Incident handler's journal

Date: 8/1/2025	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **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 after malicious actors gained access to the company's systems through a phishing attack. Once inside, they deployed ransomware that encrypted critical files. The attackers were likely financially motivated, as evidenced by a ransom note demanding a large payment in exchange for the decryption key.
Additional notes	● What security measures should be implemented to reduce the risk of future phishing and ransomware attacks? ● What are the risks and implications of paying the ransom versus pursuing alternative recovery options?

Date: 8/2/2025	**Entry:** #2
Description	Provide a brief description about the journal entry.

Tool(s) used	Wireshark
The 5 W's	• **Who** N/A • **What** N/A • **When** N/A • **Where** N/A • **Why** N/A
Additional notes	I had never used Wireshark before, so starting this lab felt a bit overwhelming at first due to the complex interface. However, I quickly got the hang of it and now understand why it's considered such a powerful tool for analyzing network traffic.

Date: 8/3/2025	**Entry:** #3
Description	Capture my first packet
Tool(s) used	tcpdump
The 5 W's	• **Who** N/A • **What** N/A • **When** N/A • **Where** N/A • **Why** N/A
Additional notes	This was my first time using `tcpdump`, and I got stuck multiple times along the way. I often used the wrong commands or syntax, which was frustrating at first. But after a lot of trial and error, things started to click. It took some effort, but I eventually figured it out and was able to capture my first packet.

Date: 8-4-2025	**Entry:** #4
Description	Investigate a suspicious file hash
Tool(s) used	VirusTotal
The 5 W's	● **Who** An unknown malicious actor ● **What** An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **When** At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **Where** An employee's computer at a financial services company ● **Why** An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	I think security awareness training should be provided to employees to prevent this from happening in the future.