

Assignment 5.1: Understanding Digital Evidence

Joshua A. Wortz

University of San Diego

CSOL-590

Prof. Fulton

02/09/2026

Part 1: Research

Definition and Importance of Digital Evidence

Digital evidence is defined as any data of investigative value that is stored or transmitted in binary form. Recognizing its importance helps forensic analysts feel assured in the reliability of their work when reconstructing the 'cyber-attack lifecycle.' This evidence is essential for attribution, scope assessment, and timeline reconstruction (Skulkin, 2022).

Phases of a Ransomware Attack

Modern ransomware attacks are complex, multi-stage operations that often focus on post-exploitation activities rather than immediate encryption. The core phases include initial access, privilege escalation, reconnaissance, credential harvesting, lateral movement, data exfiltration, and finally, ransomware deployment, each critical for understanding the attack progression (Skulkin, 2022).

1. **Initial Access:** The adversary gains a foothold via phishing, software vulnerabilities, or compromised RDP credentials.
2. **Post-Exploitation:** Privilege Escalation: Elevating rights to Admin or SYSTEM level to access protected areas.
 - **Reconnaissance:** Scanning the network and Active Directory using tools like AdFind to map assets.
 - **Credential Access:** Harvesting password hashes and Kerberos tickets from LSASS memory.
3. **Lateral Movement:** Navigating through the network using legitimate protocols like SMB or RDP.

4. **Data Exfiltration:** Moving sensitive data to an attacker-controlled server, often referred to as "double-extortion."
5. **Ransomware Deployment:** The final encryption of files and presentation of the ransom note.

Common Types of Digital Evidence

Investigators find digital evidence in both volatile and persistent storage locations. These include memory artifacts such as NTLM hashes and Kerberos tickets, file system metadata such as Master File Table (\$MFT) timestamps, and registry hives such as Amcache and Shimcache. Furthermore, investigators also source digital evidence from relevant log files, specifically Windows Event IDs 4688 and 4624 (NCyTE, 2026).

- **Log Files:** Critical records include Windows Event IDs 4688 (Process Creation) and 4624 (Logon Events).
- **Registry Hives:** Files such as the Amcache track program execution details, while the Shimcache stores metadata about executable files to improve compatibility (NCyTE, 2026).
- **Memory Artifacts:** RAM contains volatile data like NTLM hashes, Kerberos tickets, and active network connections.
- **Filesystem Metadata:** The Master File Table (\$MFT) provides timestamps (MACB) for file creation and modification.

Principles of Handling and Preserving Digital Evidence

Maintaining the integrity of evidence is critical for legal and corporate admissibility.

- **Volatility Management:** Responders must prioritize collecting data in RAM, as memory-resident malware is lost upon system reboot (Plunkett, 2026).
- **Integrity Protection:** Hashing (MD5, SHA256) ensures that the evidence remains unchanged. Hardware write blockers are used during imaging to prevent any data from being written back to the source (Plunkett, 2026).
- **Chain of Custody:** A chronological record must be maintained, documenting who held the evidence and for what purpose to prevent tampering.

Part 2: Case Study Analysis

Incident Summary: Sandworm Team (Ukraine Power Grid)

In 2016, the Russian-linked Sandworm Team conducted a high-profile attack on the Ukrainian power grid. This case illustrates the complex forensic challenges professionals face when analyzing lateral movement and credential compromise in real-world cyberattacks, thereby fostering respect for their expertise.

Digital Evidence Involved

Several types of evidence were crucial in analyzing the Sandworm incident:

- **Credential Dumping Artifacts:** Forensics identified the use of Mimikatz to dump LSASS process memory. Even if the tool was deleted, traces remained in the Amcache.hve registry hive.
- **Active Directory Databases:** Attackers used the Windows utility ntdsutil.exe to create backups of the ntds database. This file contains all domain hashes.
- **PowerShell Console History:** This revealed how the group used fileless techniques to load malicious scripts directly into memory.

Challenges in Handling and Comparing Evidence

The Sandworm case highlights significant forensic challenges:

1. **Contextual Noise:** The use of "Living off the Land" Binaries (LoLBins), such as `ntdsutil.exe`, made it difficult to distinguish legitimate system maintenance from malicious activity.
2. **Invisibility of Memory Attacks:** Since many tools were loaded reflectively via PowerShell, traditional disk-based scans found no malicious executables.
3. **Timestomping:** The attackers manipulated MACB timestamps to hide their activity within the filesystem, requiring analysts to cross-reference multiple artifacts (such as the \$MFT and the Registry) to identify discrepancies.

References

Skulkin, O. (2022). Incident Response Techniques for Ransomware Attacks. Packt Publishing.

<https://usd.vitalsource.com/books/9781803233994>

Google. (2026). *Gemeini* (Gemini 3 Flash) [LLM]. <https://gemini.google.com/>

National Cybersecurity Training & Education Center (NCyTE). (2026). *Module 5 (M5) glossary terms*.

Plunkett, T. (2026). *Presentation 5.1: Computer forensics tools* [Transcript]. University of San Diego.