Session 10 Capturing Traffic in Wireshark

1. Selecting the Right Interface

    Wireshark displays all available network interfaces (Ethernet, Wi-Fi, Loopback, etc.)
    Identify the active interface by observing packet counters
    Select the interface that is currently in use for internet connection

2. Starting a Capture

    Highlight the desired interface
    Click the start capture icon (shark fin)
    Packets begin to appear in real-time

3. Generating Traffic for Capture

    Open a browser and visit a website (example: google.com)
    DNS requests and TCP connections will be visible
    Background applications may also generate network traffic

4. Using Display Filters

    Apply filters to focus on specific traffic:
        dns (shows only DNS traffic)
        tcp (shows only TCP traffic)
        udp (shows only UDP traffic)
        http (shows unencrypted HTTP traffic)
        ip.addr == 8.8.8.8 (shows packets to or from Google DNS)

5. Understanding the Capture Panes

    Top Pane: Packet list summary (each row represents one packet)
    Middle Pane: Detailed view of the selected packet (layer-wise: IP, TCP/UDP, Application)
    Bottom Pane: Raw hexadecimal representation of the packet data

6. Stopping and Saving the Capture

    Use the stop button to end the capture
    Save the file in .pcapng format using File > Save As