

Course:Cloud and Network Security – C3 - 2025

Module:Network Standards, Models & Protocols

Week1 Assignment2 Class Exercise:

Using Wireshark To View Network Traffic

Student Name:Eunice Atieno Adoyo

Student ID:CS-CNS10-25091

Submission Date: September 22, 2025

Introduction

This report summarizes a two-part networking lab focused on how data packets travel across networks. Using `ipconfig /all` and Wireshark, ICMP packets were captured to compare local and remote communication. The first part examined pings within a LAN, showing how IP and MAC addresses enable direct host-to-host interaction. The second part explored pings to remote servers, highlighting how packets are routed through a gateway. The analysis illustrates the roles of Layer 2 and Layer 3 addressing and how ARP helps resolve MAC addresses, offering insight into how packet headers direct data to its destination.

Table Of Content

Introduction	1
Answers To Questions	3
Part 1: Capture and Analyze Local ICMP Data in Wireshark	3
Step 1: Retrieve your PC interface addresses.	3
Step 2: Start Wireshark and begin capturing data.	4
Step 3: Examine the captured data	5
Part 2: Capture and Analyze Remote ICMP Data in Wireshark	8
Step 1: Start capturing data on the interface.	8
Step 2: Examining and analyzing the data from the remote hosts.	12
Reflection Question	13
Conclusion	14

Answers To Questions

Part 1: Capture and Analyze Local ICMP Data in Wireshark

In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will then analyze the IP and MAC addresses for the source and destination. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC interface addresses.

For this lab, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

- a. In a command prompt window, enter `ipconfig /all` to the IP address of your PC interface, its description, and its MAC (physical) address.

```
C:\WINDOWS\system32\cmd. x + v
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. . . . . : 92-5B-AD-35-34-C7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : 
Description . . . . . : Realtek RTL8821CE 802.11ac PCIe Adapter
Physical Address. . . . . : 10-5B-AD-35-34-C7
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::c50:d67d:ce1a:ff4h%3(Preferred)
IPv4 Address. . . . . : 192.168.1.4(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, September 22, 2025 10:33:32 AM
Lease Expires . . . . . : Tuesday, September 23, 2025 10:37:26 AM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 51403693
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-2E-28-55-C4-65-16-8D-6A-8E
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:
```

MAC (Physical) Address: 10-5B-AD-35-34-C7

IP Address: 192.168.1.4

Default Gateway(Router): 192.161.1.1

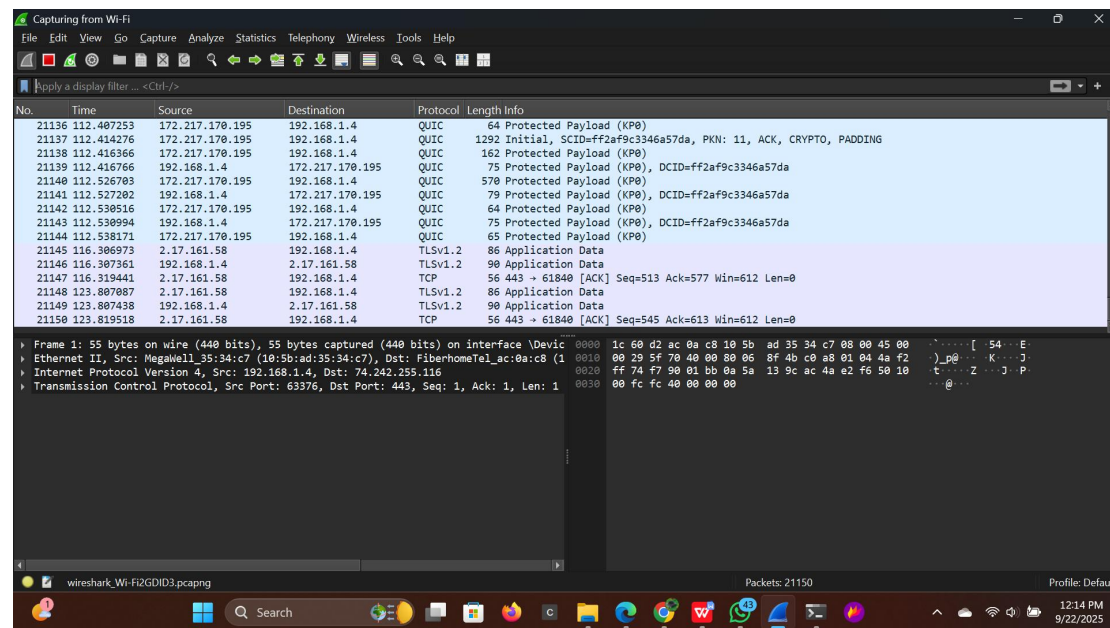
b. Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not proceed with your own MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

a. Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.

b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors depending on the protocol.

This information will scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark.



For this lab, we are only interested in displaying ICMP PDU's. Type icmp in the Filter box at the top of Wireshark and then press Enter or click the Apply button. This will display only ICMP (ping) PDUs.

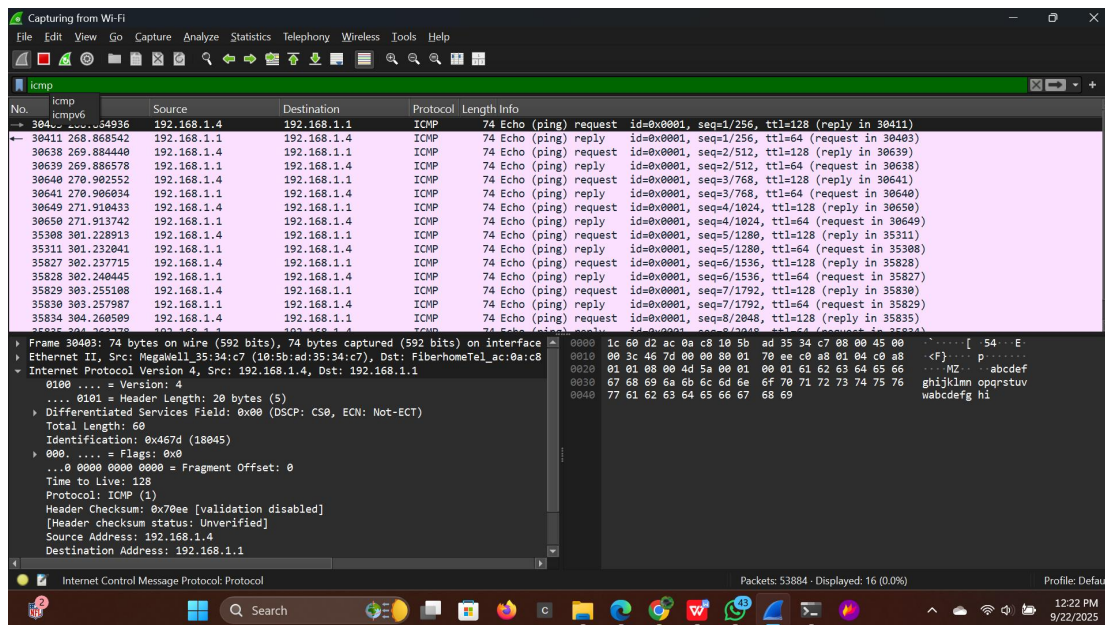
c. The filter causes all data in the top window to disappear, but you are still capturing traffic on the interface. Navigate to a command prompt window and ping the IP address that you received from your team member.

```
C:\WINDOWS\system32\cmd. x + v
C:\Users\PC> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\PC>
```



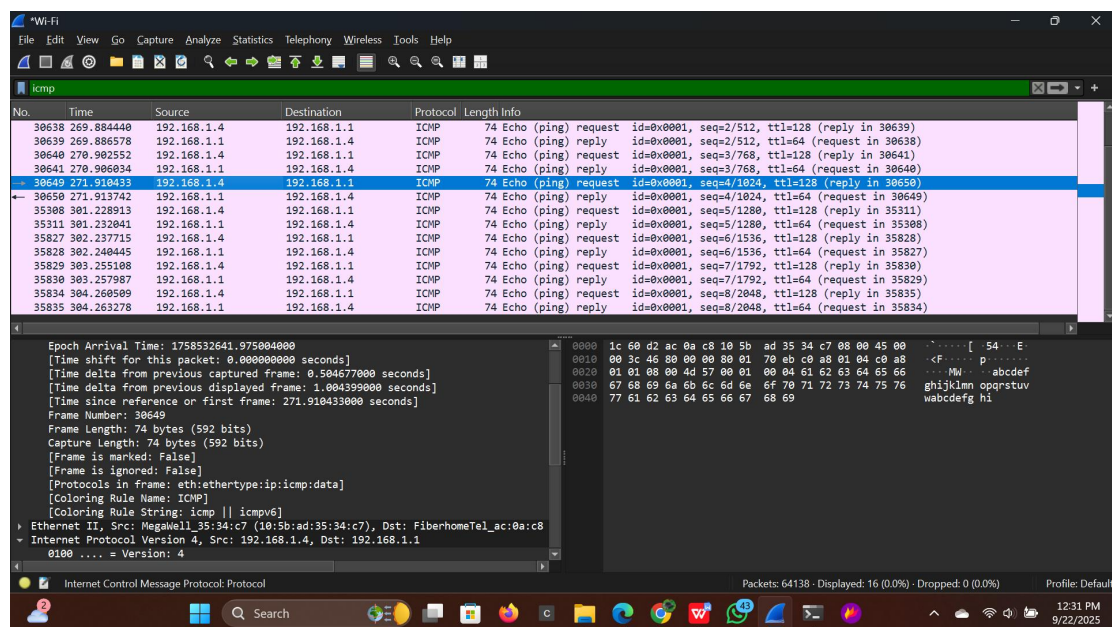
d. Stop capturing data by clicking the Stop Capture icon.

Step 3: Examine the captured data.

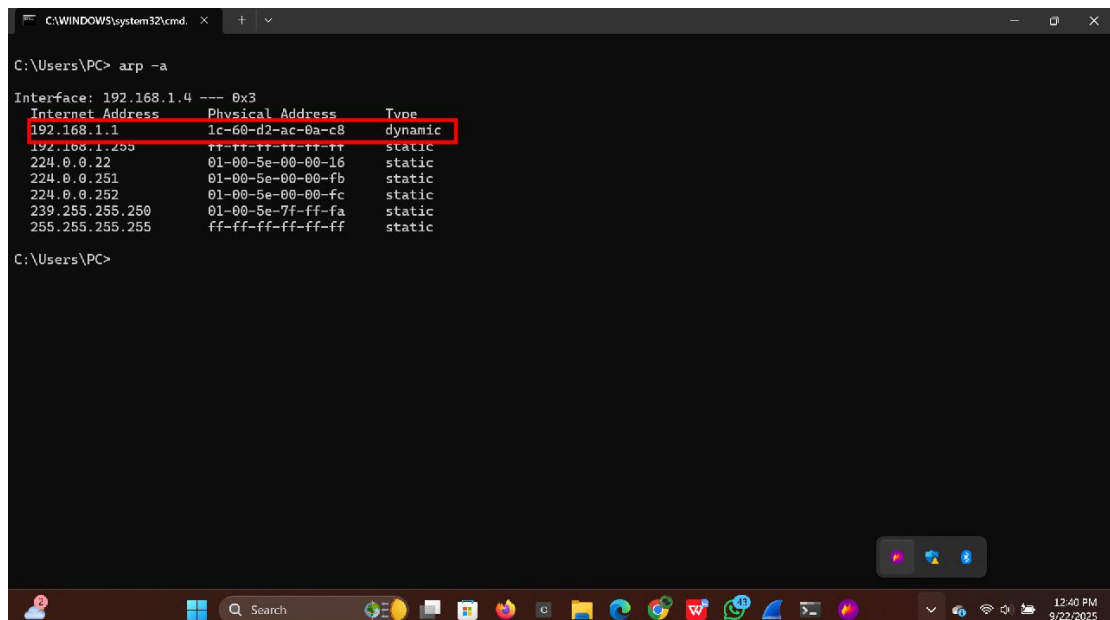
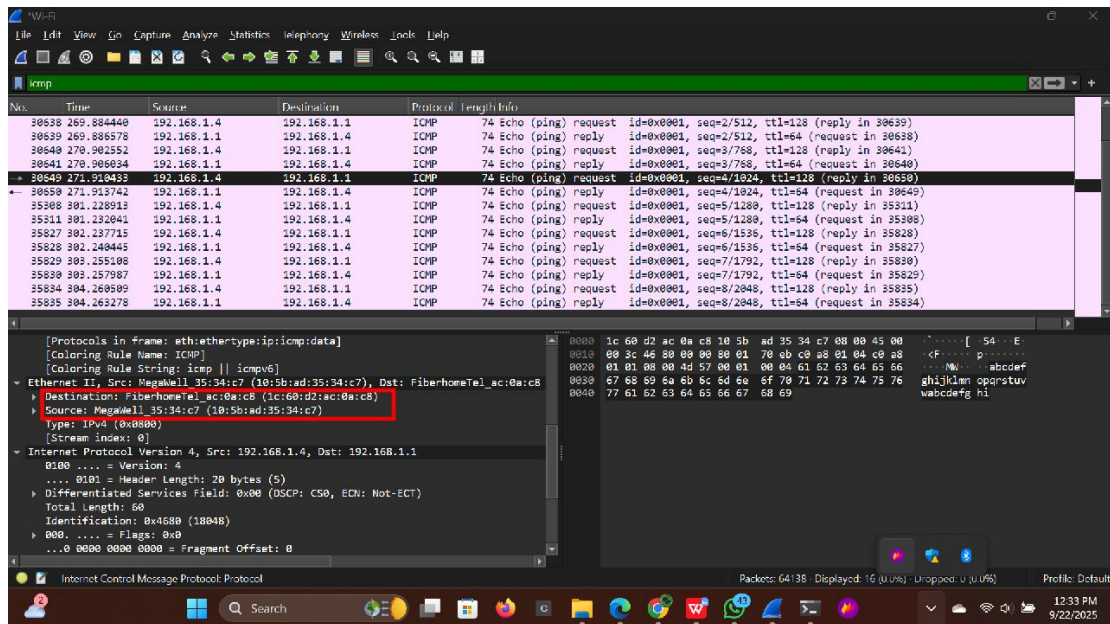
In Step 3, examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections: 1) the top section displays

the list of PDU frames captured with a summary of 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, and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

- a. 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 of the teammate PC that you pinged.



- b.
- c. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.



Does the source MAC address match your PC interface?

Yes, The source MAC address in Wireshark matches my MAC (Physical) Address which is 10-5B-AD-35-34-C7

Does the destination MAC address in Wireshark match your team member MAC address?

Yes, The destination MAC address(1c-60-d2-ac-0a-c8

) in Wireshark matches my router IP address since I pinged my default gateway(192.168.1.1) instead.

How is the MAC address of the pinged PC obtained by your PC?

My PC obtains the MAC address of the default gateway using the Address Resolution Protocol (ARP). i.e arp -a command

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about the data from the first experiment in Part 1.

Step 1: Start capturing data on the interface.

- a. Start the data capture again.
- b. A window prompt will ask to save the previously captured data before starting another capture. It is not necessary to save the data. Click Continue without Saving.
- c. With the capture active, ping the following three website URLs from a Windows command prompt:

www.yahoo.com

```
C:\WINDOWS\system32\cmd. x + v

C:\Users\PC> ping www.yahoo.com

Pinging me-ycpi-cf-www.g06.yahoodns.net [102.165.180.206] with 32 bytes of data:
Reply from 102.165.180.206: bytes=32 time=59ms TTL=54
Reply from 102.165.180.206: bytes=32 time=61ms TTL=54
Reply from 102.165.180.206: bytes=32 time=59ms TTL=54
Reply from 102.165.180.206: bytes=32 time=57ms TTL=54

Ping statistics for 102.165.180.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 57ms, Maximum = 61ms, Average = 59ms

C:\Users\PC>
```

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
6189	65.688342	192.168.1.4	102.165.180.206	ICMP	74	Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 6187)
6187	65.742176	102.165.180.206	192.168.1.4	ICMP	74	Echo (ping) reply id=0x0001, seq=9/2304, ttl=54 (request in 6186)
6188	66.794227	192.168.1.4	102.165.180.206	ICMP	74	Echo (ping) request id=0x0001, seq=10/2580, ttl=128 (reply in 6189)
6189	66.755260	102.165.180.206	192.168.1.4	ICMP	74	Echo (ping) reply id=0x0001, seq=10/2580, ttl=54 (request in 6188)
6190	67.719548	192.168.1.4	102.165.180.206	ICMP	74	Echo (ping) request id=0x0001, seq=11/2816, ttl=128 (reply in 6191)
6191	67.778913	102.165.180.206	192.168.1.4	ICMP	74	Echo (ping) reply id=0x0001, seq=11/2816, ttl=54 (request in 6190)
6592	68.734245	192.168.1.4	102.165.180.206	ICMP	74	Echo (ping) request id=0x0001, seq=12/3072, ttl=128 (reply in 6591)
6631	68.791457	102.165.180.206	192.168.1.4	ICMP	74	Echo (ping) reply id=0x0001, seq=12/3072, ttl=54 (request in 6592)

Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: MegaWell_35:34:c7 (10:5b:ad:35:34:c7), Dst: FiberhomeTel_ac:0a:c8
 Destination: FiberhomeTel_ac:0a:c8 (1c:60:d2:ac:0a:c8)
 Source: MegaWell_35:34:c7 (10:5b:ad:35:34:c7)
 Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 102.165.180.206
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60

0000 1c 60 d2 ac 0a c8 10 5b ad 35 34 c7 08 00 45 00 54... E
0010 00 3c 5b b8 00 00 00 01 01 09 c0 a8 01 04 66 a5 <<..... f
0020 b4 ce 08 00 4d 52 00 01 00 09 61 52 63 64 65 66NR... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

Wi-Fi <live capture in progress> Packets: 40407 Displayed: 8 (0.0%) Profile: Default

www.cisco.com

```
C:\WINDOWS\system32\cmd. x + v

C:\Users\PC> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 bytes of data:
Reply from 2.17.168.94: bytes=32 time=11ms TTL=58
Reply from 2.17.168.94: bytes=32 time=12ms TTL=58
Reply from 2.17.168.94: bytes=32 time=12ms TTL=58
Reply from 2.17.168.94: bytes=32 time=13ms TTL=58

Ping statistics for 2.17.168.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\Users\PC>
```

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	icmp	Source	Destination	Protocol	Length	Info
77	20.907452	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 78)
78	21.912356	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=58 (request in 77)
80	21.924535	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 80)
81	22.921693	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 82)
82	22.934042	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=58 (request in 81)
86	23.935158	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 87)
87	23.948591	192.168.1.4	2.17.168.94	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=58 (request in 86)

Capture Length: 74 bytes (592 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:icmp:data]

[Coloring Rule Name: ICMP]

[Coloring Rule String: icmp || icmpv6]

Ethernet II, Src: Megawell_35:34:c7 (10:5b:ad:35:34:c7), Dst: FiberhomeTel_ac:0a:c8 (1c:60:d2:ac:0a:c8)

Source: Megawell_35:34:c7 (10:5b:ad:35:34:c7)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.1.4, Dst: 2.17.168.94

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

0000 1c 60 d2 ac 0a c8 10 5b ad 35 34 c7 08 00 45 00 [54 ... E

0010 00 3c 42 a0 00 00 00 01 8c 05 c0 a8 01 04 02 11 <B<

0020 a8 5e 08 00 4d 42 00 01 00 19 61 62 63 64 65 66 ^..MB...abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcedfg hi

Internet Control Message Protocol: Protocol

Packets: 870 - Displayed: 8 (0.9%)

Profile: Default

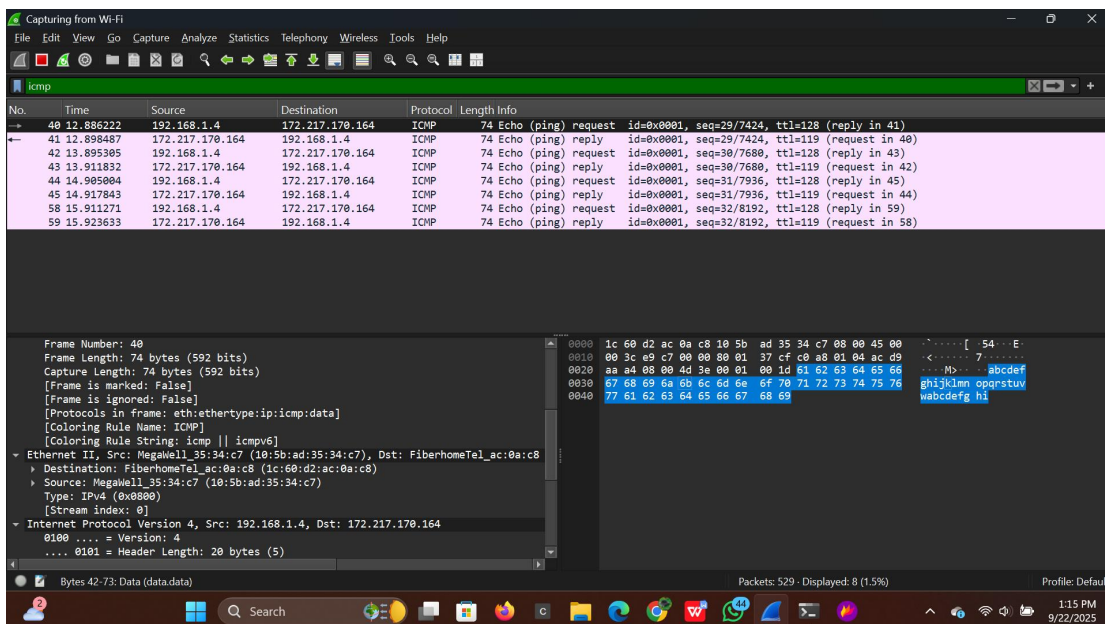
www.google.com

```
C:\WINDOWS\system32\cmd. x + v
C:\Users\PC> ping www.google.com

Pinging www.google.com [172.217.170.164] with 32 bytes of data:
Reply from 172.217.170.164: bytes=32 time=12ms TTL=119
Reply from 172.217.170.164: bytes=32 time=16ms TTL=119
Reply from 172.217.170.164: bytes=32 time=13ms TTL=119
Reply from 172.217.170.164: bytes=32 time=12ms TTL=119

Ping statistics for 172.217.170.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 16ms, Average = 13ms

C:\Users\PC>
```



- c. As soon as you begin pinging the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP addresses received for each URL.
- d. You can stop capturing data by clicking the Stop Capture icon.

Step 2: Examining and analyzing the data from the remote hosts.

Review the captured data in Wireshark and examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

IP address for www.yahoo.com:

102.165.180.206

MAC address for www.yahoo.com:

1c-60-d2-ac-0a-c8

IP address for www.cisco.com:

2.17.168.94

MAC address for www.cisco.com:

1c-60-d2-ac-0a-c8

IP address for www.google.com:

172.217.170.164

MAC address for www.google.com:

1c-60-d2-ac-0a-c8

What is significant about this information?

Even though websites like Yahoo, Cisco, and Google have different IP addresses, my computer sends data to the same MAC address i.e my router's. That's because my PC doesn't send data directly to those websites; it sends it to the default gateway (router), which then forwards the packets to the correct destination on the internet. So in Wireshark, the destination MAC address seen is that of my router, not the final server.

How does this information differ from the local ping information you received in Part 1?

This differs from a local ping because a local ping communicates directly with another device on the same network. My computer uses ARP to find the MAC address of that device and sends the packet straight to it. In contrast, with a remote ping, my computer can't access the MAC address of the distant server, so it sends the packet to the router's MAC address instead. The router then forwards it to the correct destination on the internet.

Reflection Question

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

Wireshark shows actual MAC addresses for local hosts because LANs operate at Layer 2 of the OSI model, where MAC addresses are used for direct host-to-host communication. When you ping a local device, your PC uses ARP to find and store its MAC address, then sends the packet directly to it.

In contrast, when pinging a remote host like Google or Yahoo, your PC sends the packet to the default gateway's MAC address. The gateway forwards it to the destination. As the packet moves across the internet, MAC addresses change at each hop and are only relevant within each local network segment. That's why Wireshark only shows the MAC address of your router not the final destination.

Conclusion

This lab demonstrated how network protocols function across different layers to enable communication. Wireshark analysis showed that local pings include both source and destination MAC addresses, resolved via ARP within the same network segment. In contrast, remote pings display destination IPs but use the MAC address of the default gateway, confirming that external traffic is first routed through the gateway. This highlights the role of MAC addresses in local delivery and IP addresses in end-to-end communication across networks, offering key insight into how data travels through the Internet.