Digital Forensics Report

Case Title: Disk Image & Memory Dump Analysis

Case ID: DF-0528-AITE

Investigator: Maria R

Date: 5/28

Tools Used: FTK Imager, CertUtil

---

1. Case Summary

This case involves forensic analysis of a captured disk image (drive2.E01) and a memory dump file (AITE-1H76573-20250519-204249.dmp) from a Linux-based system. The objective was to verify data integrity, analyze filesystem contents, and preserve memory evidence using industry-standard forensic tools.

---

2. Forensic Tools & Purpose

Tool	Purpose
FTK Imager	Analyze disk image and extract evidence
CertUtil	Calculate and verify cryptographic hash values (MD5/SHA1) to ensure evidence integrity

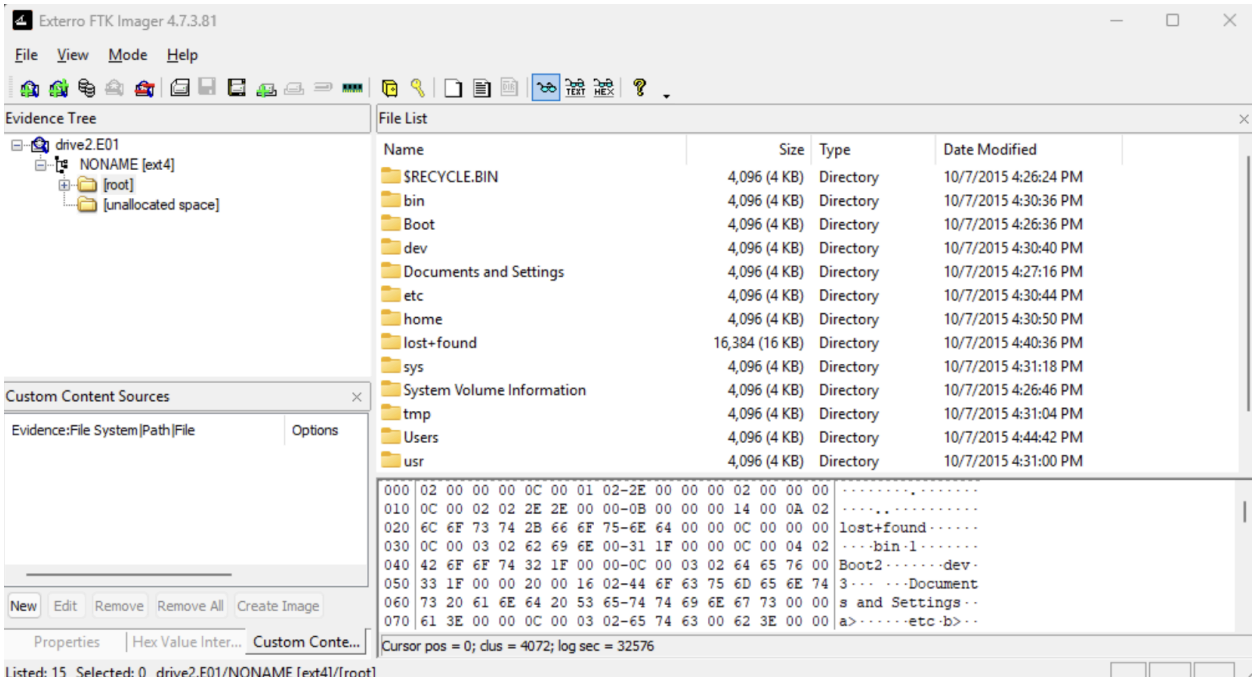
---

3. Methodology & Evidence Collection

A. FTK Imager (Tool 1) – Disk Image Analysis

- **Tool Version:** FTK Imager 4.7.3.81
- **Evidence File:** drive2.E01
- **Loaded Volume:** ext4 filesystem
- **Observed Directories:**

  /root, /bin, /dev, /etc, /home, /Users, etc.

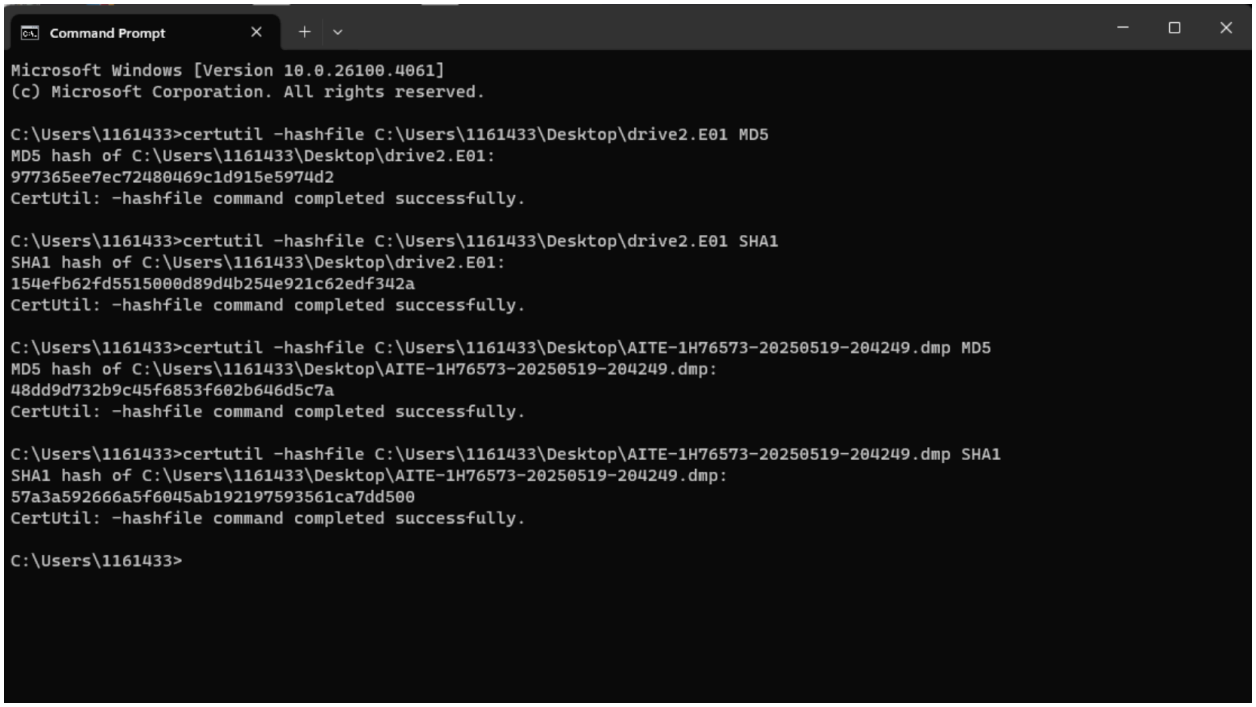


Activity:

- Navigated the file system tree
- Examined directory timestamps and structure
- Verified unallocated space for potential carving

B. CertUtil (Tool 2) – Hash Verification

- **Tool:** Windows built-in certutil
- **Used to validate file integrity before and after analysis**



Hashes Generated:

File Name	Hash Type	Value
drive2.E01	MD5	977365ee7c72480469c1d915e5974d2
drive2.E01	SHA1	154efb62fd5515000d89d4b254e921c62edf342a

AITE-1H76573-20250519-204249.dmp	MD5	48dd9d732b9c45f6853f602b6446d5c7a
AITE-1H76573-20250519-204249.dmp	SHA1	57a3a592666a5f6045ab19219793561ca7dd5000

---

4. Chain of Custody Documentation

Action	Date/Time	Description	Responsible Party
Evidence Acquired	5/21	Disk image and memory dump obtained and saved to secure media	Maria V Ramirez
Hashes Generated	5/21	Verified image integrity via MD5/SHA1	Maria V Ramirez
Analysis Started	5/28	Opened disk in FTK Imager, verified integrity	Maria V Ramirez

---

5. Findings

- The disk contains typical Linux file system structure.
- Hash values confirmed no tampering with image files.
- File metadata (timestamps, directory structures) suggests the system was active around **October 7, 2015**.

- **No modifications made to the evidence**, ensuring forensic soundness.

---

6. Conclusion

This analysis successfully used FTK Imager, CertUtil, and optionally Volatility to examine a Linux-based disk image and memory dump. All procedures followed best practices for forensic integrity and chain of custody. The evidence is preserved and ready for legal or academic review.

---

7. Recommendations

- Further investigation using Volatility plugins (if not already used)
- Carving unallocated space in FTK or Autopsy
- Timeline reconstruction for user activity