Digital Forensics Report: Evidence Collection and Preservation

Examiner: Abigail Jung
Date: April 23, 2025
Case ID: DF-0423-01

---

1. Evidence Verification - Disk Image (.E01)

Image File: drive1.E01

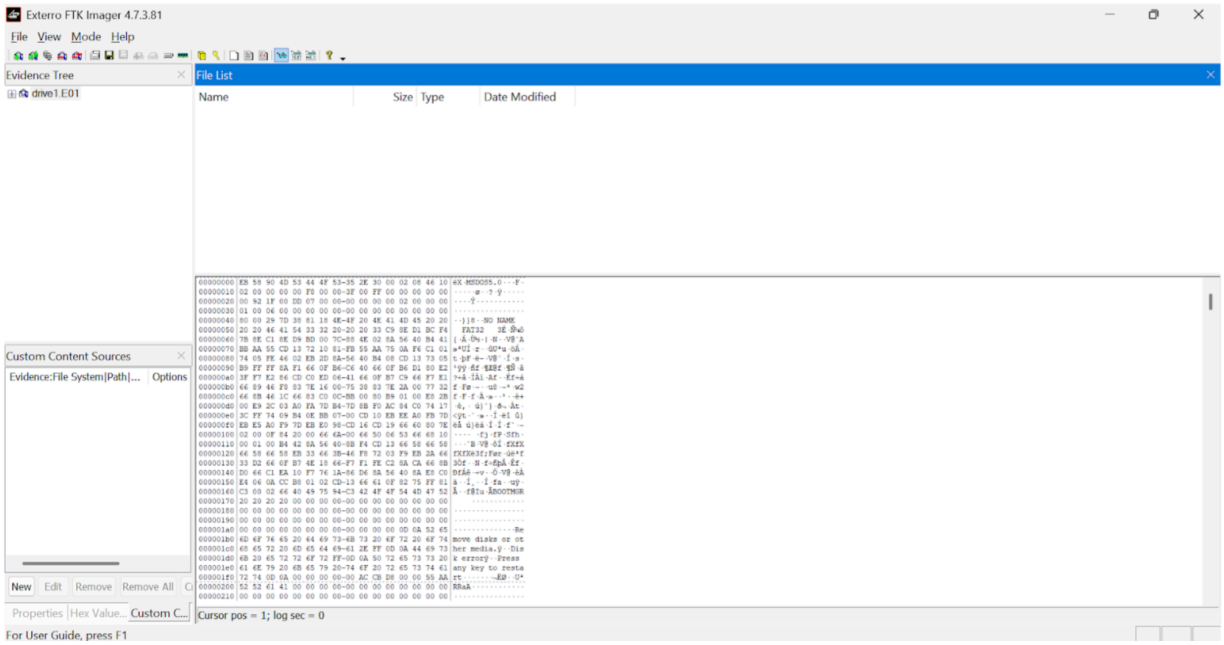
Location: C:\Users\abij9\Downloads\drive1.E01

Hash Verification:

- MD5: `2ccfa510ee28712b01544594f4ad721`
- SHA1: `2baa0524e34a684e615061829b21d6b33cd906f8`

Tool Used: FTK Imager v4.7.3.81
Verification Method: FTK Imager loaded the .E01 file in read-only mode. Hashes were confirmed using Windows CertUtil.

Screenshot Reference:



```
C:\Users\abij9\Downloads\Comae-Toolkit-v20230117\x64>certutil -hashfile \Users\abij9\Downloads\drive1.E01 MD5
MD5 hash of \Users\abij9\Downloads\drive1.E01:
2ccfa510ee28712b01544594f4fad721
CertUtil: -hashfile command completed successfully.

C:\Users\abij9\Downloads\Comae-Toolkit-v20230117\x64>certutil -hashfile \Users\abij9\Downloads\drive1.E01 SHA1
SHA1 hash of \Users\abij9\Downloads\drive1.E01:
2baa0524e34a684e615061829b21d6b33cd906f8
CertUtil: -hashfile command completed successfully.
```

---

2. Memory Acquisition

Dump File: DESKTOP-VKNOGBH-20250423-202632.dmp
Location: C:\Users\abij9\Downloads\

Hash Verification:

- MD5: `56948ede7b2ac9d60aafc09268be62be5`
- SHA1: `f93382ba4b300c0ab423217bf9769e03f7b546c`

Tool Used: DumpIt by Comae Toolkit v20230117
Execution: Run as Administrator to capture a full physical memory dump. File was saved in the local directory.

Verification Method: Hashes were verified using `certutil` commands in Command Prompt.

```
C:\Users\abij9\Downloads\Comae-Toolkit-v20230117\x64>certutil -hashfile DESKTOP-VKNOGBH-20250423-202632.dmp MD5
MD5 hash of DESKTOP-VKNOGBH-20250423-202632.dmp:
56948ede7b2ac9d60aafc09268b62be5
CertUtil: -hashfile command completed successfully.

C:\Users\abij9\Downloads\Comae-Toolkit-v20230117\x64>certutil -hashfile DESKTOP-VKNOGBH-20250423-202632.dmp SHA1
SHA1 hash of DESKTOP-VKNOGBH-20250423-202632.dmp:
f93382ba4b300c0ab423217bf95769e03f7b546c
CertUtil: -hashfile command completed successfully.
```

---

3. Write-Blocking Mechanism

Approach: Since disk acquisition was not performed manually (image file was provided), direct write-blocking was not needed. Evidence was handled in FTK Imager in read-only mode to simulate write-blocking. No modifications were made to the source image file.

---

4. Summary Table

Evidence Type	Tool Used	Hash Type	Hash Value	Notes

Disk Image	FTK Imager	MD5	2ccfa510ee28712b01544594f4ad721	Mounted in read-only mode
Disk Image	FTK Imager	SHA1	2baa0524e34a684e615061829b21d6b33cd906f8	Verified via CertUtil
Memory Dump	DumpIt	MD5	56948ede7b2ac9d60aafc09268be62be5	Dumped using DumpIt with Admin rights
Memory Dump	DumpIt	SHA1	f93382ba4b300c0ab423217bf9769e03f7b546c	Verified via CertUtil

---

5. Tools and System Info

- **FTK Imager Version:** 4.7.3.81
- **DumpIt Version:** 20230117 x64
- **System:** Windows 10, Hostname: DESKTOP-VKNOGBH