5-3 Project Two Stepping Stone: Digital Forensic Investigation Exploration

Joshua Merren

Southern New Hampshire University

CYB 320: Incident Response and Investigation

Professor Noah Nicholls

27 November 2024

In the digital forensic investigation of Max Ray Butler's case, two primary assets are crucial: Butler's computing devices and the financial institutions' networks he breached. On Butler's devices, investigators should examine stored files, communication logs, and software tools used for hacking activities, ensuring the evidence points to his direct involvement in the cybercrimes. Additionally, network logs from financial institutions such as Citibank and Pentagon Federal Credit Union are critical. These logs can reveal unauthorized access patterns, including specific IP addresses and timestamps of suspicious activities (Obbayi, 2024). Investigators should also look for unusual user behaviors or attempts to bypass firewalls and security systems. For example, if Butler used tools to steal and sell credit card information on his platform, CardersMarket, the network logs can link unauthorized access to his online accounts and fraudulent transactions. Searching for encrypted files and hidden partitions on Butler's devices is equally essential, as these could contain sensitive data or evidence of his illicit activities. This comprehensive approach leaves no critical information overlooked, enhancing the likelihood of a successful prosecution.

The investigation relies on hardware and software tools to collect evidence securely and without compromise. Hardware write blockers are essential to prevent data alteration when imaging storage devices. Software tools like Autopsy and Sleuth Kit can analyze file systems, recover deleted data, and extract hidden files (Team, 2023). For instance, Autopsy's graphical interface allows investigators to identify metadata related to stolen credit card files, ensuring quick analysis. Additionally, FTK Imager can be used to create forensic images, ensuring evidence preservation and authenticity (CISA, 2021). Tools like X-Ways Forensics are ideal for deep data recovery, offering detailed reporting features supporting legal proceedings. If Butler's operation involved smartphones for communication or data storage, investigators could actively deploy mobile forensic tools like Cellebrite. These tools provide a robust framework for analyzing a wide range of digital evidence, which is critical in complex cases involving multiple devices and networks.

Individuals must strictly follow documentation and handling protocols to maintain the chain of custody. Evidence collection begins with tagging items and recording details such as timestamps, locations, and collector information (GeeksforGeeks, 2020). Each evidence transfer should be logged, including signatures from all personnel involved, ensuring an unbroken trail of accountability. For instance, if a hard drive containing stolen credit card data is retrieved, investigators should document its condition, photograph it, and store it in a tamper-proof bag. Log any analysis performed to ensure transparency and maintain the investigation's integrity (CISA, 2021). Using tamper-evident seals and serialized tracking numbers can further bolster the process by minimizing the risk of unauthorized access. Periodically audit the chain of custody records to identify and address discrepancies early. These precautions collectively protect the credibility of the evidence, ensuring it remains admissible in court and reliable for internal decision-making processes.

A systems-thinking mindset enables forensic investigators to understand the interconnected components of digital ecosystems. This approach helps anticipate how adversaries exploit system vulnerabilities and hide evidence. For instance, understanding the relationship between Butler's devices, the CardersMarket website, and the financial institutions he targeted reveals how he operated within the system to execute his fraud (Guttman et al., 2022). Systems thinking also enables investigators to predict adversarial tactics, such as using encryption to obscure data trails or exploiting network vulnerabilities to bypass detection. By examining the broader ecosystem, investigators can identify indirect evidence, such as suspicious communication patterns between Butler and his accomplices. This mindset enables a proactive approach to uncover hidden links and anticipate potential countermeasures that might block the investigation. As digital systems grow increasingly complex, adopting this perspective is essential for developing strong investigative strategies and uncovering comprehensive evidence.

Data integrity is essential in digital forensic investigations because any alteration can render evidence inadmissible in court. If investigators altered metadata on stolen credit card files during the investigation, the defense could claim tampering and undermine the prosecution's case. Ensuring data integrity involves creating forensic images and conducting hash tests to verify that evidence remains unchanged (Obbayi, 2024). Investigators should use tools like FTK Imager to create bit-by-bit copies, preserving the original data for comparison during legal proceedings (Team, 2023). Additionally, the use of sterilized storage devices for transferring evidence minimizes the risk of contamination. Documenting every step of the analysis process ensures transparency and builds trust in the evidence presented. These practices strengthen the legal case and enhance the credibility of forensic investigations in non-legal scenarios, such as internal audits and compliance reviews.

The chain of custody ensures evidence is authentic, untampered, and admissible in legal proceedings. It involves documenting every interaction with the evidence, from collection to presentation in court. For example, if investigators fail to log who accessed a USB drive containing crucial files, the defense could argue that the evidence was compromised, jeopardizing the case. Following established protocols, such as using tamper-evident bags and secure storage, protects the credibility of the evidence (CISA, 2021). Courts often require detailed documentation, including timestamps, personnel identities, and the purpose of each evidence transfer, to ensure accountability (GeeksforGeeks, 2020). Regularly auditing chain-of-custody records adds another layer of security by identifying potential gaps or irregularities. Sticking to these standards ensures that the investigative process is defensible, the findings are reliable, and the evidence holds up under scrutiny during trials or corporate investigations.

References

CISA. (2021). CISA Insights. In *CISA Insights* [Report]. Retrieved November 27, 2024, from https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

GeeksforGeeks. (2020, June 2). *Chain of custody digital forensics*. GeeksforGeeks. Retrieved November 27, 2024, from https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/

Guttman, B., White, D. R., Software & Systems Division, & Walraven, T. (2022). Digital Evidence Preservation: Considerations for Evidence Handlers. In U.S. Department of Commerce, National Institute of Standards and Technology, G. M. Raimondo, & L. E. Locascio, *NIST Interagency Report*. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf

Obbayi, L. (2024, March 4). *Computer forensics: Chain of custody [updated 2019]*. Infosec Institute. Retrieved November 27, 2024, from https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-chain-custody/

Team, C. W. (2023, November 11). 10 Best Digital Forensic Investigation Tools - 2024. *Cyber Security News*. Retrieved November 27, 2024, from https://cybersecuritynews.com/free-forensic-investigation-tools/