Week 1 Assignment 2

Course: Cloud and Network Security CNS1 - 2026

Student Name: Bussllus Bertrand

Student Number: CS-CNS11-26004

Sunday, January 18, 2026

Week one Assignment two:

Class exercise: Use Wireshark to view network traffic

Table of Contents

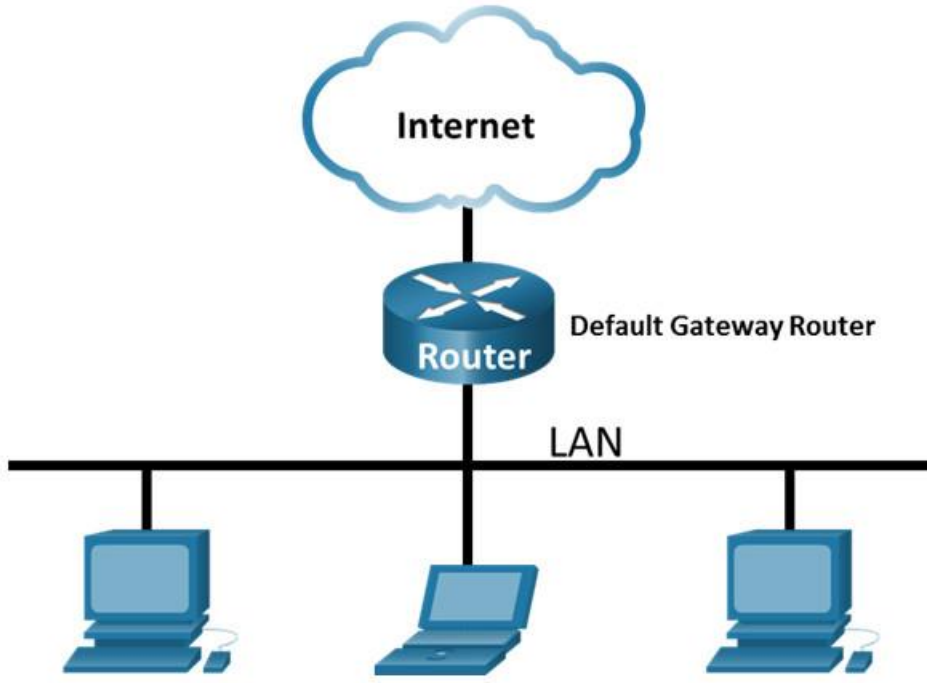
Week 1 Assignment 2

Introduction

Objective

The primary objective of this laboratory exercise is to utilize Wireshark, a network protocol analyzer, to capture and inspect network traffic. This lab focused on understanding the structure of network data by analyzing Protocol Data Units (PDUs) across different layers of the OSI model.

Topology



.

Part 1: Capture and Analyze Local ICMP Data in Wireshark

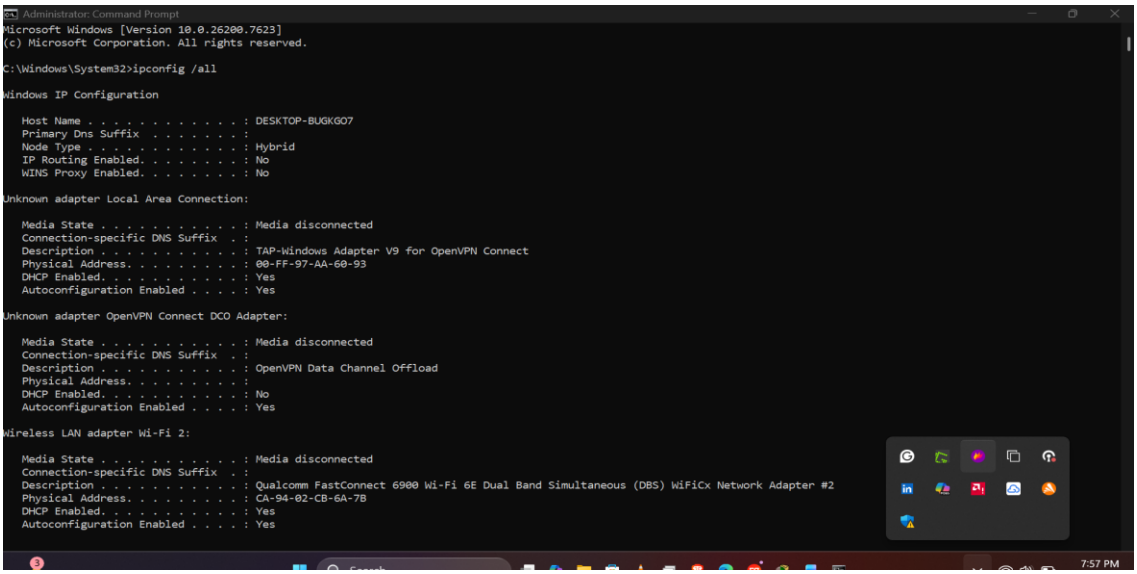
In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

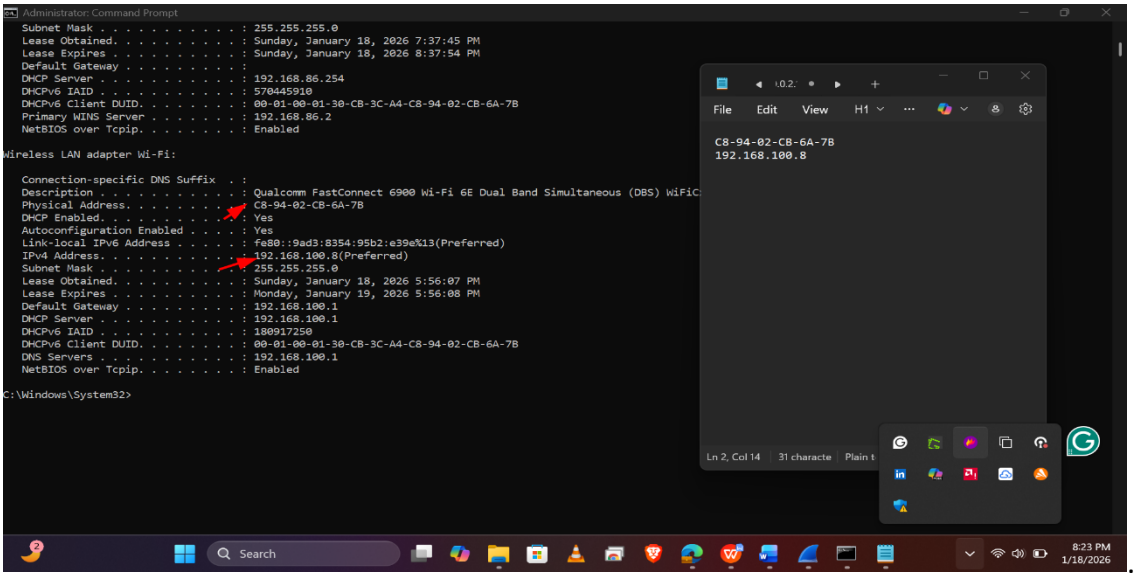
Week 1 Assignment 2

Step 1: Retrieve your PC interface addresses.

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

In a command prompt window, enter **ipconfig /all**.

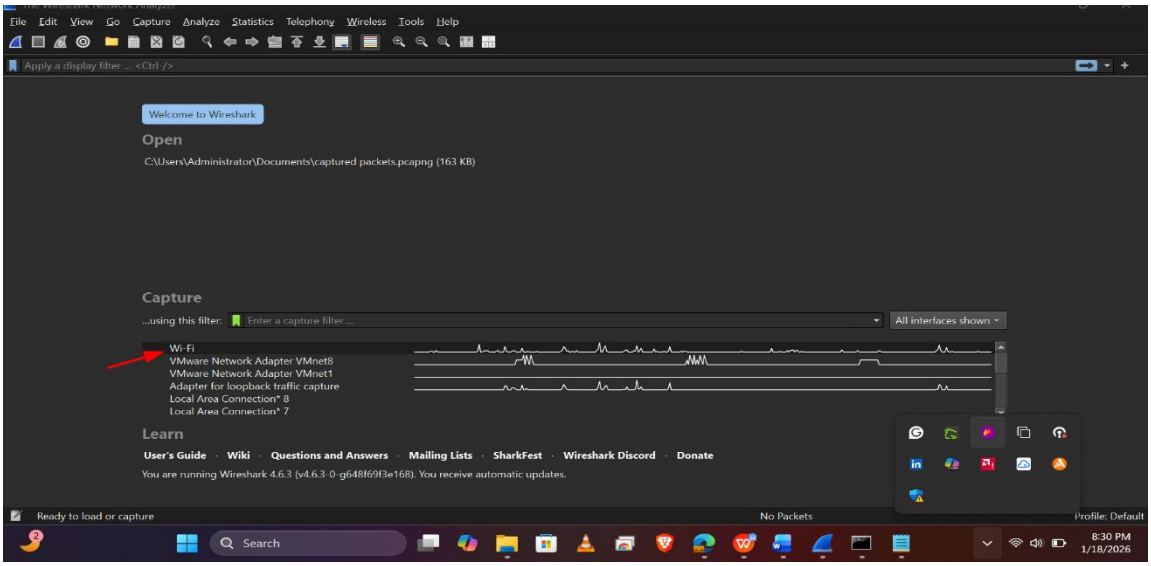




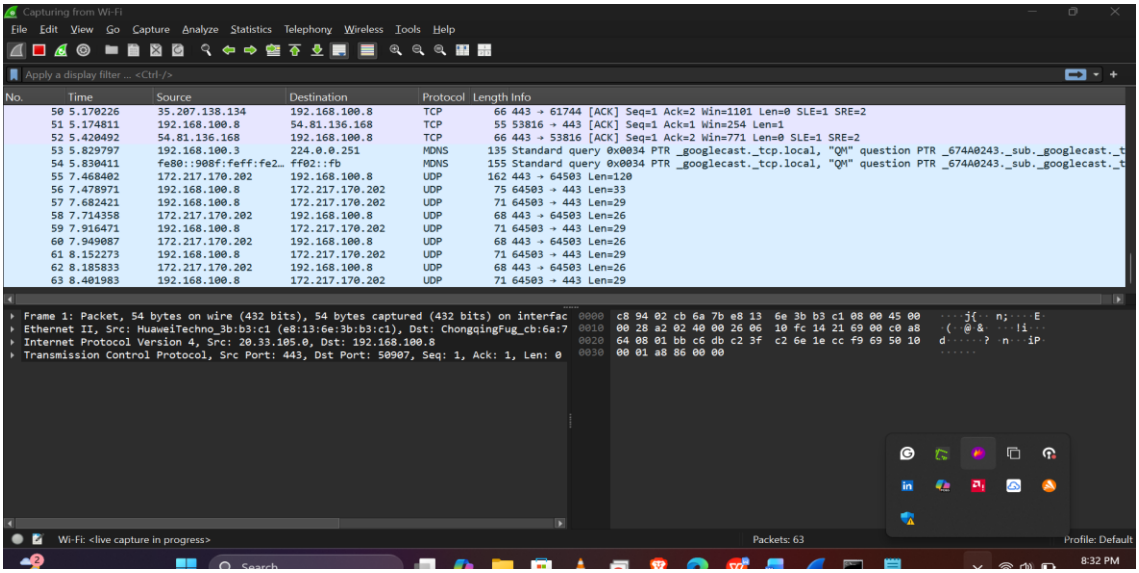
Step 2: Start Wireshark and begin capturing data.

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

Week 1 Assignment 2



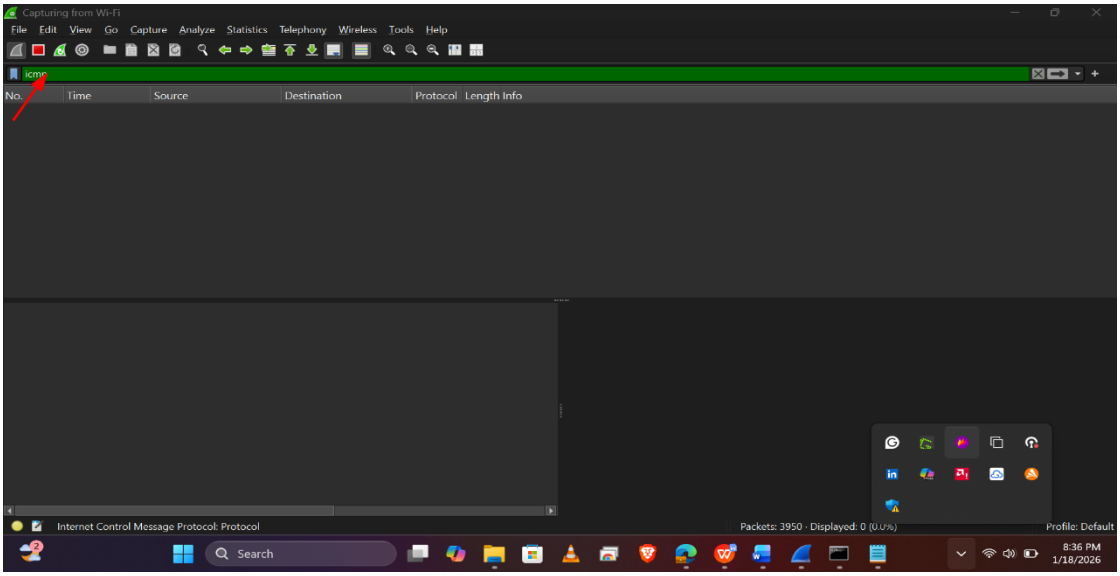
b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



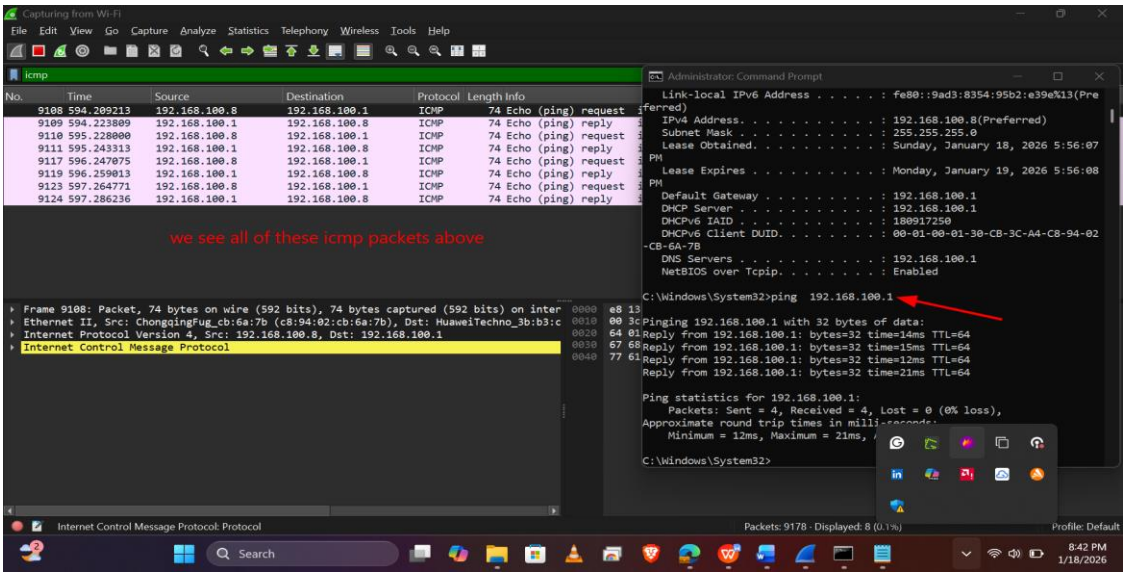
This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark.

For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the **Filter** box at the top of Wireshark and press **Enter,** or click the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.

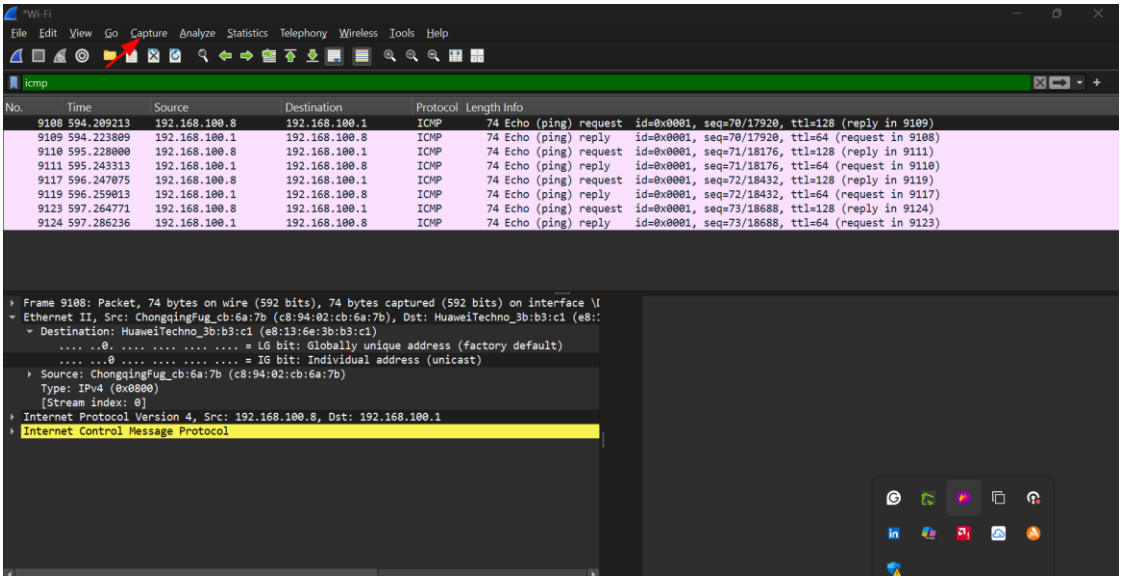
Week 1 Assignment 2



c. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Navigate to a command prompt window and ping the IP address. I will ping my default gateway which is 192.168.100.1.



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. 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; 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.

b. 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

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

Yes

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

The MAC address is obtained through an ARP request.

Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header), which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

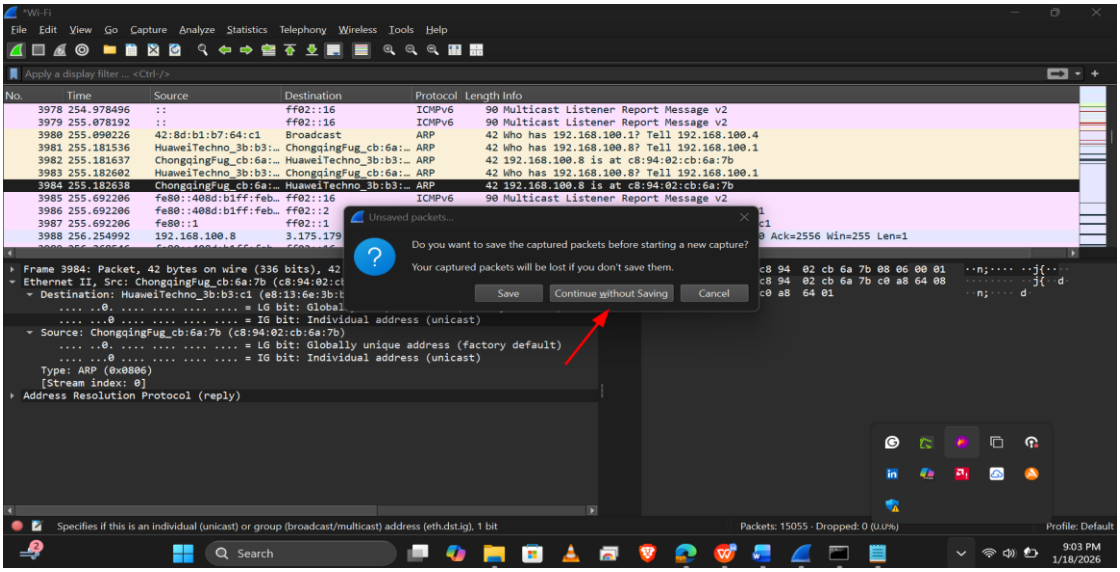
Part 2: Capture and Analyze Remote ICMP Data in Wireshark

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 this data from the data examined in Part 1.

Step 1: Start capturing data on the interface.

a. Start the data capture again.

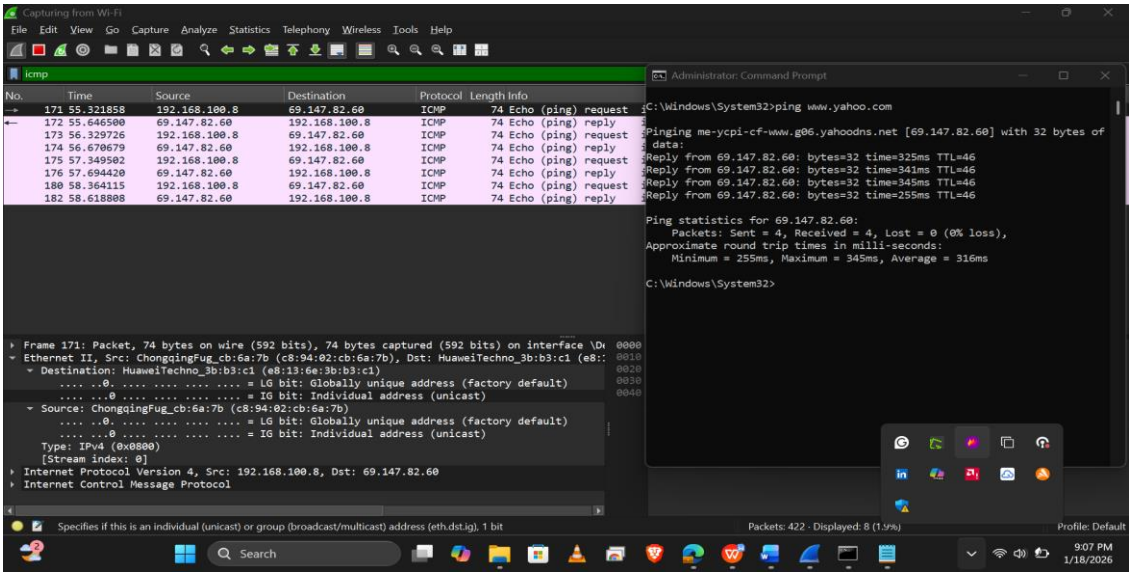
b. A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving.**



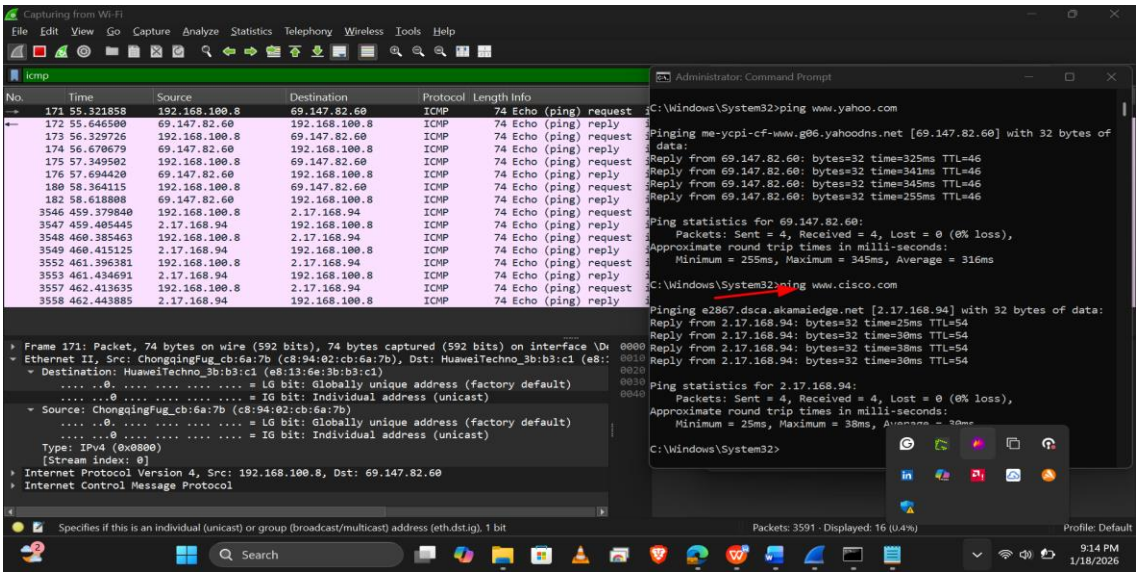
c. With the capture active, ping the following three website URLs from a Windows command prompt:

1) www.yahoo.com

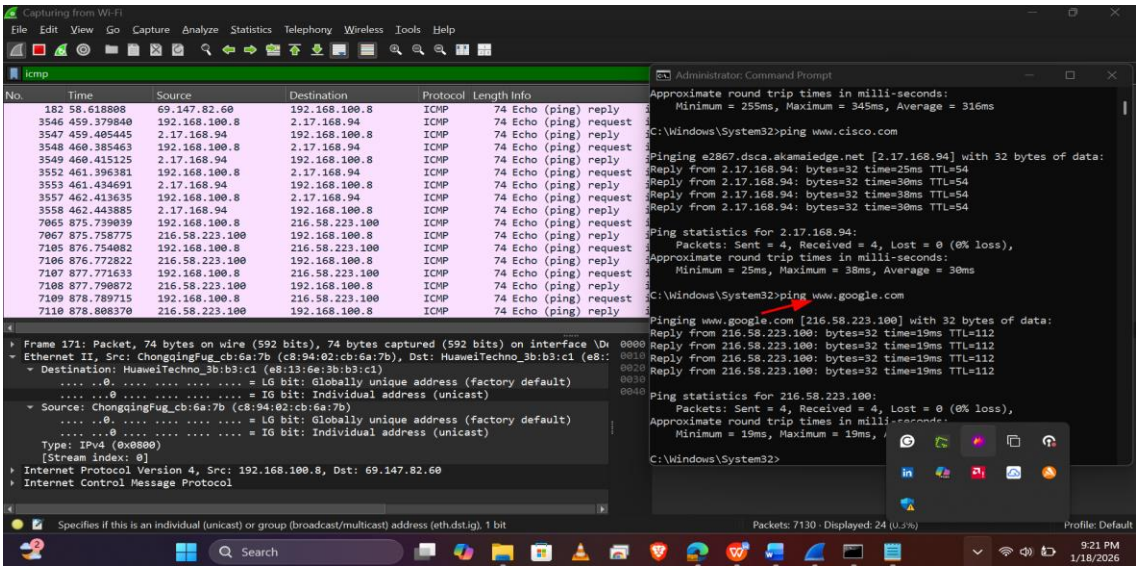
Week 1 Assignment 2



2) www.cisco.com

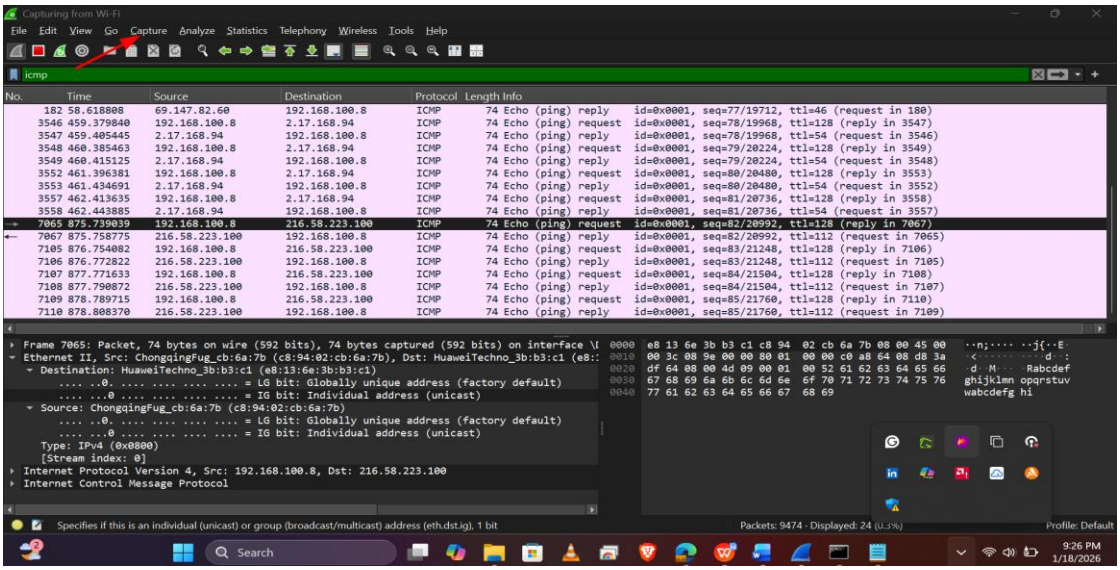


3) www.google.com



Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address 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**: 69.147.82.60

MAC address for **www.yahoo.com**: 3b:b3:c1 (e8:13:6e:3b:b3:c1)

IP address for **www.cisco.com**: 2.17.168.94

MAC address for **www.cisco.com**: 3b:b3:c1 (e8:13:6e:3b:b3:c1)

IP address for **www.google.com**: 216.58.223.100:

MAC address for **www.google.com**: 3b:b3:c1 (e8:13:6e:3b:b3:c1).

What is significant about this information?

The MAC addresses for all three locations are the same.

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

A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

Reflection Question

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

MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.

Conclusion

This lab successfully demonstrated the practical use of Wireshark as a powerful tool for network traffic analysis. Through hands-on packet capture and examination, fundamental networking concepts were reinforced, including protocol operation, packet structure, and the flow of data across networks. The ability to inspect real-time traffic is invaluable for diagnosing issues, optimizing performance, and enhancing security.