

# ASSIGNMENT TWO: USING WIRESHARK TO VIEW NETWORK TRAFFIC WRITEUP

## Introduction

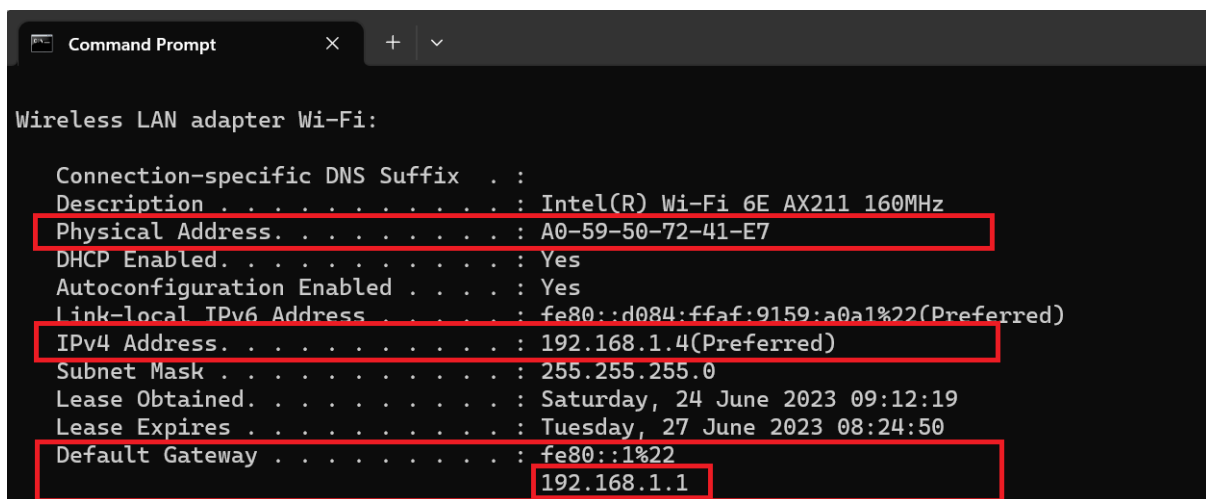
Wireshark is packet sniffer that is used for network troubleshooting, analysis, software and protocol development. This assignment is divided into two, where part one focuses on capturing and analyzing local ICMP data. By examining ICMP packets within your local network, you can gain valuable insights into network performance, identify potential bottlenecks, and troubleshoot connectivity problems within your own infrastructure while Part 2 focuses on capturing and analyzing remote ICMP data.

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

In this Part 1 of this lab, we pinged the default gateway/ router of our PC on the LAN and captured ICMP requests and replies in Wireshark. We also look inside the frames captured for specific information.

### Step 1: Retrieve your PC interface addresses.

In this step we used the ipconfig / all command on the windows command prompt to get the Ip address, mac address and the default gateway address.



```
Command Prompt

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
    Physical Address. . . . . : A0-59-50-72-41-E7
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::d084:ffaf:9159:a0a1%22(Preferred)
    IPv4 Address. . . . . : 192.168.1.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Saturday, 24 June 2023 09:12:19
    Lease Expires . . . . . : Tuesday, 27 June 2023 08:24:50
    Default Gateway . . . . . : fe80::1%22
                                192.168.1.1
```

### Step 2: Start Wireshark and begin capturing data.

In this step we navigated to Wireshark. Double-click the WIFI and filtered to ICMP since we are only interested in displaying ICMP (ping) PDUs in this lab. We then pinged the IP address of the default gateway on the command prompt window.

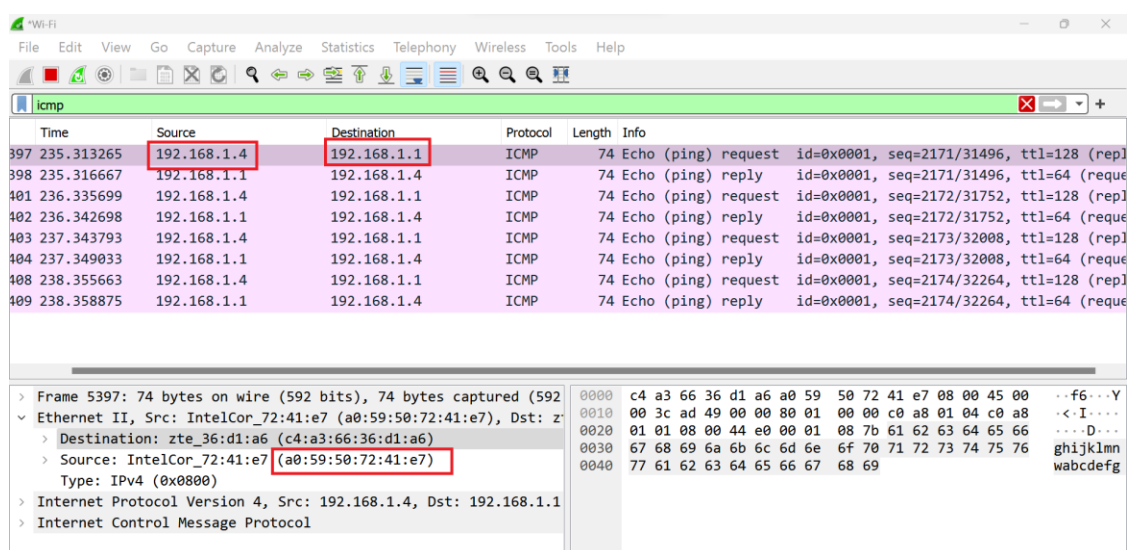
```
C:\Users\Isabe>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 4ms
```

Step 3: Examine the captured data.

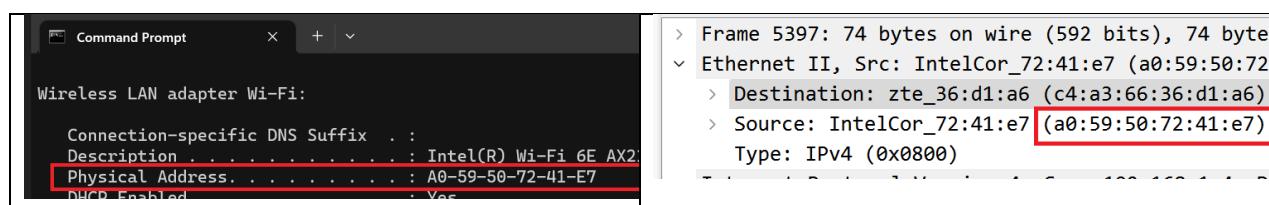
In Step 3, we examined the data that was generated by the ping requests.



Questions:

Does the source MAC address match your PC interface?

Yes, it does as displayed in figure 1 and figure 3.



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

In this case I used the router and Yes it does match.

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

This is done by ARP request.

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

In Part 2, we pinged remote hosts (hosts not on the LAN) and examine the generated data from those pings.

### Step 1: Start capturing data on the interface.

In this step, we pinged the following three website URLs from a Windows command prompt:

- 1) www.yahoo.com
- 2) www.cisco.com
- 3) www.google.com

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

In this step, we reviewed the captured data in Wireshark and examine the IP and MAC addresses of the three locations that was pinged. List the destination IP and MAC addresses for all three locations in the space provided.

Questions:

IP address for www.yahoo.com:

87.248.100.216

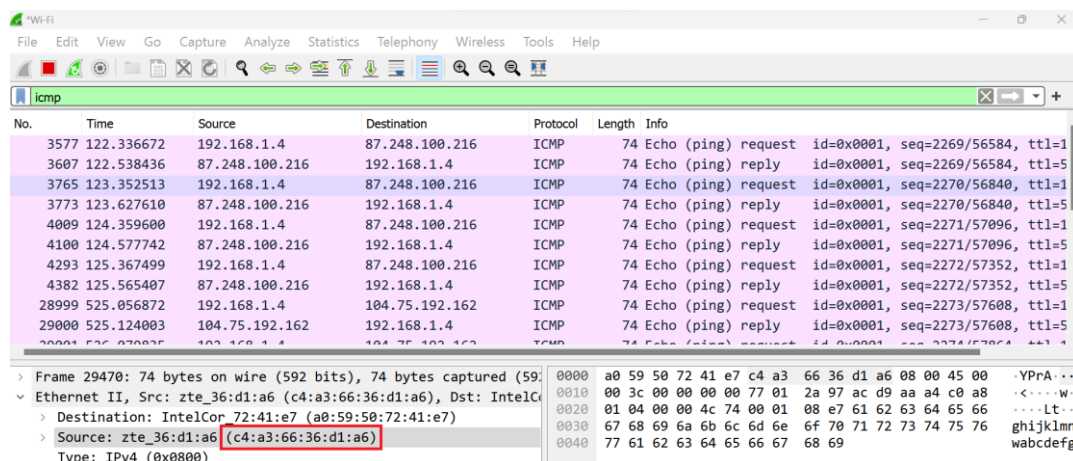
```
Command Prompt

C:\Users\Isabe>ping www.yahoo.com

Pinging new-fp-shed.wg1.b.yahoo.com [87.248.100.216] with 32 bytes of data:
Reply from 87.248.100.216: bytes=32 time=202ms TTL=53
Reply from 87.248.100.216: bytes=32 time=275ms TTL=53
Reply from 87.248.100.216: bytes=32 time=218ms TTL=53
```

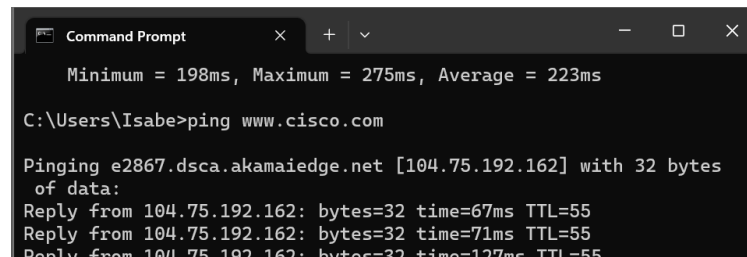
MAC address for www.yahoo.com:

C4-A3-66-36-D1-A6 (default gateway/router)



IP address for www.cisco.com:

104.75.192.162



```
Command Prompt
Minimum = 198ms, Maximum = 275ms, Average = 223ms

C:\Users\Isabe>ping www.cisco.com

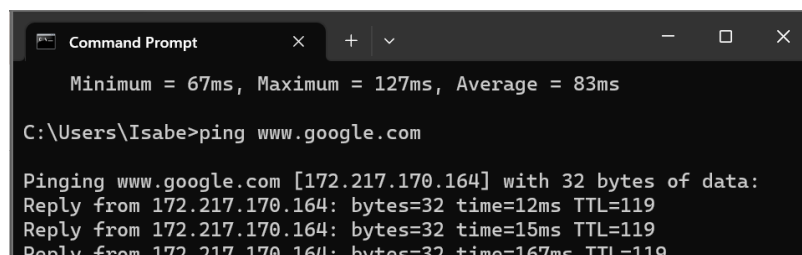
Pinging e2867.dsca.akamaiedge.net [104.75.192.162] with 32 bytes
of data:
Reply from 104.75.192.162: bytes=32 time=67ms TTL=55
Reply from 104.75.192.162: bytes=32 time=71ms TTL=55
Reply from 104.75.192.162: bytes=32 time=127ms TTL=55
```

MAC address for www.cisco.com:

C4-A3-66-36-D1-A6

IP address for www.google.com:

172.217.170.164



```
Command Prompt
Minimum = 67ms, Maximum = 127ms, Average = 83ms

C:\Users\Isabe>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=12ms TTL=119
Reply from 172.217.170.164: bytes=32 time=15ms TTL=119
Reply from 172.217.170.164: bytes=32 time=167ms TTL=119
```

MAC address for www.google.com:

C4-A3-66-36-D1-A6

What is significant about this information?

The MAC addresses for all these three locations are the same and they point to our default gateway.

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

We one pings locally it going to return the mac address of the pc network interface card but when one pings a remote host it only returns the mac address of the default gateway or LAN interface.

Reflection Question

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

Mac addresses for the remote hosts are not known on the LAN hence the default-gateway is used. After the packet reaches the default gateway router the layer 2 information is stripped off because maybe of privacy and security issues. I think this is a way to prevent hacking or the ease of it.

## Conclusion

In conclusion, Wireshark proves to be an invaluable tool for capturing and analyzing network traffic, specifically ICMP data. I gained a lot of insight on network analysis and got a deeper understanding of packet information and transfer differences between local and remote networks.