Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 01/02/2025	**Entry:** Analyze your first packet
Description	Learning how to open and analyze a packet capture file using Wireshark. Analyze a network packet capture file that contains traffic data related to a user connecting to an internet site.
Tool(s) used	Google Chrome Wireshark GoogleLab
The 5 W's	● **Who**: Myself, a security analyst ● **What**: identify the source and destination IP addresses involved in this web browsing session, ○ examine the protocols that are used when the user makes the connection to the website, and ○ analyze some of the data packets to identify the type of information sent and received by the systems that connect to each other when the network data is captured. ● **Where**: Windows VM and Wireshark ● **When:** Timestamp of packet

	● **Why:** ○ You now have practical experience using Wireshark to open saved packet capture files, view high-level packet data, and use filters to inspect detailed packet data.
Additional notes	