Quinton Green

Digital Forensics In Cybersecurity — D431

Task 1: Investigative Plan Of Action

The forensic methodologies I will use is from the U.S. Department of Justice. (n.d.). Digital forensic analysis methodology. Computer Crime and Intellectual Property Section and Western Governors University’s Forensics frameworks. I will brief the investigation team on the known information:

Who: John Smith, one of the company’s mechanical engineers of an oil company

What: He allegedly took information that was clearly identified as proprietary.

When: TBD

Where: The Oil Company

Why: The company’s legal office has requested digital evidence regarding the potential violation of company policy, which prohibits the sharing of proprietary information without prior approval. The employee was not authorized to access proprietary information. All employees sign nondisclosure agreements (NDAs) and acceptable use policies (AUPs).

Senior management and the legal office have approved this request with the goal of determining is John Smith accessed and shared proprietary information without approval and violated the company NDA and AUPs

Since the alleged suspect is an employee of the Oil Company, the property and information legally belong to the company. The employee signed policies and agreements which gives the company legal right to monitor and survey its assets that are being used by the employee. No search warrant court order or subpoena is needed because the computer is not personal property of the employee, and the investigation was requested and approved by the company’s senior management and legal team (WGU, 2020). The investigative team will maximize the evidence collected by using collection best practices with finding, preserving, and preparing the evidence. To protect evidence integrity, we will take pictures of all workstation equipment in its current location before transporting it to our forensic laboratory. The equipment will be transported directly from the site to the forensic lab and stored in a locked vault (WGU,2020). We will avoid tampering with the equipment and make a forensic bit level copy to extract the data perform the investigation so that the original equipment is not touched. Chain of custody will be implemented from start to finish to make sure the evidence is permissible in a court of law and complies with the rules of evidence standards. We will try to establish a timeline of file access and sharing, if possible, to put the puzzle pieces together. If the system is still connected to the network, we will remove any ethernet cords to prevent virus contamination or remote wiping.

To minimize impact to the organization we will avoid touching the computer equipment, take photographs at all angles, and disconnect the equipment from the network. If there is malware leaking the information or a logic bomb, disconnecting the device from the company network will prevent other computers from being affected or breached. We will use data extraction tools to create bit level forensic copies to perform the investigation on in FTK and will hash the results.

Data will be collected in the order of volatility: registers and cache, routing tables, ARP cache, process table, kernel statistics and modules, main memory, temporary file systems, secondary memory, router configuration, and network topology (Easttom 2021). The team will use the WHOIS database to trace email servers. If John Smith communicated of shared information via emails, we can discover where they went and obtain email header information. We can check network logs and perform network forensics to analyze packet captures, security logs for any failed log in attempts to access unauthorized files, and sniffers to find suspicious activity (Easttom, 2021).

The forensic tools we will use is FTK. While Encase can present the investigation in case form, using FTK can speed up the forensic analysis process because it can be distributed across three computers and lets them all process and analyze simultaneously. FTK can also examine emails thoroughly and present a timeline of email communications. If John Smith shared any information via email FTK will be able to get exact discussions and times of when the data was shared. FTK is also great at cracking password protected documents like PDF files, scan registries, and give you the ability to create a hash of the evidence to protect the integrity of the findings (Easttom, 2021).

The chain of custody form is the first step in documenting the process from start to finish. We will document who was present during the seizure of the equipment, who transported it, where and when the equipment was transported. Only authorized individuals will be able to access the lab that contains the data. Chain of custody sign in/ out protocols would apply and separate forms will be used for each drive found or analyzed. Photographs will be used to capture and recreate the original scene from all angles. The lab will be secure physically to the point that it would be difficult to attempt a break-in. The data will be housed in a place protected from electromagnetic interference and with no internet connectivity, wireless, or cellular interference. All forensic tools used will be up to par with NIST standards and thoroughly documented what tools, techniques, and software was used. (Easttom, 2021)

The team will examine the evidence in the order of volatile which consists of swap files, state of running processes, and state of network connections, temporary, and then persistent data. We want to minimize file loss and file corruption as much as possible. (Easttom, 2021) We will document times, dates, document types, and file names. We will check deleted files, trash, or recycle folders/bins. We will check for any file modifications in name, size, type or program changes, and anomalies. We will check for steganography and encrypted files, bookmarks, history, web browser caches, script files, session files on a bit level search. (Easttom, 2021). We also will check for data mining.

The investigation will be in accordance with company policy to protect their proprietary assets and information. No further information should be able to be leaked or shared to additional sources. No data will be altered. The data must remain in its integrity and fall under the rules of evidence so that the legal team can present the case to the court of law.

The team will create a comprehensive report that includes a summary of the investigation, findings, conclusions, and recommendations. We will present the findings in a clear and concise manner, avoiding technical terms so senior management can understand the results and how the violated policy. We would only highlight the accused actions and what was found regarding those actions and violations. Their goal is determining a corrective action and protecting the company. We do not want to confuse them with too many technical terms. During and at the end of the investigation, we ensure that all actions are well-documented, and the chain of custody is maintained for all collected evidence. Confidentiality will be maintained of the investigation to prevent potential tampering or destruction of evidence while conforming to guidelines and best practices to ensure we performed a thorough investigation. The information will be presented in a generated report from FTK. There is still confidential information in the report and if a word document or PowerPoint was used those can be altered or shared faster then a hashed report from a forensic tool.

REFERENCES

1. Easttom, Chuck. Digital Forensics, Investigation, and Response. Available from: Western Governors University, (4th Edition). Jones & Bartlett Learning, 2021
2. Western Governors University. (2020). Forensics frameworks. Available from <https://access.wgu.edu/ASP3/aap/content/c840_forensics_frameworks.pdf3>
3. U.S. Department of Justice. (n.d.). Digital forensic analysis methodology. Computer Crime and Intellectual Property Section. https://access.wgu.edu/ASP3/aap/content/forensics\_methodology\_doj.pdf