Cloud and Network Security-C1-2026

Student Name: Felix Webbo

Student No: CS-CNS11-26044

MONDAY, JANUARY 20, 2026

Week 1: Assignment 2

Class Exercise: **Use of Wireshark to View and Analyze Network Traffic**

1 ABSTRACT

This laboratory exercise investigated the use of Wireshark as a network protocol analyzer to capture and analyze Internet Control Message Protocol (ICMP) traffic on both local and remote networks. The experiment focused on identifying IP and MAC addressing behavior, protocol encapsulation, and the role of network devices in packet delivery. Through controlled ping operations and packet inspection, the study demonstrated how data is structured at different OSI layers and highlighted the differences between local and remote network communication.

Table of Contents

1 ABSTRACT ii
2 INTRODUCTION 2
3 OBJECTIVES 2
4 NETWORK TOPOLOGY 2
5 RESOURCES 2
6 METHODOLOGY 3
6.1 Part 1: Capture and Analyze Local ICMP Data 3
6.1.1 Step 1: Retrieving Interface Information 3
6.1.2 Step 2: Starting Wireshark Capture 4
6.1.3 Step 3: Examine the captured data. 7
6.2 Part 2: Capture and Analyze Remote ICMP Data in Wireshark 8
6.2.1 Step 1: Start capturing data on the interface. 8
6.2.2 Step 2: Examining and analyzing the data from the remote hosts. 10
6.3 The significant of this information 10
6.4 Differences Between Local and Remote ICMP Ping Information 11
6.5 Reflection Question 11
7 SECURITY CONSIDERATIONS 11
8 CONCLUSION 11
9 References 11

2 INTRODUCTION

Modern computer networks rely on layered communication models to transmit data efficiently and reliably. Tools such as Wireshark enable network engineers and students to visualize real packet exchanges, making theoretical concepts easier to understand. ICMP, commonly used by the ping utility, provides an ideal protocol for studying packet flow, addressing, and encapsulation.

This lab aimed to analyze ICMP packets generated from both local and remote hosts using Wireshark, with emphasis on Ethernet frame MAC addresses and IP packet addressing.

3 OBJECTIVES

The objectives of this experiment were:

1. To capture and analyze local ICMP traffic using Wireshark.
2. To capture and analyze remote ICMP traffic using Wireshark.
3. To compare MAC and IP addressing behavior between local and remote communication.
4. To understand packet encapsulation in Ethernet and IP layers.

4 NETWORK TOPOLOGY

- ✓ Internet
- ✓ Default Gateway Router
- ✓ Router
- ✓ LAN

A Windows PC was connected to a local-area network through a router that provided access to the internet.

5 RESOURCES

- ❖ One Windows PC with internet access
- ❖ Additional PCs on the LAN
- ❖ Wireshark software

6 METHODOLOGY

6.1 Part 1: Capture and Analyze Local ICMP Data

6.1.1 Step 1: Retrieving Interface Information

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

The command **ipconfig /all** was executed in the command prompt to obtain:

- IPv4 address
- Subnet mask
- Default gateway
- MAC (physical) address

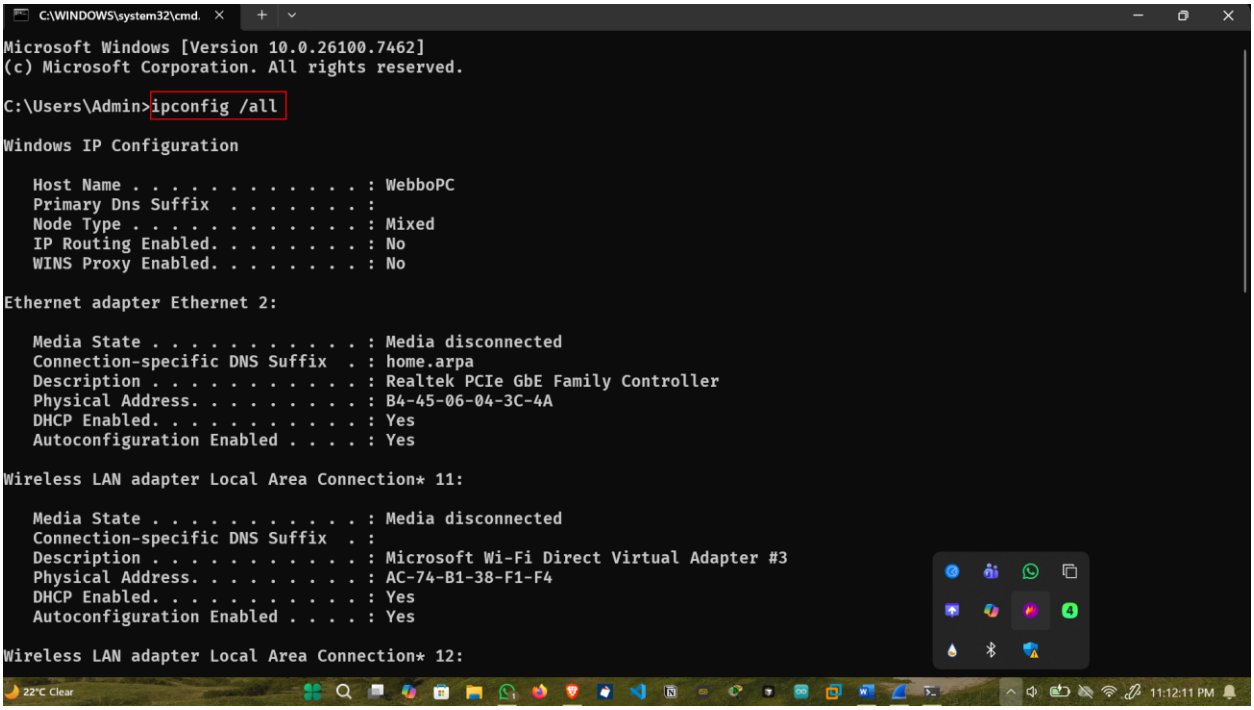

fig 6.1 ipconfig result

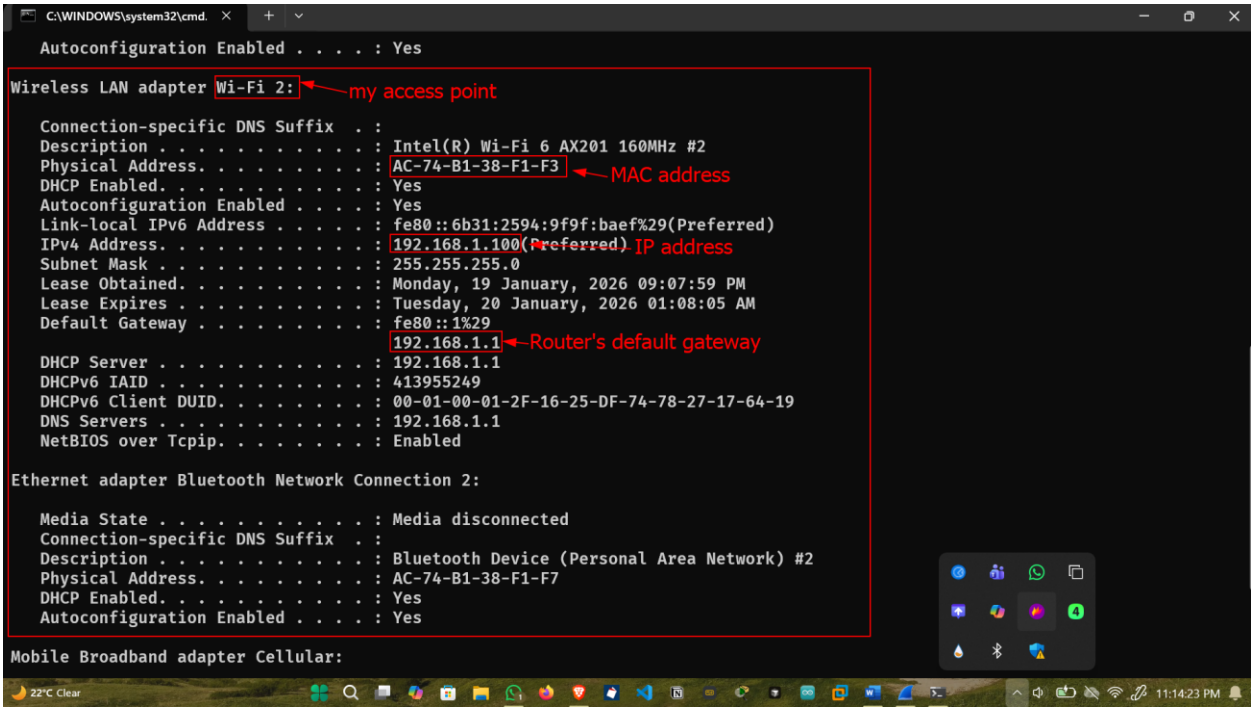

fig 6.2 ipconfig

6.1.2 Step 2: Starting Wireshark Capture

- Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.
- Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol. A filter was apply to make it easier to view and work with the data that is being captured by Wireshark.
- This 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. (here, router's default gateway IP)
- Stop capturing data by clicking the **Stop Capture** icon.

Wireshark was launched and the active network interface was selected. Packet capture began immediately, displaying multiple protocol frames in different colors.

To focus only on ICMP traffic, a filter was applied:

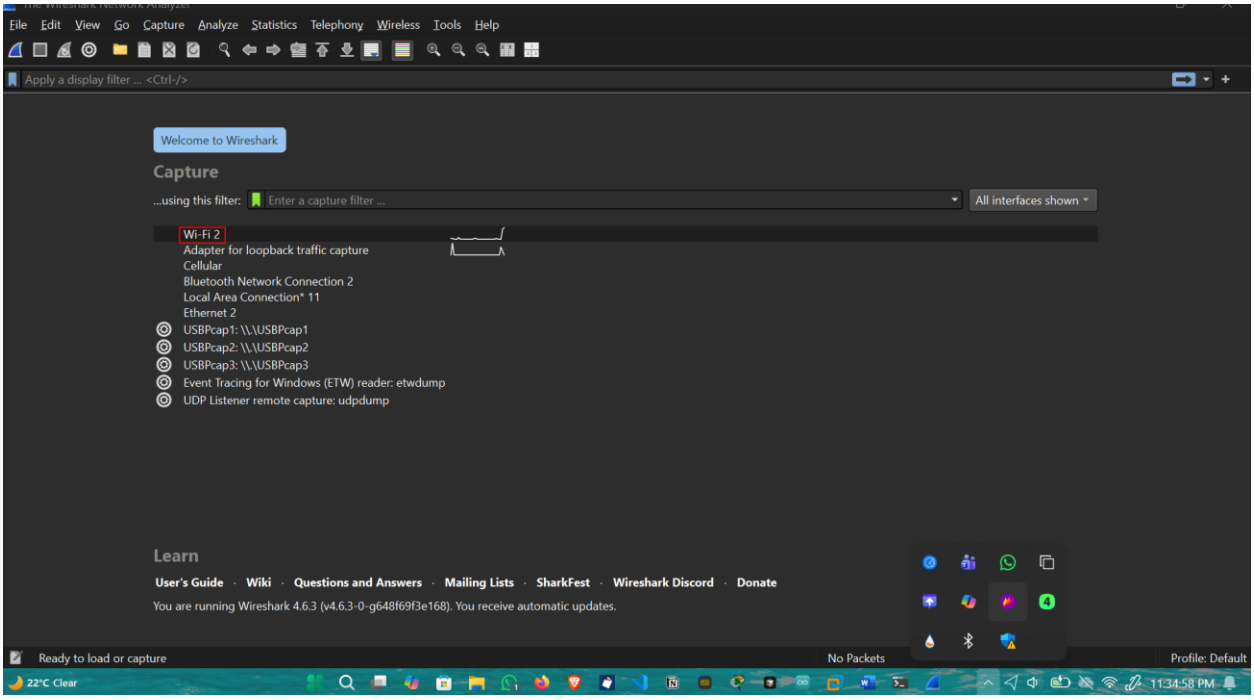

fig 6.3 wireshark

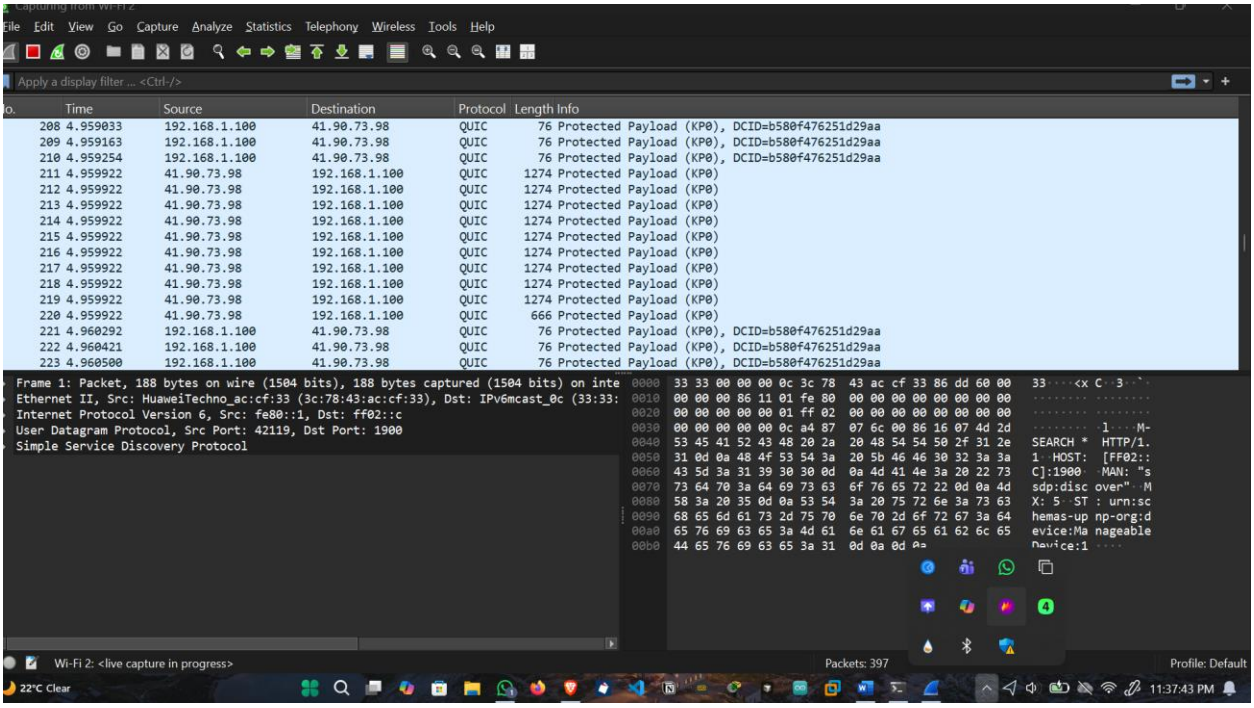

fig 6.4 wireshark

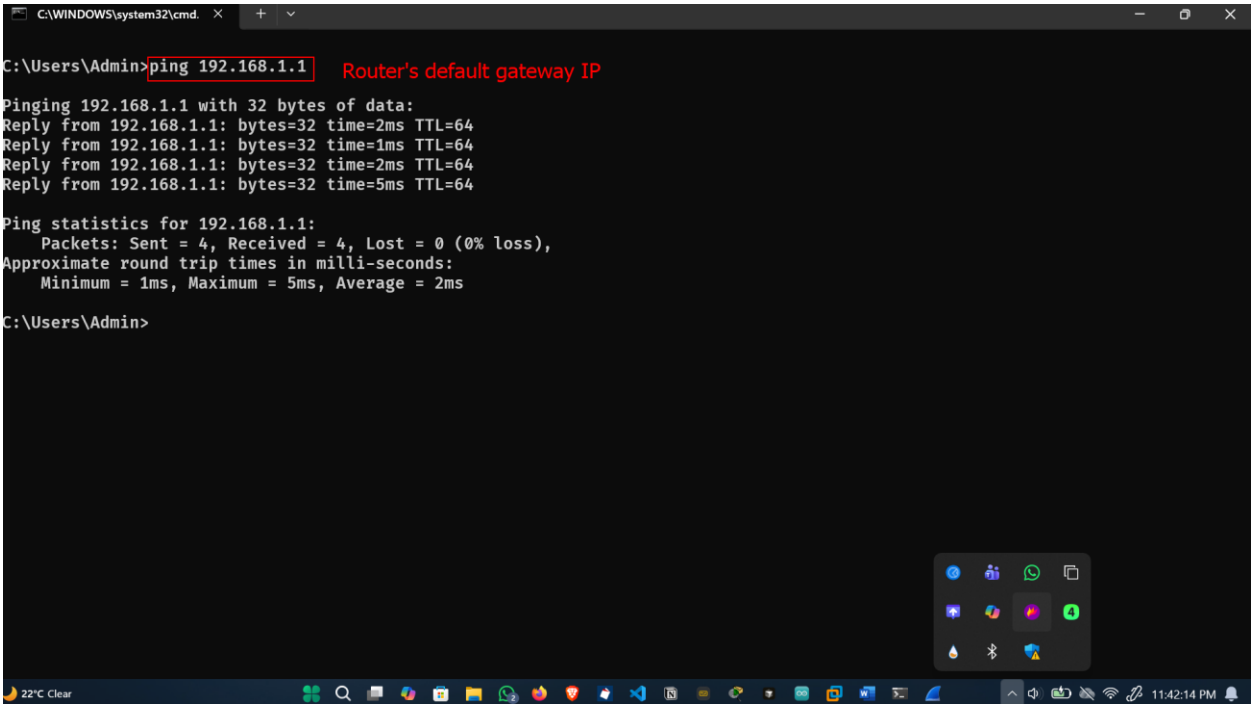
C:\WINDOWS\system32\cmd.
C:\Users\Admin>ping 192.168.1.1
Router's default gateway IP
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms 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 = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\Admin>
22°C Clear
11:42:14 PM

fig 6.5

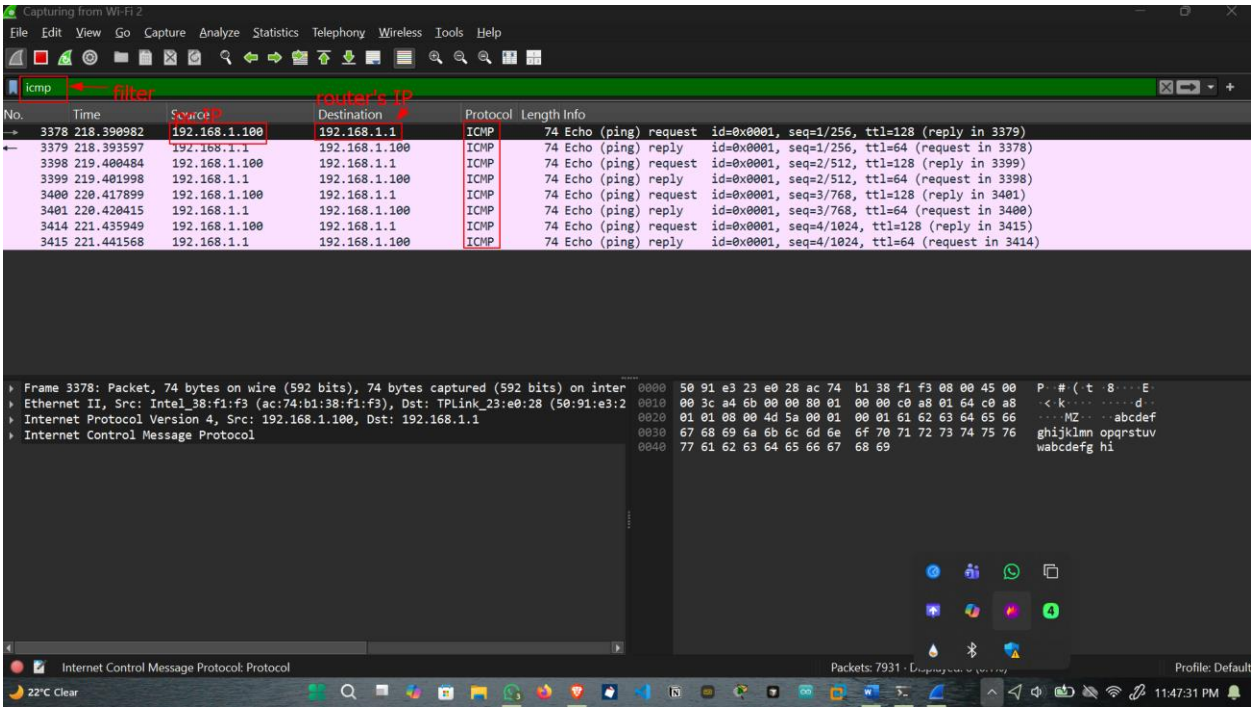
Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
filter
router's IP
No. Time Source Destination Protocol Length Info
3378 218.390982 192.168.1.100 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 3379)
3379 218.393597 192.168.1.1 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 3378)
3398 219.400484 192.168.1.100 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 3399)
3399 219.401998 192.168.1.1 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 3398)
3400 220.417899 192.168.1.100 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 3401)
3401 220.420415 192.168.1.1 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 3400)
3414 221.435949 192.168.1.100 192.168.1.1 ICMP 74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 3415)
3415 221.441568 192.168.1.1 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 3414)
Frame 3378: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inter
Ethernet II, Src: Intel_38:f1:f3 (ac:74:b1:38:f1:f3), Dst: TPLink_23:e0:28 (50:91:e3:2
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.1
Internet Control Message Protocol
0000 50 91 e3 23 e0 28 ac 74 b1 38 f1 f3 08 00 45 00
0010 00 3c a4 6b 00 00 80 01 00 00 c0 a8 01 64 c0 a8
0020 01 01 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
Internet Control Message Protocol: Protocol
Packets: 7931
Profile: Default
22°C Clear
11:47:31 PM

fig 6.6

6.1.3 Step 3: Examine the captured data.

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 of the teammate PC that you pinged.
    * 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.

The captured packets were analyzed using the three Wireshark panes:

1. Frame list
2. Packet details
3. Raw packet data

Observations

Answers to the questions

- The source MAC matched the local interface MAC.
- The destination MAC matched the Router MAC.
- The MAC address of the destination PC was obtained using the Address Resolution Protocol (ARP), confirming that ARP was responsible for mapping IP addresses to MAC addresses on the LAN.

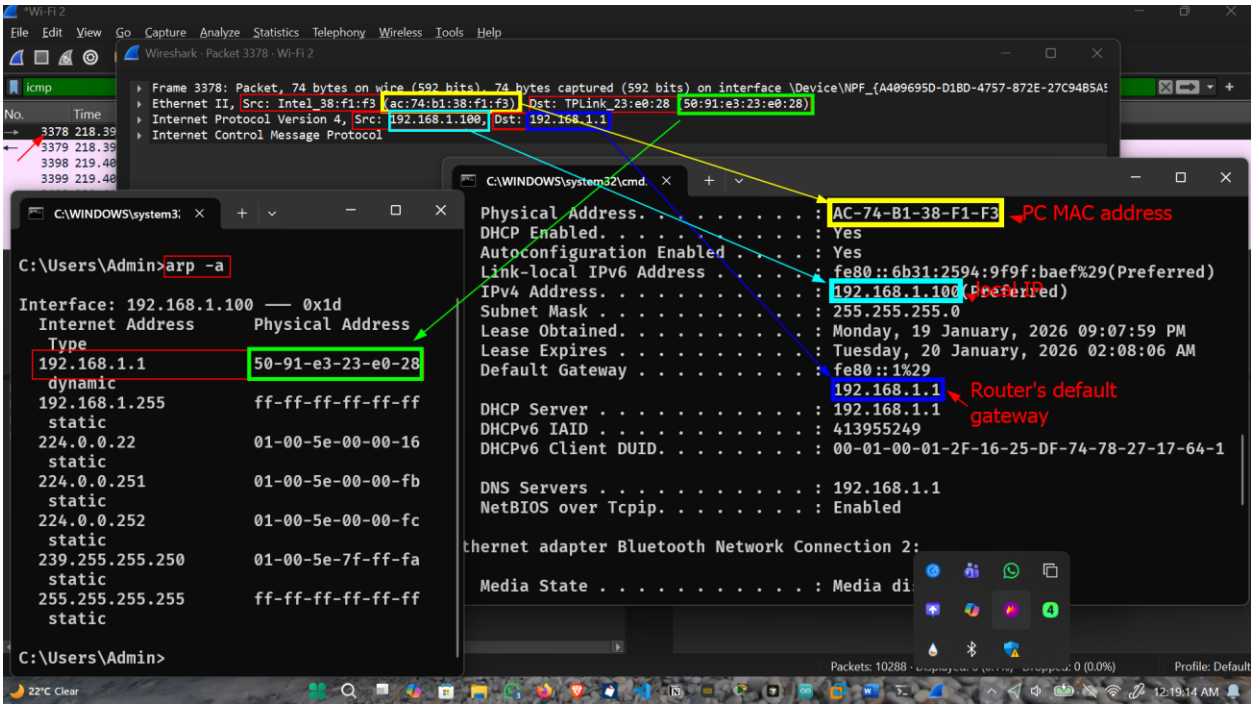

fig 6.7

6.2 Part 2: Capture and Analyze Remote ICMP Data in Wireshark

A ping was performed on remote hosts (hosts not on the LAN) and examined the generated data from those pings.

6.2.1 Step 1: Start capturing data on the interface.

- Start the data capture again.
- A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.
- With the capture active, ping the following three website URLs from a Windows command prompt:
  - www.yahoo.com
  - www.cisco.com
  - www.google.com
- You can stop capturing data by clicking the **Stop Capture** icon.

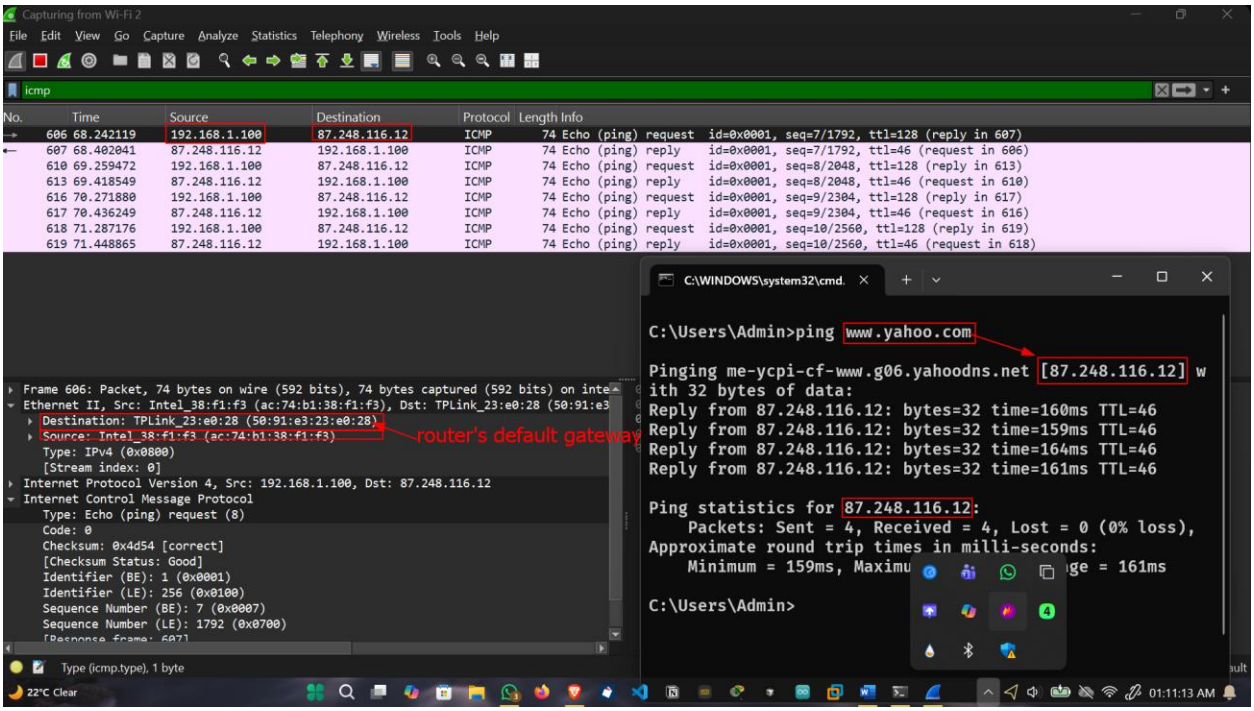
Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
606 68.242119 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 607)
607 68.402041 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=46 (request in 606)
610 69.259472 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 613)
613 69.418549 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=8/2048, ttl=46 (request in 610)
616 70.271880 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 617)
617 70.436249 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=46 (request in 616)
618 71.287176 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 619)
619 71.448865 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=46 (request in 618)
Frame 606: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on inte
Ethernet II, Src: Intel_38:f1:f3 (ac:74:b1:38:f1:f3), Dst: TPLink_23:e0:28 (50:91:e3
Destination: TPLink_23:e0:28 (50:91:e3:23:e0:28)
Source: Intel_38:f1:f3 (ac:74:b1:38:f1:f3)
router's default gateway
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 87.248.116.12
Internet Control Message Protocol
Type: Echo (ping) request (8)
Code: 0
Checksum: 0x4d54 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 7 (0x0007)
Sequence Number (LE): 1792 (0x0700)
Type (icmp.type), 1 byte
C:\WINDOWS\system32\cmd.
C:\Users\Admin>ping www.yahoo.com
Pinging me-ycpi-cf-www.g06.yahoodns.net [87.248.116.12] w
ith 32 bytes of data:
Reply from 87.248.116.12: bytes=32 time=160ms TTL=46
Reply from 87.248.116.12: bytes=32 time=159ms TTL=46
Reply from 87.248.116.12: bytes=32 time=164ms TTL=46
Reply from 87.248.116.12: bytes=32 time=161ms TTL=46
Ping statistics for 87.248.116.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 159ms, Maximu
ge = 161ms
C:\Users\Admin>
22°C Clear
01:11:13 AM

fig 6.8

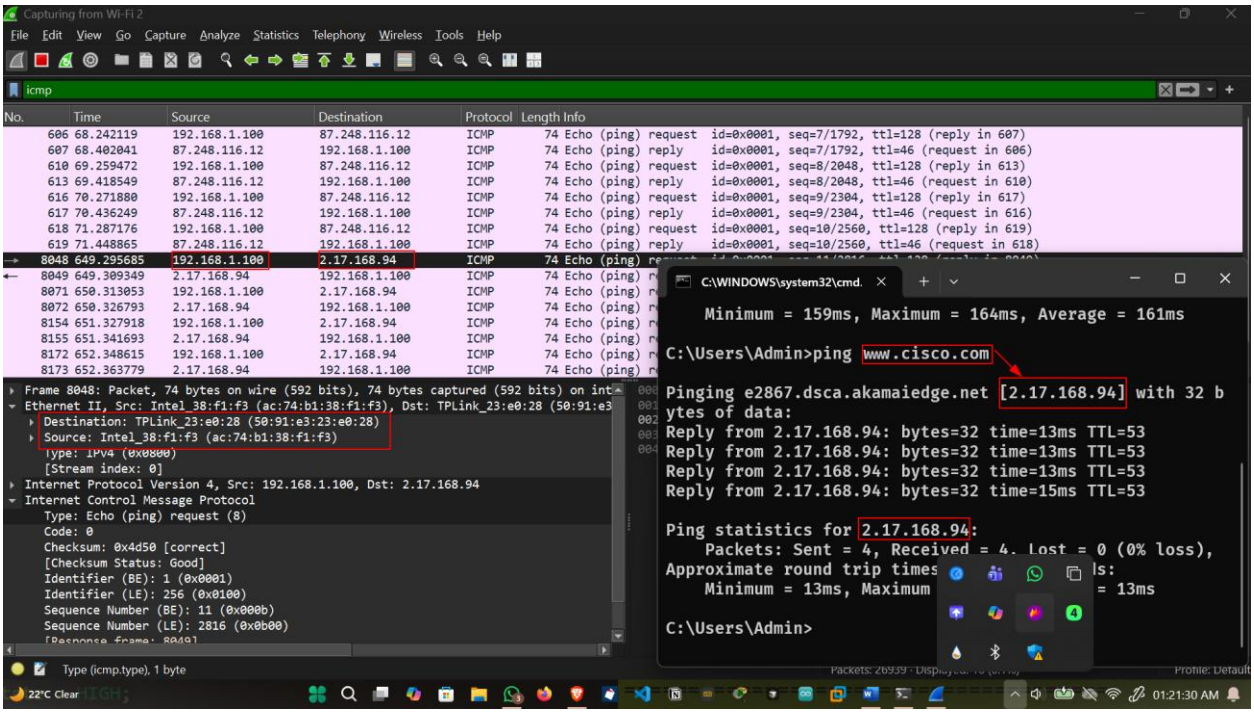
Capturing from Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
606 68.242119 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 607)
607 68.402041 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=7/1792, ttl=46 (request in 606)
610 69.259472 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 613)
613 69.418549 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=8/2048, ttl=46 (request in 610)
616 70.271880 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=9/2304, ttl=128 (reply in 617)
617 70.436249 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=9/2304, ttl=46 (request in 616)
618 71.287176 192.168.1.100 87.248.116.12 ICMP 74 Echo (ping) request id=0x0001, seq=10/2560, ttl=128 (reply in 619)
619 71.448865 87.248.116.12 192.168.1.100 ICMP 74 Echo (ping) reply id=0x0001, seq=10/2560, ttl=46 (request in 618)
8048 649.295685 192.168.1.100 2.17.168.94 ICMP 74 Echo (ping)
8049 649.309349 2.17.168.94 192.168.1.100 ICMP 74 Echo (ping)
8071 650.313053 192.168.1.100 2.17.168.94 ICMP 74 Echo (ping)
8072 650.326793 2.17.168.94 192.168.1.100 ICMP 74 Echo (ping)
8154 651.327918 192.168.1.100 2.17.168.94 ICMP 74 Echo (ping)
8155 651.341693 2.17.168.94 192.168.1.100 ICMP 74 Echo (ping)
8172 652.348615 192.168.1.100 2.17.168.94 ICMP 74 Echo (ping)
8173 652.363779 2.17.168.94 192.168.1.100 ICMP 74 Echo (ping)
Frame 8048: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on int
Ethernet II, Src: Intel_38:f1:f3 (ac:74:b1:38:f1:f3), Dst: TPLink_23:e0:28 (50:91:e3
Destination: TPLink_23:e0:28 (50:91:e3:23:e0:28)
Source: Intel_38:f1:f3 (ac:74:b1:38:f1:f3)
Type: IPv4 (0x0800)
[Stream index: 0]
Internet Protocol Version 4, Src: 192.168.1.100, Dst: 2.17.168.94
Internet Control Message Protocol
Type: Echo (ping) request (8)
Code: 0
Checksum: 0x4d50 [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 11 (0x000b)
Sequence Number (LE): 2816 (0x0b00)
Type (icmp.type), 1 byte
C:\WINDOWS\system32\cmd.
Minimum = 159ms, Maximum = 164ms, Average = 161ms
C:\Users\Admin>ping www.cisco.com
Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 b
ytes of data:
Reply from 2.17.168.94: bytes=32 time=13ms TTL=53
Reply from 2.17.168.94: bytes=32 time=13ms TTL=53
Reply from 2.17.168.94: bytes=32 time=13ms TTL=53
Reply from 2.17.168.94: bytes=32 time=15ms TTL=53
Ping statistics for 2.17.168.94:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times
ls:
Minimum = 13ms, Maximum
= 13ms
C:\Users\Admin>
22°C Clear
01:21:30 AM

fig 6.9

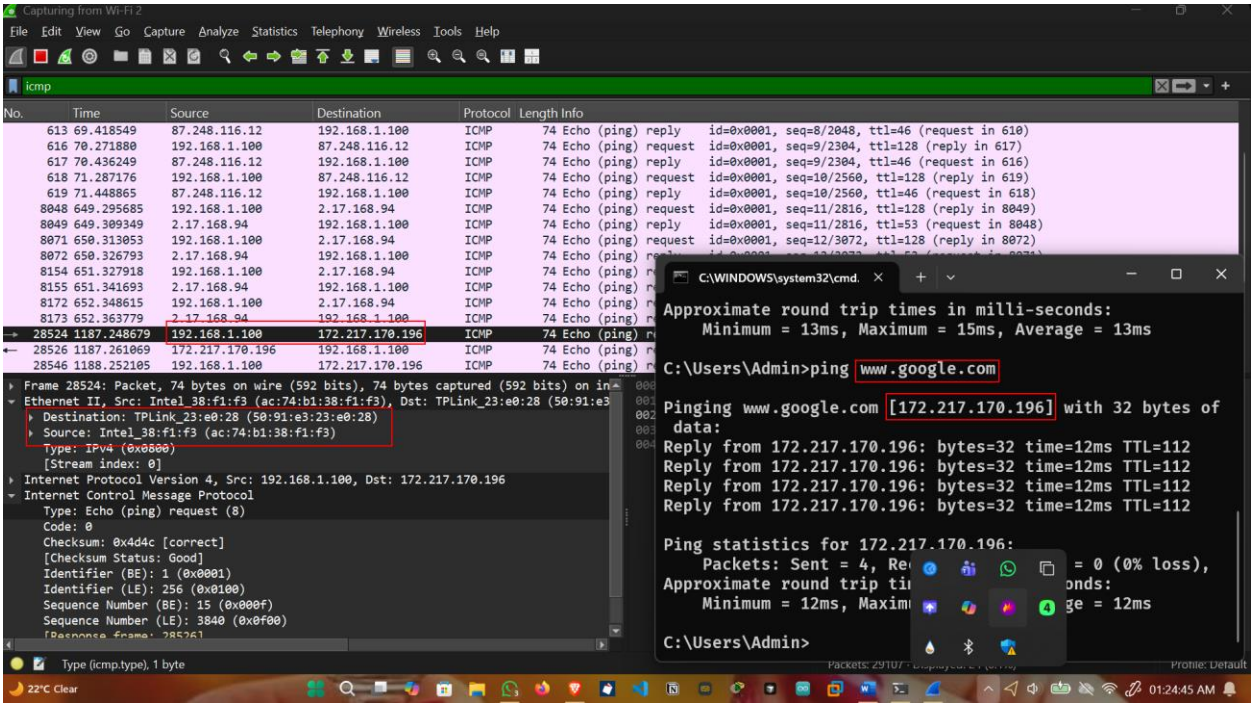

fig 6.10

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

The ICMP packets were analyzed and the following were observed.

Table 6.1

Website	Destination IP	Destination MAC
Yahoo	87.248.116.12	Router Default gateway MAC (50-91-e3-23-e0-28)
Cisco	2.17.168.94	Router Default gateway MAC (50-91-e3-23-e0-28)
Google	172.217.170.196	Router Default gateway MAC (50-91-e3-23-e0-28)

6.3 The significant of this information

The significant observation was that although the destination IP addresses corresponded to the remote servers (Yahoo, Cisco, and Google), the destination MAC address in all captured frames belonged to the local default gateway router. This demonstrated that Ethernet communication only occurs within the local network segment, and packets destined for remote networks are always forwarded first to the router, which then handles further delivery across the internet.

This confirmed the layered operation of networking, where Layer 2 addresses are used only for local delivery, while Layer 3 addresses identify the final destination.

6.4 Differences Between Local and Remote ICMP Ping Information

In Part 1, when pinging a local host, both the destination IP address and destination MAC address belonged to the target PC on the same LAN. The communication occurred directly between the two devices.

In contrast, in Part 2, when pinging remote hosts, the destination IP addresses belonged to remote servers, but the destination MAC addresses always belonged to the default gateway router. This difference highlighted the role of the router as an intermediary device for all off-LAN communication.

6.5 Reflection Question

Wireshark only captured MAC addresses of devices on the local network segment. Remote hosts were not directly reachable at Layer 2, so frames were addressed to the router's MAC address instead. The router then forwarded packets across multiple networks until they reached the remote host.

7 SECURITY CONSIDERATIONS

The lab emphasized that packet sniffing can expose sensitive network data. This reinforced the importance of network security policies and access controls when using packet capture tools.

8 CONCLUSION

The Wireshark laboratory successfully demonstrated how ICMP packets were transmitted and encapsulated across network layers. The differences between local and remote communication were clearly observed through MAC and IP address analysis. The experiment reinforced theoretical concepts of ARP, DNS, routing, and OSI layering while providing practical hands-on experience with real network traffic.

9 References

1. Cisco Networking Academy
2. Wireshark User Documentation