Incident handler's journal

Date: Record the date of the journal entry.	**Entry:** #001
Description	A small U.S. health care clinic faced a ransomware attack on Tuesday at 9:00 a.m. The attack was done using a phishing email by an organized group of unethical hackers and now are demanding money for decrypting keys.
Tool(s) used	None
The 5 W's	• Who caused the incident? An organized group of unethical hackers • What happened? Ransomware attack • When did the incident occur? Tuesday at 9:00 a.m. • Where did the incident happen? A small U.S. health care clinic • Why did the incident happen? Malware installed on employees' computers which was delivered using a phishing email. The intention behind this hack was financial gain.
Additional notes	Can this be protected in future? If yes, how.... Can we trust hackers to not ask for more money if the ransom is paid? Did the hackers get their hands on crucial stuffs which can be leaked? Can the business pay the ransom?

Date: Record the date of the journal entry.	**Entry:** #002
Description	Analyzing a packet capture file
Tool(s) used	Wireshark is used to analyze a packet capture file. Wireshark has a graphical user interface. This can help in detecting and investigating malicious activity.
The 5 W's	• **There was no incident, it is just to analyze packet capture**
Additional notes	Wireshark has a lot of features to ease the process of packet analysis, including a GUI. It also provides filter and other options.

Date: Record the date of the journal entry.	**Entry:** #003
Description	Capture packets in tcpdump
Tool(s) used	Tcpdump is a network protocol analyzer that's accessed using the command-line interface. It is similar to Wireshark.

The 5 W's	• **There was no incident, it is just to analyze packet capture**
Additional notes	Tcpdump is based on command-line interface and can be used in scripting and automation. It is perfect when there is no GUI option available that maybe while remoting into servers.

Date: Record the date of the journal entry.	**Entry:** #004
Description	Investigating a file hash for malware
Tool(s) used	VirusTotal was used. It 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 to quickly check if an indicator of compromise like a website or file has been reported.
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 • ● 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 file • ● Why: An employee was able to download and execute a malicious file

	• attachment via e-mail.
Additional notes	Employees should be provided with more phishing training and awareness. The company is being targetted so the company should up their defense. The company can also use cloud browsers to prevent getting affected by these kinds of attaks in future.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.