Hard Drive and Tools Follow-Up Questions

Ramon Lopez Jr

Department of Cyber Security, University of Advancing Technology

CFR101: Computer Forensic Essentials

Professor Aaron Rodriguez

October 23rd, 2022

Hard Drive and Tools Follow-Up Questions

In digital forensics, incident response teams must be able to extract and analyze data from a system's hard drive. Specialized tools exist to support this process, but their use requires careful planning, proper procedure, and legal considerations. Accurate data extraction is essential for identifying malicious activity, preserving evidence, and ensuring admissibility in court.

Steps and Considerations for Imaging a Hard Drive

Imaging a hard drive is a critical process that ensures data is preserved in its original state. The procedure begins by powering down the target system and booting into a forensic imaging environment. An imager or forensic workstation is then connected to duplicate the drive. Key steps in the imaging process include:

- Using write-blocking hardware to prevent alterations to the original data.
- Selecting an appropriate format such as the Advanced Forensic Format (AFF).
- Segmenting and saving the source drive into AFF image files.
- Generating and preserving hash values to verify the integrity of both the original and duplicated drives.

One major consideration during imaging is the operational status of the device. If the system is offline (also known as "static acquisition"), hash values can be used to ensure that no changes have occurred during imaging. However, any failure to properly hash or log data may raise concerns over evidence validity.

Validating New Forensic Tools

Before using any new forensic tool in an investigation, validation is essential. A forensic tool should meet the following criteria:

- Accurately account for all accessible data.
- Create a complete and verifiable copy of the original media.
- Handle read errors without failing (e.g., by logging issues and inserting placeholders).
- Avoid modifying any original data during operation.
- Generate comprehensive, third-party verifiable reports.
- Maintain error logs and detailed activity records.

Unvalidated tools can compromise evidence integrity and may be challenged in legal proceedings, making this step a foundational requirement.

Identifying FTP Traffic in PCAP Files

Packet Capture (PCAP) files can contain vast amounts of network data across multiple sessions. To identify **FTP traffic**, investigators can filter for communications on:

- **Port 21** – used for FTP commands.
- **Port 20** – used for FTP data transfers.

FTP traffic is relatively easy to spot by reviewing command strings and inspecting source/destination ports.

Are Network Services Critical in an Investigation

Network services are critical in forensic investigations because they leave behind detailed audit trails. Devices such as:

- **Routers**
- **Firewalls**
- **Intrusion Detection Systems (IDS)**
- **Servers**

…generate logs that document traffic, events, and user behavior.

For example, **DHCP servers** log each IP assignment to a specific MAC address at a given time. These logs can help determine which device held a certain IP address during a suspected incident. If DHCP logs are unavailable, analysts can search for the MAC address across logs to trace its activity over time. Identifying which services and applications are active on a system often relies on analyzing system and event logs. Useful identifiers include:

- **Event ID Codes**: Categorize system activity and help pinpoint specific actions or failures.
- **Timestamps**: Record when an event occurred.
- **IP Addresses**: Show the source or destination of network activity.
- **Hostnames**: Identify the devices initiating or receiving communication.
- **MAC Addresses**: Help uniquely identify the physical device on a network.

These elements work together to reconstruct an incident timeline, verify authenticity, and attribute digital actions to specific devices. This assignment highlights several essential components of digital forensic investigations—from imaging hard drives and validating tools to interpreting network traffic and leveraging system logs. Proper procedures, accurate documentation, and the use of validated forensic tools are crucial for conducting credible and legally sound investigations.

References

G, D. (2018, December 19). *What is FTP: File transfer protocol explained for beginners*. Hostinger Tutorials. https://www.hostinger.com/tutorials/what-is-ftp

Pepe, M., Luttgens, J. T., Kazanciyan, R., & Mandia, K. (2014). *Incident response & computer forensics*. Mcgraw-Hill Education.

Pratik. (2019, March 6). *How to Find IP Address of Any Device On Your Network*. TechWiser. https://techwiser.com/find-ip-address-of-any-device/#:~:text=How%20to%20Find%20IP%20Address%20of%20Any%20Device