Lab - Use Wireshark to View Network Traffic

Report by:AHMED MOHAMUD, CS-CNS06-24114

Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

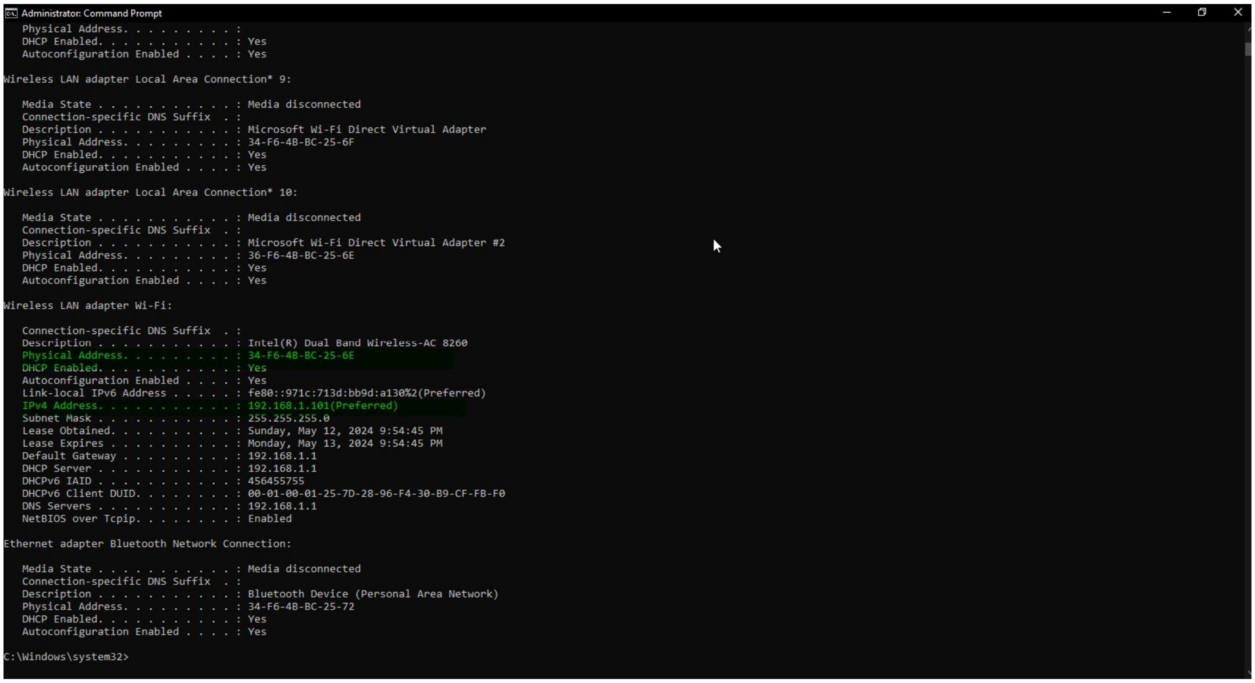
Introduction

In this report, we explore the capabilities and functionalities of Wireshark, a renowned software protocol analyzer, used extensively for network troubleshooting, protocol analysis, and educational purposes. Through the structured lab exercises, we investigate the detailed process and insights gained from capturing and analyzing both local and remote Internet Control Message Protocol (ICMP) data. This analysis is crucial for understanding packet behaviors and network dynamics, particularly how data packets are structured, transmitted, and interpreted across network interfaces. This aims to provide a comprehensive understanding of network traffic analysis, which is essential for enhancing network security, performance, and troubleshooting methodologies

Instructions

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Step 1:Retrieve your PC interface addresses.



```
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 34-F6-4B-BC-25-6F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 36-F6-4B-BC-25-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   Physical Address. . . . . . . . . : 34-F6-4B-BC-25-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::971c:713d:bb9d:a130%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, May 12, 2024 9:54:45 PM
   Lease Expires . . . . . . . . . . : Monday, May 13, 2024 9:54:45 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 456455755
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-7D-28-96-F4-30-B9-CF-FB-F0
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   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. . . . . . . . . : 34-F6-4B-BC-25-72
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>
```

b. Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

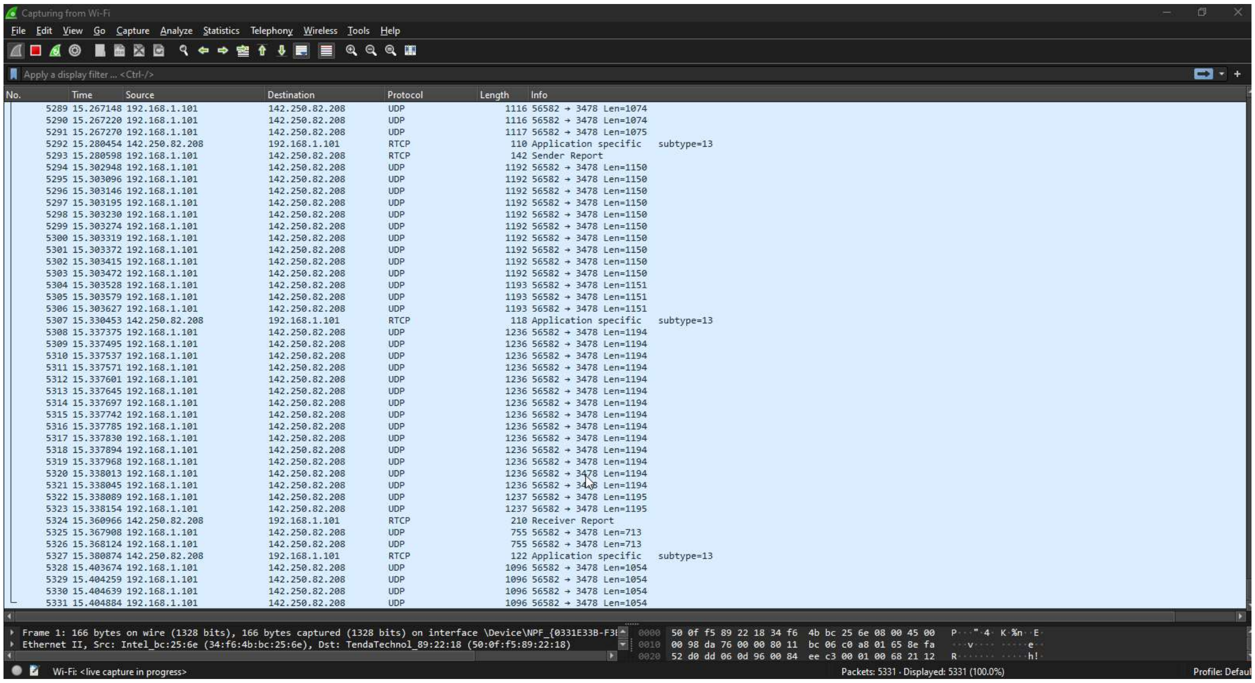
Team member ip:192.168.1.100

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.

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.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time      Source          Destination     Protocol  Length Info
   5289 15.267148 192.168.1.101   142.250.82.208  UDP         1116 56582 → 3478 Len=1074
   5290 15.267220 192.168.1.101   142.250.82.208  UDP         1116 56582 → 3478 Len=1074
   5291 15.267270 192.168.1.101   142.250.82.208  UDP         1117 56582 → 3478 Len=1075
   5292 15.280454 142.250.82.208  192.168.1.101   RTCP         110 Application specific   subtype=13
   5293 15.280598 192.168.1.101   142.250.82.208  RTCP         142 Sender Report
   5294 15.302948 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5295 15.303096 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5296 15.303146 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5297 15.303195 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5298 15.303230 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5299 15.303274 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5300 15.303319 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5301 15.303372 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5302 15.303415 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5303 15.303472 192.168.1.101   142.250.82.208  UDP         1192 56582 → 3478 Len=1150
   5304 15.303528 192.168.1.101   142.250.82.208  UDP         1193 56582 → 3478 Len=1151
   5305 15.303579 192.168.1.101   142.250.82.208  UDP         1193 56582 → 3478 Len=1151
   5306 15.303627 192.168.1.101   142.250.82.208  UDP         1193 56582 → 3478 Len=1151
   5307 15.330453 142.250.82.208  192.168.1.101   RTCP         118 Application specific   subtype=13
   5308 15.337375 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5309 15.337495 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5310 15.337537 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5311 15.337571 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5312 15.337601 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5313 15.337645 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5314 15.337697 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5315 15.337742 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5316 15.337785 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5317 15.337830 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5318 15.337894 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5319 15.337968 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5320 15.338013 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5321 15.338045 192.168.1.101   142.250.82.208  UDP         1236 56582 → 3478 Len=1194
   5322 15.338089 192.168.1.101   142.250.82.208  UDP         1237 56582 → 3478 Len=1195
   5323 15.338154 192.168.1.101   142.250.82.208  UDP         1237 56582 → 3478 Len=1195
   5324 15.360966 142.250.82.208  192.168.1.101   RTCP         210 Receiver Report
   5325 15.367908 192.168.1.101   142.250.82.208  UDP          755 56582 → 3478 Len=713
   5326 15.368124 192.168.1.101   142.250.82.208  UDP          755 56582 → 3478 Len=713
   5327 15.380874 142.250.82.208  192.168.1.101   RTCP         122 Application specific   subtype=13
   5328 15.403674 192.168.1.101   142.250.82.208  UDP         1096 56582 → 3478 Len=1054
   5329 15.404259 192.168.1.101   142.250.82.208  UDP         1096 56582 → 3478 Len=1054
   5330 15.404639 192.168.1.101   142.250.82.208  UDP         1096 56582 → 3478 Len=1054
   5331 15.404884 192.168.1.101   142.250.82.208  UDP         1096 56582 → 3478 Len=1054
```

```
Frame 1: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits) on interface \Device\NPF_{0331E33B-F3E
Ethernet II, Src: Intel_bc:25:6e (34:f6:4b:bc:25:6e), Dst: TendaTechnol_89:22:18 (50:0f:f5:89:22:18)

0000  50 0f f5 89 22 18 34 f6  4b bc 25 6e 08 00 45 00   P···"·4· K·%n··E·
0010  00 98 da 76 00 00 80 11  bc 06 c0 a8 01 65 8e fa   ···v···· ·····e··
0020  52 d0 dd 06 0d 96 00 84  ee c3 00 01 00 68 21 12   R······· ·····h!·
```

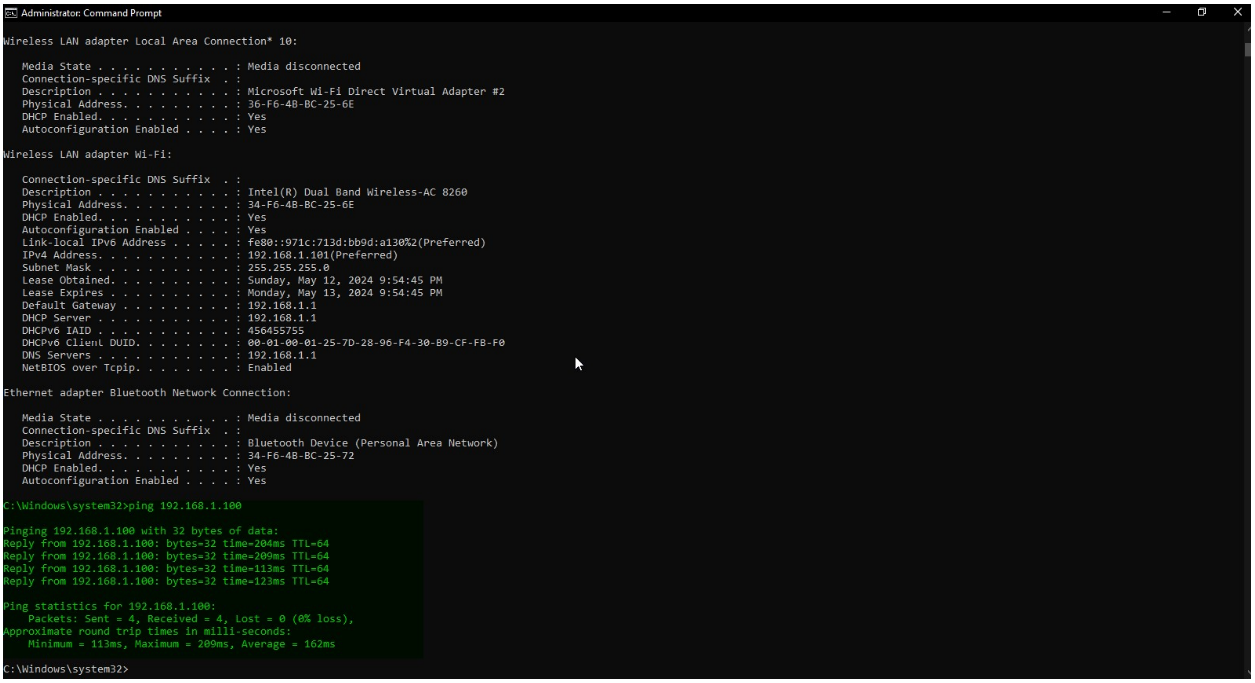
```
Wi-Fi: <live capture in progress>          Packets: 5331 · Displayed: 5331 (100.0%)          Profile: Defaul
```

Lab - Use Wireshark to View Network Traffic

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.

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 that you received from your team member.

```
C:\> ping 192.168.1.100
```

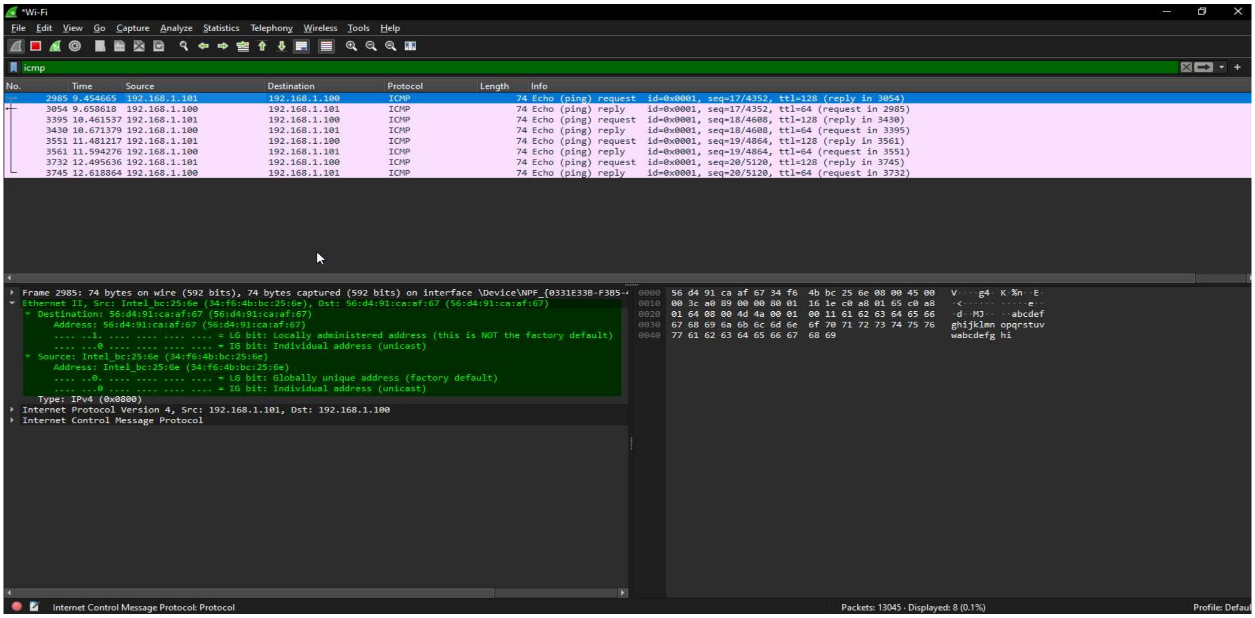


Administrator: Command Prompt

```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 36-F6-4B-BC-25-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8260
   Physical Address. . . . . . . . . : 34-F6-4B-BC-25-6E
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::971c:713d:bb9d:a130%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.101(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, May 12, 2024 9:54:45 PM
   Lease Expires . . . . . . . . . . : Monday, May 13, 2024 9:54:45 PM
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 456455755
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-7D-28-96-F4-30-B9-CF-FB-F0
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   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. . . . . . . . . : 34-F6-4B-BC-25-72
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=204ms TTL=64
Reply from 192.168.1.100: bytes=32 time=209ms TTL=64
Reply from 192.168.1.100: bytes=32 time=113ms TTL=64
Reply from 192.168.1.100: bytes=32 time=123ms TTL=64

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 113ms, Maximum = 209ms, Average = 162ms

C:\Windows\system32>
```

Step 3: Examine the captured data

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 of the teammate PC that you pinged.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.



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

```
No.     Time      Source         Destination    Protocol  Length Info
   2985 9.454665  192.168.1.101  192.168.1.100  ICMP        74 Echo (ping) request  id=0x0001, seq=17/4352, ttl=128 (reply in 3054)
   3054 9.658618  192.168.1.100  192.168.1.101  ICMP        74 Echo (ping) reply    id=0x0001, seq=17/4352, ttl=64 (request in 2985)
   3395 10.461537 192.168.1.101  192.168.1.100  ICMP        74 Echo (ping) request  id=0x0001, seq=18/4608, ttl=128 (reply in 3430)
   3430 10.671379 192.168.1.100  192.168.1.101  ICMP        74 Echo (ping) reply    id=0x0001, seq=18/4608, ttl=64 (request in 3395)
   3551 11.481217 192.168.1.101  192.168.1.100  ICMP        74 Echo (ping) request  id=0x0001, seq=19/4864, ttl=128 (reply in 3561)
   3561 11.594276 192.168.1.100  192.168.1.101  ICMP        74 Echo (ping) reply    id=0x0001, seq=19/4864, ttl=64 (request in 3551)
   3732 12.495636 192.168.1.101  192.168.1.100  ICMP        74 Echo (ping) request  id=0x0001, seq=20/5120, ttl=128 (reply in 3745)
   3745 12.618864 192.168.1.100  192.168.1.101  ICMP        74 Echo (ping) reply    id=0x0001, seq=20/5120, ttl=64 (request in 3732)
```

```
> Frame 2985: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{0331E33B-F3B5-
v Ethernet II, Src: Intel_bc:25:6e (34:f6:4b:bc:25:6e), Dst: 56:d4:91:ca:af:67 (56:d4:91:ca:af:67)
  v Destination: 56:d4:91:ca:af:67 (56:d4:91:ca:af:67)
      Address: 56:d4:91:ca:af:67 (56:d4:91:ca:af:67)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: Intel_bc:25:6e (34:f6:4b:bc:25:6e)
      Address: Intel_bc:25:6e (34:f6:4b:bc:25:6e)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.100
> Internet Control Message Protocol
```

```
0000  56 d4 91 ca af 67 34 f6  4b bc 25 6e 08 00 45 00   V···g4· K·%n··E·
0010  00 3c a0 89 00 00 80 01  16 1e c0 a8 01 65 c0 a8   ·<······ ·····e··
0020  01 64 08 00 4d 4a 00 01  00 11 61 62 63 64 65 66   ·d··MJ·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Control Message Protocol: Protocol

Packets: 13045 · Displayed: 8 (0.1%)

Profile: Defaul

Does the source MAC address match your PC interface?

Yes
Source MAC : 34:f6:4b:bc:25:6e
PC interface: 34:f6:4b:bc:25:6e

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

Yes

DST MAC: 56:d4:91:ca:af:67

TEAM MAC: 56:d4:91:ca:af:67

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

This mac address is obtained by the pc after requested sent an ARP(address resolution protocol) that translated the pinged IP address to get its mac

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Step 1: Start capturing data on the interface.

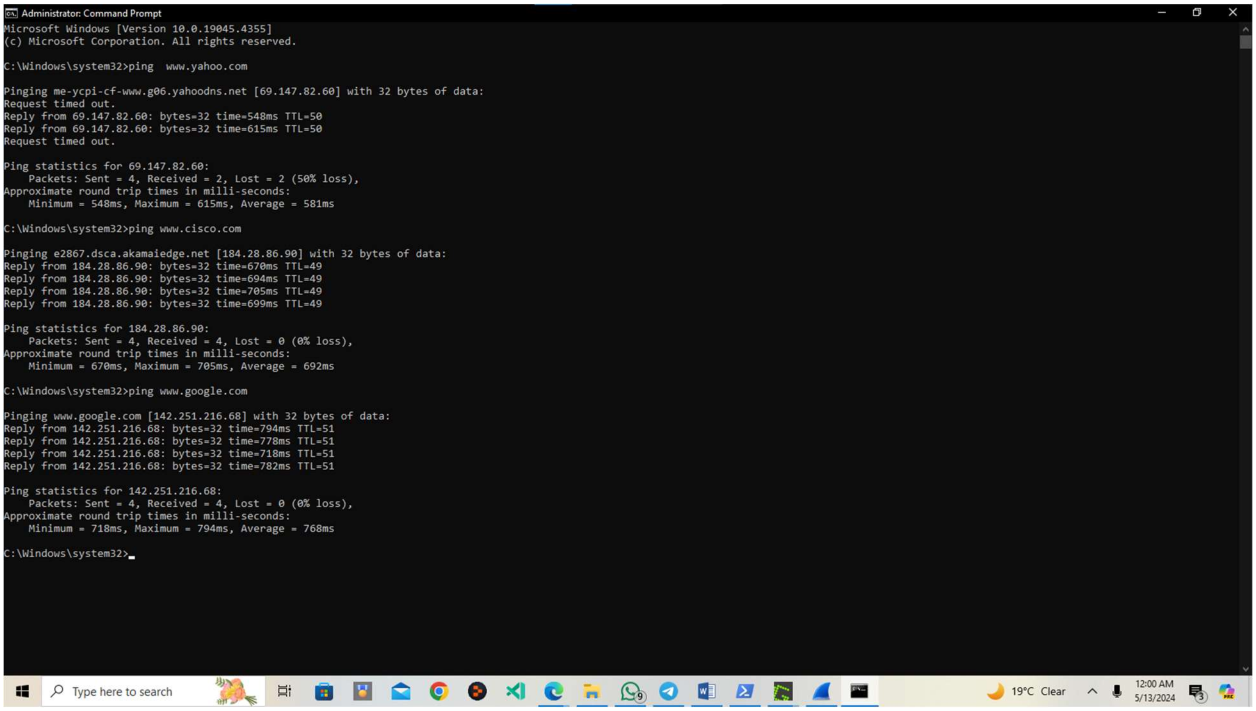
With the capture active, ping the following three website URLs from a Windows command prompt:

1) www.yahoo.com

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.



```
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping  www.yahoo.com

Pinging me-ycpi-cf-www.g06.yahoodns.net [69.147.82.60] with 32 bytes of data:
Request timed out.
Reply from 69.147.82.60: bytes=32 time=548ms TTL=50
Reply from 69.147.82.60: bytes=32 time=615ms TTL=50
Request timed out.

Ping statistics for 69.147.82.60:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 548ms, Maximum = 615ms, Average = 581ms

C:\Windows\system32>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [184.28.86.90] with 32 bytes of data:
Reply from 184.28.86.90: bytes=32 time=670ms TTL=49
Reply from 184.28.86.90: bytes=32 time=694ms TTL=49
Reply from 184.28.86.90: bytes=32 time=705ms TTL=49
Reply from 184.28.86.90: bytes=32 time=699ms TTL=49

Ping statistics for 184.28.86.90:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 670ms, Maximum = 705ms, Average = 692ms

C:\Windows\system32>ping www.google.com

Pinging www.google.com [142.251.216.68] with 32 bytes of data:
Reply from 142.251.216.68: bytes=32 time=794ms TTL=51
Reply from 142.251.216.68: bytes=32 time=778ms TTL=51
Reply from 142.251.216.68: bytes=32 time=718ms TTL=51
Reply from 142.251.216.68: bytes=32 time=782ms TTL=51

Ping statistics for 142.251.216.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 718ms, Maximum = 794ms, Average = 768ms

C:\Windows\system32>_
```

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:

50:0f:f5:89:22:18

IP address for www.cisco.com:

184.28.86.90

MAC address for www.cisco.com:

50:0f:f5:89:22:18

IP address for www.google.com:

142.251.216.68

MAC address for www.google.com:

50:0f:f5:89:22:18

What is significant about this information?

The destination MAC addresses for all those three pings is the same (default gateway MAC address)

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

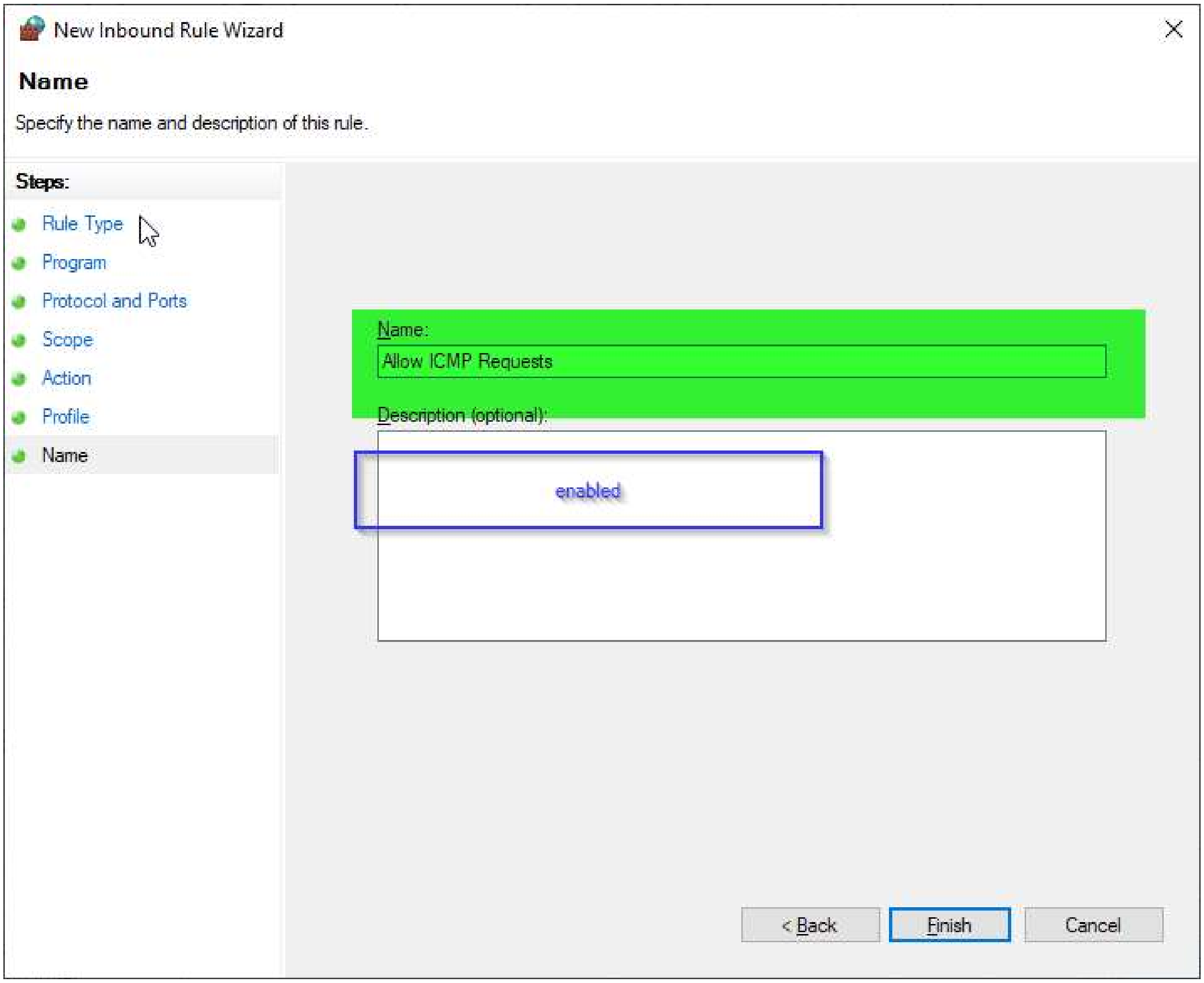
This information is differ from the local ping,in local ping the destination MAC address was the exact MAC address of the ping device compared to this part 2,which we have the MAC of the destination device as the MAC address of the default gateway.

Reflection Question

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

The Wireshark was able to reach the MAC address of the local host directly this is because they were in the same LAN network, whereas the remote hosts are on different network hence the Wireshark was able to reach the nearest routers hardware address, which was my local routers MAC address.

Part 1: Create a new inbound rule allowing ICMP traffic through the firewall.



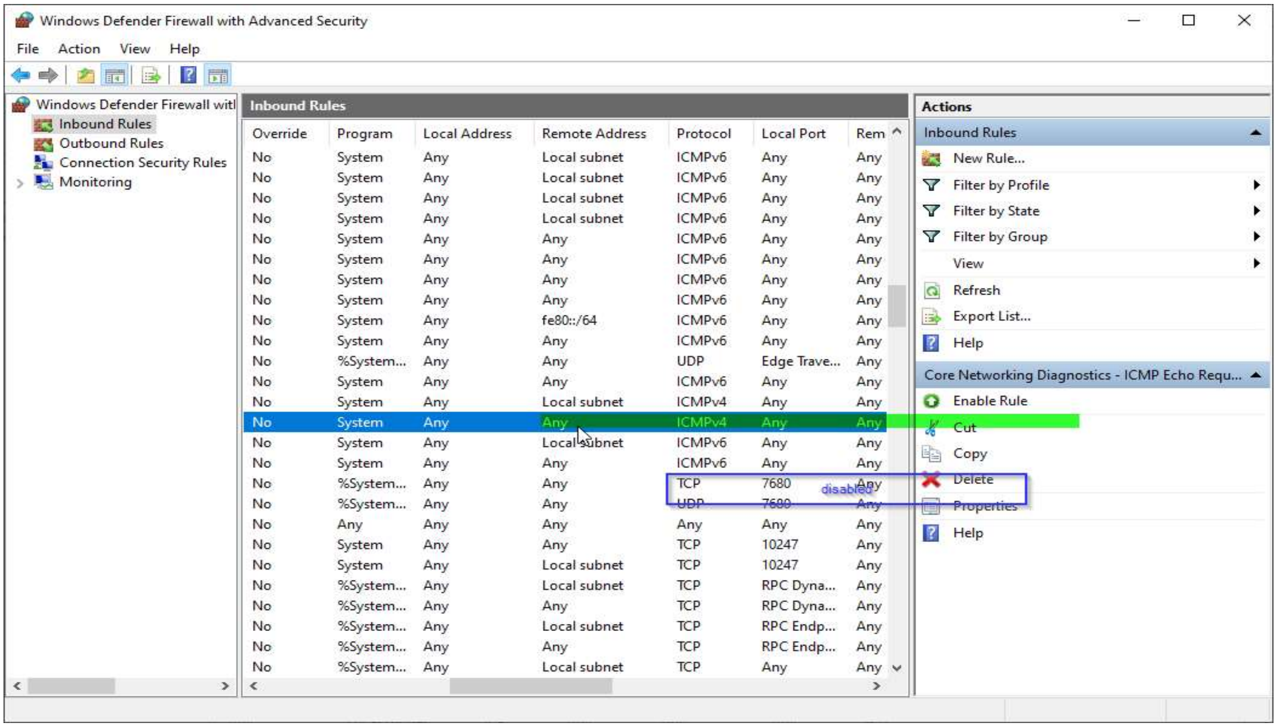
Name

Specify the name and description of this rule.

Name:
Allow ICMP Requests

Description (optional):
enabled

Part 2: Disabling or deleting the new ICMP rule.



Override	Program	Local Address	Remote Address	Protocol	Local Port	Rem
No	System	Any	Local subnet	ICMPv6	Any	Any
No	System	Any	Local subnet	ICMPv6	Any	Any
No	System	Any	Local subnet	ICMPv6	Any	Any
No	System	Any	Local subnet	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	System	Any	fe80::/64	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	%System...	Any	Any	UDP	Edge Trave...	Any
No	System	Any	Any	ICMPv6	Any	Any
No	System	Any	Local subnet	ICMPv4	Any	Any
No	System	Any	Any	ICMPv4	Any	Any
No	System	Any	Local subnet	ICMPv6	Any	Any
No	System	Any	Any	ICMPv6	Any	Any
No	%System...	Any	Any	TCP	7680	Any
No	%System...	Any	Any	~~UDP~~	~~7680~~	~~Any~~
No	Any	Any	Any	Any	Any	Any
No	System	Any	Any	TCP	10247	Any
No	System	Any	Local subnet	TCP	10247	Any
No	%System...	Any	Local subnet	TCP	RPC Dyna...	Any
No	%System...	Any	Any	TCP	RPC Dyna...	Any
No	%System...	Any	Local subnet	TCP	RPC Endp...	Any
No	%System...	Any	Any	TCP	RPC Endp...	Any
No	%System...	Any	Local subnet	TCP	Any	Any

Conclusion

The lab exercises conducted using Wireshark have significantly enhanced our understanding of network packet analysis and the critical role of ICMP in network communication. By capturing and analyzing ICMP data, both locally and remotely, we gained practical insights into the network's operational aspects, such as IP and MAC address functionalities, data encapsulation, and the importance of adhering to security protocols while using network analysis tools. These exercises not only reinforced theoretical knowledge but also provided hands-on experience in network troubleshooting and analysis. Moving forward, the skills acquired from this lab will be invaluable in furthering our expertise in network management and security, preparing us to tackle complex network issues with confidence and precision.