5-2 Journal: Anti-Forensics

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

27 November 2024

Anti-forensics refers to the deliberate use of techniques and tools to obstruct forensic investigations and hinder the discovery of digital evidence. These methods are employed by adversaries to avoid detection, disrupt evidence collection, or delay an investigation, making it harder to link activities to the perpetrator. The main goals of anti-forensics include avoiding detection, increasing the time required for forensic analysis, and casting doubt on the reliability of findings (Garfinkel, 2007). For instance, by manipulating metadata, adversaries can create confusion about when or how specific files were accessed. A real-world example involves attackers using timestamping tools like "Touch" to alter file creation and modification dates, tricking investigators into misinterpreting the timeline of events. Additionally, these techniques often seek to exploit or bypass digital forensic tools, frustrating the efforts of investigators (Garfinkel, 2007). Anti-forensic techniques are not only technical barriers but strategic methods to undermine the effectiveness of forensic processes, ensuring the attackers' tracks remain concealed.

One common anti-forensic technique is data wiping, which involves securely erasing files or even entire drives to make data irretrievable. Drive Wiper and File Shredder actively overwrite data multiple times, preventing its recovery with conventional forensic tools (EC-Council, 2022). The "SDelete" utility from the Sysinternals suite securely overwrites free space on a drive to prevent the recovery of deleted files. Another technique is timestamping, where attackers alter file metadata to mislead investigators about a file's creation or modification time. For instance, an attacker might modify timestamps using tools like "Timestamp" to make files appear older than the attack itself, misleading forensic experts and delaying the investigation (Perlman, 2024). Encryption is also a frequently used method, where attackers transform files into unreadable formats, making access impossible without the correct decryption key. An

example is ransomware attacks, where attackers encrypt entire systems and demand payment for decryption keys, effectively blocking investigators from accessing crucial evidence (EC-Council, 2022). These techniques demonstrate how anti-forensics can significantly obstruct investigative processes.

Lastly, advanced methods like steganography and virtual machines complicate forensic investigations further. Steganography involves hiding malicious data within benign files, such as images or videos, making detection extremely challenging (Perlman, 2024). For example, tools like "Stego Watch" can embed harmful code within a seemingly innocent .jpeg file, allowing attackers to exfiltrate data covertly. Virtual machines allow attackers to execute malicious activities in isolated environments, leaving minimal or no traces on the host system (Garfinkel, 2007). For instance, attackers often deploy a virtual machine to perform illegal activities and delete the virtual environment afterward, leaving almost no evidence on the host computer. These methods reduce the digital footprint left behind and make it harder to track adversaries. The use of these sophisticated techniques underscores the importance of continuous advancements in forensic tools and training to counter anti-forensic strategies. As attackers develop increasingly innovative techniques, forensic investigators must actively implement proactive measures to detect and dismantle these barriers, ensuring they stay ahead and justice prevails.

References:

Ec-Council. (2022, March 24). *Five Anti-Forensic techniques used to cover digital footprints*. Cybersecurity Exchange. Retrieved November 27, 2024, from https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/anti-forensic-techniques-used-to-cover-digital-footprints/

Garfinkel, S. L. (2007). Anti-Forensics: Techniques, detection and countermeasures. In *Naval Postgraduate School*. Retrieved November 27, 2024, from https://pdfs.semanticscholar.org/b0c0/275024deb3660928d57c2220ab643993db11.pdf

Perlman, A. (2024, September 3). *Anti-Forensics techniques*. All-in-One Cybersecurity Platform - Cynet. Retrieved November 27, 2024, from https://www.cynet.com/attack-techniques-hands-on/anti-forensics-techniques/