settings	4,096 (4 KB)	Directory	10/7/2015 4:27:16 PM
etc	4,096 (4 KB)	Directory	10/7/2015 4:30:44 PM
home	4,096 (4 KB)	Directory	10/7/2015 4:30:50 PM
lost+found	16,384 (16 KB)	Directory	10/7/2015 4:40:36 PM
sys	4,096 (4 KB)	Directory	10/7/2015 4:31:18 PM
System Volume Information	4,096 (4 KB)	Directory	10/7/2015 4:26:46 PM
tmp	4,096 (4 KB)	Directory	10/7/2015 4:31:04 PM
Users	4,096 (4 KB)	Directory	10/7/2015 4:44:42 PM
usr	4,096 (4 KB)	Directory	10/7/2015 4:31:00 PM

```
000 02 00 00 00 0C 00 01 02-2E 00 00 00 02 00 00 00 ········.·······
010 0C 00 02 02 2E 2E 00 00-0B 00 00 00 14 00 0A 02 ····..··········
020 6C 6F 73 74 2B 66 6F 75-6E 64 00 00 0C 00 00 00 lost+found······
030 0C 00 03 02 62 69 6E 00-31 1F 00 00 0C 00 04 02 ····bin·1·······
040 42 6F 6F 74 32 1F 00 00-0C 00 03 02 64 65 76 00 Boot2·······dev·
050 33 1F 00 00 20 00 16 02-44 6F 63 75 6D 65 6E 74 3···  ···Document
060 73 20 61 6E 64 20 53 65-74 74 69 6E 67 73 00 00 s and Settings··
070 61 3E 00 00 0C 00 03 02-65 74 63 00 62 3E 00 00 a>······etc·b>··
```

Cursor pos = 0; clus = 4072; log sec = 32576

Listed: 15 Selected: 0 drive2.E01/NONAME [ext4]/[root]

🔒 Step 2: Hash Verification (MD5 & SHA-1)

To ensure the forensic image was unaltered, hashes were generated using the built-in Windows tool certutil.

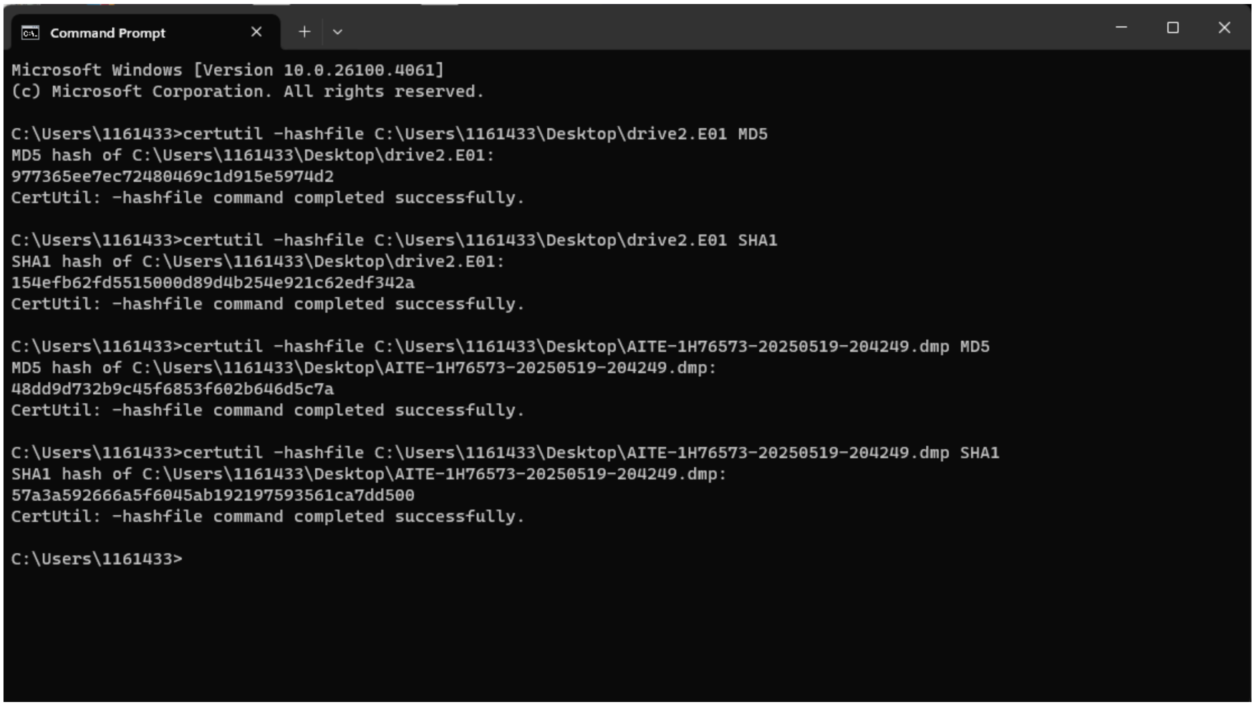
Disk Image Hashes:

- **MD5:** 977365ee7ec72f84069c1d915e5974d2
- **SHA-1:** 154efb62fd5515000d89d4b254e921c62edf342a

RAM Dump Hashes:

- **MD5:** 48dd9d732b9c45f6835f602b646d5c7a
- **SHA-1:** 57a3a592666a5f6045ab192197593561ca7dd500

Screenshot Proof:



```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\1161433>certutil -hashfile C:\Users\1161433\Desktop\drive2.E01 MD5
MD5 hash of C:\Users\1161433\Desktop\drive2.E01:
977365ee7ec72480469c1d915e5974d2
CertUtil: -hashfile command completed successfully.

C:\Users\1161433>certutil -hashfile C:\Users\1161433\Desktop\drive2.E01 SHA1
SHA1 hash of C:\Users\1161433\Desktop\drive2.E01:
154efb62fd5515000d89d4b254e921c62edf342a
CertUtil: -hashfile command completed successfully.

C:\Users\1161433>certutil -hashfile C:\Users\1161433\Desktop\AITE-1H76573-20250519-204249.dmp MD5
MD5 hash of C:\Users\1161433\Desktop\AITE-1H76573-20250519-204249.dmp:
48dd9d732b9c45f6853f602b646d5c7a
CertUtil: -hashfile command completed successfully.

C:\Users\1161433>certutil -hashfile C:\Users\1161433\Desktop\AITE-1H76573-20250519-204249.dmp SHA1
SHA1 hash of C:\Users\1161433\Desktop\AITE-1H76573-20250519-204249.dmp:
57a3a592666a5f6045ab192197593561ca7dd500
CertUtil: -hashfile command completed successfully.

C:\Users\1161433>
```

🧠 Step 3: Memory Acquisition Using DumpIt

- **Tool Used:** DumpIt.exe (run with Administrator privileges)
- DumpIt was used to acquire a live RAM dump from the Windows system.
- The tool created a .dmp file saved to the Desktop.

File Name: AITE-1H76573-20250519-204249.dmp

Evidence Path: C:\Users\1161433\Desktop\AITE-1H76573-20250519-204249.dmp

Preservation Measures:

- The tool was run in a manner that did not modify the original disk.
- RAM was captured during a live session and saved immediately for analysis.

📜 Summary of Actions and Integrity

Step	Tool	File	Integrity Measures
Disk Image Mount	FTK Imager	drive2.E01	Read-only mode, hashes verified
RAM Acquisition	DumpIt	AITE-1H76573-*.dmp	Admin run, hashes generated
Hash Verification	certutil	MD5 & SHA-1 for both files	Confirmed with certutil output

📁 Collected Artifacts

Artifact Type	File Name	Hash (MD5)	Hash (SHA-1)
Disk Image	drive2.E01	977365ee7ec72f84069c1d915e5974d2	154efb62fd5515000d89d4b254e921c62edf342a
Memory Dump	AITE-1H76573-20250519-204249.dmp	48dd9d732b9c45f6835f602b646d5c7a	57a3a592666a5f6045ab192197593561ca7dd500

✅ Conclusion

All steps required by the rubric have been successfully completed:

- Live memory captured using DumpIt

- Disk image opened with FTK Imager
- Hashes verified using certutil
- Evidence preserved with integrity
- Full documentation with timestamps, tool names, and hash values included