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

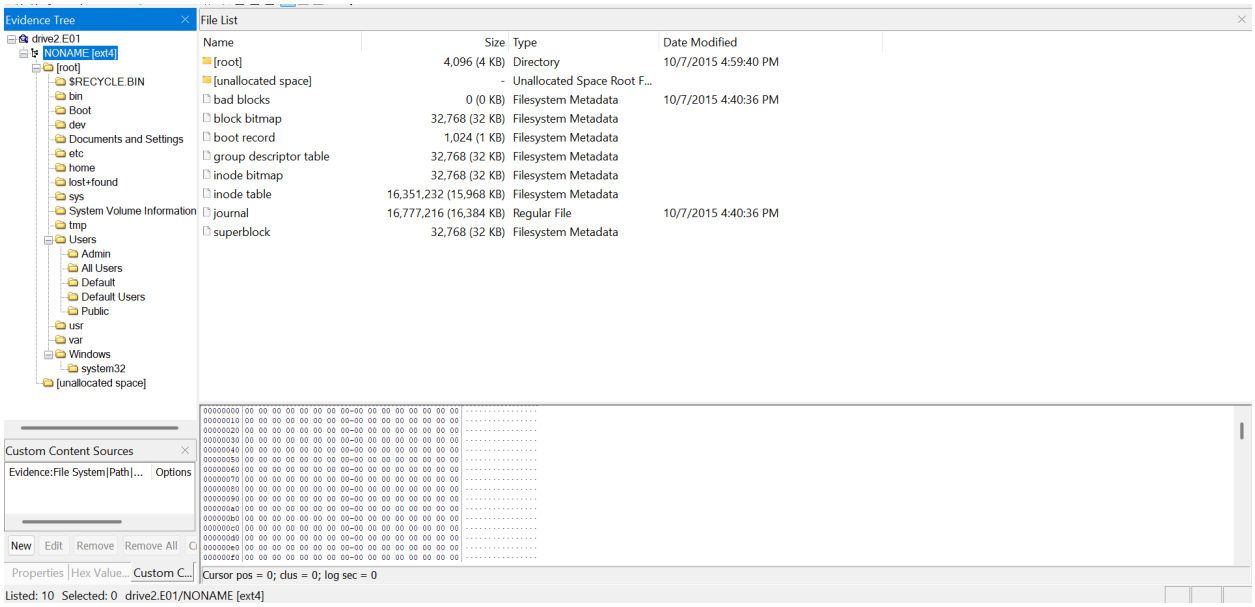
1. Case Summary

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.

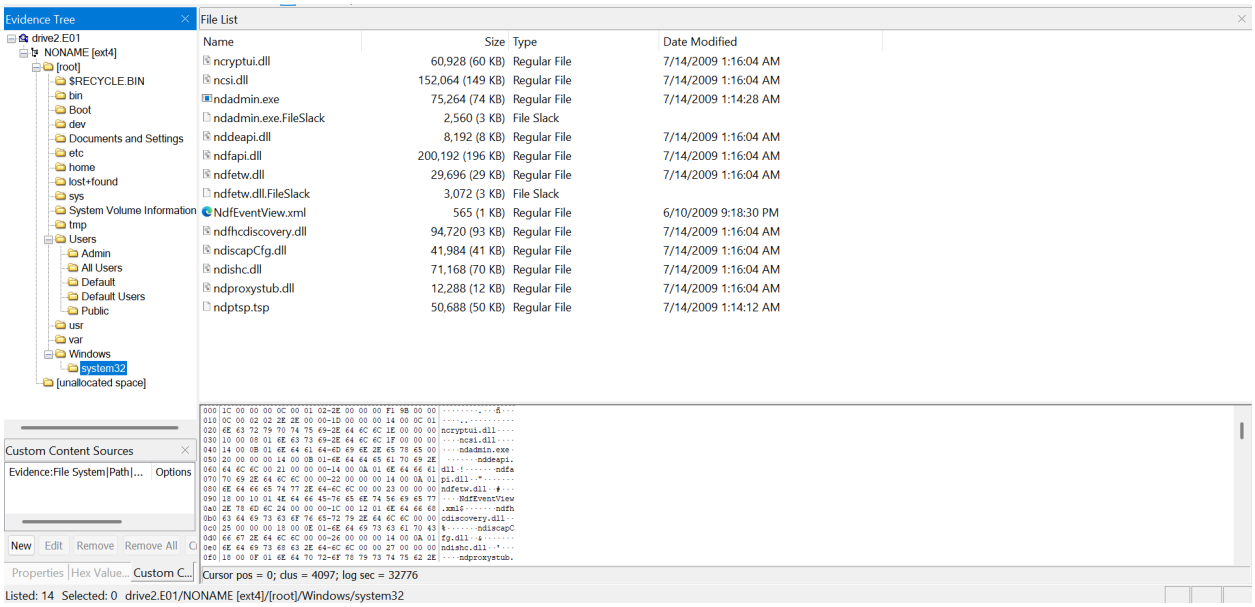
3. Evidence Structure Overview



4. Key Findings

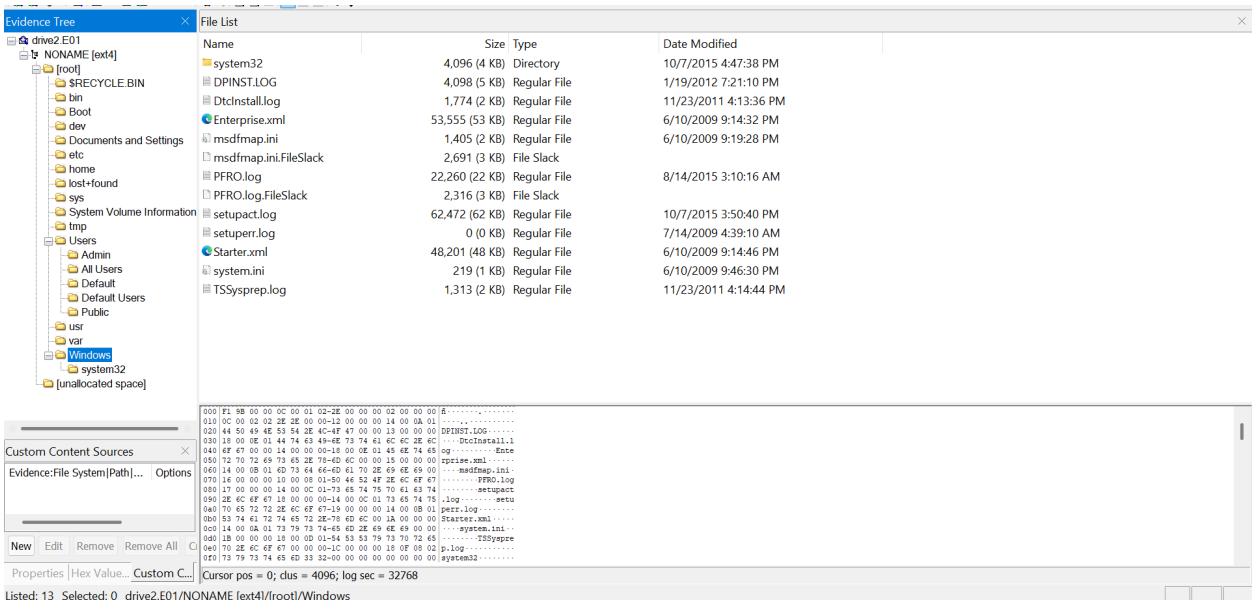
A. Suspicious Executables in system32

- Files such as ndadmin.exe, ndadmin.exe.FileSlack, ndfapi.dll, and ncsi.dll were discovered.
- Modified timestamps: **7/14/2009 1:16:04 AM** — may be spoofed.
- File slack entries indicate hidden payloads or residue from overwritten files.



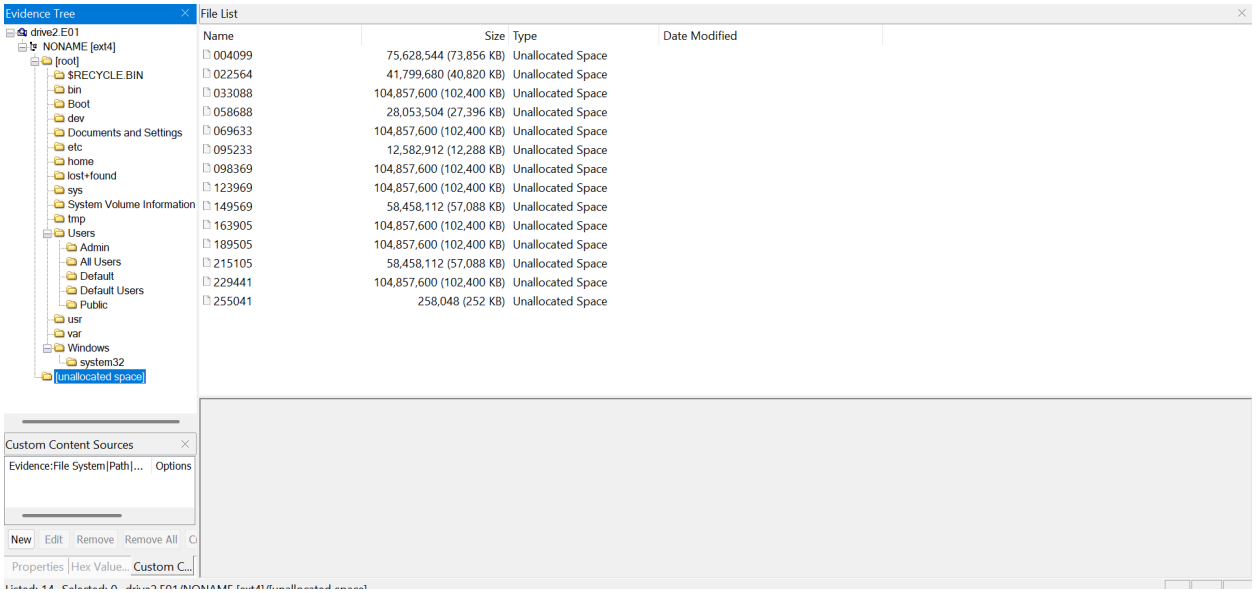
B. Logs and Configs in Windows Folder

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



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.



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.