



USE WIRESHARK TO VIEW NETWORK TRAFFIC REPORT



YUNIS MOHAMED

Contents

Introduction	2
Use Wireshark to View Network Traffic	2
Part 1: Capture and Analyze Local ICMP Data in Wireshark	2
Step 1: Retrieve your PC interface addresses	2
Step 2: Start Wireshark and begin capturing data.	3
Step 3: Examine the captured data.....	4
Part 2: Capture and Analyze Remote ICMP Data in Wireshark	5
Step 1: Start capturing data on the interface.....	5
Step 2: Examining and analyzing the data from the remote hosts.....	6
Question	8
Reflection Question	8
Conclusion.....	8

Introduction

In this lab I will be viewing and examining network traffic using Wireshark software. Requirements for this lab include; a PC with internet access, an additional PC on the LAN. I will also be capturing packets from both local and remote addresses. Sites such as www.google.com, www.cisco.com will be used as remote addresses. This report will explore the significant observations, findings, and reflections obtained from the analysis conducted using Wireshark. Emphasis will be placed on the crucial role that protocols play in facilitating seamless communication.

Use Wireshark to View Network Traffic

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Step 1: Retrieve your PC interface addresses

- In a command prompt window, enter `ipconfig /all`, to the IP address of your PC interface, its description, and its MAC (physical) address.

Description: Qualcomm Atheros AR9485WB-EG wireless Network Adapter.

Mac address: 50-B7-C3-ee-34-BC

IPv4 Address: 192.168.43.161

C:\Users\Student> ipconfig /all

```
Administrator: Command Prompt

ipconfig /all

Windows IP Configuration

Ethernet adapter {F80B16977C809CFFA312E13E} (Preferred):
    . . . . .
    Description . . . . . : Qualcomm Atheros AR9485WB-EG Wireless Network Adapter
    Physical Address. . . . . : 50-B7-C3-EE-34-BC
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80:16977:c09c:ffa312e13e (Preferred)
    IPv4 Address. . . . . : 192.168.43.161 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : 23 June 2023 15:58:20
    Lease Expires . . . . . : 23 June 2023 17:58:00
    Default Gateway . . . . . : 192.168.43.1
    DHCP Server . . . . . : 192.168.43.1
    DHCPv6 IAID . . . . . : 357611459
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-C1-90-98-50-07-C3-91-38-08
    DNS Servers . . . . . : 192.168.43.1
    NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter {FA67B417-7575-484C-B596-7F0AE6158F76}:
    . . . . .
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft ISATAP Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

Tunnel adapter Local Area Connection* 11:
    . . . . .
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft Teredo Tunneling Adapter
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::138ff:f94e:d6ae:4cd9 (Preferred)
    IPv6 Address. . . . . : 2001:0:2551:702c:138ff:f94e:d6ae:4cd9 (Preferred)
    Default Gateway . . . . . : ::
    DHCPv6 IAID . . . . . : 482653184
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1F-C1-90-98-50-07-C3-91-38-08
    NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter {59953E06-966C-4F72-9722-7D4FD65E081E}:
    . . . . .
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 
    Description . . . . . : Microsoft ISATAP Adapter #2
    Physical Address. . . . . : 00-00-00-00-00-00-E0
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . . : Yes

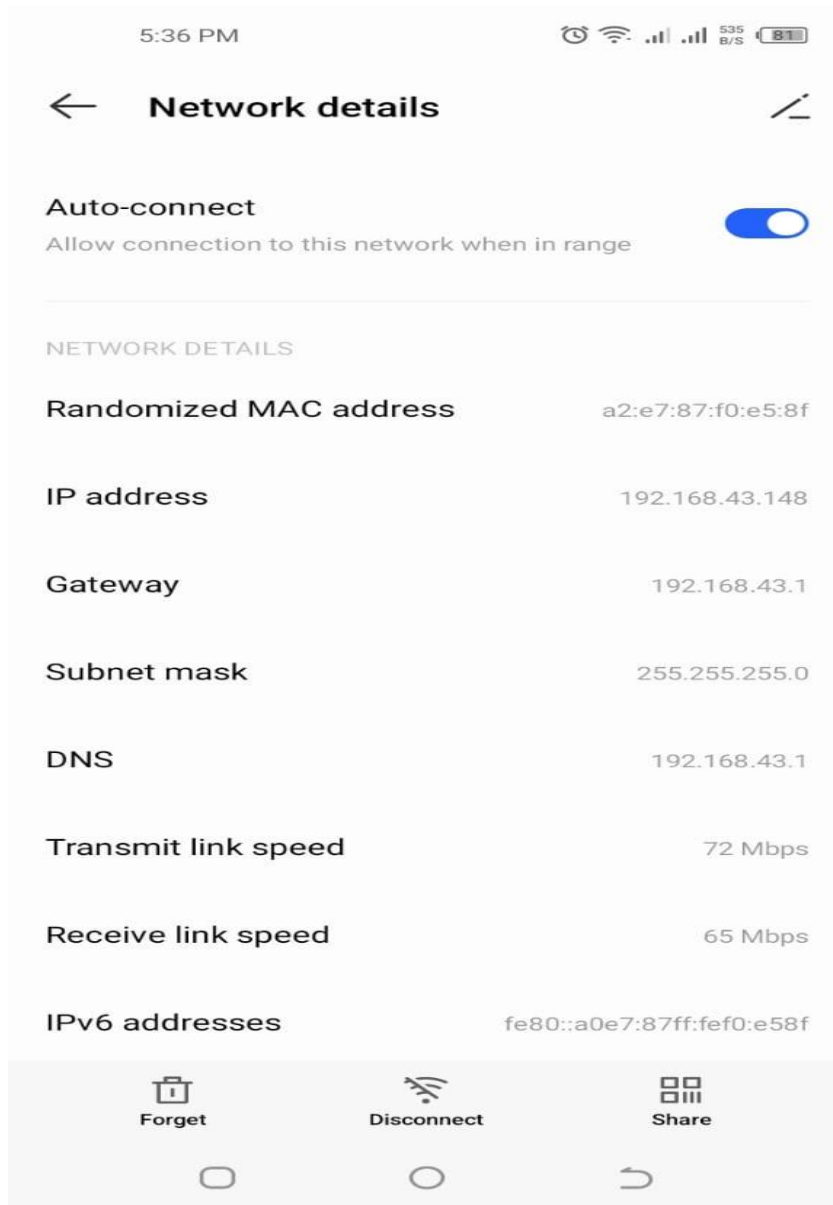
C:\WINDOWS\system32_
```

Figure 1 mypc information

- b) 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.

IPv4 address: 192.168.43.148

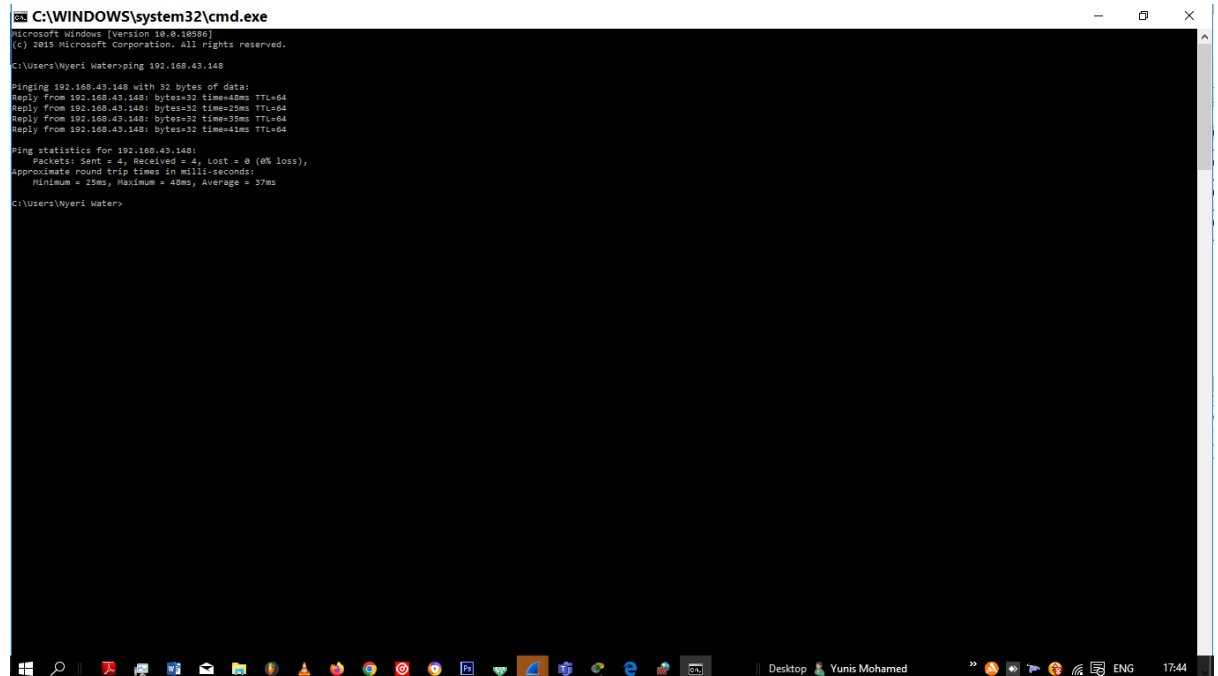
MAC ADDRESS: a2:e7:87:f0:e5:8f



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) 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. 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 192.168.43.148



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.16099]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Myeri Water>ping 192.168.43.148

Pinging 192.168.43.148 with 32 bytes of data:
Reply from 192.168.43.148: bytes=32 time=48ms TTL=64
Reply from 192.168.43.148: bytes=32 time=25ms TTL=64
Reply from 192.168.43.148: bytes=32 time=35ms TTL=64
Reply from 192.168.43.148: bytes=32 time=48ms TTL=64

Ping statistics for 192.168.43.148:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 48ms, Average = 37ms

C:\Users\Myeri Water>
```

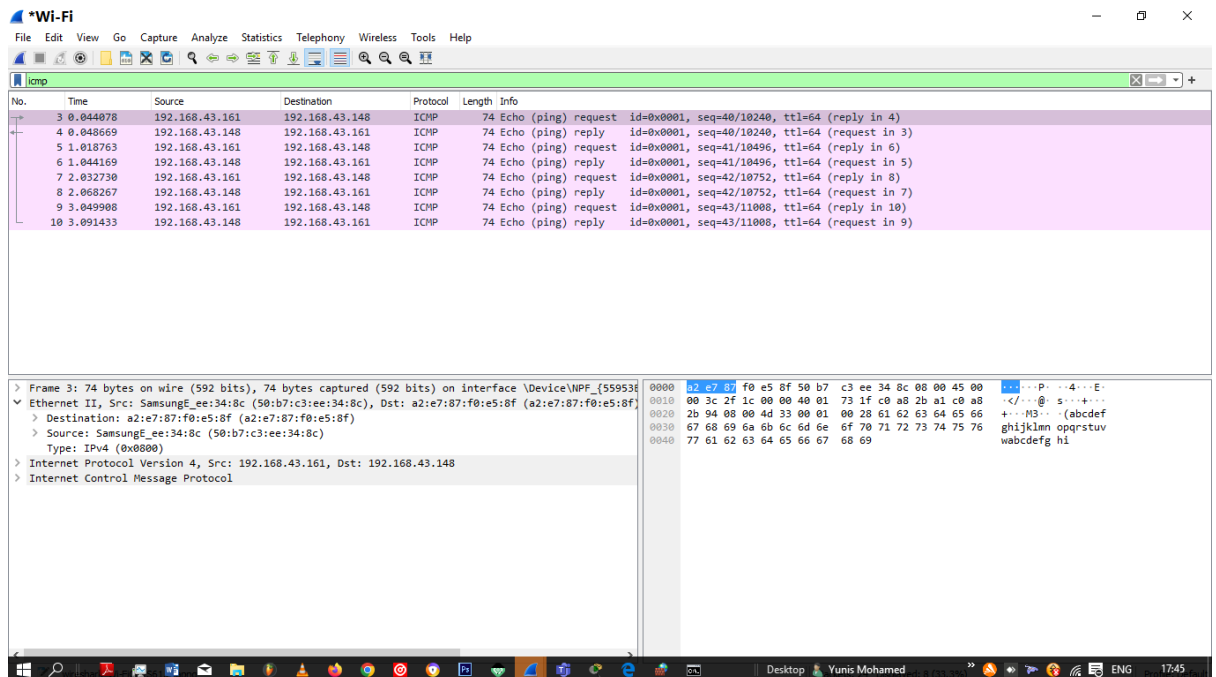
c) Notice that you start seeing data appear in the top window of Wireshark again.

Step 3: Examine the captured data

In Step 3, examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections:

- 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed;
- 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers; and
- 3) The bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.
 - 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.
 - b) 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.
 - i. Does the source MAC address match your PC interface? **Yes it is 50-B7-C3-ee-34-BC**

- ii. Does the destination MAC address in Wireshark match your team member MAC address? Yes it is **a2:e7:87:f0:e5:8f**
- iii. How is the MAC address of the pinged PC obtained by your PC?
The MAC address is obtained by my pc via the ARP request sent by the PC.



Part 2: Capture and Analyze Remote ICMP Data in Wireshark

In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

Step 1: Start capturing data on the interface.

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

- 1) www.yahoo.com

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Nyeri Water>ping ww.yahoo.com

Pinging 212.82.100.150 [212.82.100.150] with 32 bytes of data:
Reply from 212.82.100.150: bytes=32 time=210ms TTL=45
Reply from 212.82.100.150: bytes=32 time=278ms TTL=45
Reply from 212.82.100.150: bytes=32 time=232ms TTL=45
Reply from 212.82.100.150: bytes=32 time=176ms TTL=45

Ping statistics for 212.82.100.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 176ms, Maximum = 278ms, Average = 224ms

C:\Users\Nyeri Water>
```

- 2) www.cisco.com

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Myerl Water>ping www.yahoo.com

Pinging www.yahoo.com [212.82.100.150] with 32 bytes of data:
Reply from 212.82.100.150: bytes=32 time=26ms TTL=52
Reply from 212.82.100.150: bytes=32 time=26ms TTL=52
Reply from 212.82.100.150: bytes=32 time=26ms TTL=52
Reply from 212.82.100.150: bytes=32 time=26ms TTL=52

Ping statistics for 212.82.100.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 26ms, Maximum = 26ms, Average = 26ms
C:\Users\Myerl Water>
```

3) www.google.com

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.18362]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Myerl Water>ping www.google.com

Pinging www.google.com [216.58.223.100] with 32 bytes of data:
Reply from 216.58.223.100: bytes=32 time=26ms TTL=52
Reply from 216.58.223.100: bytes=32 time=26ms TTL=52
Reply from 216.58.223.100: bytes=32 time=55ms TTL=52
Reply from 216.58.223.100: bytes=32 time=26ms TTL=52

Ping statistics for 216.58.223.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 26ms, Maximum = 55ms, Average = 33ms
C:\Users\Myerl Water>
```

Figure 2 www.google.com

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

a) IP address for www.yahoo.com :212.82.100.150

The image shows a Wireshark packet capture of an ICMP Echo (ping) request and reply. The packet list on the left shows a single packet (No. 1) of type ICMP Echo (ping) request, 74 bytes in length, sent from 192.168.43.161 to 212.82.100.150. The packet details pane on the right shows the following structure:

- Frame 49: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF... (5505)
- Ethernet II, Src: SamsungE_ee:34:8c (50:b7:c3:ee:34:8c), Dst: 5a:db:15:f8:2d:fb (5a:db:15:f8:2d:fb)
- Destination: 5a:db:15:f8:2d:fb (5a:db:15:f8:2d:fb)
- Source: SamsungE_ee:34:8c (50:b7:c3:ee:34:8c)
- Type: IPv4 (0x0000)
- Internet Protocol Version 4, Src: 192.168.43.161, Dst: 212.82.100.150
- Internet Control Message Protocol

The packet bytes pane on the right shows the raw data of the packet, including the Ethernet II header, the IPv4 header, and the ICMP Echo (ping) request data.

Figure 3 www.yahoo.com

- b) IP address for www.cisco.com: 23:61:92:55
- c) MAC address for www.cisco.com : 5a: db: 15: f8: 2d: fb

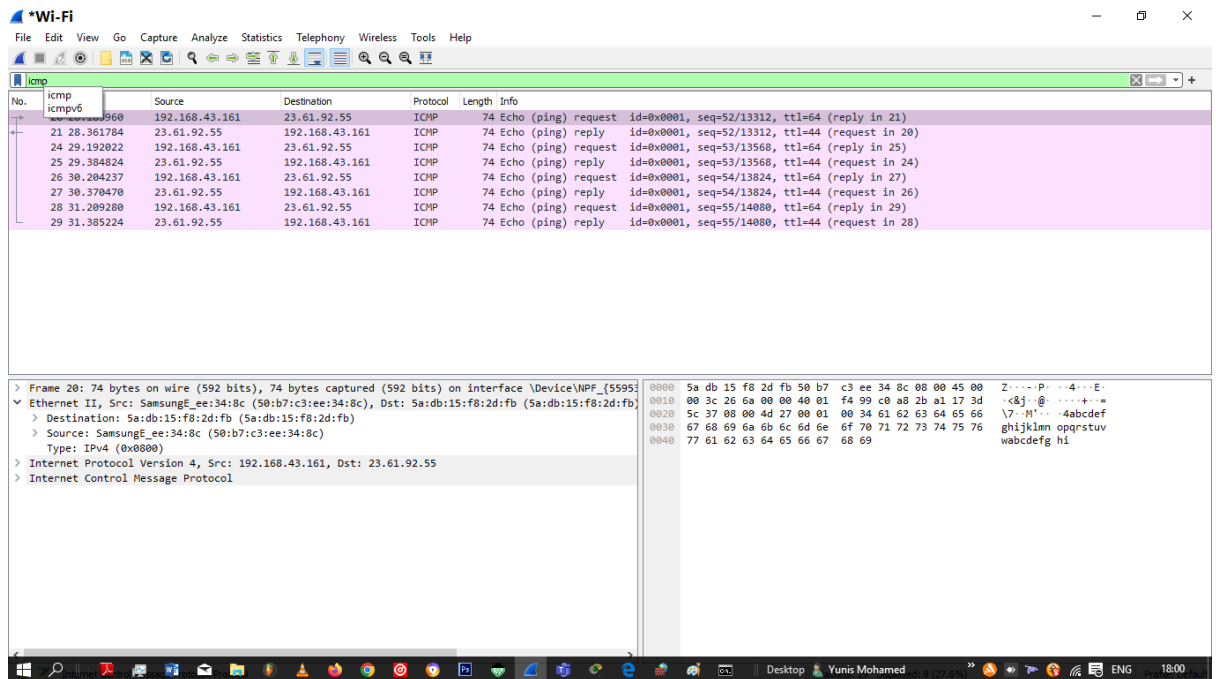


Figure 4 www.cisco.com

- d) IP address for www.google.com : 216:58:223:100
- e) MAC address for www.google.com: 5a: db: 15: f8: 2d: fb

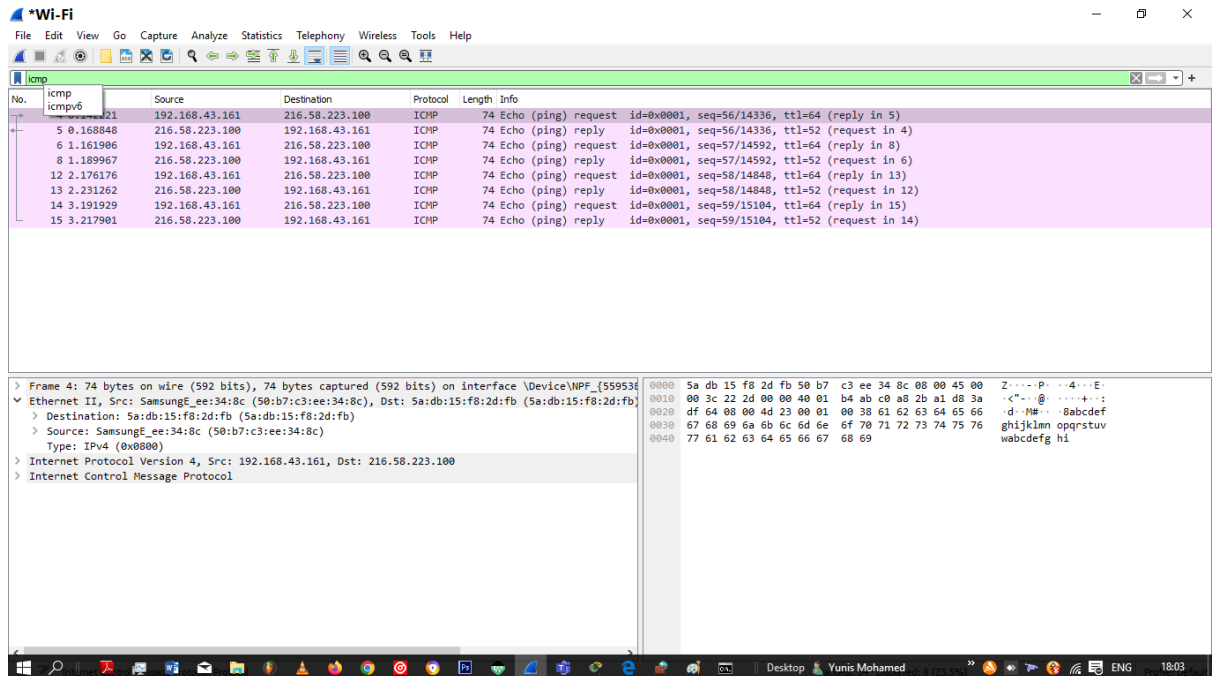


Figure 5 www.google.com

Question

What is significant about this information?

The IP addresses of the three sites are different while the MAC address for the three sites is the same. This is because the sites are using the physical LAN address which is the MAC Address of the router.

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

A ping to a local host returns the MAC address of the PC NIC while a ping to a remote host returns MAC address of the default gateway of the 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?

The MAC address of the local host are on the same LAN, hence can be shown easily. The remote host's addresses are not known on the local area so the MAC address of the default Gateway is used.

Conclusion

The utilization of Wireshark for viewing network traffic in Packet Tracer has proven to be an enlightening and informative journey. By carefully analyzing the captured packets, I have acquired valuable insights into the intricate mechanics of network communication and the associated protocols. Wireshark's packet analysis capabilities provided a deeper understanding of various network protocols such as TCP, UDP, and ICMP. By examining the packet headers, I could observe the source and destination IP addresses, port numbers, and protocol-specific information. This allowed me to identify the different types of traffic and analyse their behaviour, helping me troubleshoot network issues and optimize performance. In conclusion, the utilization of Wireshark alongside Packet Tracer has provided me with a profound perspective on network communication. This experience has not only broadened my knowledge but also equipped me with the necessary tools to proficiently monitor and analyse network traffic.

.