WEEK-2

Asad Muhammd Channar

DHC-56

Task-5:

Capture Network Traffic with Wireshark (Advanced Task)

Required:

- Capture network traffic using Wireshark (build upon Week 1 tool exploration).
- Analyze: Filter and analyze the traffic to identify any suspicious activity or common patterns (e.g., DNS requests, HTTP traffic).
- Document: Write a short report (1 page) on what you learned, including any interesting insights from the captured traffic.

Wireshark

Wireshark is a popular open-source network protocol analyzer that allows users to capture and examine data traveling across a network in real time. It provides detailed insights into network traffic by breaking down each packet, enabling users to troubleshoot network issues, analyze security vulnerabilities, and understand network protocols. Wireshark supports a wide range of protocols and offers powerful filtering capabilities to isolate specific traffic of interest. It runs on multiple platforms, including Windows, macOS, and Linux. Network administrators, cybersecurity

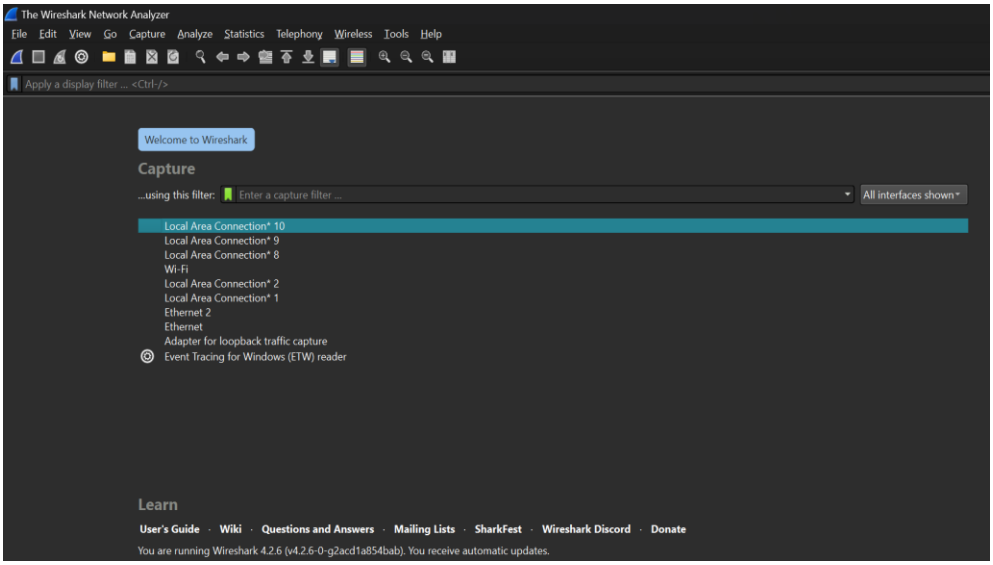
professionals, and developers frequently use Wireshark for monitoring, diagnostics, and forensics in network environments.

Packet Hunt:

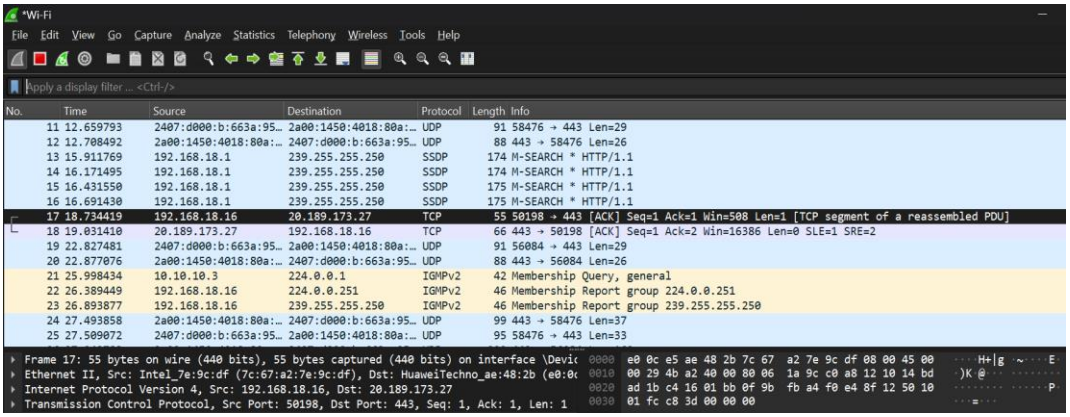
Now ,we will capture network traffic using wireshark and examines the packets in detail.

Following are the steps to **hunt packets.**

- Open the wireshark.
- Select the network interface you want to capture the packets



- Once select the interface , press the capture button in the top right corner and the inbound and outbound packets will be shown to you.



- As we can see , packets capturing has been started . We see different types of packets here. Some are **UDP protocols ,** some **TCP .** Type of packets really depend on the applications you are running .

- As show below , there are different sections of a protocol which give us more insight about the packet . By examining these packets , we collect significant amount of details about a specific packet. It's **destination** and **source IP** , **ports** , **flags** , and a ton of information

SO, this was packets capturing and examining in detail using wireshark . You can download wireshark from the following link.

Download Wireshark

That's it!