Date: 26/08/2024

Lab Practical #08:

Study Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

Practical Assignment #08:

1. Explain usage of Wireshark tool.

- **Capture Traffic:** Start capturing network traffic by selecting the appropriate network interface. **Apply Filters:** Use capture filters (before capturing) or display filters (after capturing) to focus on specific traffic, like http for HTTP traffic or ip.addr == 192.168.1.1 for traffic to/from a specific IP.
- **Analyze Packets:** Examine packet details, including protocol layers, headers, and payloads. Expand sections for in-depth analysis.
- **Follow Streams:** Use the "Follow TCP/UDP Stream" feature to view continuous data exchanges between endpoints.
- **Identify Issues:** Spot anomalies, such as retransmissions, duplicate packets, or protocol errors, to diagnose network problems.
- **Export Data:** Save captured data in various formats, or export specific packets for further analysis.
- **Use Statistics:** Access tools like "Protocol Hierarchy," "Conversations," and "Endpoint" statistics for summary views of the traffic.
- **Customize Views:** Colorize packets and customize columns to highlight important information for easier analysis.
- **Decrypt SSL/TLS Traffic:** If you have the right keys, decrypt SSL/TLS traffic for deeper inspection. **Automate Tasks:** Use command-line tools like T-shark for automated packet capturing and analysis.

2. Packet capture and header analysis by Wireshark (HTTP, TCP, UDP, IP, etc.)

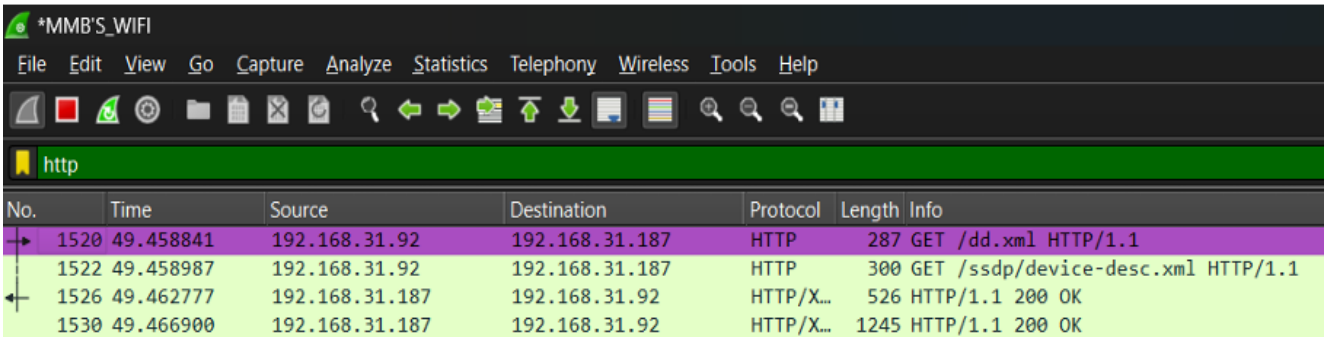
⇨ Steps Of Packet capture and header analysis by Wireshark:

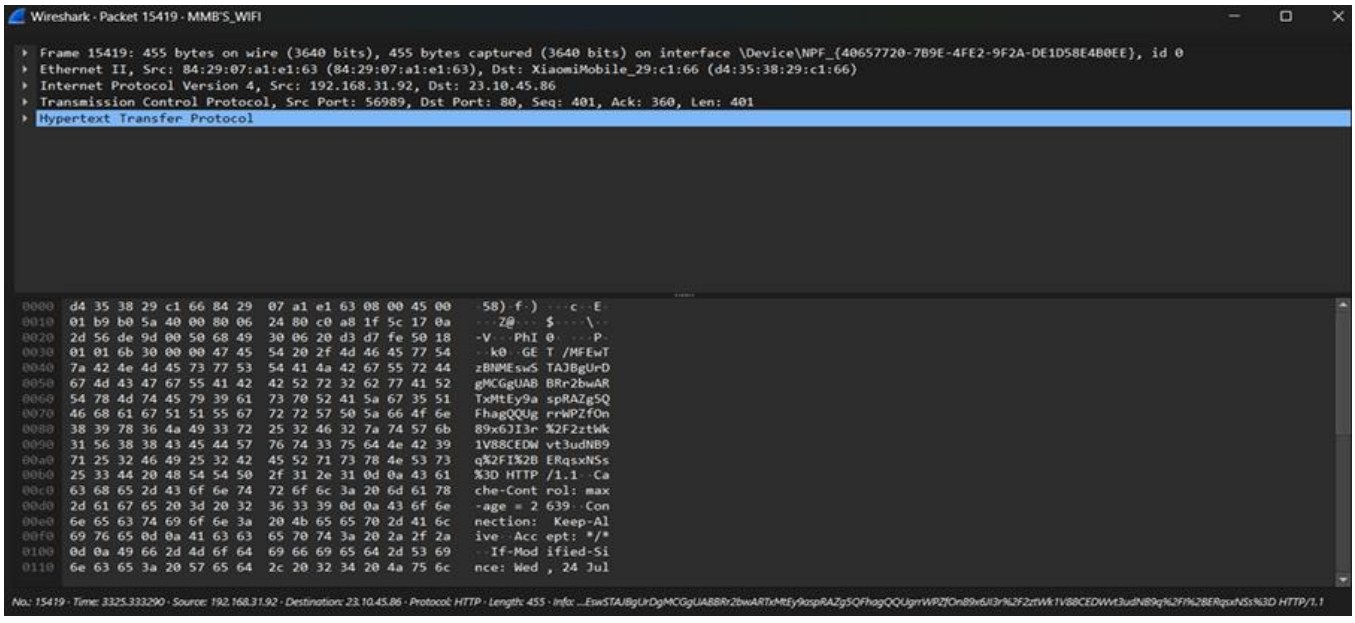
- Install and Launch Wireshark
  - Download and Install: Get Wireshark from its official website. Launch Wireshark: Open the application after installation.
- Start Packet Capture
  - Select Network Interface: Choose the network interface you want to monitor (e.g., Wi-Fi, Ethernet). You will see a list of interfaces with activity graphs.
  - Begin Capturing: Click the "Start Capturing Packets" button (the shark fin icon) to begin capturing packets.
- Generate Network Traffic
  - While Wireshark is capturing, generate some network traffic related to the protocols you're interested in (e.g., visit a website for HTTP traffic, use a network application for TCP/UDP traffic). 4. Stop Capture
  - Once you've captured enough packets, click the red stop button to stop capturing.
- Filter Packets
  - Apply Protocol Filters: Use the filter bar at the top to focus on specific protocols. For example: HTTP: Type http in the filter bar.
  - TCP: Type tcp.

Date: 26/08/2024

- DP: Type udp.
- IP: Type ip.
- Apply Filter: Press Enter after typing the filter to view only the relevant packets. ➢ 6. Select and Analyze Packets
- Packet List Pane: This pane shows a summary of captured packets, including time, source, destination, protocol, and length.
- Packet Details Pane: Click on a packet in the list to see its details in the middle pane. This pane displays a hierarchical view of the packet's headers.

HTTP:





Date: 26/08/2024

TCP: