Incident handler's journal

Template for recording findings after completing an activity or to take notes on lessons learned about a specific tool or concept.

Date: 24/01/2026	**Entry:** 001
Description	This entry covers the handling of a security incident at a healthcare clinic, their business operations were halted when they suffered a ransomware attack caused by a phishing email that contained a malicious attachment.
Tool(s) used	None.
The 5 W's	● **Who**: An organised group of unethical hackers. ● **What**: A ransomware security incident. ● **When**: At a health care company. ● **Where**: Tuesday 9:00 a.m. ● **Why**: This incident was due to some unethical hackers obtaining access to a healthcare company's systems using a phishing attack. After they gained access, the attackers launched their ransomware on the company's systems, encrypting critical files. It seems that the motivation for the attackers were just financial because they left a note demanding a large sum of money in exchange for the decryption key.
Additional notes	1. Should the company pay the ransom to retrieve the decryption key, and how can they prevent an incident like this in the future? 2. Conduct more training for employees on the several and common forms of phishing and internet attack.

Date: 26/01/2026	**Entry:** 002
Description	This entry is for notes and lessons on analyzing a packet capture file
Tool(s) used	I used Wireshark to analyze a packet capture file.
The 5 W's	● **Who** - n/a ● **What** - n/a ● **When** - n/a ● **Where** - n/a ● **Why** - n/a
Additional notes	Wireshark is a powerful network protocol analyser that uses GUI and lets security analysts capture network traffic which helps in detecting and investigating malicious activity.

Date: 30/01/2026	**Entry:** 003
Description	This entry is for note and lessons on capturing a packet with tcpdump
Tool(s) used	For this activity, I used tcpdump to capture and analyze network traffic.

The 5 W's	- **Who** - n/a - **What** - n/a - **When** - n/a - **Where** n/a - **Why** n/a
Additional notes	Because tcpdump uses CLI to capture and filter network traffic, it can present some challenges sometimes but the thrill of a quick remote capture does have its pecks. For deep forensics, real-time/offline capture, etc, wireshark would be the ideal tool.

Date: 02/02/2026	**Entry:** 004
Description	This entry is for investigating a suspicious file hash that was detected by the IDS
Tool(s) used	I used VirusTotal, which is an investigative tool that analyses files and URLs for malicious contents.
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 organisation’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	In this scenario, the incident happened at the Detection and Analysis phase. As a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security system in place, I had to perform a deeper analysis and investigation to determine if the alert signified a real threat. a. How can we prevent this incident in the future? b. Should more security awareness training be provided to the employees?