Incident handler's journal

Date: Mon, Aug 7, 2023	**Entry:** 001
Description	Cybersecurity Incident
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. ● An organized group of unethical hackers ● The hackers deployed ransomware ● The incident took place on a Tuesday morning at around 9:00 a.m. ● The incident occurred within the small U.S. healthcare clinic ● The incident was triggered by the hackers' use of targeted phishing emails containing malicious attachments, which allowed them to gain unauthorized access to the clinic's network and subsequently deploy ransomware to encrypt critical files. The hackers sought to exploit this situation to demand a substantial ransom in exchange for the decryption key.
Additional notes	Should they pay the ransom to decrypt their files?

Date: Thur, Aug 10, 2023	**Entry:** 002
Description	Investigating a file that was downloaded through an email.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● An employee at a financial services company downloaded a file from an email which came from outside the network. ● The file was a password protected spreadsheet, the password was provided in the email. Once the file was access a malicious payload was then executed on their computer. ● Aug 10th fro 1:11 pm - 11:20pm ● Within a financial services company. ● The incident was triggered by the malicious actor's use of phishing which consisted of an email with a malicious attachment. The email contained FlagPro which is a type of malware that, when executed, can collect user data, download and execute a tool, and perform commands in the OS.
Additional notes	● Could the malware have been found before opening the file?

Date: Fri Aug 11, 2023	**Entry:** 003
Description	Analyzing a packet capture file
Tool(s) used	WireShark
The 5 W's	Capture the 5 W's of an incident. ● **Who**: N/A ● **What**: N/A ● **When**: N/A ● **Where**: N/A ● **Why**: N/A
Additional notes	The only experience I had before this was analyzing a screenshot of a Wireshark log. Although I felt quite intimidated, I was genuinely eager to delve into the program, learn its intricacies, and become more familiar with its functionality. The prospect of gaining hands-on experience excited me, despite the initial apprehension.

Date: Fri Aug 11, 2023	**Entry:** 004
Description	Capturing a packet
Tool(s) used	tcpdump
The 5 W's	Capture the 5 W's of an incident. ● **Who**: N/A ● **What**: N/A ● **When**: N/A

	● **Where**: N/A ● **Why**: N/A
Additional notes	Using a CLI has been a challenge for me as I am very familiar with regular GUI on operating systems like MacOS and Windows. Fortunately, I was able to learn quickly and tcpdump helped me get familiar with commands.

Reflections/Notes: Record additional notes.