Cybersecurity Lab Journal - #1

Lab Description:

In this lab, I used **Wireshark** to explore and filter network traffic from a sample packet capture (.pcap) file. The goal was to practice identifying IP addresses, protocols, and payload data by using different filters. I also learned how to inspect specific packets, analyze DNS and TCP data, and search for text in packet payloads.

Date: Record the date of the journal entry.	**Entry:** #1
Description	Packet analysis using Wireshark. I opened a capture file and applied filters to explore DNS, TCP, and HTTP traffic. This helped me understand how packets move between source and destination systems.
Tool(s) used	Wireshark (network protocol analyzer)
Key Findings / Skills Practiced:	• Used Wireshark filters like ip.addr, udp.port, and tcp.contains to isolate packets. • Identified source and destination IPs and protocol types such as ICMP, TCP, and UDP. • Viewed DNS queries and responses, including the resolved IP for opensource.google.com. • Explored packet layers (Frame, Ethernet II, IPv4, TCP). • Learned how TTL, header length, and frame size appear inside captured packets.
Additional notes	In this lab, I used **Wireshark** to explore and filter network traffic from a sample packet capture file. The goal was to practice identifying IP addresses, protocols, and packet data by using different filters. I also learned how to

	inspect DNS and TCP packets and spot patterns in how devices communicate online.
