Collin Williams

Reading Assignment 1

Incident Response and Handling (`ITSY-2442-007`)

Brian Stuhl

Explain various techniques used to collect non-volatile information from Windows-based systems.

Non-volatile information is “persistent data that [is] not lost in the event of system crash or power off. This information generally resides in the internal hard disk, flash drive, or external hard disk of the system. From a forensic perspective, it reveals valuable artifacts such as information contained in Windows registry, file systems, database files, external devices connected to the system, and hidden partition information” (EC-Council, 2016).

Non-hidden Non-volatile Data

Non-hidden non-volatile data refers to the information that is immediately accessible and visible to the operating system and the user. This primarily includes active files and directories, such as documents, photos, installed programs, and database files (like those used by web browsers or email clients) that have not been deleted.

Hidden Non-volatile Data

Hidden non-volatile data is information that is persistent on the disk but is not immediately viewable through standard operating system functions. Recovering this category of data often provides the most crucial evidence regarding a user’s intent and history. Techniques for collecting and interpreting hidden data focus on artifacts, metadata, and unused space on the disk. One of the most valuable sources of hidden information on a Windows system is the Windows Registry. While the registry itself is essential for the operating system, many of the keys and values are not meant to be seen or modified by the average user. Specialized parsing tools are used to collect and analyze the individual registry hives (like NTUSER.DAT). Analysis of the these hives can reveal data regarding recently executed programs, the history of files accessed, and connections of external devices (Triage, 2025).

The forensic process must combine the complete acquisition of non-hidden data via disk imaging with the targeted logical analysis of hidden artifacts to build a comprehensive case.

Bibliography

EC-Council. (2016). *Computer forensics: Investigation procedures and response (CHFI)* (11th ed., p. 481). Cengage Learning.

Triage, C. (2025,). *NTUSER.DAT Forensics Analysis 2025.* https://www.cybertriage.com/blog/ntuser-dat-forensics-analysis-2025/