Session 9 Hands-on: Wireshark Installation and Setup

1. Download Wireshark

Visit the official Wireshark website:
[https://www.wireshark.org/download.html]
(https://www.wireshark.org/download.html)

Select the appropriate installer for your operating system (Windows, macOS, or Linux)

Download the latest stable version

2. Install Wireshark

Windows:

Run the installer file

During installation, enable Npcap installation (necessary for packet capturing)

USBPcap installation is optional

macOS:

Download the .dmg file

Drag Wireshark into the Applications folder

Install any additional capture libraries if prompted

Linux (Ubuntu/Debian):

Update repositories: sudo apt update

Install Wireshark: sudo apt install wireshark -y

Add user to Wireshark group: sudo usermod -aG wireshark \$USER

Log out and log in again to apply permissions

3. Launch Wireshark

Open Wireshark from the applications or start menu

A list of network interfaces will appear (Wi-Fi, Ethernet, Loopback, etc.)

4. Start a Capture

Select the active network interface (commonly Wi-Fi on laptops)

Start capturing by clicking the capture icon

Stop capturing with the stop button

5. Verify Setup

Open a website such as google.com while capturing
Return to Wireshark and confirm packets are visible
Apply filters to view specific traffic:

http (HTTP traffic)
ip.addr == 8.8.8.8 (traffic to or from Google DNS)

6. Additional Hands-On Steps

Capture the first packet by browsing any site and stopping capture
Use filters to analyze different protocols:

dns (DNS traffic)
tcp (TCP traffic)
udp (UDP traffic)
http (unencrypted HTTP traffic)

Save the capture file using File > Save As in .pcapng format
Explore packet details using the three Wireshark panes:

Top pane: Packet list summary
Middle pane: Protocol details with OSI layers
Bottom pane: Raw hexadecimal data