

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

```
Command Prompt      +  ▾
C:\Users\sudha>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LUCKY
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 8C-E9-EE-FC-8D-B2
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 8E-E9-EE-FC-8D-B1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

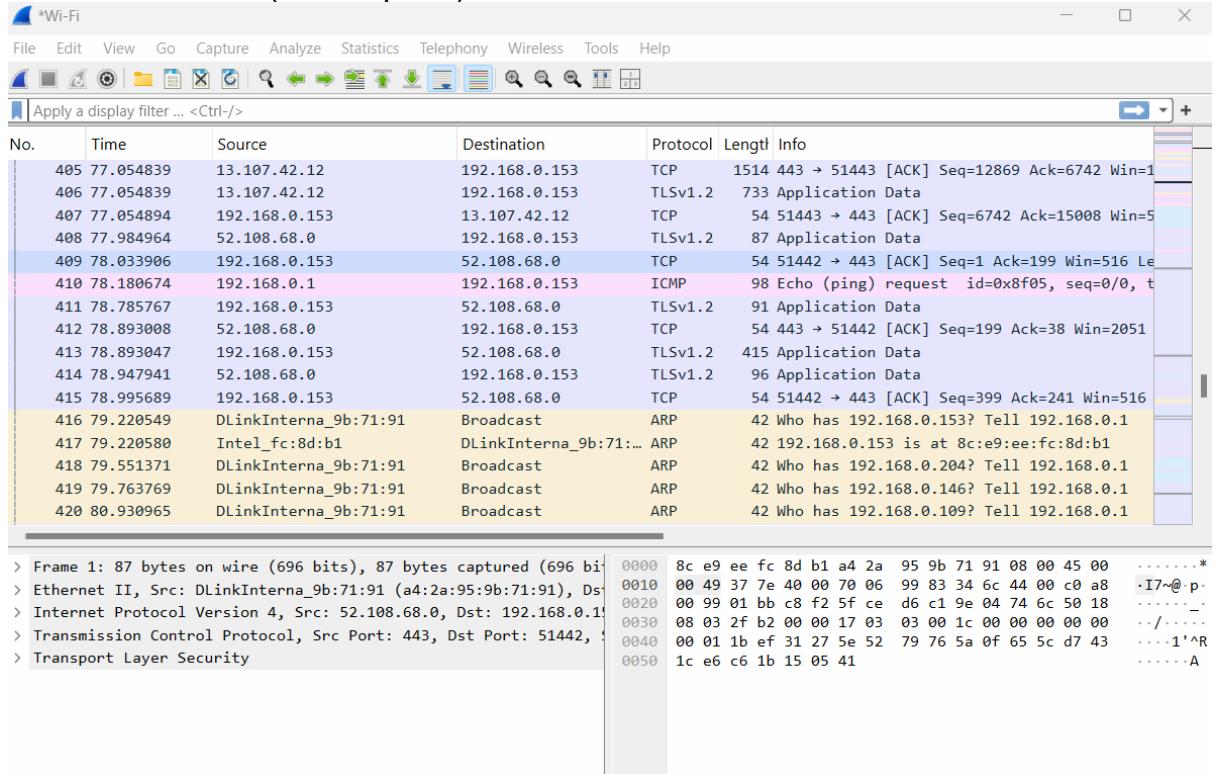
Connection-specific DNS Suffix . . . . . :
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : 8C-E9-EE-FC-8D-B1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::686e:2ea:26c6:8a05%12(Preferred)
IPv4 Address. . . . . : 192.168.0.153(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 03 December 2024 11:09:24
Lease Expires . . . . . : 10 December 2024 11:36:04
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 1266675438
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-BA-58-05-00-EE-BC-DB-9E-02
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

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

```
Command Prompt
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
C:\Users\sudha>ping google.com

Pinging google.com [142.250.193.142] with 32 bytes of data:
Reply from 142.250.193.142: bytes=32 time=16ms TTL=115
Reply from 142.250.193.142: bytes=32 time=20ms TTL=115
Reply from 142.250.193.142: bytes=32 time=17ms TTL=115
Reply from 142.250.193.142: bytes=32 time=17ms TTL=115

Ping statistics for 142.250.193.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 20ms, Average = 17ms

C:\Users\sudha>ping sdc.com

Pinging sdc.com [18.155.49.11] with 32 bytes of data:
Reply from 18.155.49.11: bytes=32 time=3ms TTL=247
Reply from 18.155.49.11: bytes=32 time=67ms TTL=247
Reply from 18.155.49.11: bytes=32 time=34ms TTL=247
Reply from 18.155.49.11: bytes=32 time=4ms TTL=247

Ping statistics for 18.155.49.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 67ms, Average = 27ms
```

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.

The screenshot shows the Wireshark interface with the following details:

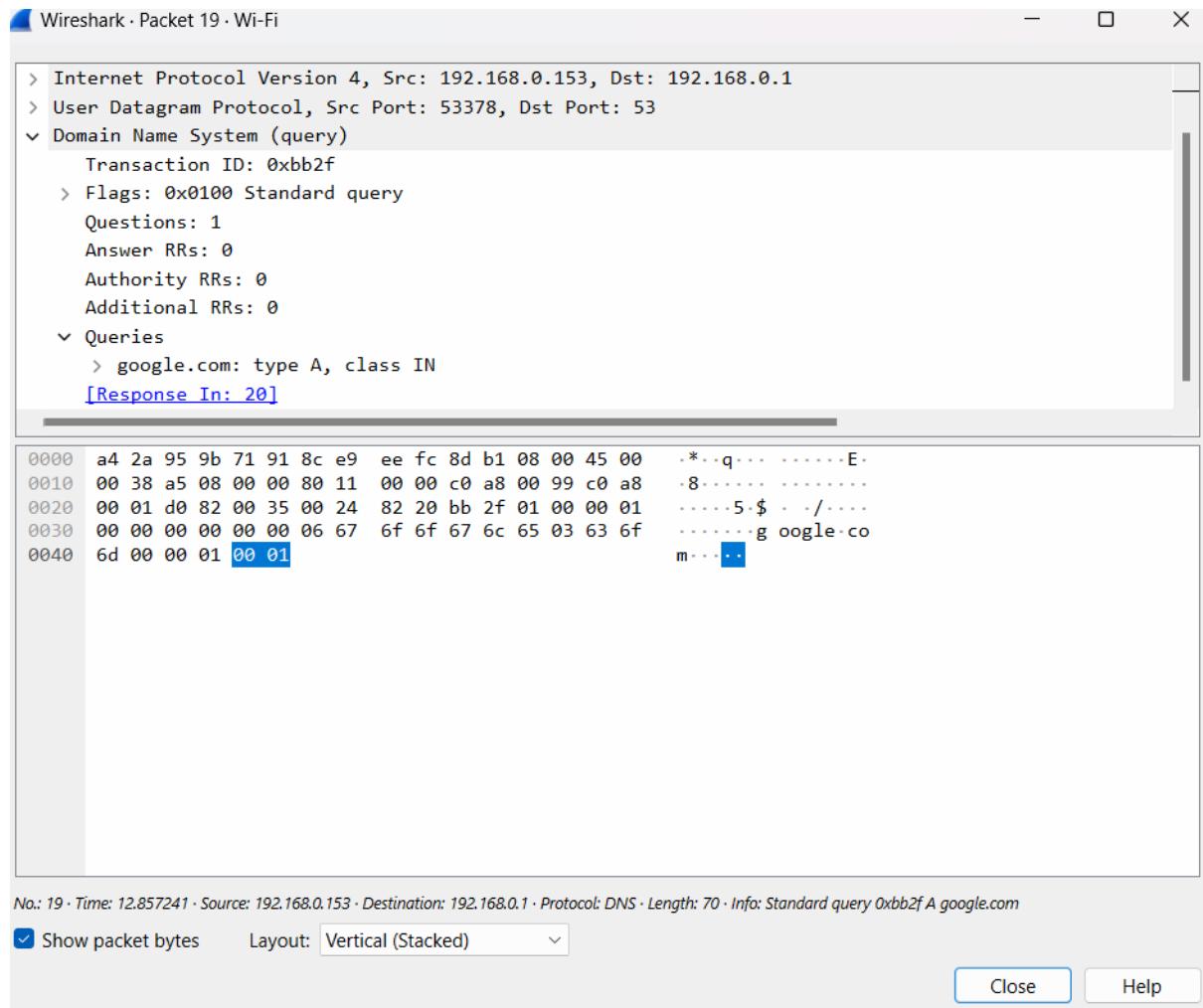
- Top Section (List View):** Shows a list of 21 captured frames. Frame 21 is selected, highlighted in purple. Other frames are numbered 22 through 27. The columns include No., Time, Source, Destination, Protocol, Length, and Info.
- Middle Section (Details View):** Displays the details for Frame 21. It includes:
 - Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 bits).
 - Ethernet II, Src: Intel_fc:8d:b1 (8c:e9:ee:fc:8d:b1), Dst: DLINK (08:00:27:00:00:00)
 - Internet Protocol Version 4, Src: 192.168.0.153, Dst: 142.250.193.142
 - Internet Control Message Protocol
- Bottom Section (Hex/ASCII View):** Shows the raw data for Frame 21 in both Hex and ASCII formats. The ASCII output includes characters from 'a' to 'z' and some control characters like '\n' and '\r'.

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.

