Collin Williams

Week 1 Reading Assignment 1

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

Brian Stuhl

In today’s digital world, where information is constantly being created, shared, and stored electronically, the need for computer forensic investigators has become increasingly critical. As cybercrime continues to rise and digital evidence becomes central to both criminal and civil cases, organizations and law enforcement agencies rely heavily on these professionals to uncover the truth hidden within digital systems.

The Need for Computer Forensic Investigators

The digital age has brought countless benefits but also a surge in cyber threats like hacking, identity theft, data breaches, financial fraud, and online harassment. According to a recent global report by LexisNexis Risk Solutions, the global digital attack rate increased 20% year over year in 2022 compared to 2021, showing that digital fraud and cyber-attacks are growing rapidly (O’Connor, 2023). Criminals often use sophisticated technologies to commit or cover up their crimes, leaving behind digital footprints. This is where a computer forensic investigator becomes essential.

Computer forensic investigators are trained to recover, analyze, and preserve digital evidence from computers. Their work ensures that vital information is not lost, tampered with, or destroyed and that it can be presented in court as credible and admissible evidence.

Roles and Responsibilities of a Computer Forensic Investigator

One of the most critical responsibilities of a computer forensic investigator is the collection and preservation of digital evidence. This process involves identifying, securing, and duplicating data from electronic devices—including hard drives, USBs, mobile devices—while preserving the integrity of the original information. Investigators use specialized tools to create exact forensic images to avoid alteration, and follow rigorous chain-of-custody procedures so evidence can be trusted in legal proceedings. For example, Granja & Rodríguez found that many digital preservation models lack sufficient measures for metadata management, audit trails, or protection against human error, which can lead to digital evidence being ruled inadmissible if these integrity standards are not met (Granja & Rafael, 2017).

Another core responsibility is the analysis and interpretation of recovered data. Once the digital evidence is collected, the investigator have to sift through lots of information to find relevant artifacts, like deleted files, internet history, or system logs. This analysis requires technical expertise and an understanding of how digital behaviors align with criminal or suspicious activities. The findings must be documented clearly and may be presented in court, where the investigator could be called to explain their methods and conclusions as an expert witness.

Bibliography

Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1–18. https://doi.org/10.1504/IJESDF.2017.081749

O'Connor, A. (2023, May). *LexisNexis Risk Solutions Cybercrime Report Reveals 20% Annual Increase in Global Digital Attack Rate*. https://risk.lexisnexis.com/about-us/press-room/press-release/20230517-cybercrime-report