Task -11(b)

11(b)

I. Install Wireshark and view

II. Network Traffic

III. Examine ethernet frames View Wired and Wireless NIC information.

Objectives:

a) Capture and analyse local ICMP data in Wireshark
b) Capture and analyse Remote ICMP data in Wireshark

I. Install Wireshark and view

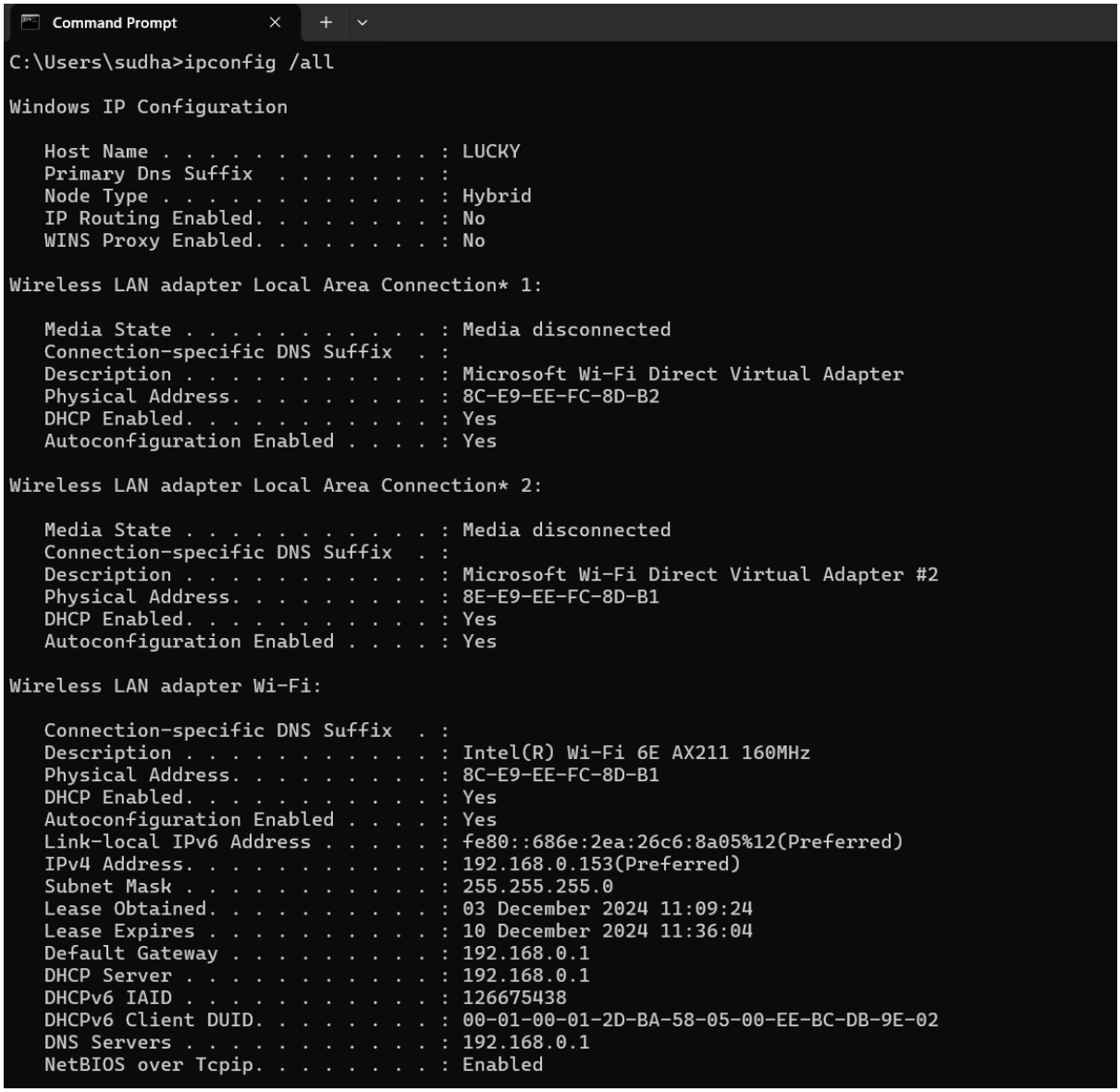
Download & Install: Go to the Wireshark website and download the latest version suitable for your operating system (Windows)

II. Network Traffic

Step 1: Retrieve your PC interface addresses

Retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

a. Open command window, type **ipconfig /all**, and then press Enter of your PC.
b. Note the IP address of your PC interface, its description, and its MAC (physical) address

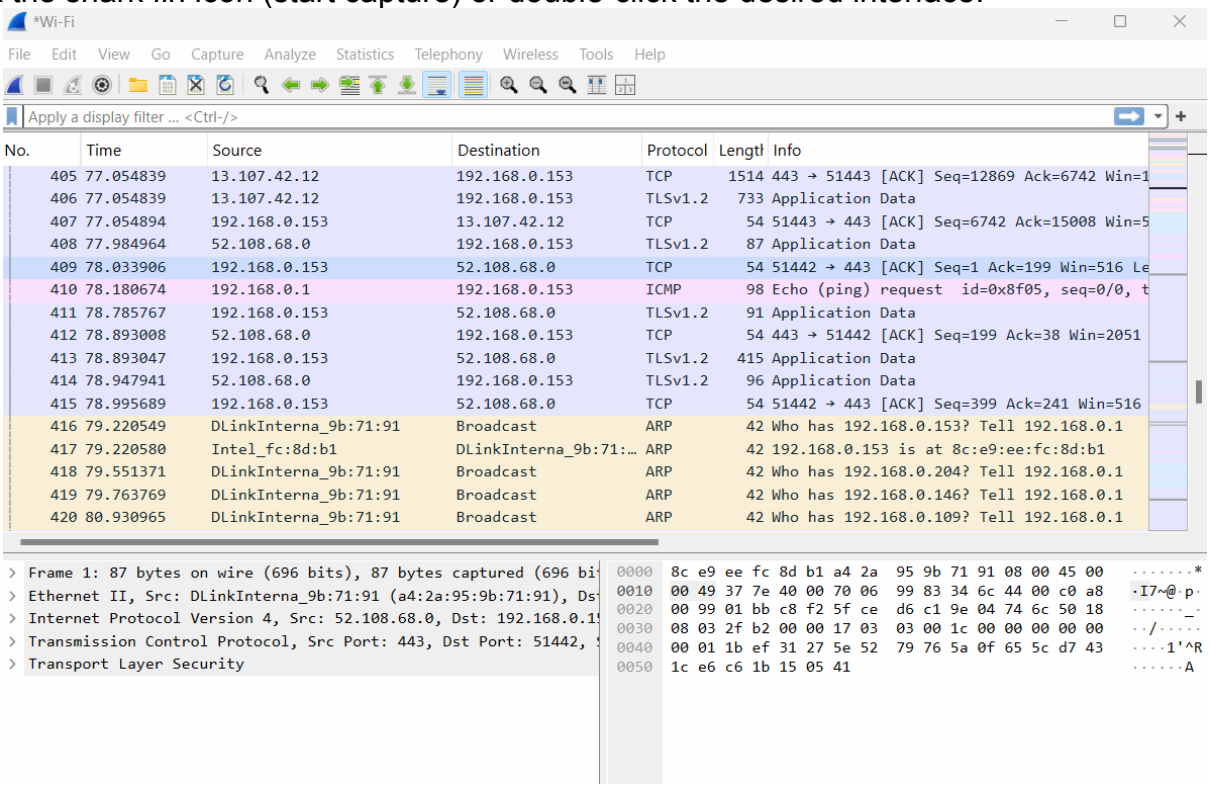


Step 2: Launch Wireshark

Open Wireshark

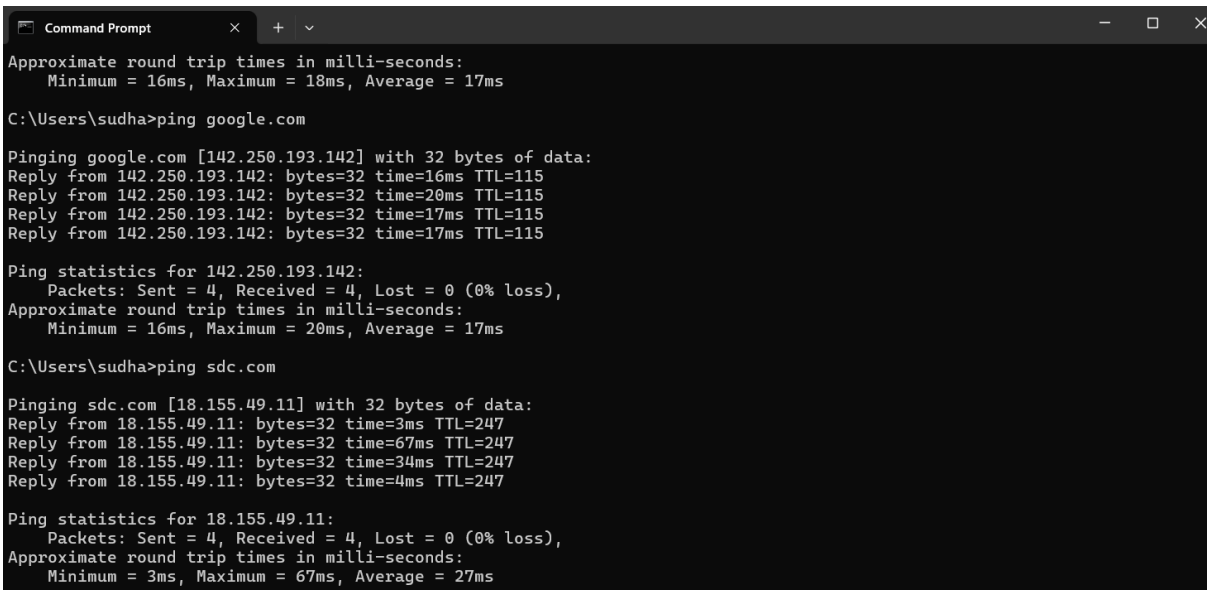
- Launch Wireshark. The interface shows a list of available network interfaces on your system.
- **Select a Network Interface** like
    - Your wireless (Wi-Fi) adapter.
    - Your wired Ethernet connection.
    - Virtual interfaces (e.g., VPN).
- Open wire shark and start capturing the packets. The data lines will appear in different colours based on protocol.

1.Click the shark fin icon (start capture) or double-click the desired interface.



2.Open command prompt from your PC

ping any URL
Ex: ping google.com
ping sdc.in
ping yahoo.com
ping cisco.com



3.Stop capturing the packets.

Step 3: Examine the captured data.

Wireshark data is displayed in three sections:

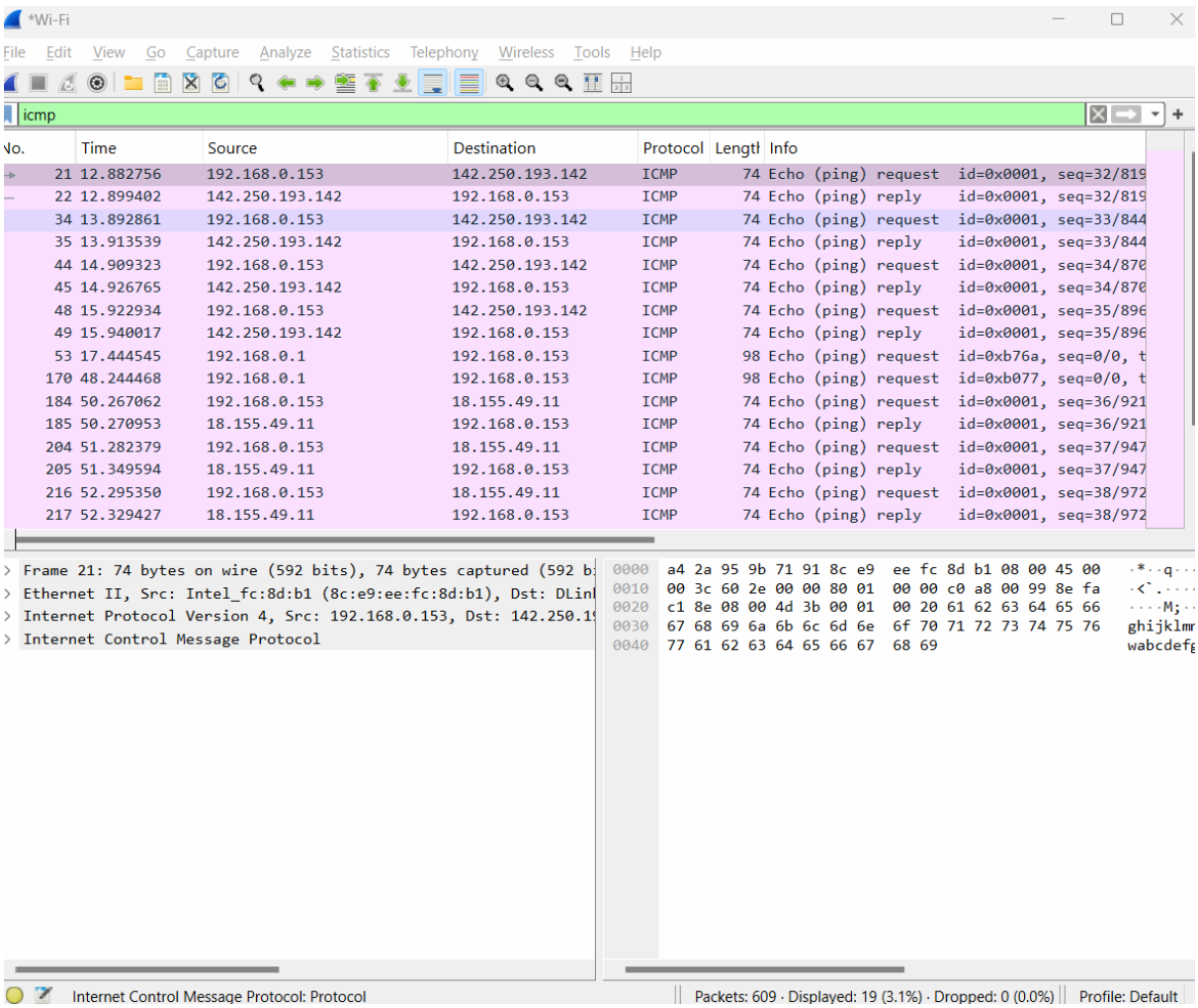
1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed.

2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers.

3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

Click the first ICMP request PDU frames in the top section of Wireshark.

Notice that the Source column has your PC IP address, and the Destination column contains the IP address you pinged.

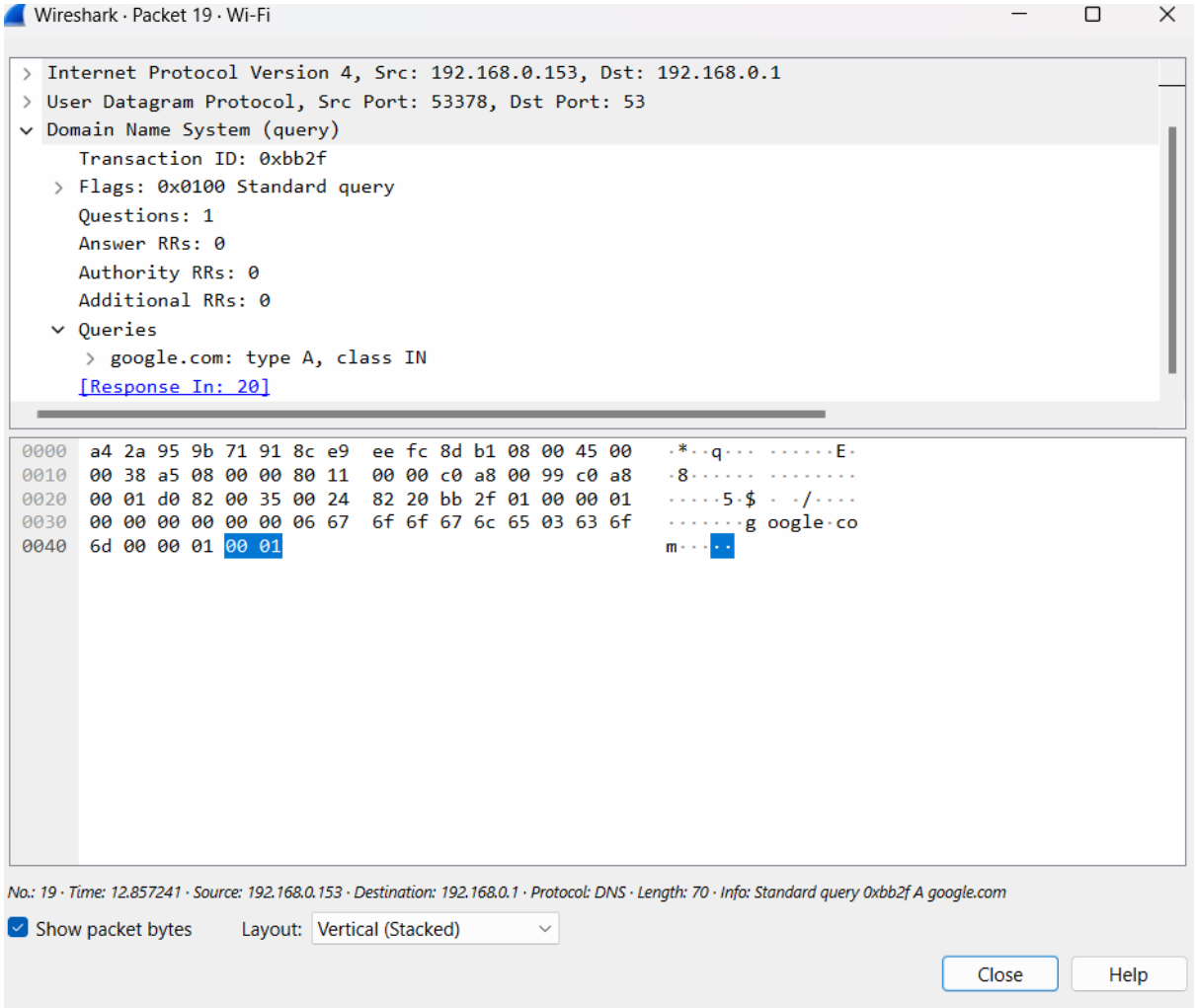


2. Go to the filter bar and type and check the following protocols ICMP enter.

DNS TCP UDP ARP

And observe the packets.

3. Examine the Ethernet frame fields in the middle section:



III. Examine ethernet frames View Wired and Wireless NIC information.

View Wired and Wireless NIC information:

Step 1: Use the Network and Sharing Center.

a. Open the Network and Sharing Center by clicking the Windows Start button > Control Panel > View network status and tasks under Network and Internet heading in the Category View.

b. In the left pane, click the Change adapter settings link.

c. The Network Connections window displays, which provides the list of NICs available on this PC. Look for your Local Area Connection and Wireless Network Connection adapters in this window.

Or

1. Right click on start (windows button) Settings – status – properties

Compare with:

Open a command window prompt and type **ipconfig /all**
And observe the above addresses, both must be same.