Exploring Network Layer Packet Details with Wireshark

Objective:

The objective of this Wireshark lab assignment is to provide hands-on experience with analyzing network layer packet details using Wireshark. By completing this assignment, students will gain a deeper understanding of the network layer protocols, packet structures, and how data is transmitted over the network.

Instructions:

Part 1: Capturing Packets

Launch Wireshark on your computer.
Select the network interface you want to capture packets from (e.g., Ethernet, Wi-Fi).
Start capturing packets by clicking on the 'Start' button or using the Ctrl + E shortcut.

Part 2: Analyzing Packets

Capture packets for various network activities such as:

- Browsing a website
- Sending an email
- Downloading a file
- Streaming a video
  Stop capturing packets after each activity by clicking on the 'Stop' button or using the Ctrl + E shortcut.

Analyze the captured packets to identify the following network layer details:

- Source and destination IP addresses
- IP header information (version, length, TTL, etc.)
- Protocol type (IPv4, IPv6)
- Network layer protocols (ICMP, TCP, UDP)
- Packet fragmentation (if applicable)
- Any other relevant network layer information

Part 3: Packet Filtering

Use Wireshark's filtering capabilities to focus on specific types of packets (e.g., ICMP packets, TCP packets).

Apply filters to analyze only the packets relevant to the network layer.
Observe how packet filtering can help in isolating and analyzing specific types of network traffic.

Part 4: Exporting Results

Export the captured packets and analysis results for each activity.

Save the exported results in a format that can be shared with your instructor or peers (e.g., .pcap, .csv).

Discussion Questions:

Based on your analysis, what are the typical characteristics of network layer packets?

How do the source and destination IP addresses influence the routing of packets in a network?
Discuss the significance of Time-To-Live (TTL) in the IP header and its role in packet delivery.
Compare and contrast the IPv4 and IPv6 headers. What are the key differences?

Additional Challenges (Optional):

- Analyze network layer packets captured from a different network environment (e.g., home network vs. university network).
- Investigate network layer packets exchanged during a VoIP (Voice over Internet Protocol) call.

Conclusion:

Reflect on your experience with analyzing network layer packet details using Wireshark. Discuss any challenges faced during the analysis and the insights gained from this exercise.

Note: Ensure that you follow ethical guidelines and obtain necessary permissions before capturing and analyzing network traffic. Avoid capturing sensitive information or data that you are not authorized to access.