Incident handler's journal

Date: April 30, 2025	**Entry: 1**
Description	I analyzed a ransomware attack on a small clinic caused by phishing. The response focused on detecting the breach and quickly containing the infected systems, following the NIST Incident Response Lifecycl
Tool(s) used	**None.**
The 5 W's	Capture the 5 W's of an incident. • Who: A group known for targeting healthcare orgs. • What: Ransomware locked up important patient data and demanded money to unlock it. • When: Happened early Tuesday morning around 9:00 AM. • Where: A clinic in the U.S. that provides primary care. • Why: An employee accidentally opened a phishing email attachment that installed the malware.
Additional notes	Additional notes: This kind of attack shows why employee training on phishing is so important. The clinic could've also benefited from having solid backups and a plan for ransomware response.

Date: April 30, 2025	**Entry: 2**

Description	This was my first experience with Wireshark. I used it to go through packet data from a network capture and learned how to find specific types of traffic using filters.
Tool(s) used	Wireshark
The 5 W's	Capture the 5 W's of an incident. ● Who: n/a ● What: Learned how to use wireshark. ● When: n/a ● Where: n/a ● Why: To understand how to use wireshark.
Additional notes	At first Wireshark was kind of overwhelming with how much info it shows, but once I figured out how to filter things, it started to make a lot more sense. I can see how this would be super useful during an actual investigation.

Date: April 30, 2025	**Entry:** 3
Description	Looked into a suspicious file hash using VirusTotal. This is part of the Detection and Analysis phase.
Tool(s) used	VirusTotal

The 5 W's	Capture the 5 W's of an incident. ● Who: Unknown attacker — possibly an APT group. ● What: A fake job applicant sent malware in a password-protected file. ● When: Alert came through at 1:20 PM. ● Where: A financial company's employee email. ● Why: Someone opened the file, which installed malware.
Additional notes	VirusTotal showed that the file was flagged as malicious. This showed me how even one bad click can lead to major problems. Makes me think we need better training and maybe stricter email filtering.

Date: April 30, 2025	**Entry:** 4
Description	Investigated failed SSH logins to the root account of a mail server using Splunk. This is in the Detection and Analysis phase.
Tool(s) used	**Splunk cloud**

The 5 W's	Capture the 5 W's of an incident. ● **Who: Unknown attackers using multiple IPs.** ● **What: Repeated failed SSH login attempts — likely brute force.** ● **When: Repeated daily between 2/27/25 and 3/6/25 at around 1:39 AM.** ● **Where: Mail server of an online game store.** ● **Why: Probably trying to guess the password and gain root access.**
Additional notes	It felt cool figuring this out through log patterns. Splunk made it easier once I figured out how to filter the search right. We'd need MFA and rate-limiting to help defend against this in real life.

Reflections

Challenges: Splunk was tricky at first—I wasn't sure how to use the right search terms, but it clicked after some practice.

What I Learned: I realized incident response isn't just about stopping attacks—it's also about finding, understanding, and learning from them.

Favorite Tool: I really liked VirusTotal. It was fun to use, and it was quick and easy to check for threats.
