Course: **Cloud and Network Security -C2 -2025**

Student Name: **Daniel-Caleb Cheruiyot**

Student No: **CS-CNS09-25014**

Tuesday, May, 20th 2024

# Week 1 Assignment 2:

# Use Wireshark to Examine Network Traffic

# Table of Contents

# Introduction

In this report, I used Wireshark to capture and analyze Internet Control Message Protocol (ICMP) traffic. It is widely used by network tools such as *ping* and *traceroute* to test connectivity and determine the health of a network path. I examined both local ICMP traffic within the same network and remote ICMP traffic across different networks.

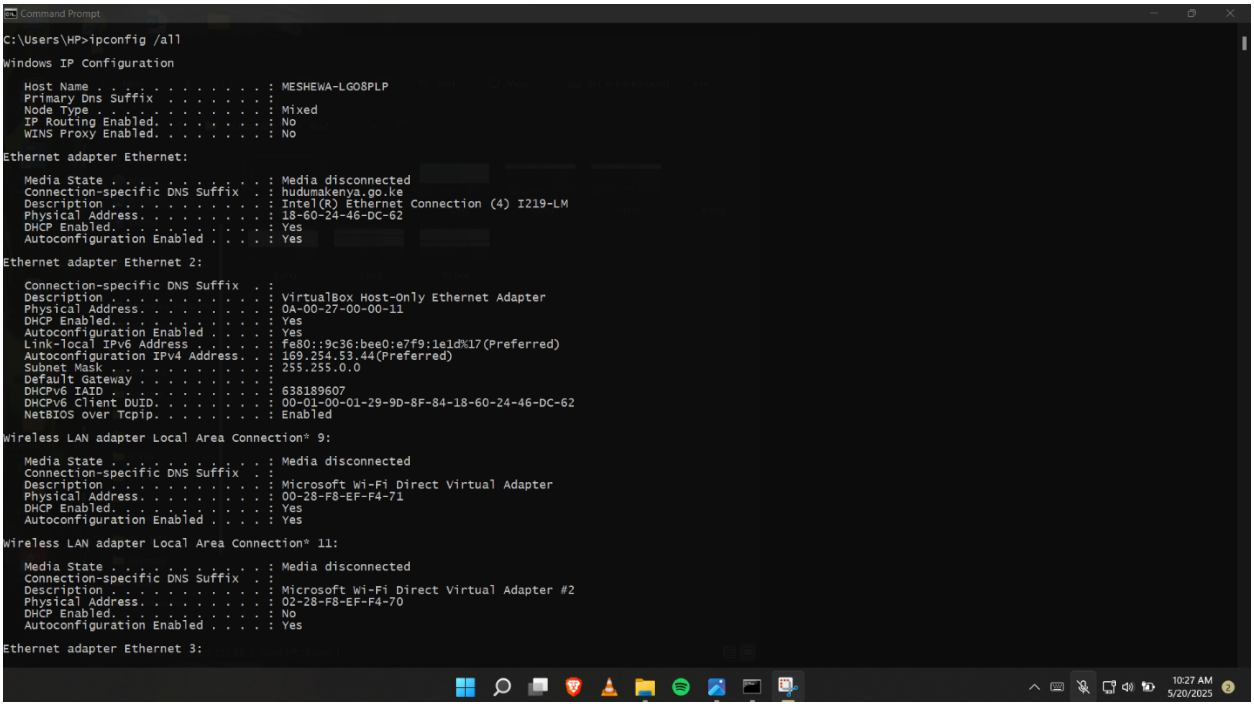
## Objectives

- To capture and analyze local ICMP Data in Wireshark
- To capture and analyze remote ICMP Data in Wireshark

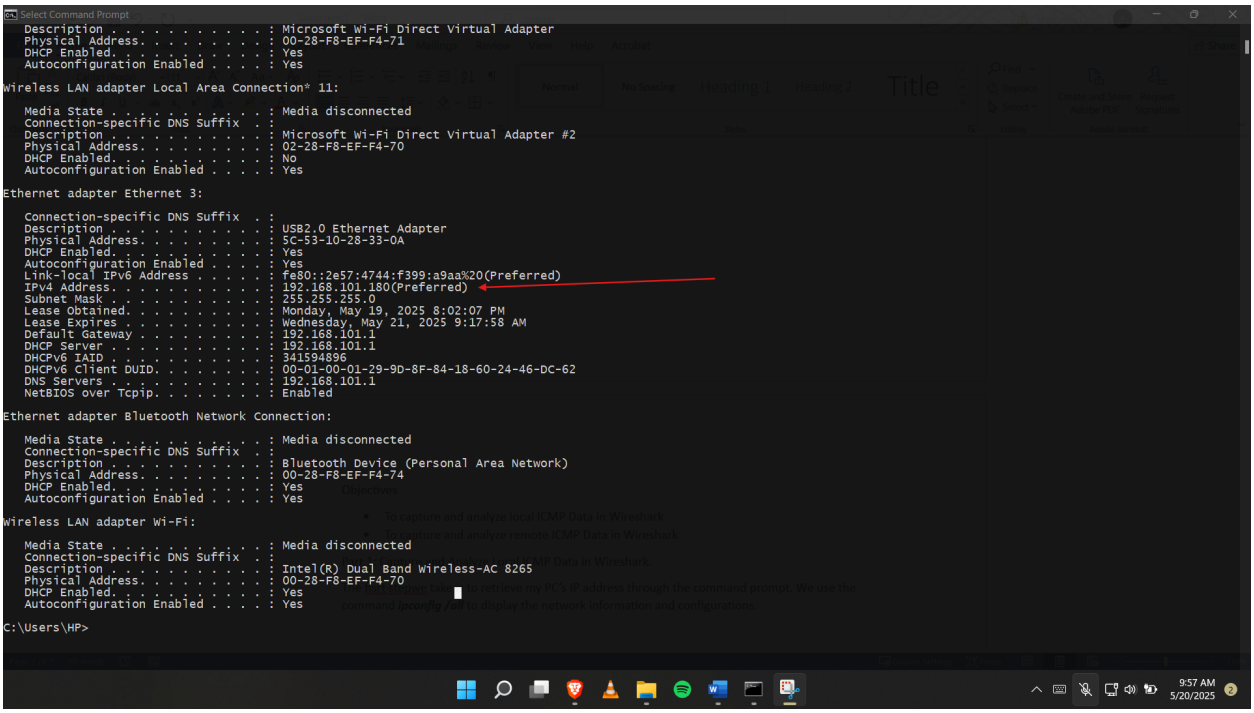
## Part 1: Capture and Analyze Local ICMP Data in Wireshark.

### Step 1: Retrieve IP Address

The first step we take is to retrieve my PC's IP address through the command prompt. We use the command ***ipconfig /all*** to display the network information and configurations.

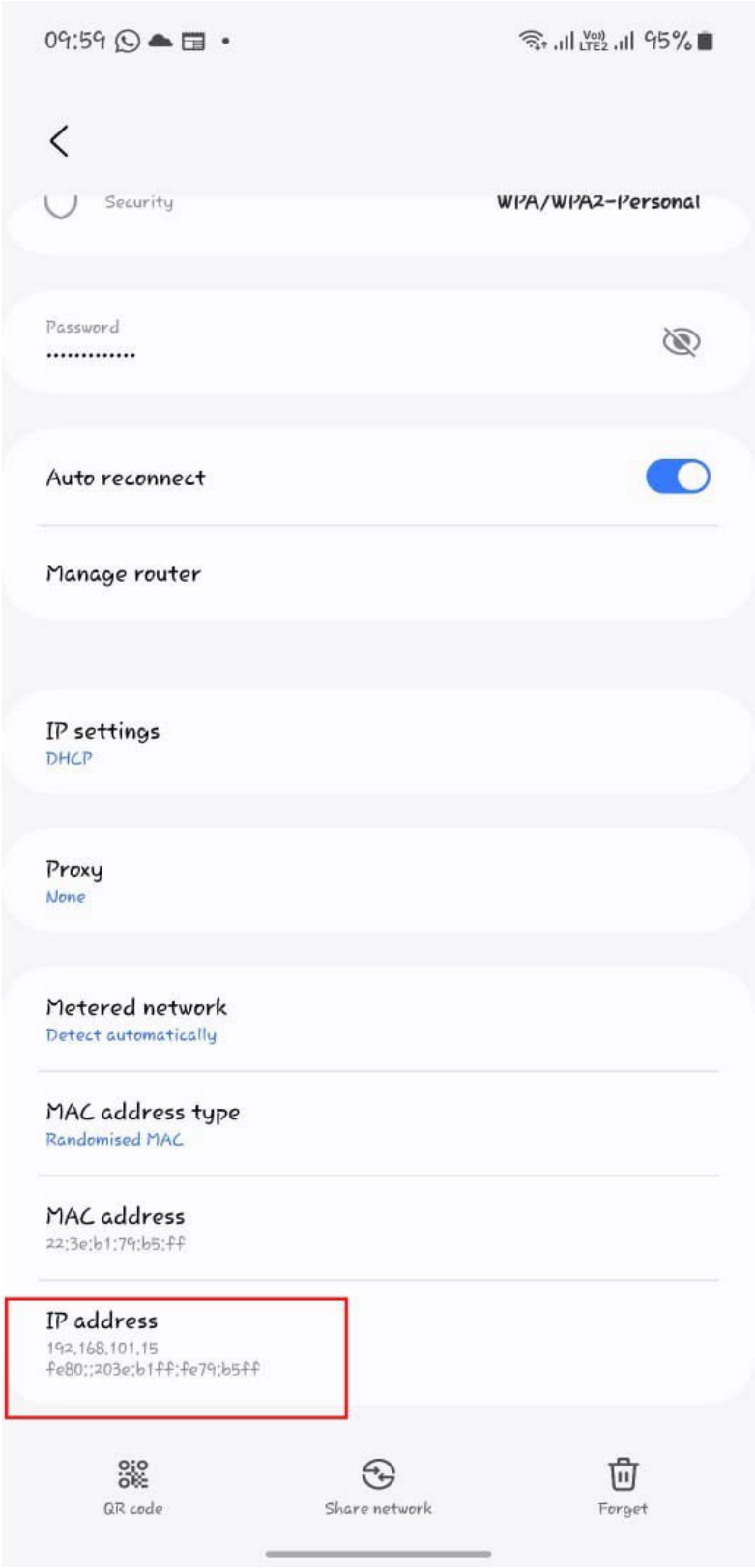


```
Command Prompt
C:\Users\HP>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : MESHEWA-LGO8PLP
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : hudumakenya.go.ke
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (4) I219-LM
   Physical Address. . . . . . . . . : 18-60-24-46-DC-62
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   Physical Address. . . . . . . . . : 0A-00-27-00-00-11
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::9c36:bee0:e7f9:1e1d%17(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.53.44(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 638189607
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-9D-8F-84-18-60-24-46-DC-62
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 00-28-F8-EF-F4-71
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 02-28-F8-EF-F4-70
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:
```



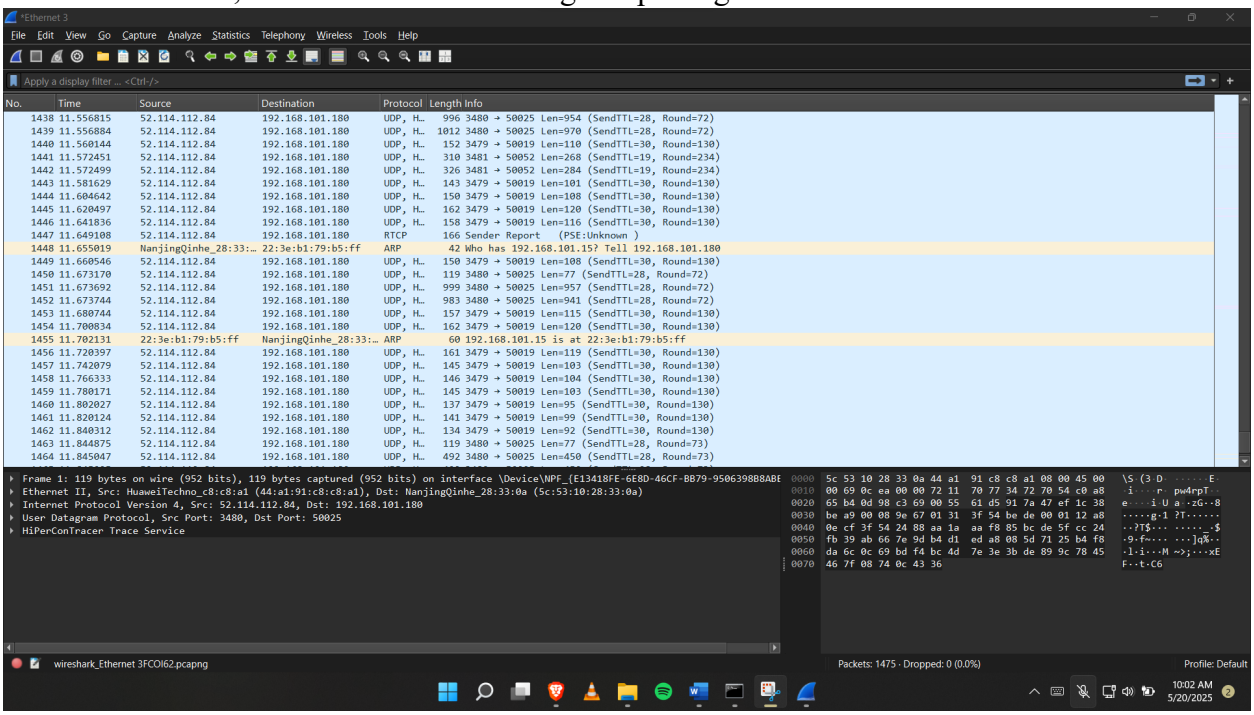
```
Select Command Prompt
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 00-28-F8-EF-F4-71
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 02-28-F8-EF-F4-70
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : USB2.0 Ethernet Adapter
   Physical Address. . . . . . . . . : 5C-53-10-28-33-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2e57:4744:f399:a9aa%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.101.180(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, May 19, 2025 8:02:07 PM
   Lease Expires . . . . . . . . . . : Wednesday, May 21, 2025 9:17:58 AM
   Default Gateway . . . . . . . . . : 192.168.101.1
   DHCP Server . . . . . . . . . . . : 192.168.101.1
   DHCPv6 IAID . . . . . . . . . . . : 341594896
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-9D-8F-84-18-60-24-46-DC-62
   DNS Servers . . . . . . . . . . . : 192.168.101.1
   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. . . . . . . . . : 00-28-F8-EF-F4-74
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : 00-28-F8-EF-F4-70
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Users\HP>
```

We find my PC IP addresses as ***192.168.101.180,*** and for my other device in the same network as ***192.168.101.15*** as shown below:

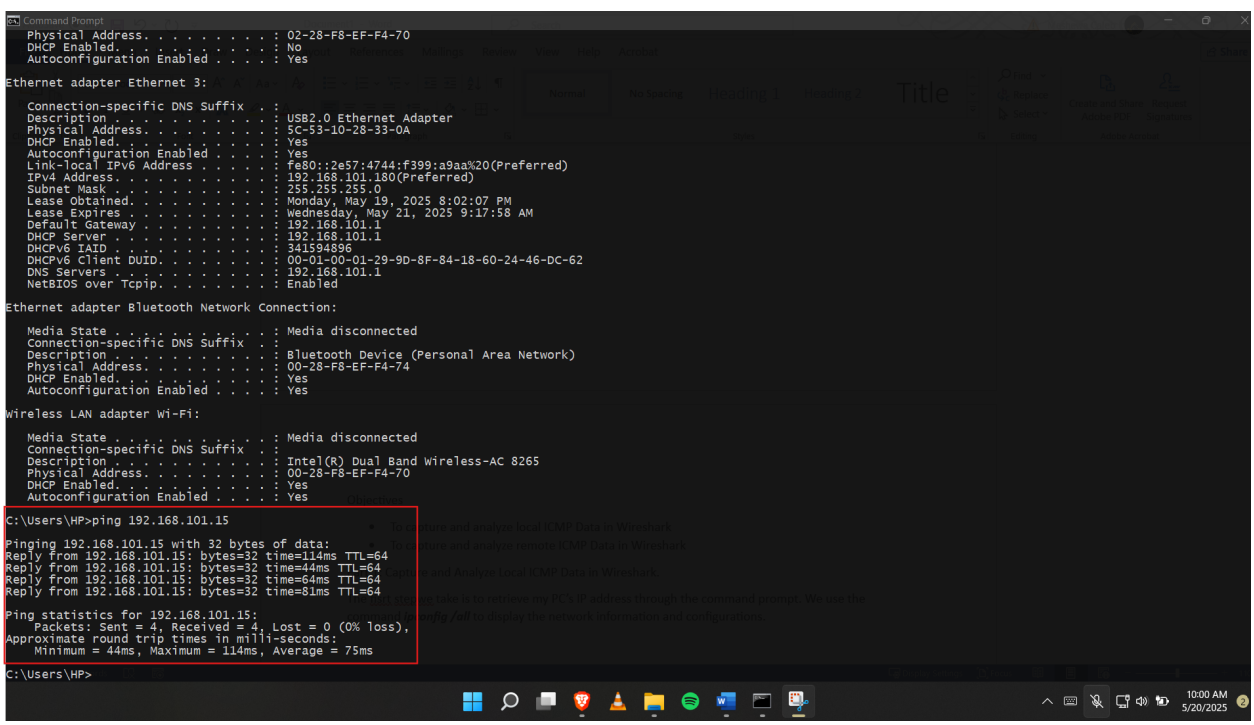


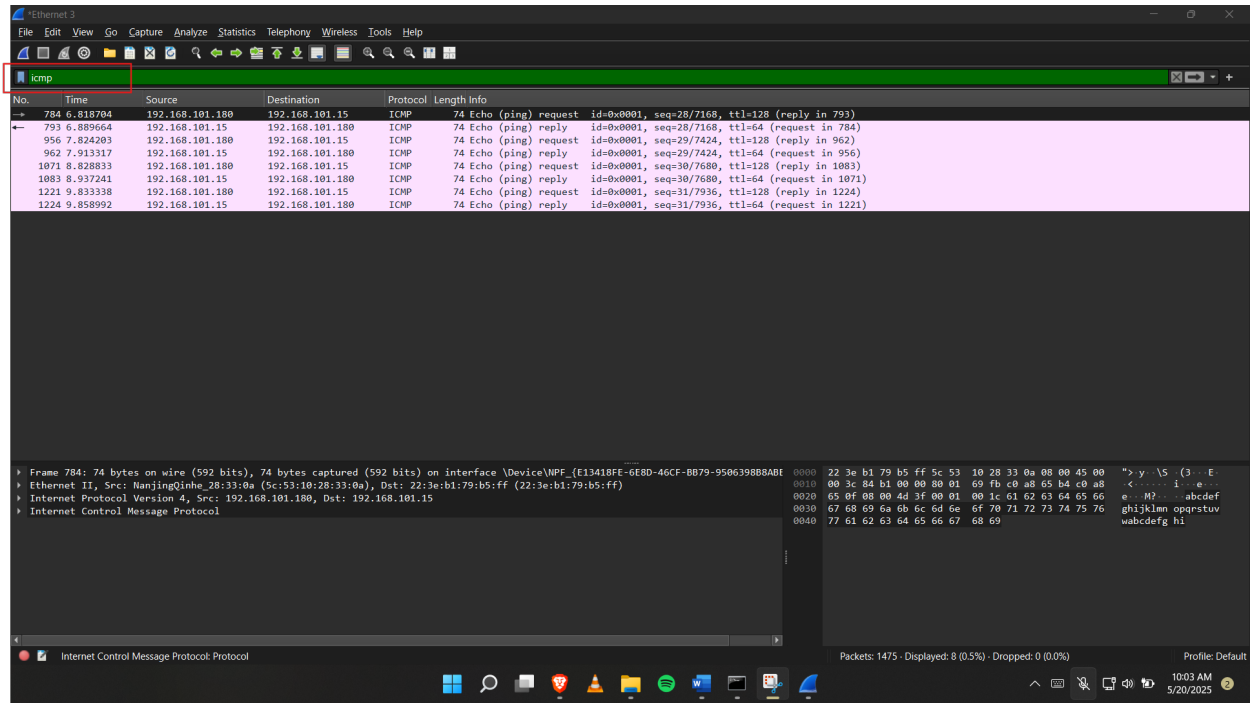
## Step 2: Start Wireshark

On the other hand, we start Wireshark to begin capturing data.



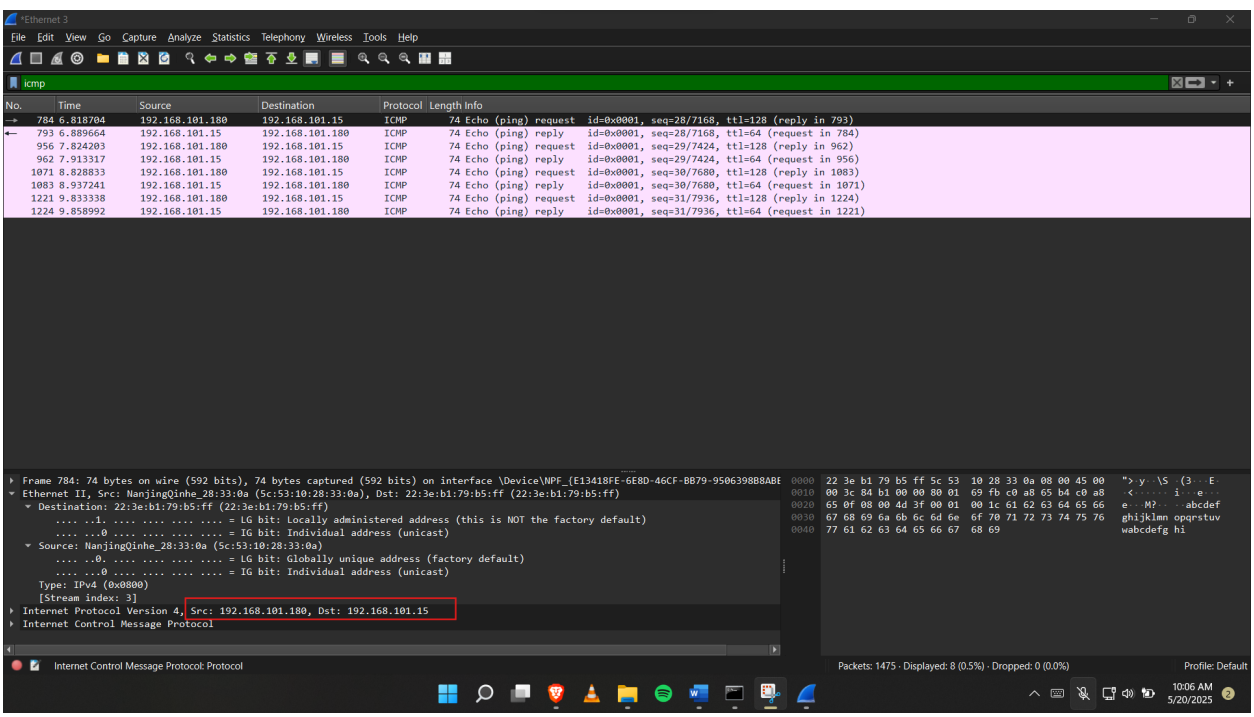

Back in my command prompt termina, I ping my other device that is ***ping 192.168.101.15*** , and since I am only interested in ICMP (ping) PDUs, we type **icmp** in the filter box and press enter (in Wireshark).






## Step 3: Examine the captured data.

We can see the data generated by the ping requests to my other device. I clicked the first ICMP request and we can see the Source column has my PC's IP address and the destination column contains my phone's IP addresses as shown earlier.

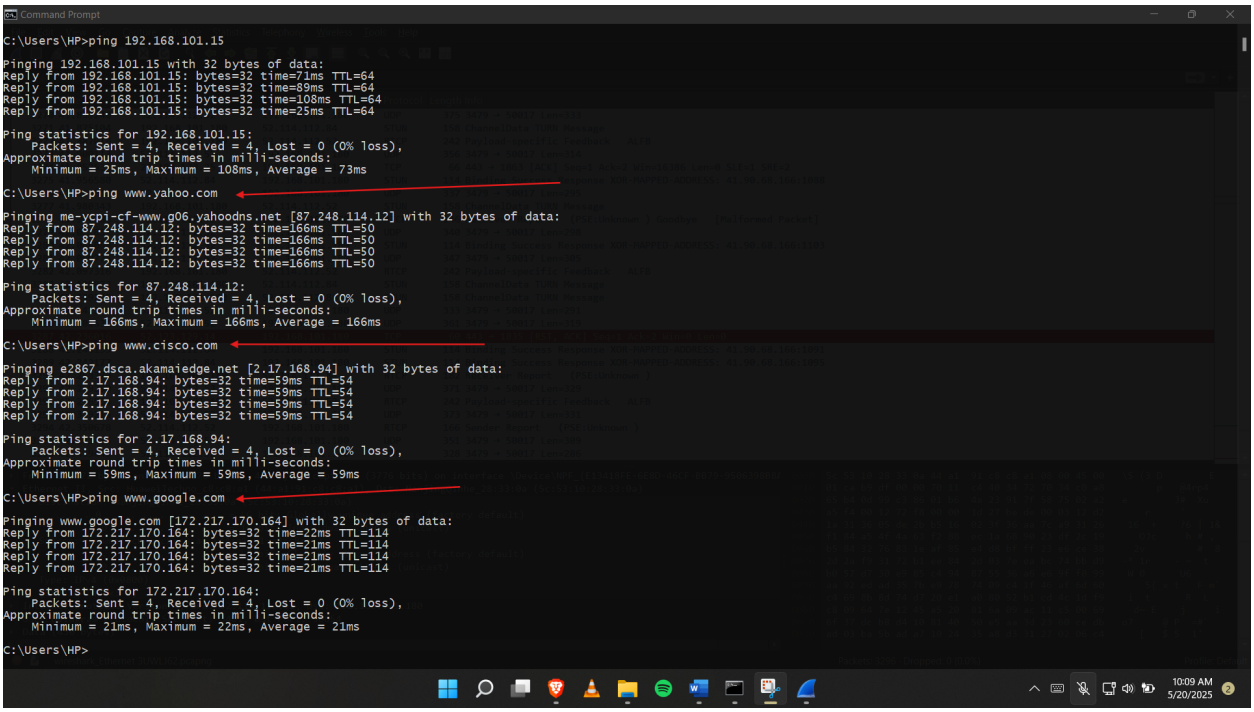


## Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Here the task is to ping remote hosts (host not on the LAN) and examine the generated data from those pings.

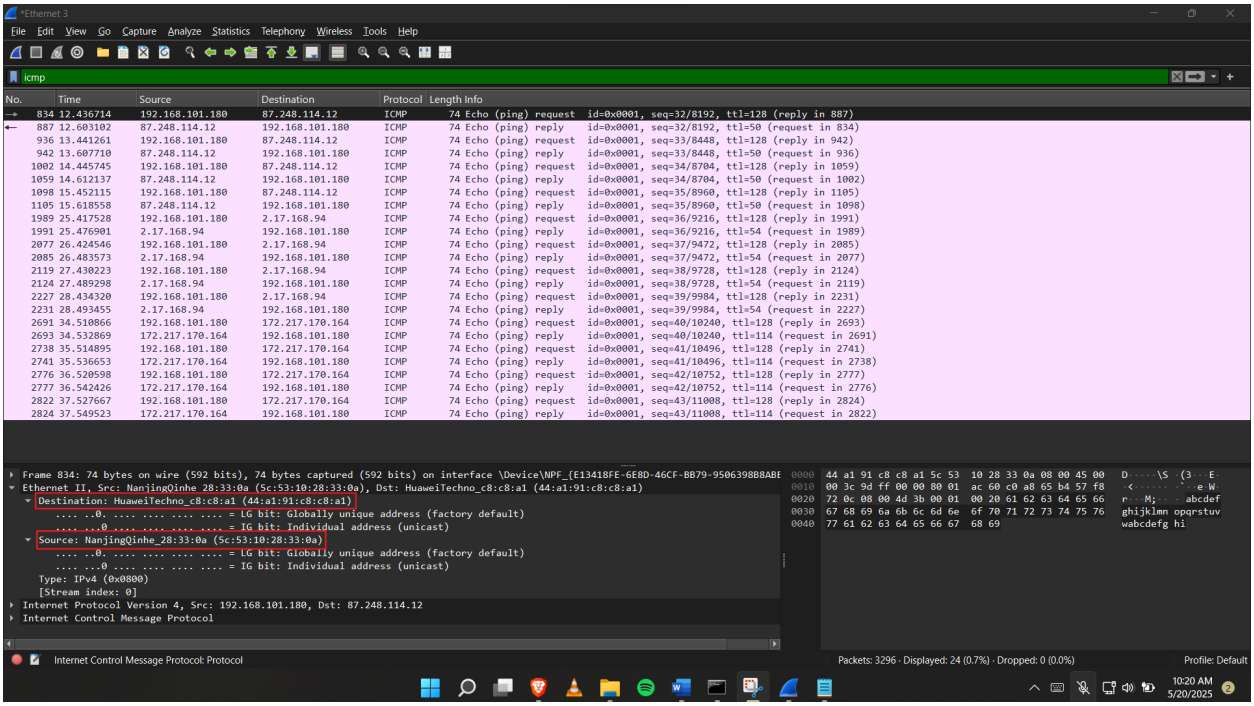
I pinged the following URLs from my command prompt:

- www.yahoo.com
- www.cisco.com
- www.google.com

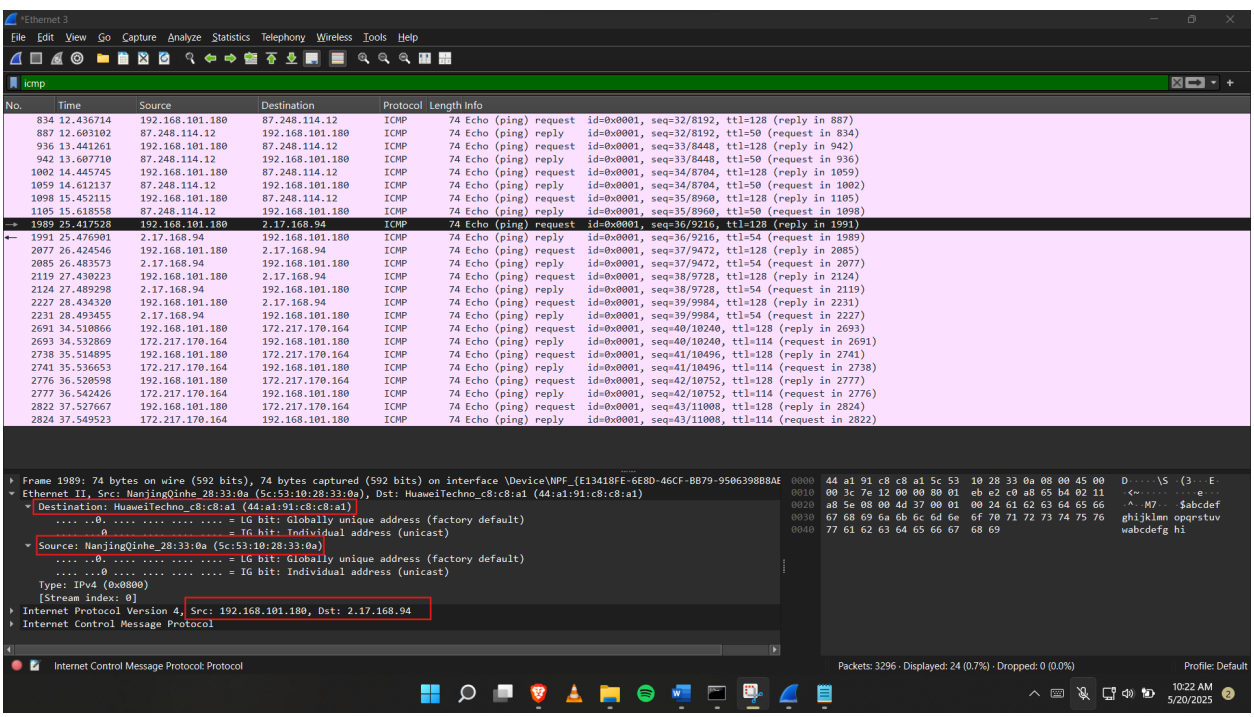



We see the ip addresses of the URLS as:

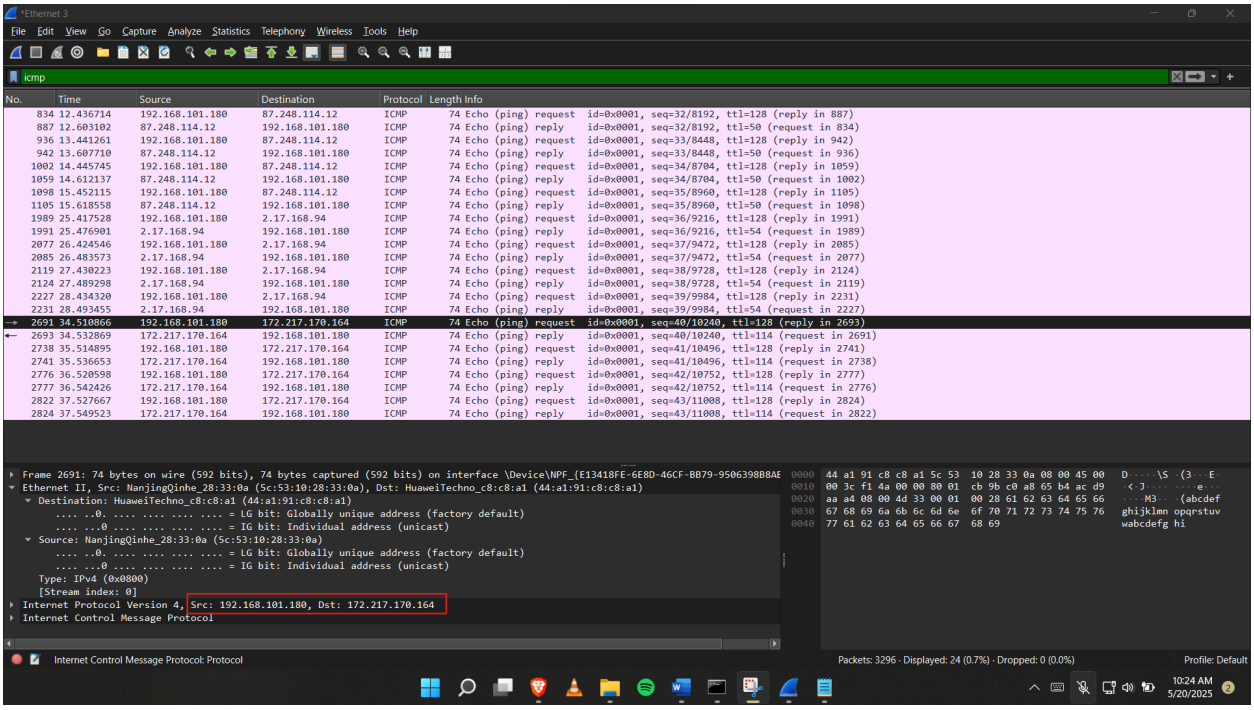
***87.248.114.12 --------- www.yahoo.com***




## *2.17.168.94 --------- www.cisco.com*



***170.217.170.164*** ----- [www.google.com](http://www.google.com)




## Conclusion

After this lab, we learn that Wireshark shows the actual MAC addresses of local hosts because MAC addresses are only used within the local network (LAN). When two devices on the same LAN communicate, they use ARP to find each other's MAC addresses, which Wireshark can capture. However, when communicating with remote hosts, packets are sent to the local router, and the destination MAC address is that of the router, not the remote host. As packets move through routers across the internet, each router replaces the MAC address with its own.