Topic 4 Discussion 2

Research how network-connected devices, such as a smartphone, can be used in a network forensics investigation. Discuss at least two cases.

Hello Class,

Network-connected devices, particularly smartphones, play a crucial role in network forensics investigations. These devices can provide valuable data that helps investigators understand network breaches, track malicious activities, and gather evidence for legal proceedings.

Data Collection - Smartphones store a wealth of information, including call logs, text messages, emails, and app data. This data can be analyzed to trace communications and interactions related to a cybercrime(EC-Council, 2024). For instance, network forensics can involve examining the metadata of messages sent or received during a specific timeframe to identify potential suspects or accomplices.

Network Traffic Analysis - Smartphones often connect to various networks, making them a source of network traffic data. By analyzing the traffic generated by a smartphone, investigators can identify unusual patterns that may indicate unauthorized access or data exfiltration(Forensic Focus, 2023). This analysis can reveal the IP addresses of external servers the device communicated with, which is critical in tracing the origin of an attack.

Notable Cases

The BTK Killer Case - In this infamous case, the investigation utilized digital forensics to analyze the suspect's communications. The BTK Killer, who evaded capture for decades, was ultimately apprehended partly due to evidence gathered from his computer and smartphone, which revealed his online activities and connections to the crimes(Notable Cases, n.d.).

The Craigslist Killer - This case involved a suspect who used his smartphone to communicate with victims. Investigators analyzed the phone's call logs and text messages, which provided crucial evidence linking him to the crimes. The data helped establish a timeline and corroborate witness statements, leading to his conviction(Eclipse Forensics, 2021).

References:

EC-Council. (2024, March 20). *What Is Network Forensics? How to Successfully Examine the Network*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-network-forensics/

Eclipse Forensics. (2021, July 1). *3 Famous Cases Solved Through Digital Forensics*. Eclipse Forensics. https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/

Forensic Focus. (2023, June 28). *Types Of Devices Examined In Digital Forensics Investigations - Forensic Focus*. Forensic Focus. https://www.forensicfocus.com/articles/types-of-devices-examined-in-digital-forensics-investigations/

*Notable Cases | Digital Forensics Crime lab | Utah Tech University*. (n.d.). Dfcl.utahtech.edu. https://dfcl.utahtech.edu/notable-cases/

Srinivas. (2021, January 18). *Sources of network forensic evidence | Infosec*. Www.infosecinstitute.com. https://www.infosecinstitute.com/resources/digital-forensics/sources-of-network-forensic-evidence/