

FORENSIC REPORT

Case Title: Unauthorized Access Investigation

Case ID: CASE-2025-001

Examiner: ABIGAIL JUNG!!!

Date of Analysis: May 21, 2025

Tool Used: AccessData FTK Imager

Evidence Image: drive2.E01

Partition: NONAME [ext4]

File System: EXT4

Evidence Source: Suspect's USB Drive

Hash Validation: MD5/SHA1 - Verified during acquisition

1. Case Summary

This investigation involves the analysis of a USB drive suspected of being used in unauthorized access to a secure system. A forensic disk image (drive2.E01) was analyzed using FTK Imager to identify suspicious files, hidden data, and system anomalies.

2. Methodology

- The .E01 image was loaded into FTK Imager.
- File tree, metadata, slack space, and unallocated space were reviewed.
- System32 and Windows directories were analyzed for unauthorized binaries.
- Unallocated space was examined for deleted or fragmented data.
- Screenshots and logs were captured throughout the analysis.
- Chain of custody was maintained with hash validation and secure storage.

3. Evidence Structure Overview

- Found log/config files: Enterprise.xml, PPRO.log, FileSlack, Starter.xml.
- Some log files contain slack space with remnants of deleted data.
- May contain installation or system manipulation records.

The screenshot shows the FTK interface with the 'Evidence Tree' on the left and the 'File List' on the right. The 'Evidence Tree' shows a directory structure for 'drive2.E01' with a selected path of 'NONAME [ext4] /root /Windows'. The 'File List' displays a table of files and directories with columns for Name, Size, Type, and Date Modified. The files listed include system32, DPINST.LOG, DtdInstall.log, Enterprise.xml, msdfmap.ini, msdfmap.ini.FileSlack, PPRO.log, PPRO.log.FileSlack, setupact.log, setuperr.log, Starter.xml, system.ini, and TSysprep.log. The 'Hex View' at the bottom shows a hex dump of the selected file, with a cursor position of 0; dms = 4096; log sec = 32768.

Name	Size	Type	Date Modified
system32	4,096 (4 KB)	Directory	10/7/2015 4:47:38 PM
DPINST.LOG	4,098 (5 KB)	Regular File	1/19/2012 7:21:10 PM
DtdInstall.log	1,774 (2 KB)	Regular File	11/23/2011 4:13:36 PM
Enterprise.xml	53,555 (53 KB)	Regular File	6/10/2009 9:14:32 PM
msdfmap.ini	1,405 (2 KB)	Regular File	6/10/2009 9:19:28 PM
msdfmap.ini.FileSlack	2,691 (3 KB)	File Slack	
PPRO.log	22,260 (22 KB)	Regular File	8/14/2015 3:10:16 AM
PPRO.log.FileSlack	2,316 (3 KB)	File Slack	
setupact.log	62,472 (62 KB)	Regular File	10/7/2015 3:50:40 PM
setuperr.log	0 (0 KB)	Regular File	7/14/2009 4:39:10 AM
Starter.xml	48,201 (48 KB)	Regular File	6/10/2009 9:14:46 PM
system.ini	219 (1 KB)	Regular File	6/10/2009 9:46:30 PM
TSysprep.log	1,313 (2 KB)	Regular File	11/23/2011 4:14:44 PM

◆ C. Unallocated Space

- FTK identified multiple large fragments of unallocated space (up to 100+ MB each).
- Indicates significant deletion activity.
- These blocks may contain recoverable files or evidence remnants.

The screenshot shows the FTK interface with the 'Evidence Tree' on the left and the 'File List' on the right. The 'Evidence Tree' shows a directory structure for 'drive2.E01' with a selected path of 'NONAME [ext4] /root /Windows'. The 'File List' displays a table of unallocated space blocks with columns for Name, Size, Type, and Date Modified. The blocks listed include 004099, 022564, 033088, 058688, 069633, 095233, 098369, 123969, 149569, 163905, 189505, 215105, 229441, and 255041. The 'Hex View' at the bottom shows a hex dump of the selected file, with a cursor position of 0; dms = 4096; log sec = 32768.

Name	Size	Type	Date Modified
004099	75,628,544 (73,856 KB)	Unallocated Space	
022564	41,799,680 (40,820 KB)	Unallocated Space	
033088	104,857,600 (102,400 KB)	Unallocated Space	
058688	28,053,504 (27,396 KB)	Unallocated Space	
069633	104,857,600 (102,400 KB)	Unallocated Space	
095233	12,582,912 (12,288 KB)	Unallocated Space	
098369	104,857,600 (102,400 KB)	Unallocated Space	
123969	104,857,600 (102,400 KB)	Unallocated Space	
149569	58,458,112 (57,088 KB)	Unallocated Space	
163905	104,857,600 (102,400 KB)	Unallocated Space	
189505	104,857,600 (102,400 KB)	Unallocated Space	
215105	58,458,112 (57,088 KB)	Unallocated Space	
229441	104,857,600 (102,400 KB)	Unallocated Space	
255041	258,048 (252 KB)	Unallocated Space	

5. Hash Verification & Integrity

- Image was verified using FTK Imager's built-in hash utility.
- Both MD5 and SHA-1 values matched during import.
- No signs of image tampering or corruption observed.

6. Chain of Custody

Step	Description	Responsible Party	Timestamp
1	Image acquired from USB using FTK Imager	Abigail Jung	2025-05-20 10:00 AM
2	Image stored in evidence locker with write protection	Abigail Jung	2025-05-20 10:15 AM
3	Image loaded for analysis in FTK	Abigail Jung	2025-05-21 09:00 AM

7. Conclusion

- **Malicious Activity Suspected:** Presence of suspicious executables and hidden file slack suggest tampering.
- **Data Hiding Evidence:** Slack files and large unallocated spaces support possible file wiping/hiding.
- **Next Steps:** Perform data carving on unallocated space. Conduct deeper malware analysis on ndadmin.exe.

8. Appendix

- Screenshots of file structures and key artifacts.
- FTK log output (if available).
- MD5/SHA-1 hashes for verification.
- Tool versions and configuration settings.