Incident handler's journal

Date: Nov 1, 2025	**Entry:** #1
Description	Documenting a cybersecurity incident This incident occurred in the two phases: 1. **Detection and Analysis**: The scenario outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: To contain the incident, the company shut down their computer systems, and because they could not eradicate the ransomware, they contacted several organizations to report the incident and receive technical assistance in their recovery.
Tool(s) used	None
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident occurred as a result of a phishing attack conducted by an organized group of hackers. Once they had successfully infiltrated the healthcare company's systems they locked out many company files, hindering business operations. The hackers seem to have wanted a large sum of money in exchange for the decryption key to the encrypted files help for ransom.
Additional notes	1. The healthcare company needs to implement training of all employees on how to detect a phishing attack to prevent any future attack from occurring. 2. It is best NOT to pay the ransom as not all data may not be retrieved and hackers may feel enabled to continue to perform such attacks.

Date: Nov 2, 2025	**Entry:** #2
Description	Analyzing a packet capture file
Tool(s) used	For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a network protocol analyzer that uses a graphical user interface. The value of Wireshark in cybersecurity is that it allows security analysts to capture and analyze network traffic. This can help in detecting and investigating malicious activity.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A • **Why**: N/A
Additional notes	At first glance the sample was overwhelming but after going through the lab, the data became much more digestible.

Date: Nov 3, 2025	**Entry:** #3
Description	Capturing my first packet
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the command-line interface. Tcpdump in cybersecurity allows security analysts to capture, filter, and analyze network traffic.
The 5 W's	• **Who**: N/A • **What**: N/A • **Where**: N/A • **When**: N/A

	• **Why**: N/A
Additional notes	These commands quickly became overwhelming to understand with various configurations of tcpdump to pull data. After following the instructions it became sort of clearer on what all the attributes of each common was meant to do.

Date: Nov 4, 2025	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	For this activity, I used VirusTotal, which is an investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. For this activity, I used VirusTotal to analyze a file hash, which was reported as malicious. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
The 5 W's	• **Who**: An unknown malicious actor • **What**: An employee downloaded a malicious file attachment sent to their email with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **Where**: An employee's computer at a financial services company • **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the executable file • **Why**: An employee downloaded and executed a malicious file attachment received via their e-mail.

Additional notes	To prevent such an incident from occurring in the future, employees should receive training on how to detect a phishing email and should be instructed to report having received emails from unknown senders.