Collin Williams

Reading Assignment 1

Incident Response and Handling (ITSY-2442-007)

Brian Stuhl

What are the challenges to forensics from anti-forensics? Explain various countermeasures to defeat anti-forensics techniques.

There are a couple ways that anti-forensic techniques can impede forensic analyses. While some anti-forensic measures are rudimentary and easy to defeat, others pose serious barriers to data recovery and analysis. The primary challenges include rudimentary deletion, and sophisticated data hiding techniques.

Recycle Bin Forensics

A standard way that individuals attempt to prevent Forensic Analysts from accessing their data is by deleting it. Unfortunately for that individual, the operating system does not actually delete the data immediately. “When a user deletes a file, the OS does not actually delete the file, but marks the file entry as unallocated in the master file table (MFT) and allocates a special character. This indicates that the space is ready for use” (EC-Council, 2016) Critically, this means the raw data remains physically present until it is overwritten.

The primary countermeasure to this anti-forensic attempt is analyzing unallocated space and leveraging file system artifacts. Forensic tools can scan the unallocated clusters for file headers and footers (known as file carving) to reconstruct files. Furthermore, specific Recycle Bin artifacts, such as the `$I` and `$R` files in modern Windows systems, contain crucial metadata, including the original file name, path, and the exact date and time of deletion, effectively defeating this simple anti-forensics tactic.

Data Hiding (Steganography)

Data Hiding is an anti-forensic technique where data is concealed within non-suspicious files, a practice known as steganography. One example of Steganography is hiding data in images. “In digital steganography, images are often used to conceal information because there are a large number of elements within the digital representation of an image, and there are various ways to hide information inside an image” (Kaspersky, 2023). The challenge is not recovering lost data, but proving that hidden data exists in the first place, as the carrier file appears normal.

Countermeasures to steganography are primarily analytical. Forensic tools employ statistical analysis to detect anomalies, such as deviations in file entropy or patterns that suggest embedded data. Signature analysis compares the actual content of a file against its header signature (e.g., checking if a file labeled .jpg contains the signature of an appended .zip file).

Bibliography

EC-Council. (2016). *Computer forensics: Investigation procedures and response (CHFI)* (11th ed., p. 389). Cengage Learning.

Kaspersky. (2023, February). *What is steganography? Definition and explanation.* https://www.kaspersky.com/resource-center/definitions/what-is-steganography