| **Date:**<br>**2/09/2025** | **Entry:**<br>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.<br><br>A security analyst uses Wireshark to open and analyze a network packet capture file, identifying IP addresses, protocols, and data exchanged during a user's web browsing session.<br><br>**NIST Phase**: This task falls under the **Detection & Analysis** phase, as it involves examining network traffic to identify and analyze potential security issues or patterns in the data. |
| Tools Used | Google Chrome<br>Wireshark- Wireshark is a popular open-source network protocol analyzer used to capture and inspect network traffic in real time. It allows users to monitor and analyze the data packets that travel across a network. With Wireshark, you can view detailed information about network protocols, packet contents, and identify network issues, potential security vulnerabilities, or malicious activity. It's often used by network administrators, security analysts, and engineers for troubleshooting, performance analysis, and forensic investigations.<br>GoogleLab |
| The 5 W's | ● Who: Myself, a security analyst<br>● 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.<br>● Where: Windows VM and Wireshark<br>● When: Timestamp of packet<br>● Why:<br>○ 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 | |