Course : Cloud and Network Security- C1-2026

Name : Jacob Matara

ID No: CS-CNS11-26059

Friday, January 23,2026

Week 1, Assignment 2

Use Wireshark to Examine Network Traffic

Introduction

Wireshark is a powerful software protocol analyzer, commonly known as a packet sniffer used to troubleshoot networks, analysis and to some extent education purposes like in my case. This tool captures each Protocol Data Unit (PDU) travelling across the network and decodes its content according to the appropriate specifications.
In this lab, I used wireshark to capture and analyze ICMP (Internet Control Message Protocol) packets generated by the ***ping*** command. The objective was to examine both local and remote network traffic, understand the differences between Layer 2(MAC) & layer 3(IP) addressing and observe how packets are routed through a default gateway to reach remote destinations.

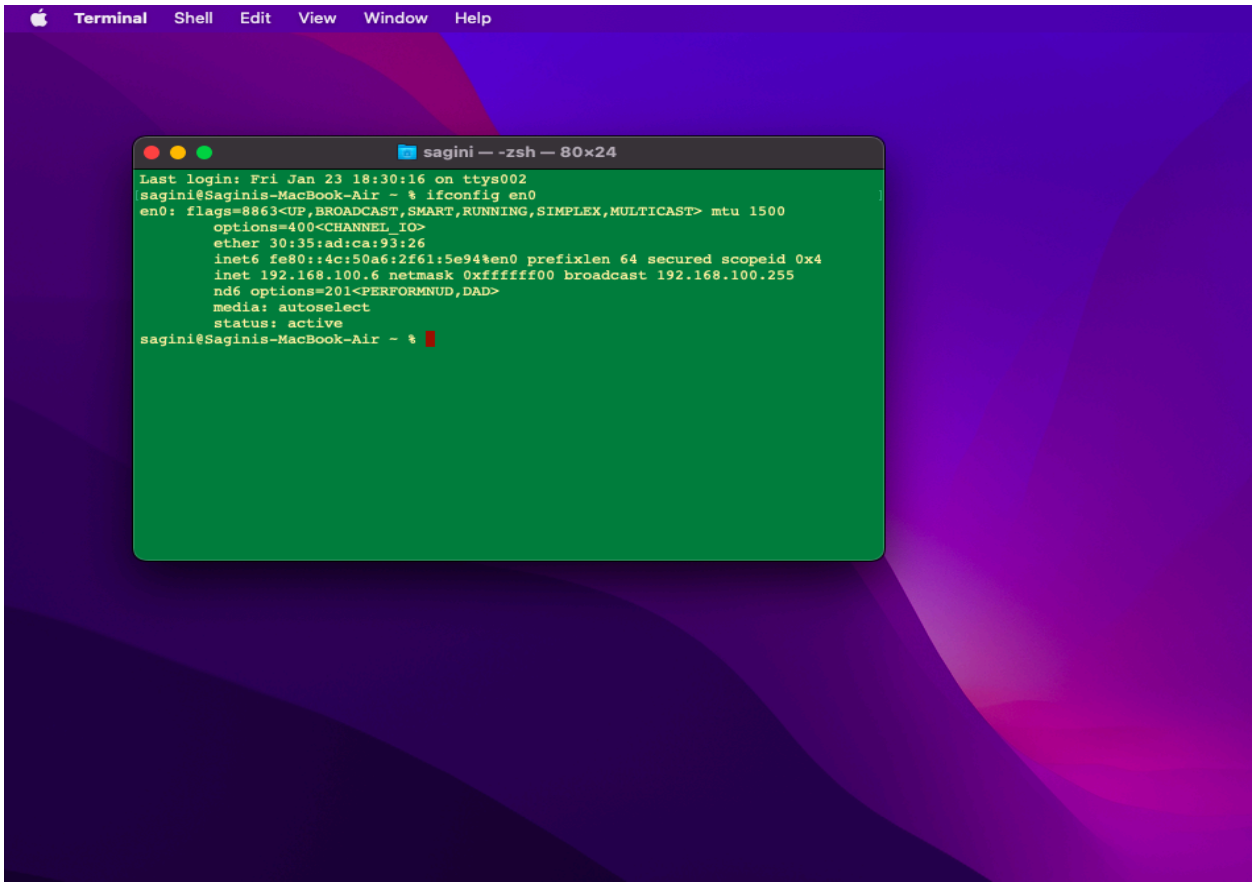
Objectives:

- ★ Part 1: Capture and Analyze Local ICMP Data in Wireshark.
- ★ Part 2: Capture and Analyze Remote ICMP Data in Wireshark.

Capture and Analyze Local ICMP Data

Retrieving PC Interface Addresses

Before capturing traffic, I retrieved my computer's IP address and MAC (Physical) address using the terminal command ***ifconfig en0***(macOS).

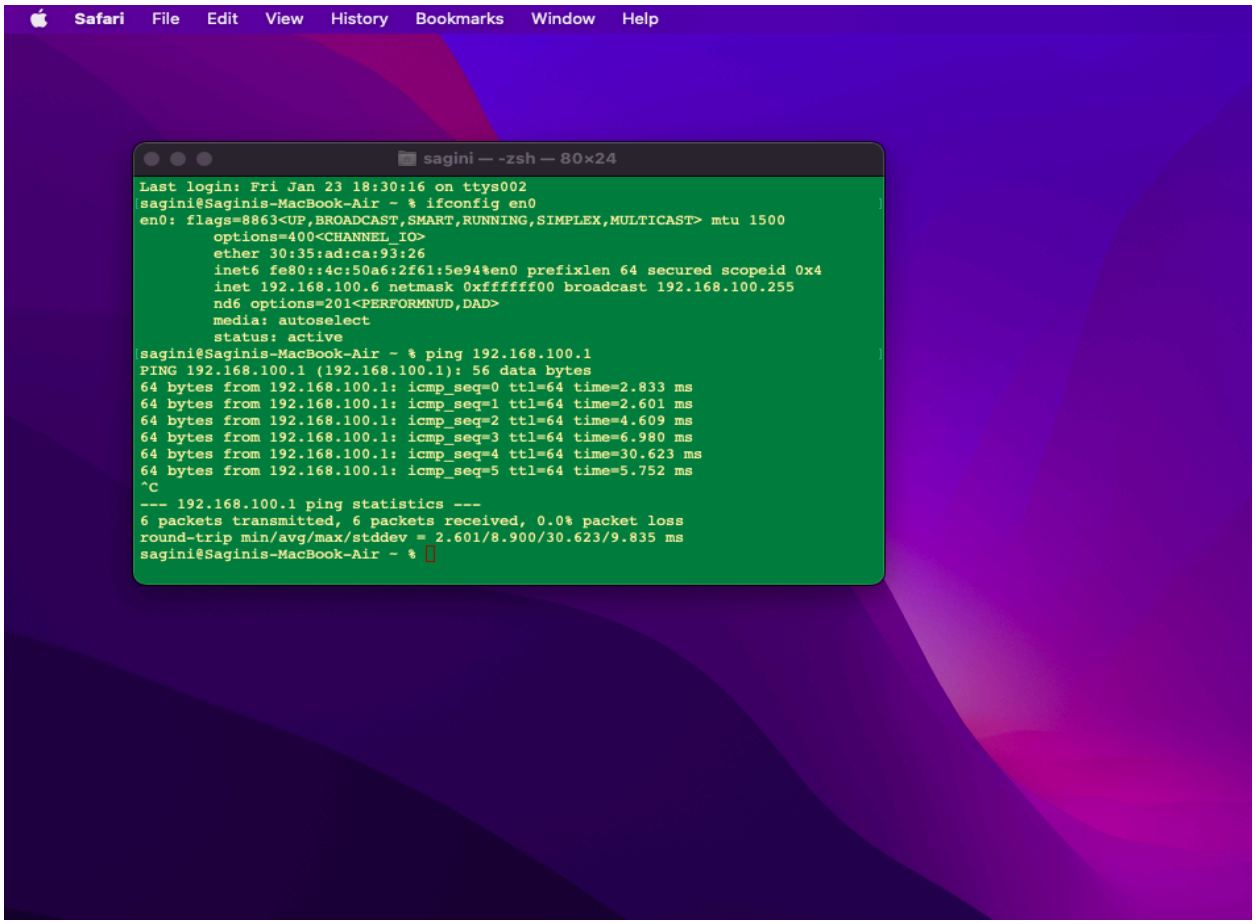


Starting Wireshark Capture

I opened wireshark and selected the Wi-Fi interface (en0) to begin capturing network traffic. I applied the filter ***icmp*** to display only ICMP (ping) packets, making it easier to analyze the relevant traffic.

Pinging a Local Device

I pinged a local device on my network (the default gateway/router) to generate ICMP traffic that wireshark could capture.



Examining Captured Data in Wireshark

After capturing the ICMP traffic, I examined the packets in Wireshark. The tool displays data in three sections; the packet list (top), packet details (middle) and raw data in hexadecimal (bottom).

Q1: Does the source MAC address match your PC interface?

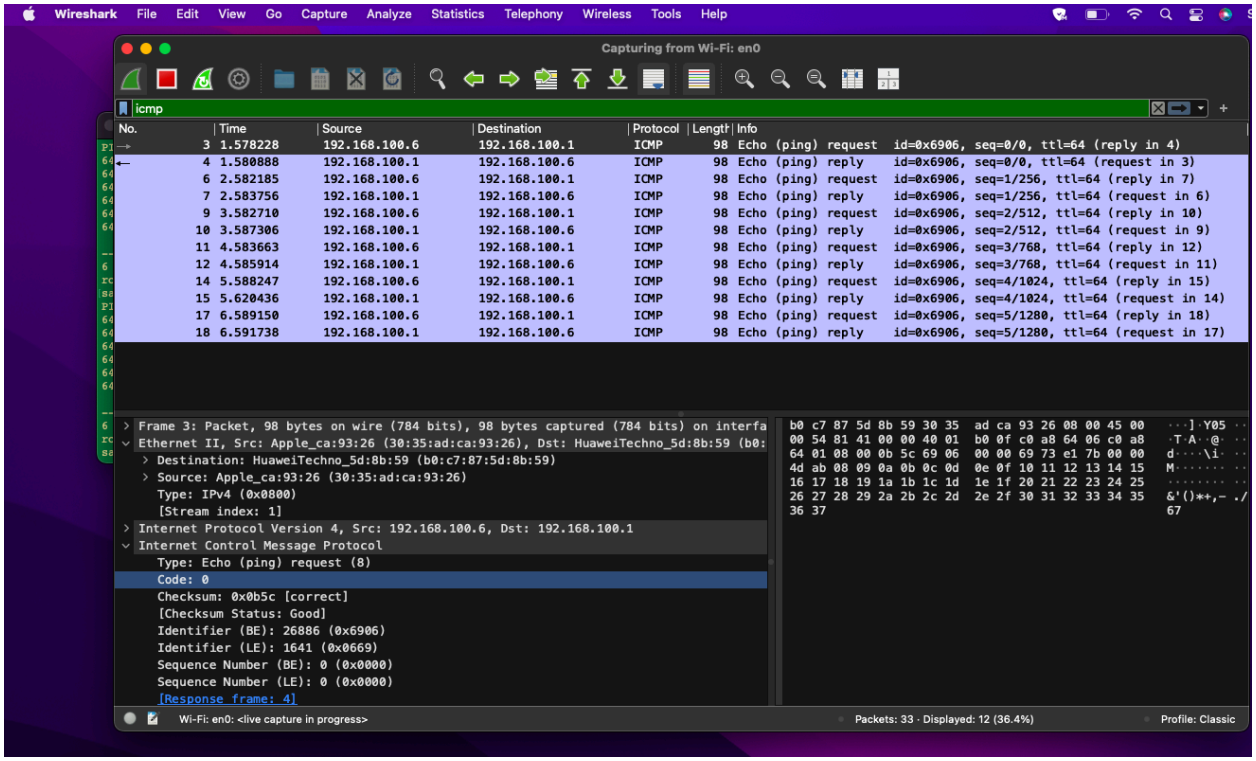
Yes, the source MAC address in wireshark (30:35:ad:ca:93:26) matches my router's MAC address.

Q2: Does the destination MAC address in Wireshark match your router's MAC address?

Yes, the destination MAC address matches my router's MAC address.

Q3: How is the MAC address of the pinged PC obtained by your PC?

The MAC address is obtained using ARP (Address Resolution Protocol). When the PC needs to send a packet to an IP address on the local network, it broadcasts an ARP request asking "Who has this IP?", then the device with that IP responds with its MAC address.

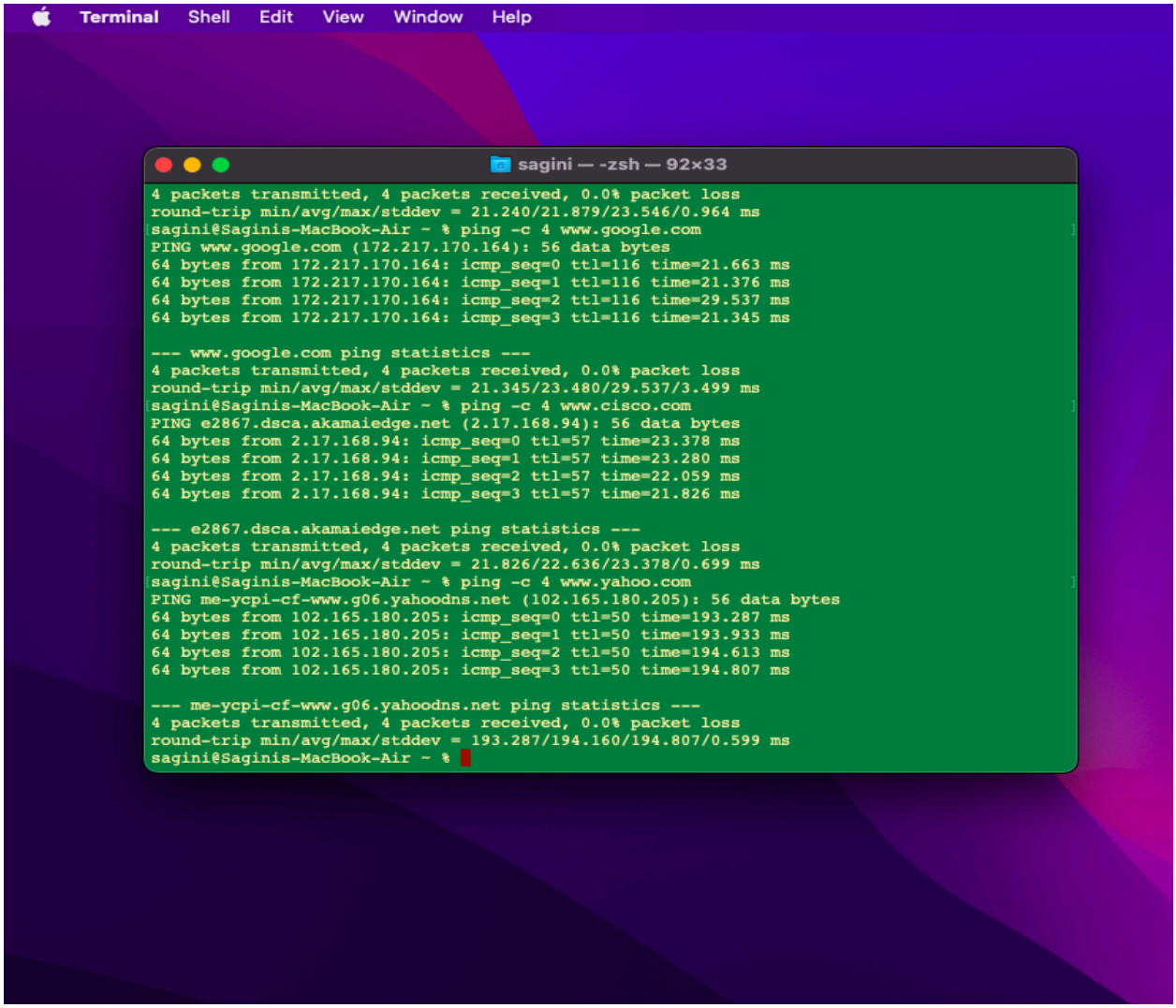


Key Concept: ICMP data is encapsulated inside an IPv4 packet which is Layer 3, then it is encapsulated in an Ethernet II frame which is Layer 2 for the transmission on the LAN.

Capture and Analyze Remote ICMP Data

Pinging Remote Hosts

In this part, I pinged remote hosts (websites) outside my local network to observe how traffic is handled differently when the destination is on the internet.



Q4: What is significant about the MAC addresses for the three remote websites?
All the three websites have the SAME destination MAC addresses. This MAC address belongs to my default gateway (router) but not to the actual remote servers.

Q5: How does this information differ from the local ping information you received in Part 1?
*In part 1 on the **local ping,** the destination MAC address was the actual MAC address of the local device. In part 2 on the **remote ping,** the destination address is the router's MAC address because remote traffic must be forwarded through the default gateway to reach the internet.*

Website	IP Address	MAC Address
www.google.com	172.217.170.164	b0:c7:87:5d:8b:59
www.yahoo.com	102.165.180.205	b0:c7:87:5d:8b:59
www.cisco.com	2.17.168.94	b0:c7:87:5d:8b:59

Key Concept: MAC addresses operate at layer 2 and are only relevant within the local network. When sending packets to remote destinations, the MAC address is set to the default gateway which is the router because the router is responsible for forwarding packets to 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 the actual MAC address for local hosts because they are on the same network segment (LAN) and communication happens directly at layer 2 using MAC addresses. For remote hosts, the actual MAC address is not shown because MAC addresses only have local significance meaning that they cannot be routed across the internet. When a packet is destined for a remote host, the PC sets the destination MAC address to its default gateway which is the router. The router then strips the old Ethernet frame, determines the next hop and creates a new Ethernet frame with appropriate MAC addresses for that network segment. This process repeats at each hop until the packet reaches its destination. Therefore, wireshark on my PC can only see the MAC address of my router but not the MAC address for the remote servers like Yahoo, Cisco or Google.

Conclusion

The work on this lab provided valuable hands-on experience in using wireshark to capture and analyze network traffic. Through this exercise, I gained a deeper understanding of:

- ★ **ICMP Protocol:** How ping uses ICMP Echo Request and Echo Reply messages to test connectivity.
- ★ **Layer 2 vs Layer 3 Addressing:** The difference between MAC addresses (physical, local scope) and IP addresses (logical, global scope).
- ★ **Encapsulation:** How ICMP data is encapsulated within IP packets, which are then encapsulated within Ethernet frames.
- ★ **Default Gateway:** The critical role of the router in forwarding traffic to destinations outside the local network.
- ★ **ARP:** How the Address Resolution Protocol maps IP addresses to MAC addresses on a local network.

The key takeaway from this lab is understanding why all remote traffic shows the router's MAC address: because MAC addresses have meaning within the local network and the router serves as the exit point for all traffic destined for the internet.
Wireshark is an essential tool for network professionals, enabling deep packet inspection for troubleshooting, security analysis and understanding network behaviour at a granular level.

- ★ ***I did not document anything concerning the firewall setup and the new ICMP rule since my ping requests didn't encounter firewalls on my macOS .***