

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:

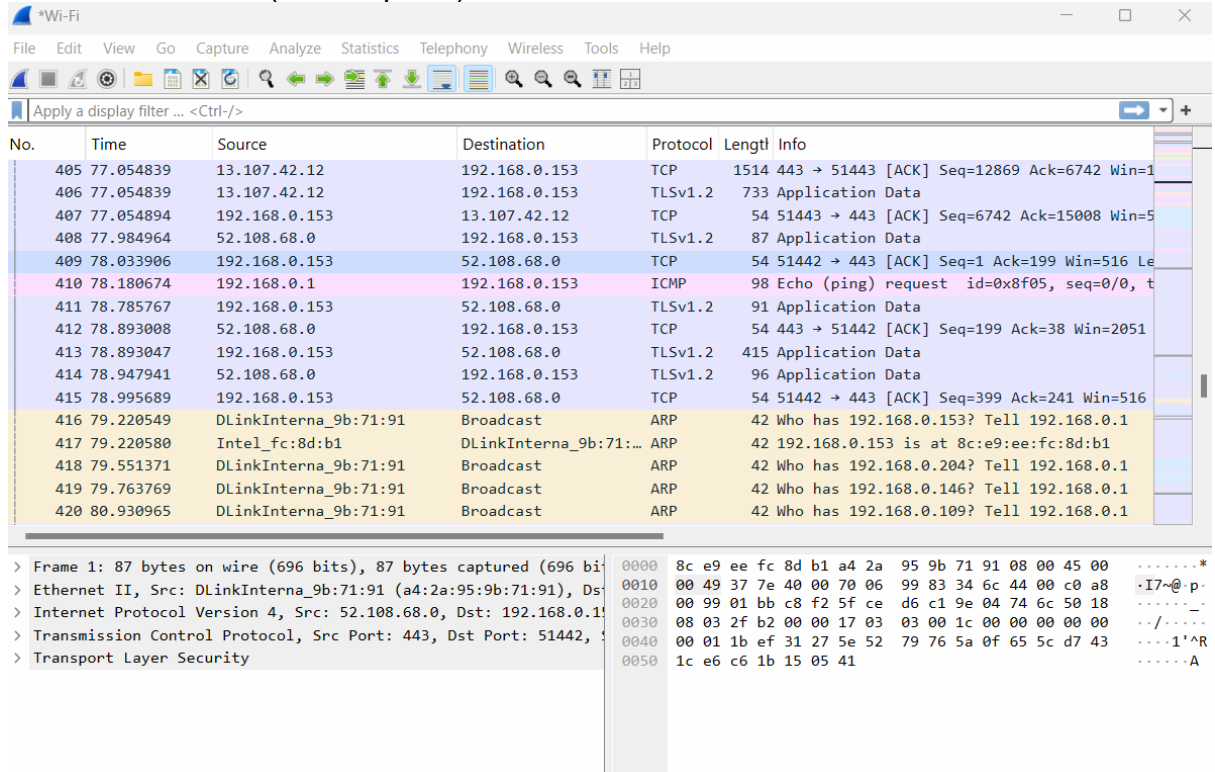
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
Physical Address. . . . . : 8C-E9-EE-FC-8D-B1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::686e:2ea:26c6:8a05%12(Preferred)
IPv4 Address. . . . . : 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 . . . . . : 126675438
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

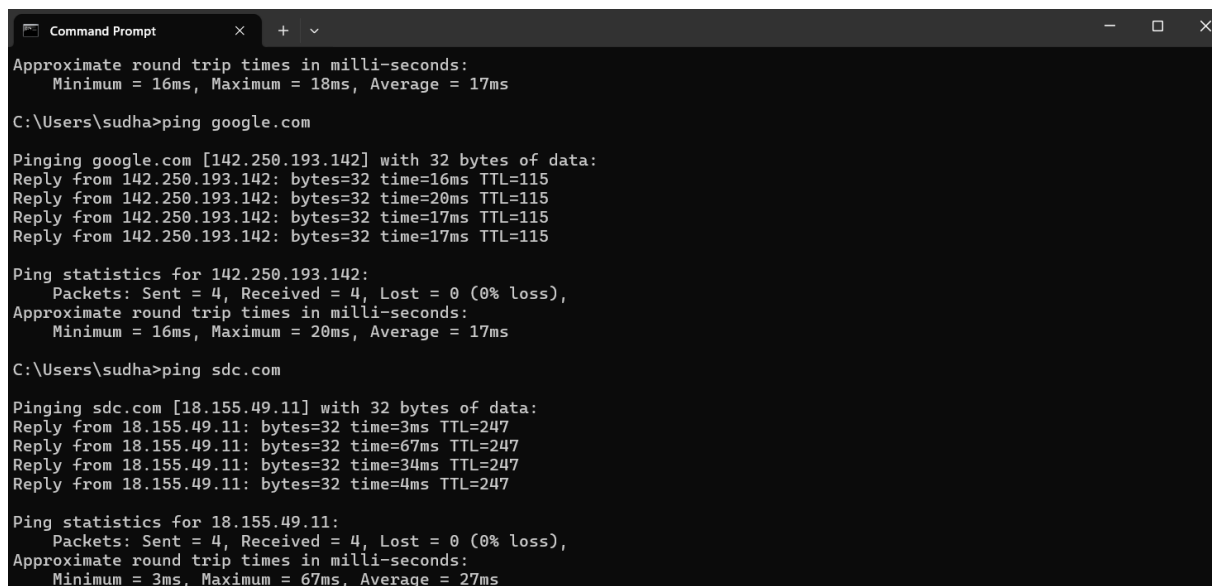
- Launch Wireshark. The interface shows a list of available network interfaces on your system.
- **Select a Network Interface** like
 - Your wireless (Wi-Fi) adapter.
 - Your wired Ethernet connection.
 - Virtual interfaces (e.g., VPN).
- Open wire shark and start capturing the packets. The data lines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



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 network protocol analyzer interface. The top pane displays a list of captured packets, with the first ICMP request packet (No. 21) selected. The middle pane shows the details of this packet, including Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP) layers. The bottom pane displays the raw data of the selected packet in hexadecimal and decimal form.

No.	Time	Source	Destination	Protocol	Length	Info
21	12.882756	192.168.0.153	142.250.193.142	ICMP	74	Echo (ping) request id=0x0001, seq=32/819
22	12.899402	142.250.193.142	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=32/819
34	13.892861	192.168.0.153	142.250.193.142	ICMP	74	Echo (ping) request id=0x0001, seq=33/844
35	13.913539	142.250.193.142	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=33/844
44	14.909323	192.168.0.153	142.250.193.142	ICMP	74	Echo (ping) request id=0x0001, seq=34/870
45	14.926765	142.250.193.142	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=34/870
48	15.922934	192.168.0.153	142.250.193.142	ICMP	74	Echo (ping) request id=0x0001, seq=35/896
49	15.940017	142.250.193.142	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=35/896
53	17.444545	192.168.0.1	192.168.0.153	ICMP	98	Echo (ping) request id=0xb76a, seq=0/0, t
170	48.244468	192.168.0.1	192.168.0.153	ICMP	98	Echo (ping) request id=0xb077, seq=0/0, t
184	50.267062	192.168.0.153	18.155.49.11	ICMP	74	Echo (ping) request id=0x0001, seq=36/921
185	50.270953	18.155.49.11	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=36/921
204	51.282379	192.168.0.153	18.155.49.11	ICMP	74	Echo (ping) request id=0x0001, seq=37/947
205	51.349594	18.155.49.11	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=37/947
216	52.295350	192.168.0.153	18.155.49.11	ICMP	74	Echo (ping) request id=0x0001, seq=38/972
217	52.329427	18.155.49.11	192.168.0.153	ICMP	74	Echo (ping) reply id=0x0001, seq=38/972

Frame 21: 74 bytes on wire (592 bits), 74 bytes captured (592 b) on interface 0
> Ethernet II, Src: Intel_fc:8d:b1 (8c:e9:ee:fc:8d:b1), Dst: DLink_8c:e9:ee:fc:8d:b1
> Internet Protocol Version 4, Src: 192.168.0.153, Dst: 142.250.193.142
> Internet Control Message Protocol

0000 a4 2a 95 9b 71 91 8c e9 ee fc 8d b1 08 00 45 00 ...*..q...
0010 00 3c 60 2e 00 00 80 01 00 00 c0 a8 00 99 8e fa ...<.....
0020 c1 8e 08 00 4d 3b 00 01 00 20 61 62 63 64 65 66 ...M;...
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ...ghijklmr
0040 77 61 62 63 64 65 66 67 68 69 ...wabcdefg

Internet Control Message Protocol: Protocol | Packets: 609 · Displayed: 19 (3.1%) · Dropped: 0 (0.0%) | Profile: Default

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:

The image shows a Wireshark packet capture window titled "Wireshark · Packet 19 · Wi-Fi". The packet list on the left shows "Internet Protocol Version 4, Src: 192.168.0.153, Dst: 192.168.0.1", "User Datagram Protocol, Src Port: 53378, Dst Port: 53", and "Domain Name System (query)". The packet details pane on the right shows the following fields:

- Transaction ID: 0xbb2f
- Flags: 0x0100 Standard query
- Questions: 1
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- Queries
 - google.com: type A, class IN

The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII. The ASCII column shows the query string "google.com" and the transaction ID "0xbb2f".

No.: 19 · Time: 12.857241 · Source: 192.168.0.153 · Destination: 192.168.0.1 · Protocol: DNS · Length: 70 · Info: Standard query 0xbb2f A google.com

☒ Show packet bytes Layout: Vertical (Stacked)

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.

