Course: Cloud and Network Security - C3 - 2025

Student Name: Johnmark Gichuki

Student No: CS-CNS10-25101

Friday, September 20, 2025

Week 1 Assignment 2:

Class Exercise: Using Wireshark to View Network Traffic

Table of Contents

Introduction

This lab focused on using Wireshark, a powerful network protocol analyzer, to capture and analyze ICMP traffic within both local and remote network environments. In Part 1, the lab involved pinging devices within the same LAN to observe how packets are encapsulated and to identify the IP and MAC addresses of local devices. In Part 2, the lab expanded to pinging remote hosts, allowing for the comparison of local traffic versus traffic routed through a default gateway to the internet. Through this lab, I gained hands-on experience in capturing network packets, applying filters, and interpreting data across multiple layers of the TCP/IP model. This exercise also helped strengthen my understanding of how DNS resolves domain names to IP addresses and how Layer 2 and Layer 3 addressing work together to deliver packets locally and remotely.

Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

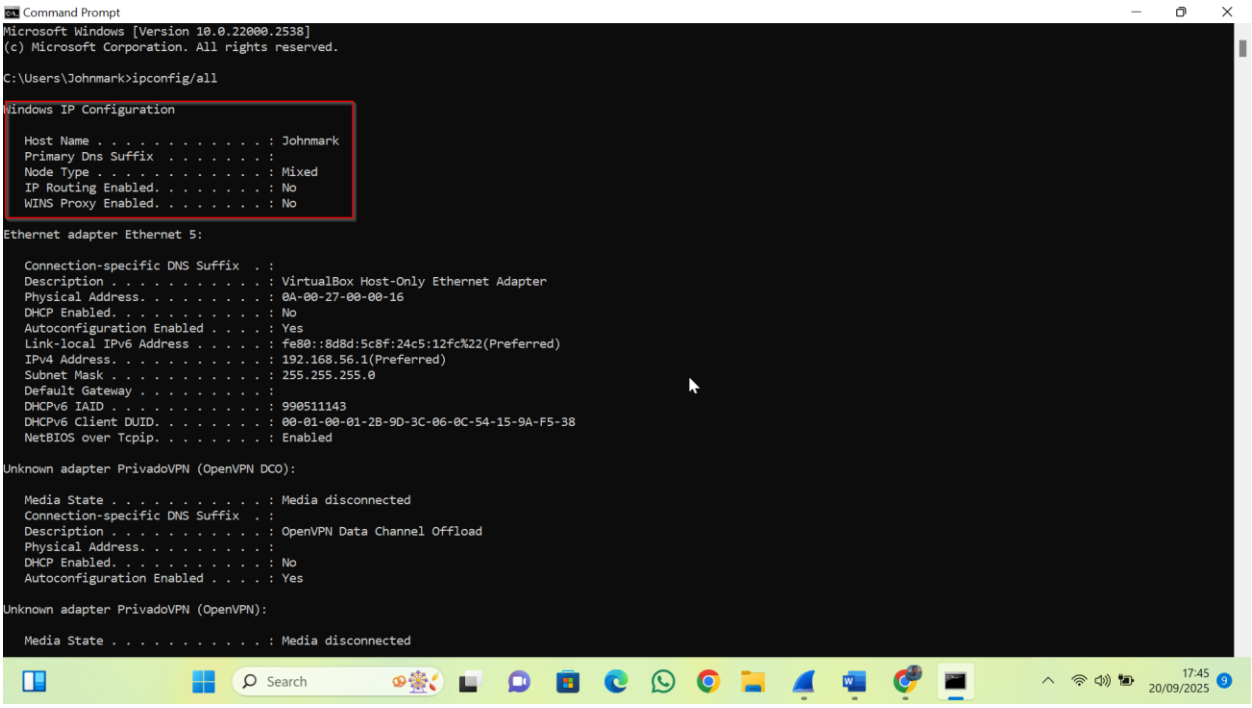
Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Part 1: Capture and Analyze Local ICMP Data in Wireshark

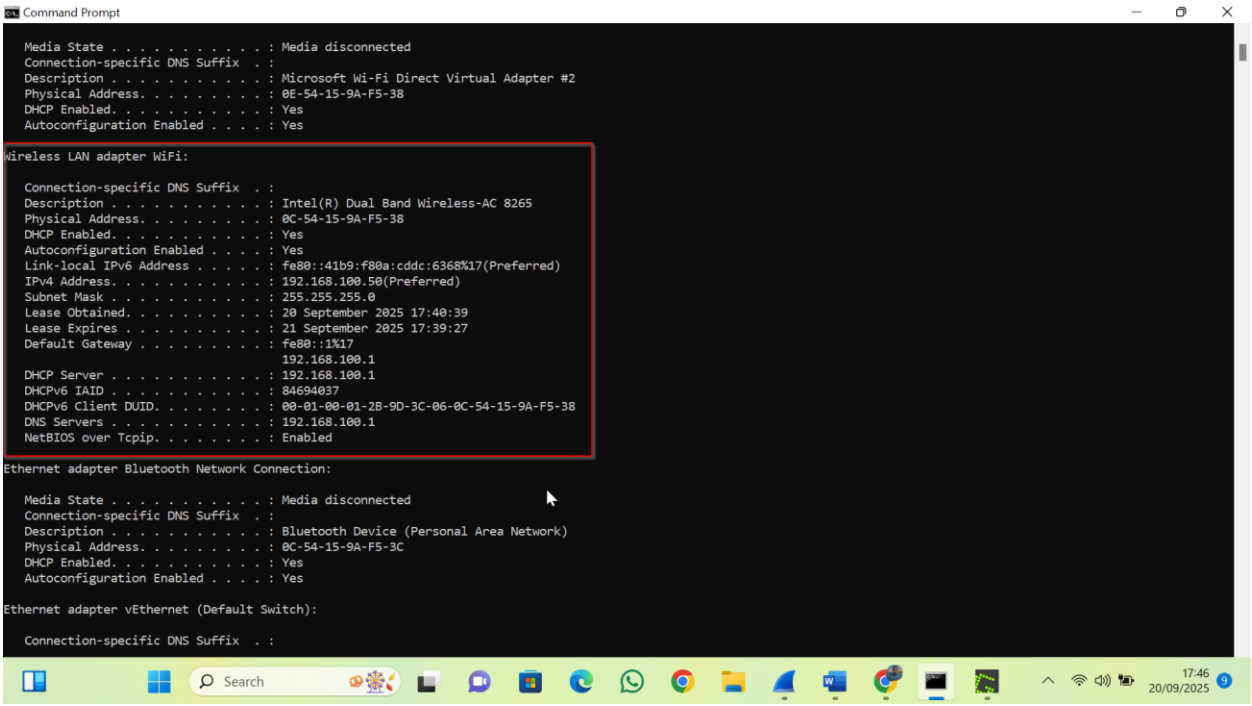
In Part 1 of this lab, I will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. I will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC interface addresses

Part a: Perform ipconfig/all on the command prompt



```
Command Prompt
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Johnmark>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Johnmark
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-16
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8d8d:5c8f:24c5:12fc%22(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.56.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 990511143
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-9D-3C-06-0C-54-15-9A-F5-38
   NetBIOS over Tcpip. . . . . . . . : Enabled

Unknown adapter PrivadoVPN (OpenVPN DCO):

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : OpenVPN Data Channel Offload
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Unknown adapter PrivadoVPN (OpenVPN):

   Media State . . . . . . . . . . . : Media disconnected
```

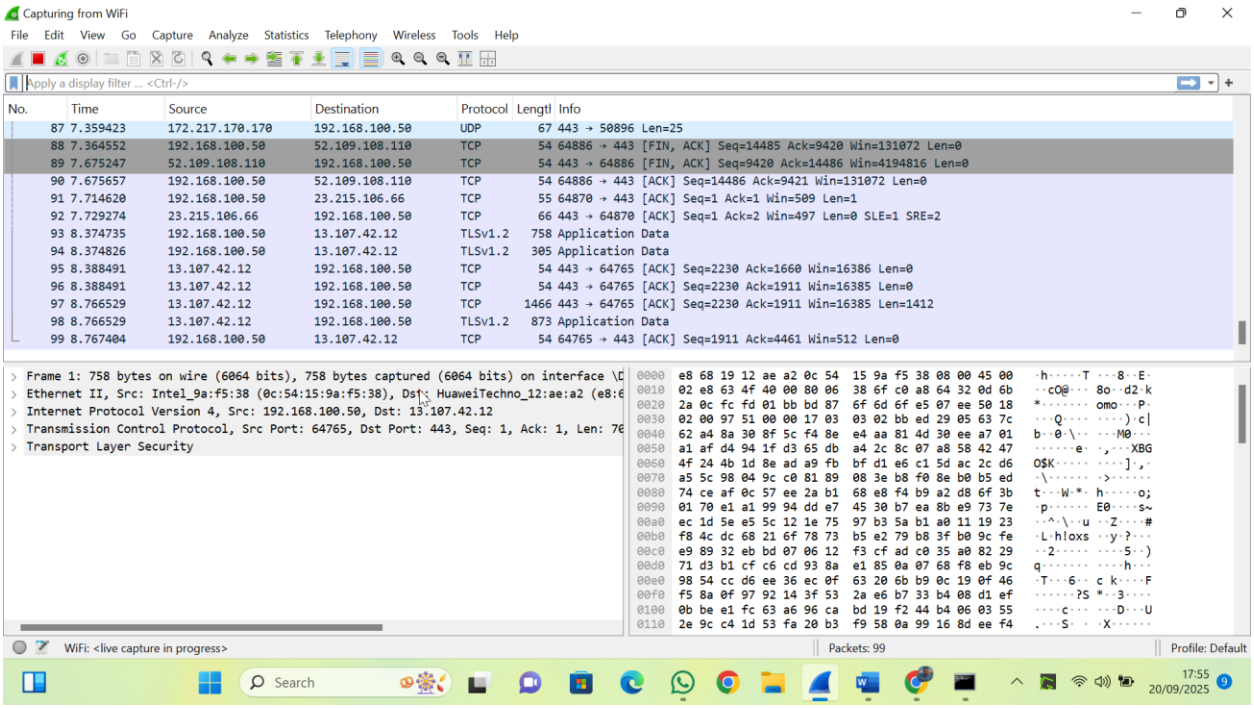


```
Command Prompt
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 0E-54-15-9A-F5-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter WiFi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 0C-54-15-9A-F5-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::41b9:f80a:cddc:6368%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.50(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 20 September 2025 17:40:39
   Lease Expires . . . . . . . . . . : 21 September 2025 17:39:27
   Default Gateway . . . . . . . . . : fe80::1%17
                                       192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 84694037
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-9D-3C-06-0C-54-15-9A-F5-38
   DNS Servers . . . . . . . . . . . : 192.168.100.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 0C-54-15-9A-F5-3C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
```

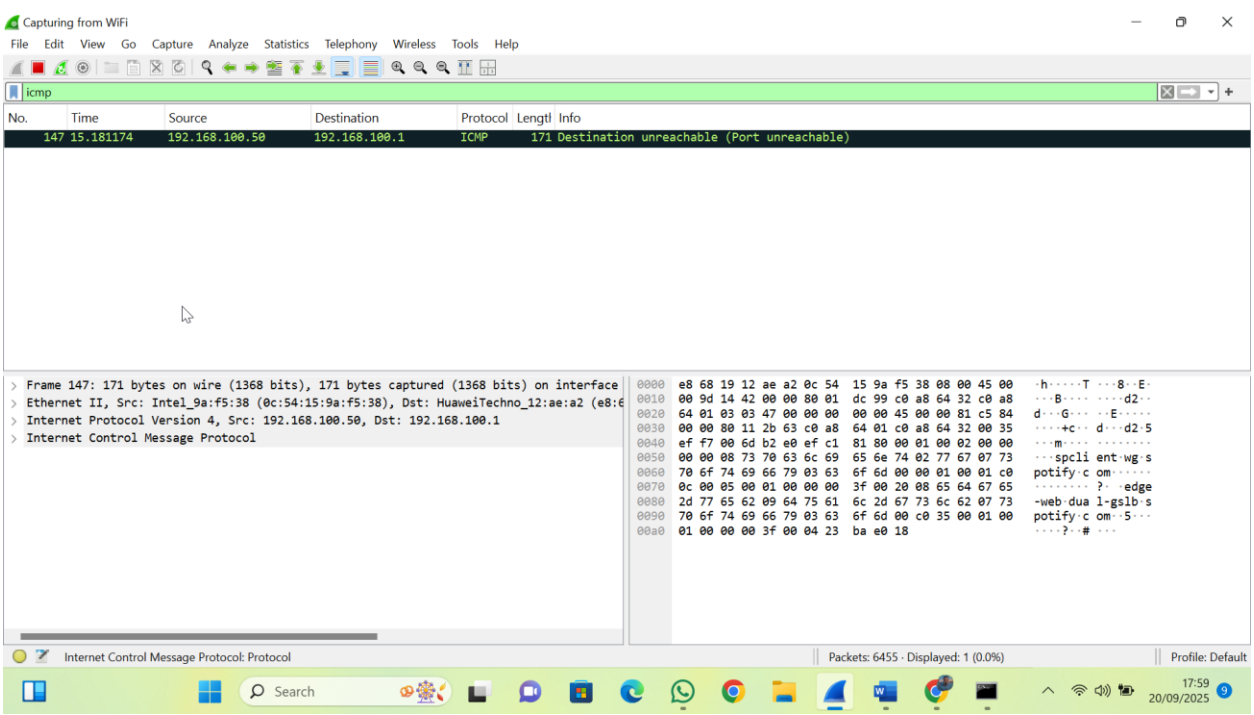
Step 2: Start Wireshark and begin capturing data.

Part a: Navigate to Wireshark and select the desired interface

Part b: Information will start scrolling down the top section in Wireshark



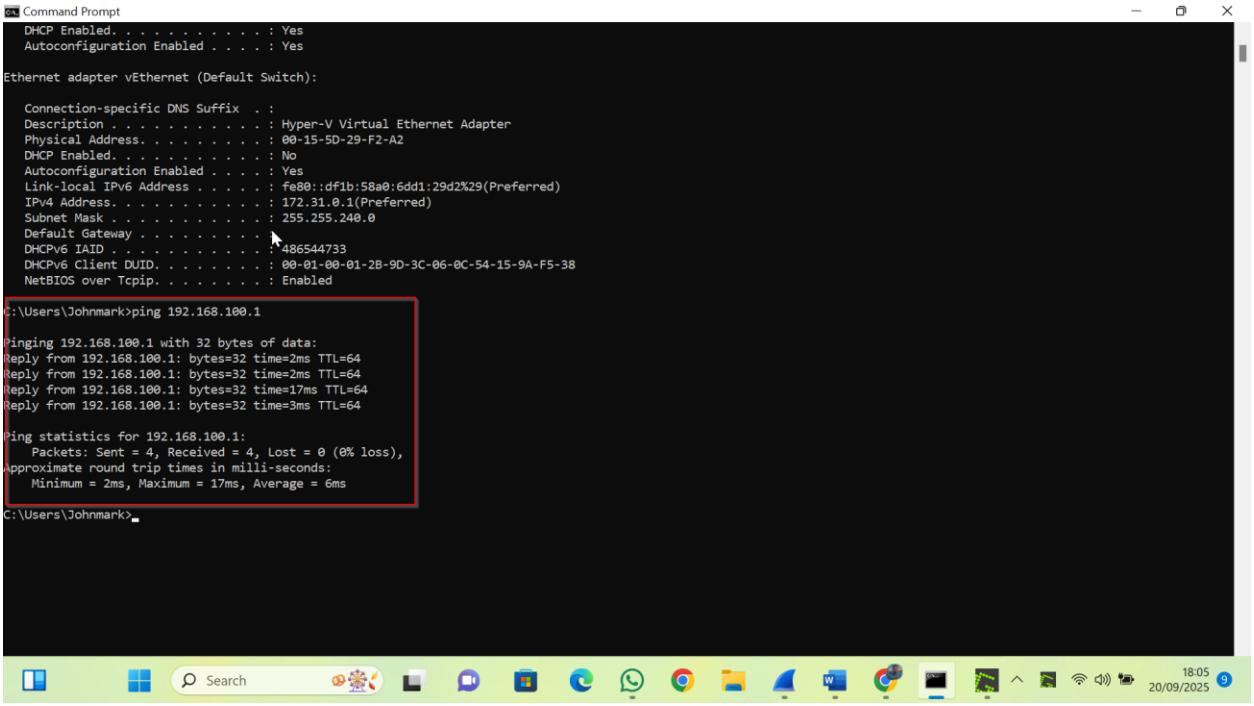
Part c: Wireshark capturing ICMP traffic with filter applied



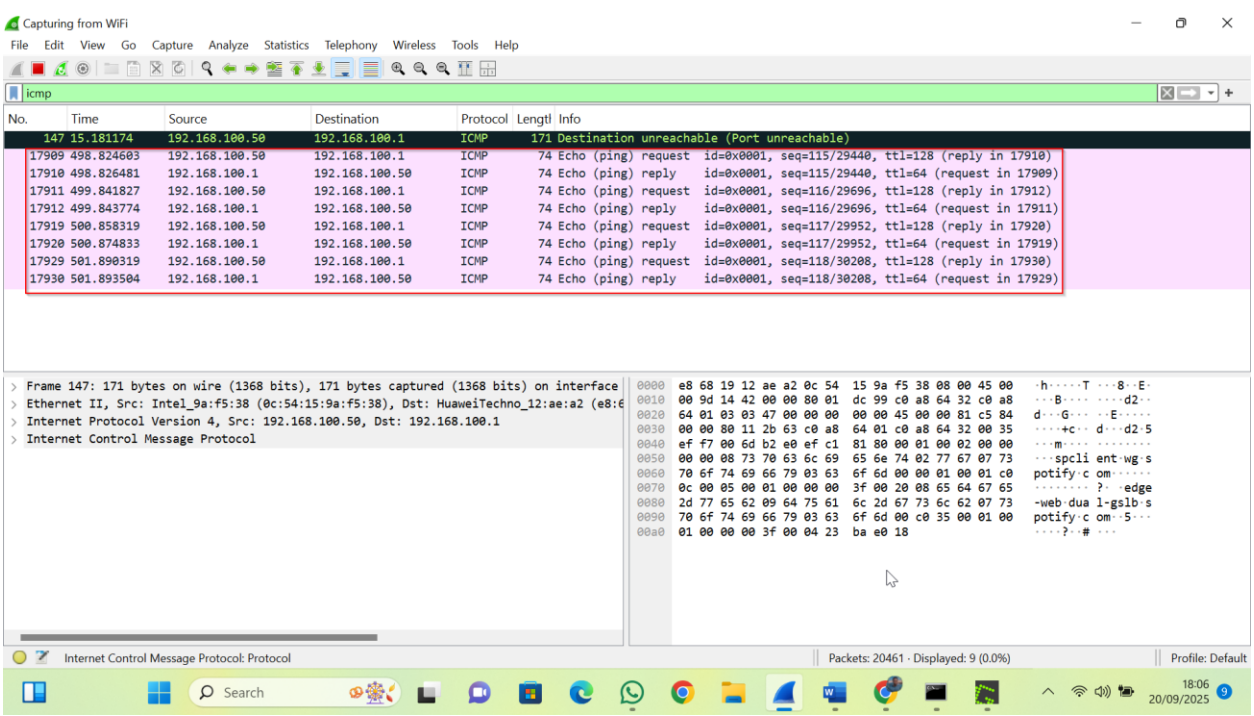
Part d: Performed a ping of my gateway/router:

192.168.100.1.

Below images are for the command prompt as well as from Wireshark to observe the traffic



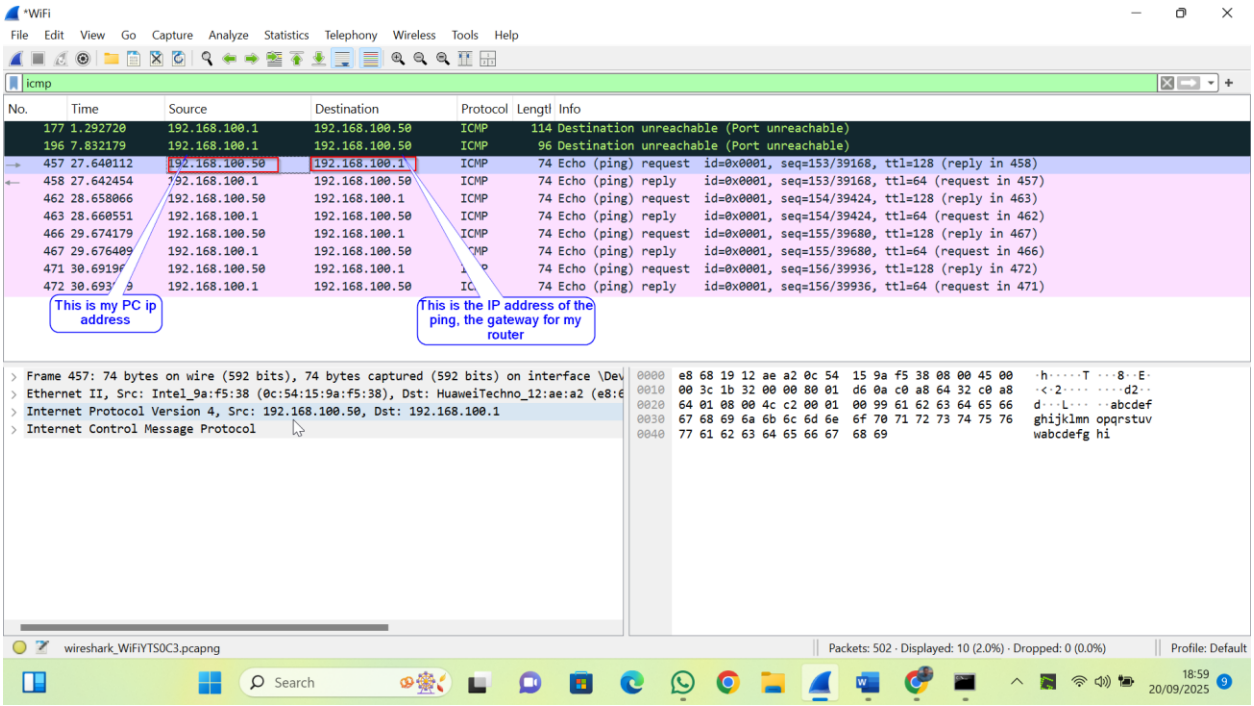
Ping command output showing successful replies



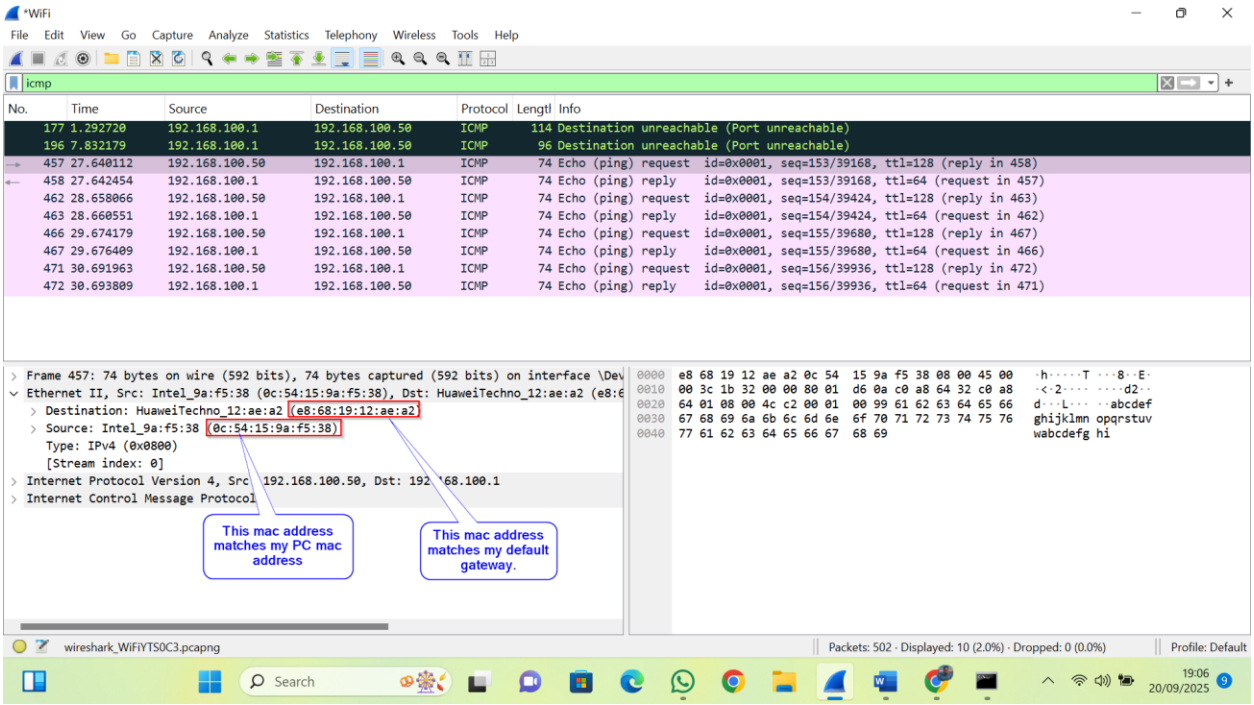
Step 3: Examine the captured data

Part a: ICMP data for router

In the top pane, the Source column displayed my PC IP (192.168.100.50), and the Destination column displayed my routers gateway IP (192.168.100.1).

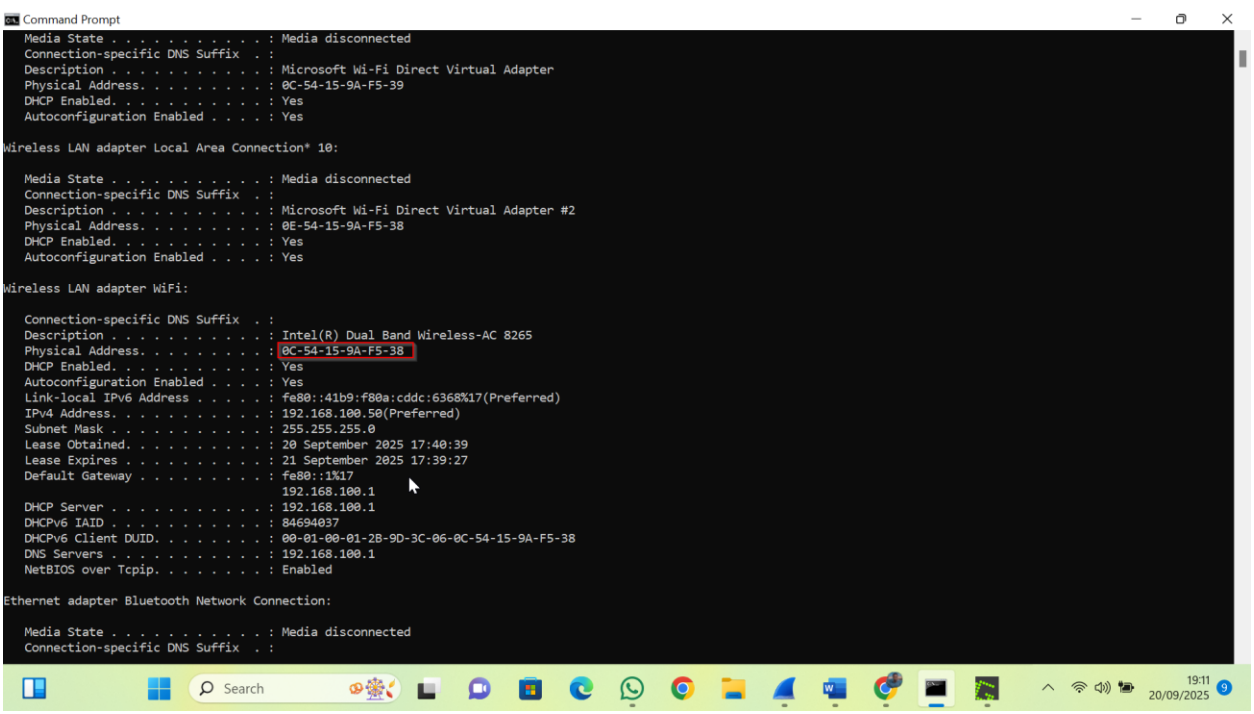


Part b: Ethernet II



1. **Does the source MAC address match your PC interface?**

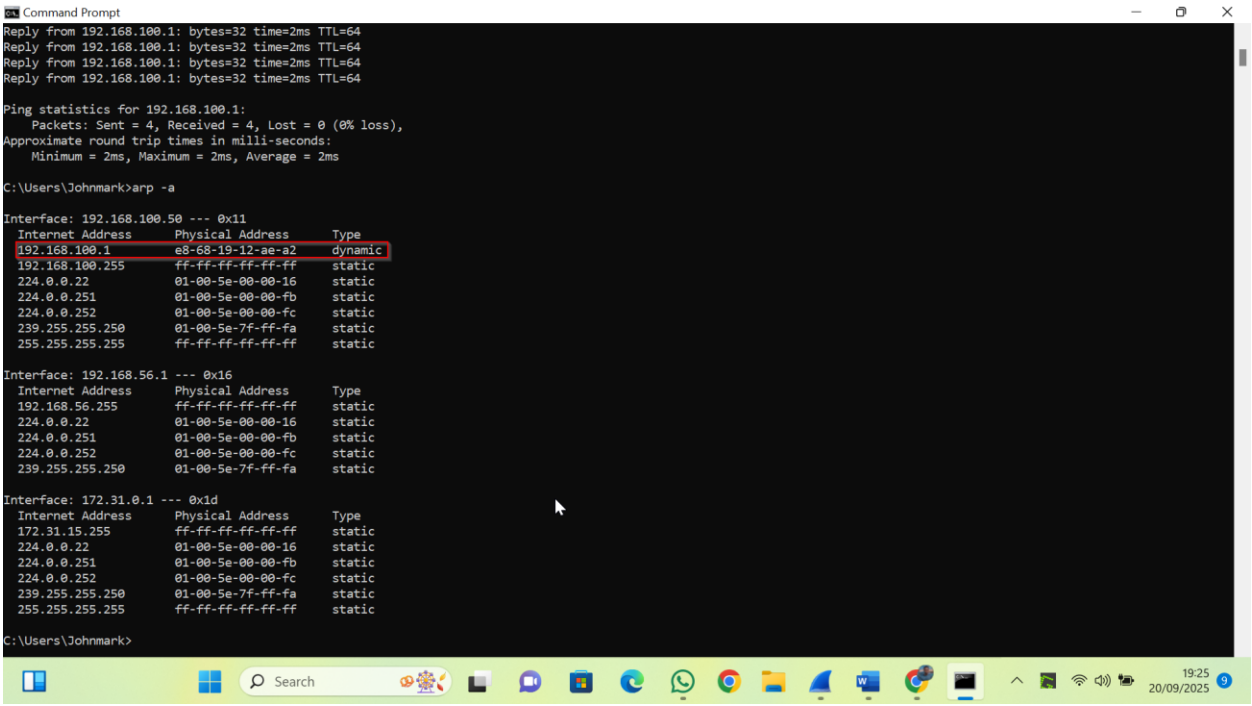
Yes, the mac address from Wireshark matches my PC Mac address: 0C-54-15-9A-F5-38



2. **Does the destination MAC address in Wireshark match your team member MAC address? (In this case my default gateway)**

Yes, it matches with the mac address of the default gateway: e8-68-19-12-ae-a2

The destination MAC address was obtained via an ARP request before the ping was sent.



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

Through the ARP protocol, which resolves IP addresses to MAC addresses within the same network.

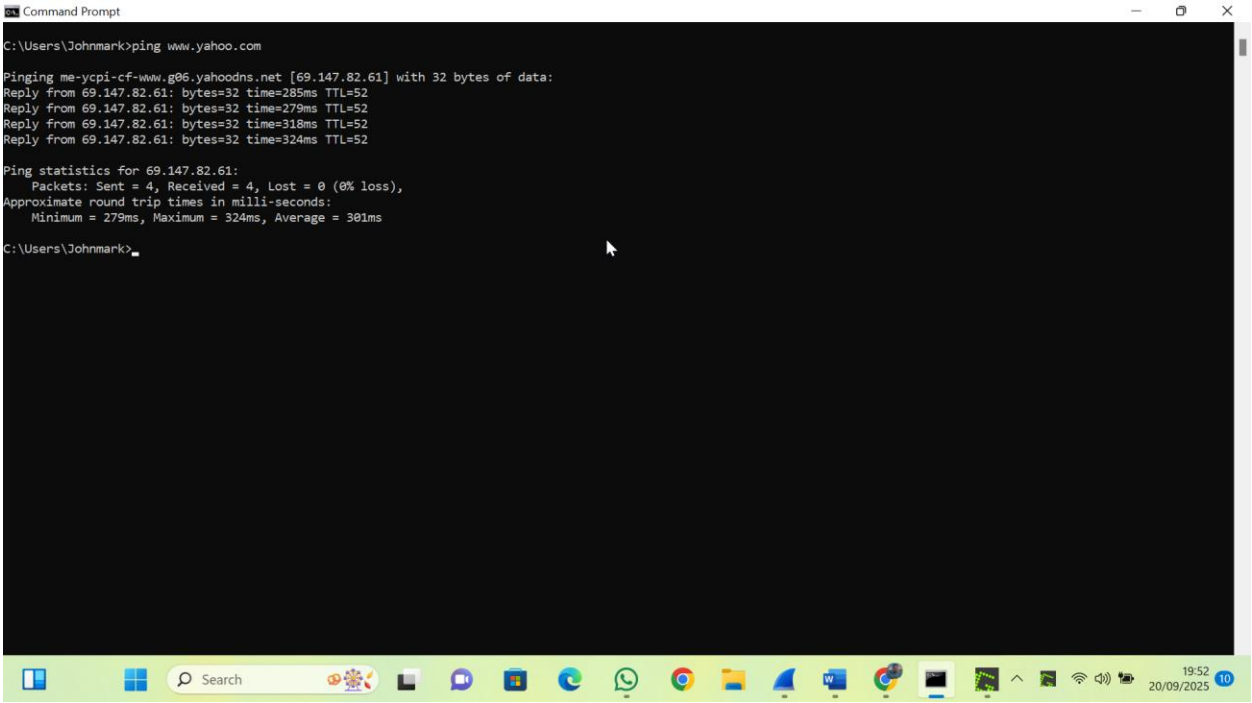
Part 2: Capture and Analyze Remote ICMP Data

This part focuses on pinging remote hosts on the internet and understanding the differences between local and remote ICMP traffic.

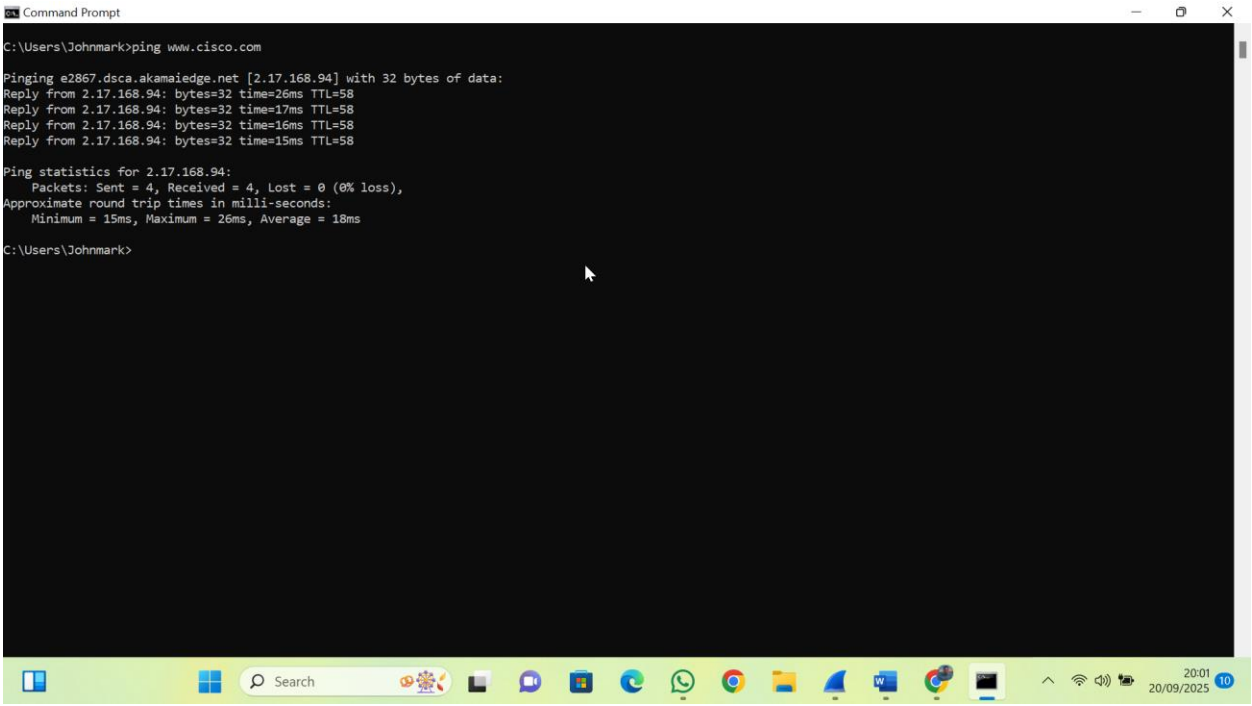
Step 1: Start capturing data on the interface.

Within this step, I will provide the Command prompt and how I pinged each and every one of this, the next step is where I will show the Wireshark traffic.

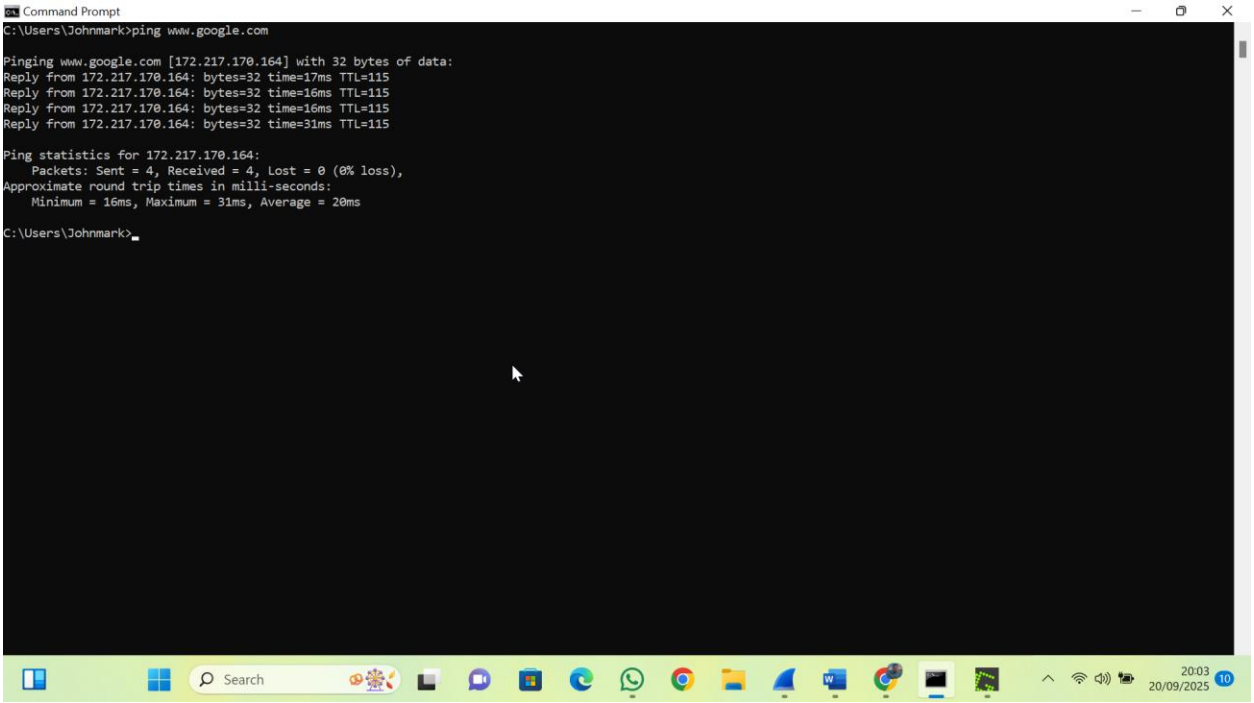
i. **www.yahoo.com**



ii. www.cisco.com

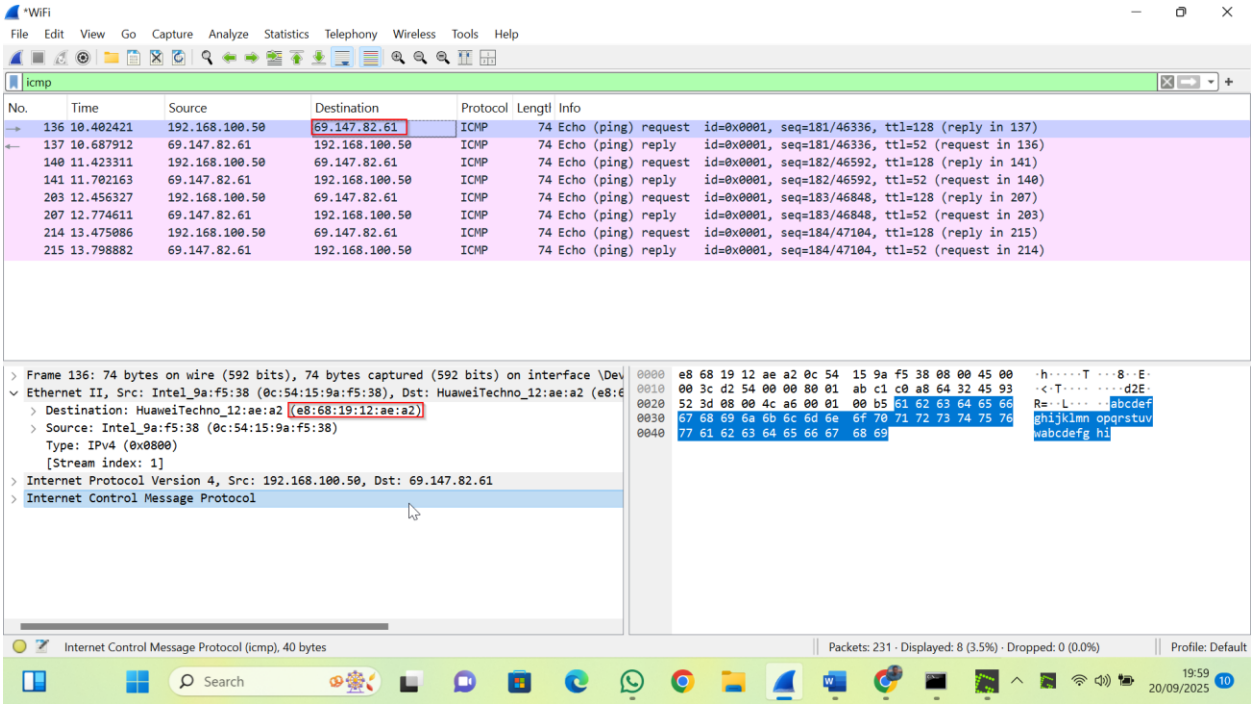


iii. www.google.com



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

part a:



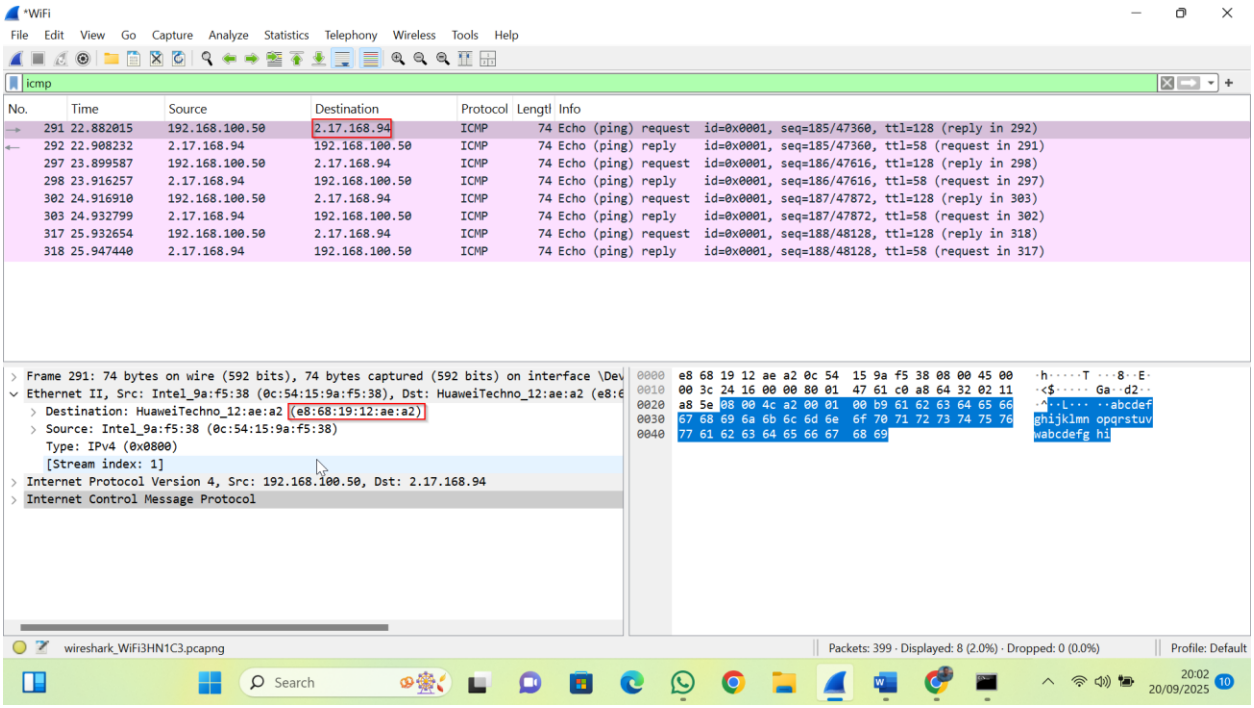
IP address for www.yahoo.com:

69.147.82.61

MAC address for www.yahoo.com:

e8-68-19-12-ae-a2 (Default Gateway/Router)

Part b:



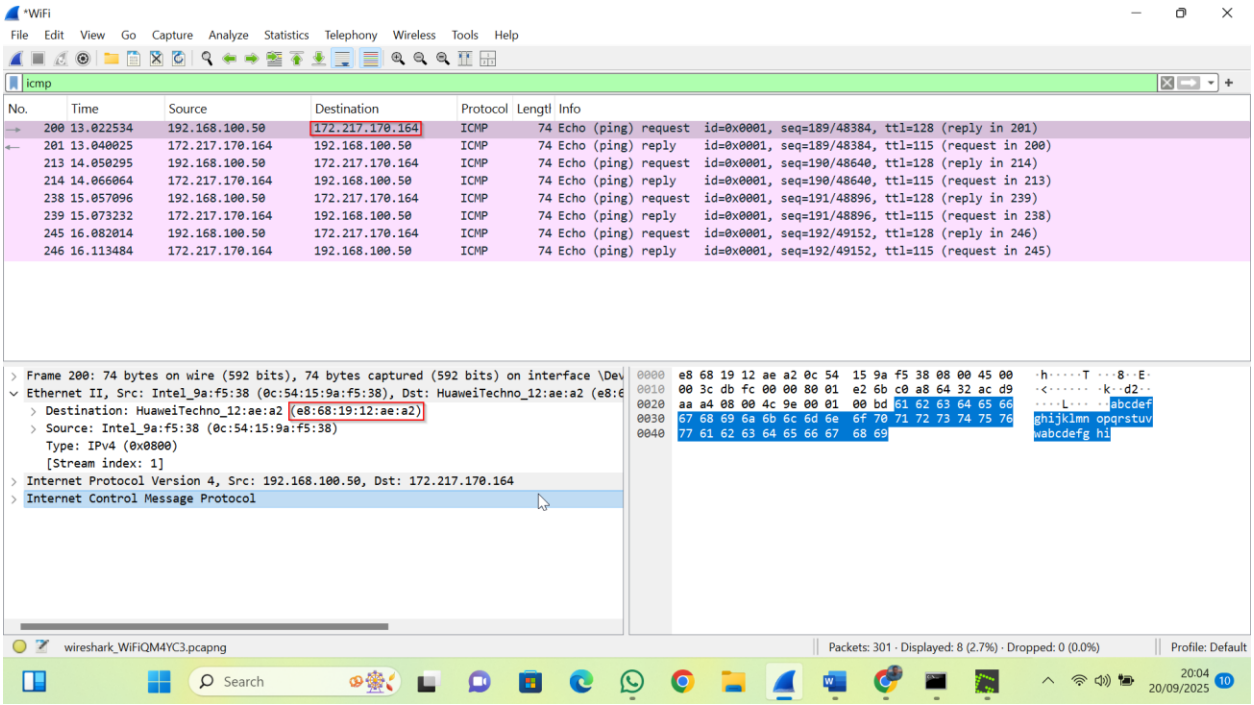
IP address for www.cisco.com:

2.17.168.94

MAC address for www.cisco.com:

e8-68-19-12-ae-a2 (Default Gateway/Router)

Part c:



IP address for www.google.com:

172.217.170.164

MAC address for www.google.com:

e8-68-19-12-ae-a2 (Default Gateway/Router)

a. **What is significant about this information?**

The MAC address remains local, meaning my computer is only communicating directly with my default gateway (router) at the data link layer.

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

When pinging a local device, Wireshark captures the physical MAC address of the target PC's NIC, since the communication happens directly within the same LAN. When pinging a remote device, Wireshark instead shows the MAC address of the default gateway, because the packet is first sent to the gateway, which then forwards it to the remote host across external networks.

Reflection Question:

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

Wireshark shows the actual MAC address of local hosts because devices on the same LAN use Layer 2 (Ethernet) communication, where frames are delivered directly between devices using their physical MAC addresses. or remote hosts, the packets must travel beyond the local network. At Layer 2, the local device can only see the gateway MAC address, since the gateway is responsible for forwarding packets to external networks.

Conclusion

By completing this lab, I developed a practical understanding of how network communication occurs at both the local and remote levels. I learned that when pinging local devices, Wireshark displays the physical MAC address of the target device, while for remote hosts, the MAC address of the default gateway is shown because traffic must pass through the gateway to reach external networks. Additionally, I observed how ICMP packets are encapsulated within IPv4 and Ethernet II frames, and how DNS plays a critical role in translating URLs to IP addresses Overall, this lab enhanced my skills in network troubleshooting and analysis, which are essential for identifying issues, monitoring network activity, and securing systems in real-world cybersecurity environments.