

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	3
Objectives	3
Part 1: Capture and Analyze Local ICMP Data in Wireshark.	3
Step 1: Retrieve IP Address	3
Step 2: Start Wireshark	6
Step 3: Examine the captured data.	7
Part 2: Capture and Analyze Remote ICMP Data in Wireshark.....	8
Conclusion	10

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.

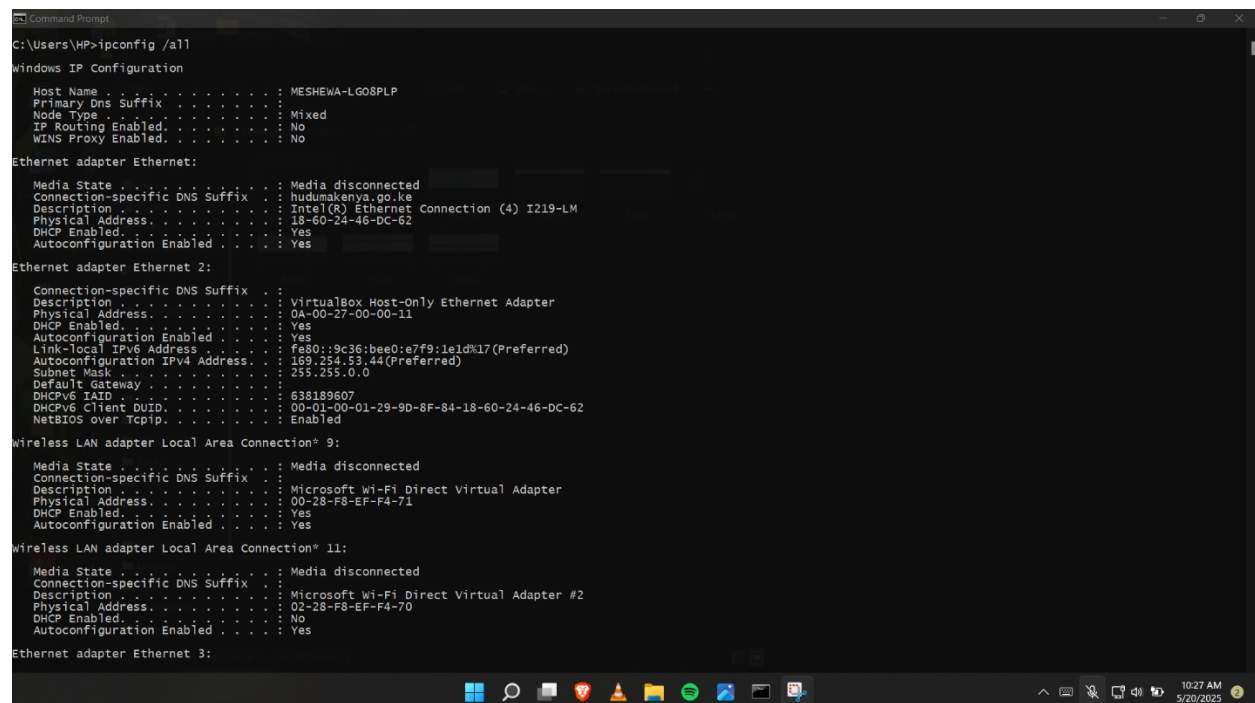
Objectives

- 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.



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

Windows IP Configuration

Host Name . . . . . : MESHEWA-LG08PLP
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

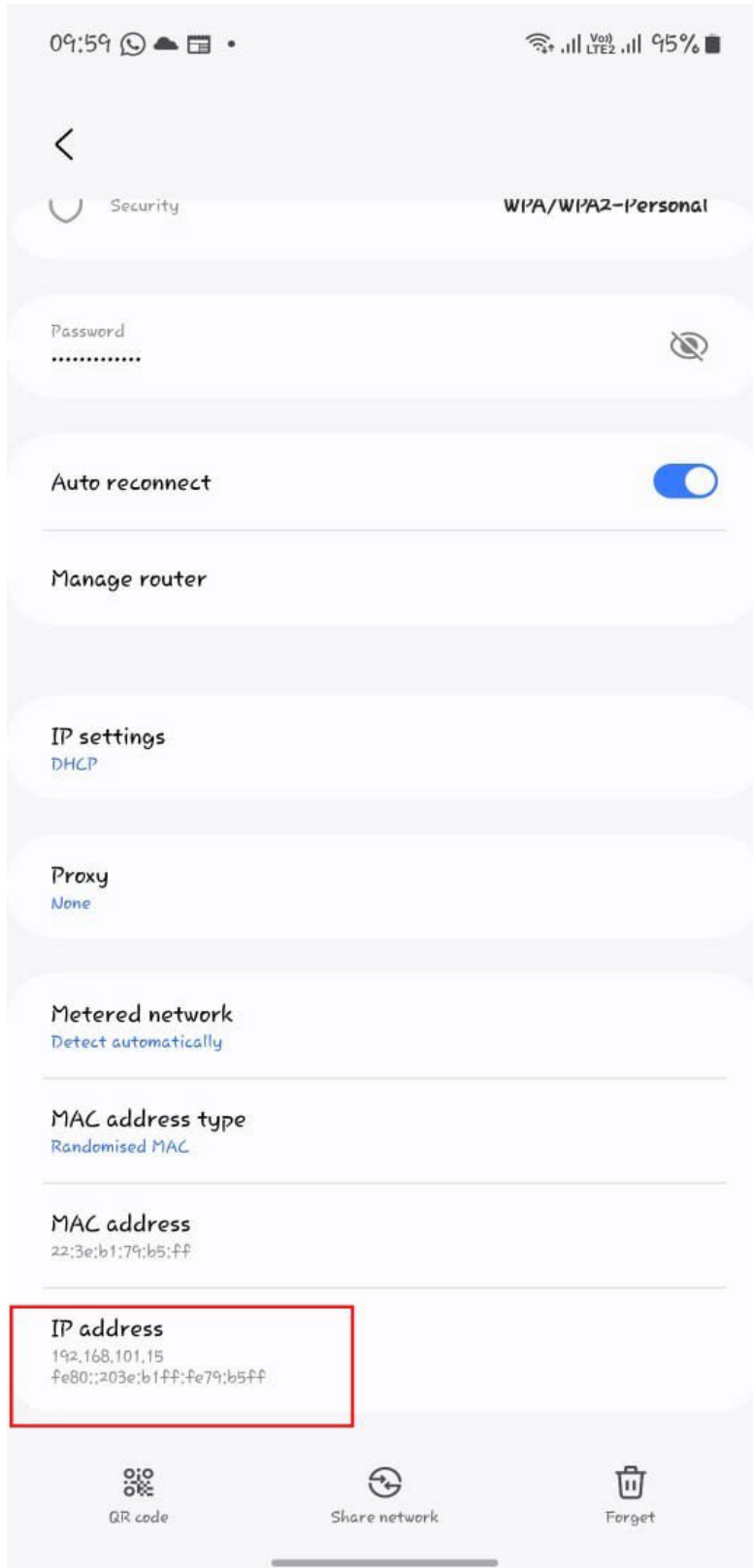
Ethernet adapter Ethernet 3:
Connection-specific DNS Suffix . . . . . :
Description . . . . . : USB2.0 Ethernet Adapter
Physical Address. . . . . : 5C-53-10-28-33-0A
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::2e57:4744:f399:a9aa%20(Preferred)
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

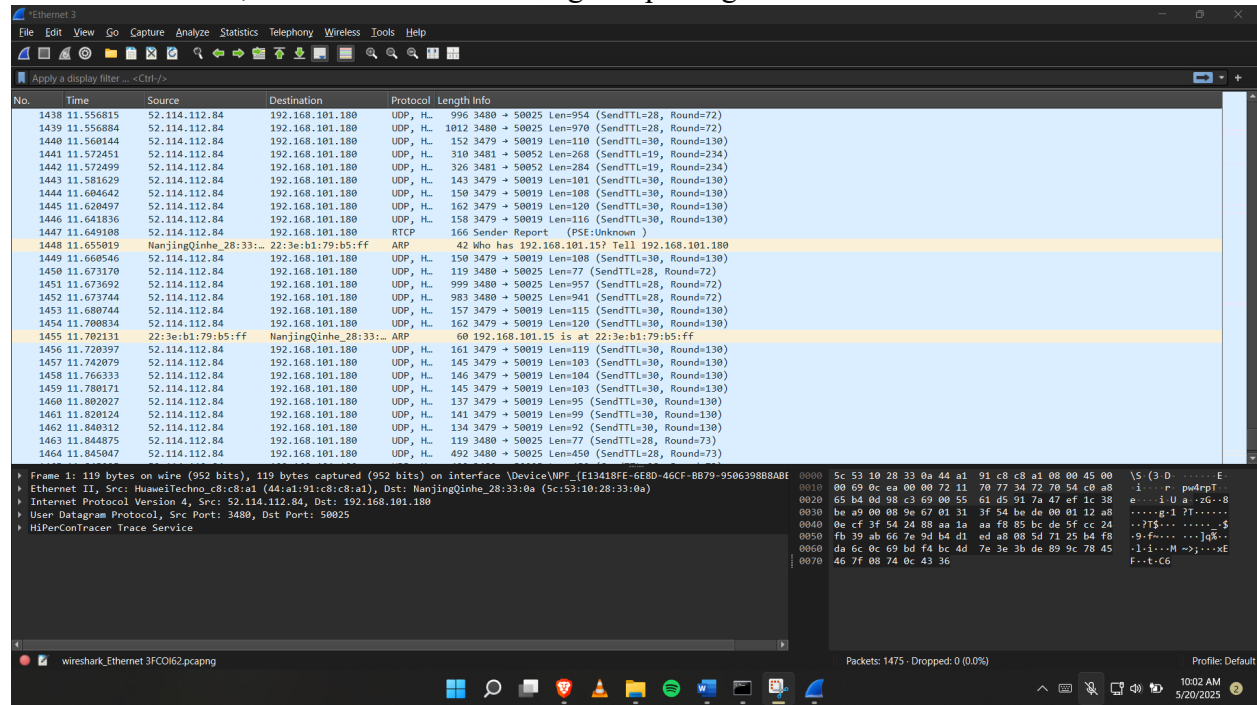
C:\Users\HP>
```

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:

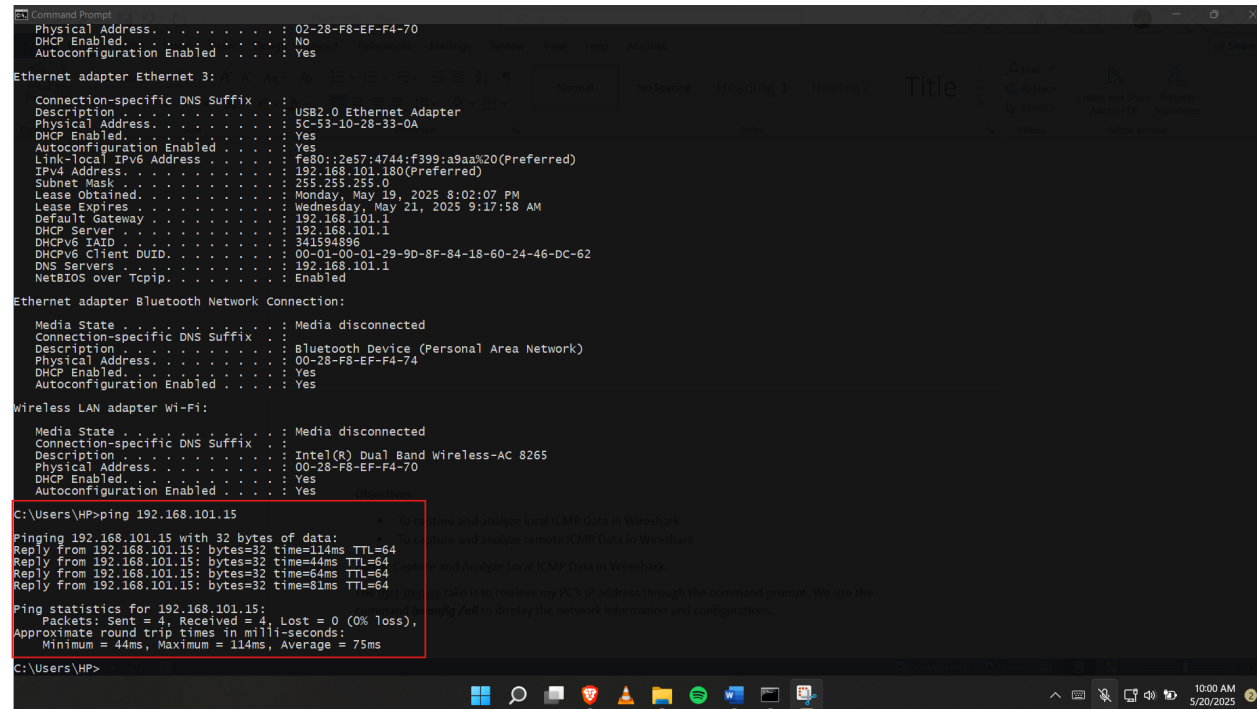


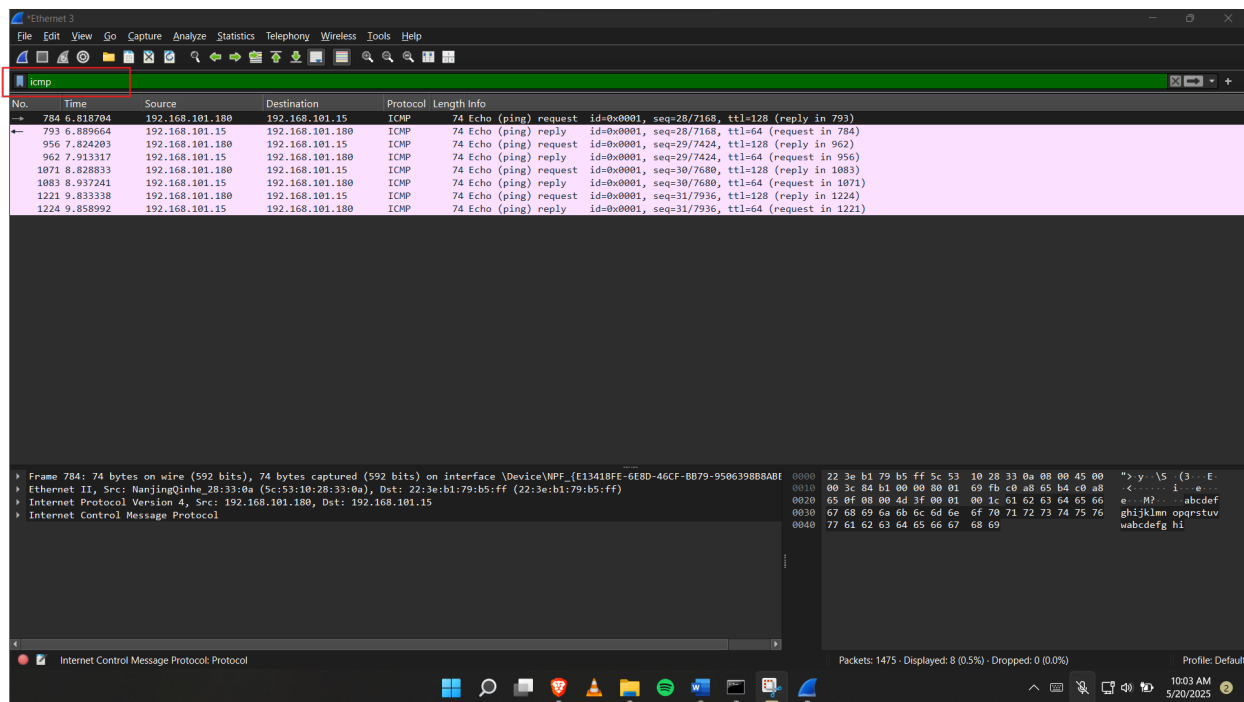
Step 2: Start Wireshark

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



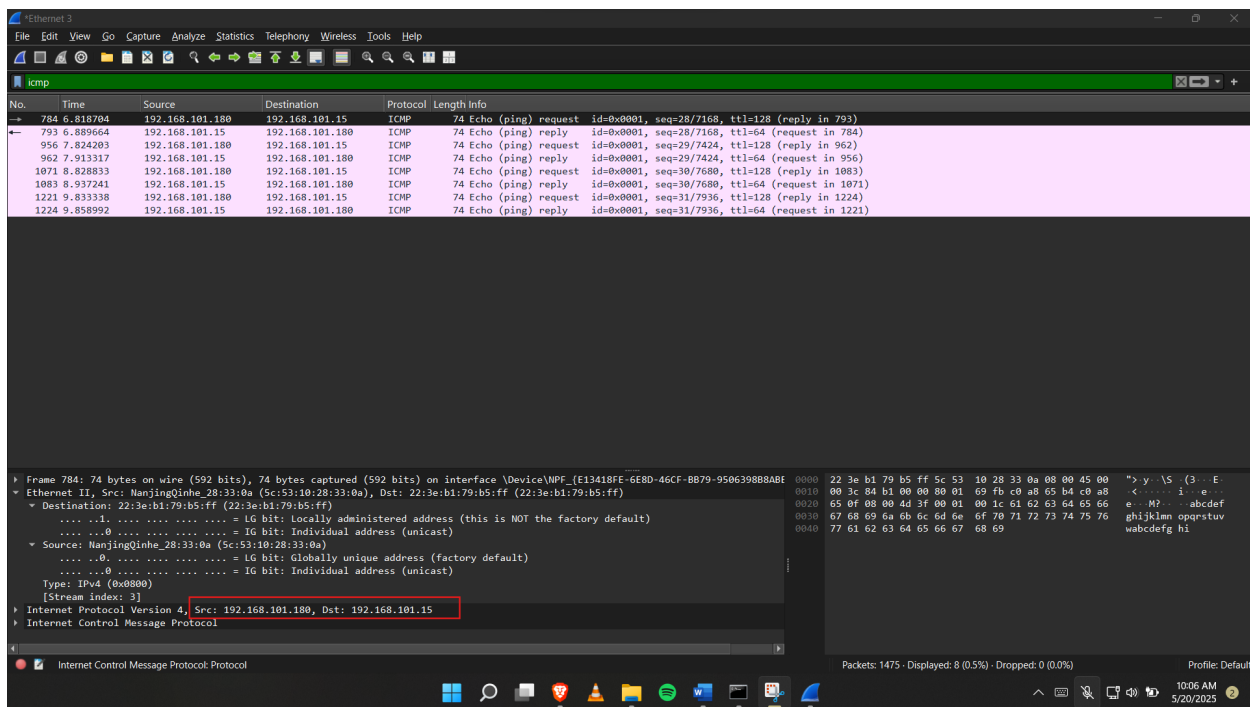
Back in my command prompt termina, I ping my other device that is *ping 192.168.101.15*, and since I am only interested in ICMP (ping) PDUs, we type **icmp** in the filter box and press enter (in Wireshark).





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

```
Command Prompt
C:\Users\HP>ping 192.168.101.15
Pinging 192.168.101.15 with 32 bytes of data:
Reply from 192.168.101.15: bytes=32 time=71ms TTL=64
Reply from 192.168.101.15: bytes=32 time=89ms TTL=64
Reply from 192.168.101.15: bytes=32 time=108ms TTL=64
Reply from 192.168.101.15: bytes=32 time=25ms TTL=64
Ping statistics for 192.168.101.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 108ms, Average = 73ms
C:\Users\HP>ping www.yahoo.com
Pinging me-ycpi-cf-www.g06.yahoodns.net [87.248.114.12] with 32 bytes of data:
Reply from 87.248.114.12: bytes=32 time=166ms TTL=50
Reply from 87.248.114.12: bytes=32 time=166ms TTL=50
Reply from 87.248.114.12: bytes=32 time=166ms TTL=50
Reply from 87.248.114.12: bytes=32 time=166ms TTL=50
Ping statistics for 87.248.114.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 166ms, Maximum = 166ms, Average = 166ms
C:\Users\HP>ping www.cisco.com
Pinging e2867.dsca.akamaiedge.net [2.17.168.94] with 32 bytes of data:
Reply from 2.17.168.94: bytes=32 time=59ms TTL=54
Reply from 2.17.168.94: bytes=32 time=59ms TTL=54
Reply from 2.17.168.94: bytes=32 time=59ms TTL=54
Reply from 2.17.168.94: bytes=32 time=59ms TTL=54
Ping statistics for 2.17.168.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 59ms, Maximum = 59ms, Average = 59ms
C:\Users\HP>ping www.google.com
Pinging www.google.com [172.217.170.164] with 32 bytes of data:
Reply from 172.217.170.164: bytes=32 time=22ms TTL=114
Reply from 172.217.170.164: bytes=32 time=21ms TTL=114
Reply from 172.217.170.164: bytes=32 time=21ms TTL=114
Reply from 172.217.170.164: bytes=32 time=21ms TTL=114
Ping statistics for 172.217.170.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 22ms, Average = 21ms
C:\Users\HP>
```

We see the ip addresses of the URLs as:

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

Wireshark capture of ICMP Echo (ping) requests and replies between 192.168.101.180 and 87.248.114.12. The capture shows a sequence of 24 packets, including requests and replies, with details expanded for the selected packet (No. 834).

No.	Time	Source	Destination	Protocol	Length	Info
834	12.436714	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 887)
887	12.603102	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=50 (request in 834)
936	13.441261	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 942)
942	13.607710	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=50 (request in 936)
1002	14.445745	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 1059)
1059	14.612137	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=50 (request in 1002)
1098	15.452115	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 1105)
1105	15.618558	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=50 (request in 1098)
1989	25.417528	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 1991)
1991	25.476901	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=54 (request in 1989)
2077	26.425446	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 2085)
2085	26.483573	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=54 (request in 2077)
2119	27.430223	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 2124)
2124	27.489298	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=54 (request in 2119)
2227	28.434320	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 2231)
2231	28.493455	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=54 (request in 2227)
2691	34.510866	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 2693)
2693	34.532869	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=114 (request in 2691)
2738	35.514895	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 2741)
2741	35.536653	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=114 (request in 2738)
2776	36.520598	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 2777)
2777	36.542426	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=114 (request in 2776)
2822	37.527667	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 2824)
2824	37.549523	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=114 (request in 2822)

Details of selected packet (No. 834):

- Frame 834: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E13418FE-6E8D-46CF-BB79-95063988BAE}
- Ethernet II, Src: NanjingQinhe 28:33:0a (5c:53:10:28:33:0a), Dst: HuaweiTechno_c8:c8:a1 (44:a1:91:c8:c8:a1)
- Destination: HuaweiTechno_c8:c8:a1 (44:a1:91:c8:c8:a1)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.101.180, Dst: 87.248.114.12
- Internet Control Message Protocol

2.17.168.94 ----- www.cisco.com

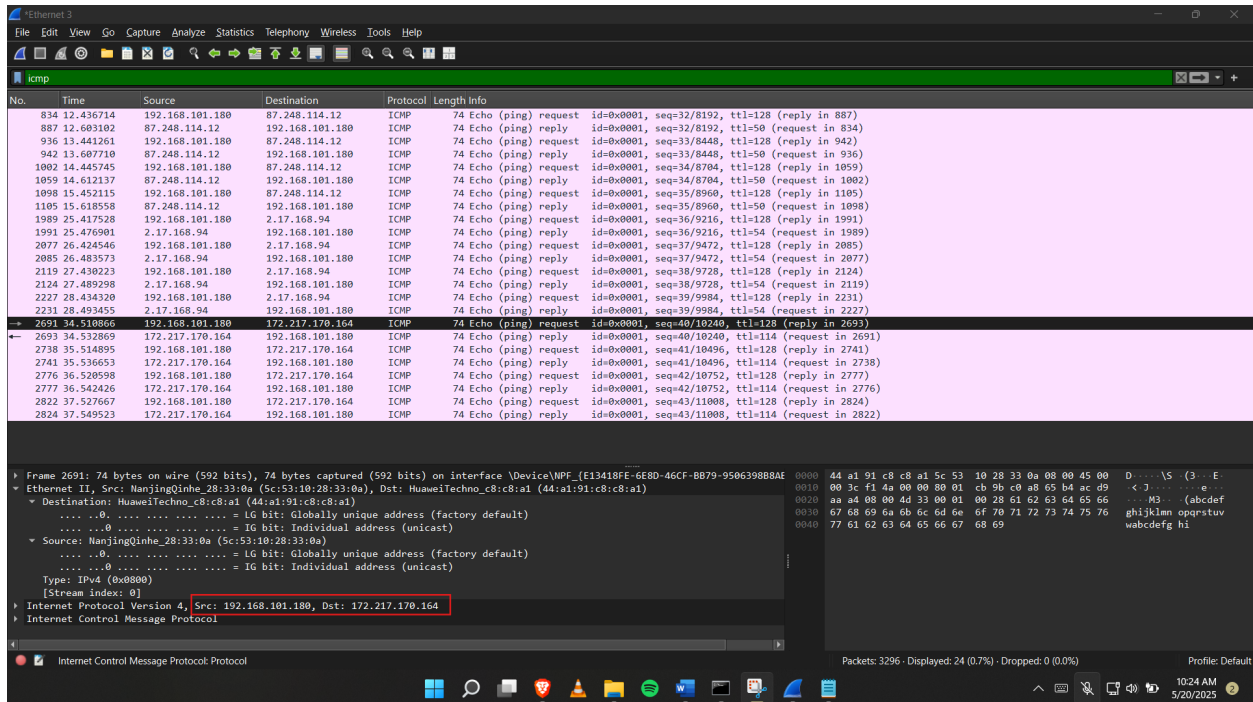
Wireshark capture of ICMP Echo (ping) requests and replies between 192.168.101.180 and 2.17.168.94. The capture shows a sequence of 24 packets, including requests and replies, with details expanded for the selected packet (No. 1989).

No.	Time	Source	Destination	Protocol	Length	Info
834	12.436714	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (reply in 887)
887	12.603102	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=32/8192, ttl=50 (request in 834)
936	13.441261	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=33/8448, ttl=128 (reply in 942)
942	13.607710	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=33/8448, ttl=50 (request in 936)
1002	14.445745	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (reply in 1059)
1059	14.612137	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=50 (request in 1002)
1098	15.452115	192.168.101.180	87.248.114.12	ICMP	74	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 1105)
1105	15.618558	87.248.114.12	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=35/8960, ttl=50 (request in 1098)
1989	25.417528	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 1991)
1991	25.476901	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=36/9216, ttl=54 (request in 1989)
2077	26.425446	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 2085)
2085	26.483573	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=37/9472, ttl=54 (request in 2077)
2119	27.430223	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 2124)
2124	27.489298	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=38/9728, ttl=54 (request in 2119)
2227	28.434320	192.168.101.180	2.17.168.94	ICMP	74	Echo (ping) request id=0x0001, seq=39/9984, ttl=128 (reply in 2231)
2231	28.493455	2.17.168.94	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=39/9984, ttl=54 (request in 2227)
2691	34.510866	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (reply in 2693)
2693	34.532869	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=40/10240, ttl=114 (request in 2691)
2738	35.514895	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (reply in 2741)
2741	35.536653	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=114 (request in 2738)
2776	36.520598	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=128 (reply in 2777)
2777	36.542426	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=114 (request in 2776)
2822	37.527667	192.168.101.180	172.217.170.164	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=128 (reply in 2824)
2824	37.549523	172.217.170.164	192.168.101.180	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=114 (request in 2822)

Details of selected packet (No. 1989):

- Frame 1989: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E13418FE-6E8D-46CF-BB79-95063988BAE}
- Ethernet II, Src: NanjingQinhe 28:33:0a (5c:53:10:28:33:0a), Dst: HuaweiTechno_c8:c8:a1 (44:a1:91:c8:c8:a1)
- Destination: HuaweiTechno_c8:c8:a1 (44:a1:91:c8:c8:a1)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.101.180, Dst: 2.17.168.94
- Internet Control Message Protocol

170.217.170.164 ----- 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.