

COURSE

**Cloud and Network Security- C3 – 2025**

**Week one assignment.**

Student Details:

**Name:**

**Godfrey Otieno Odhiambo**

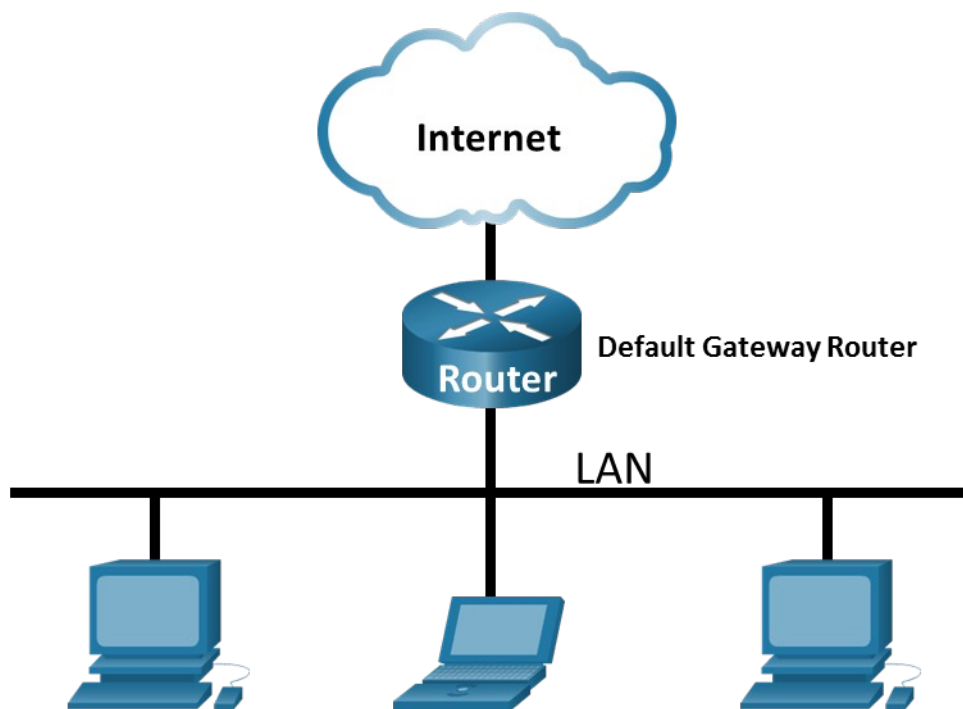
**ID:**

**cs-cns10-25107**

Submission Date:

**September 23<sup>rd</sup> 2025.**

## Topology



## Objectives

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

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

## Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

## Required Resources

- 1 PC (Windows with internet access)
- Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

Using a packet sniffer such as Wireshark may be considered a breach of the security policy of the school. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

## 1 Instructions

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

In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

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

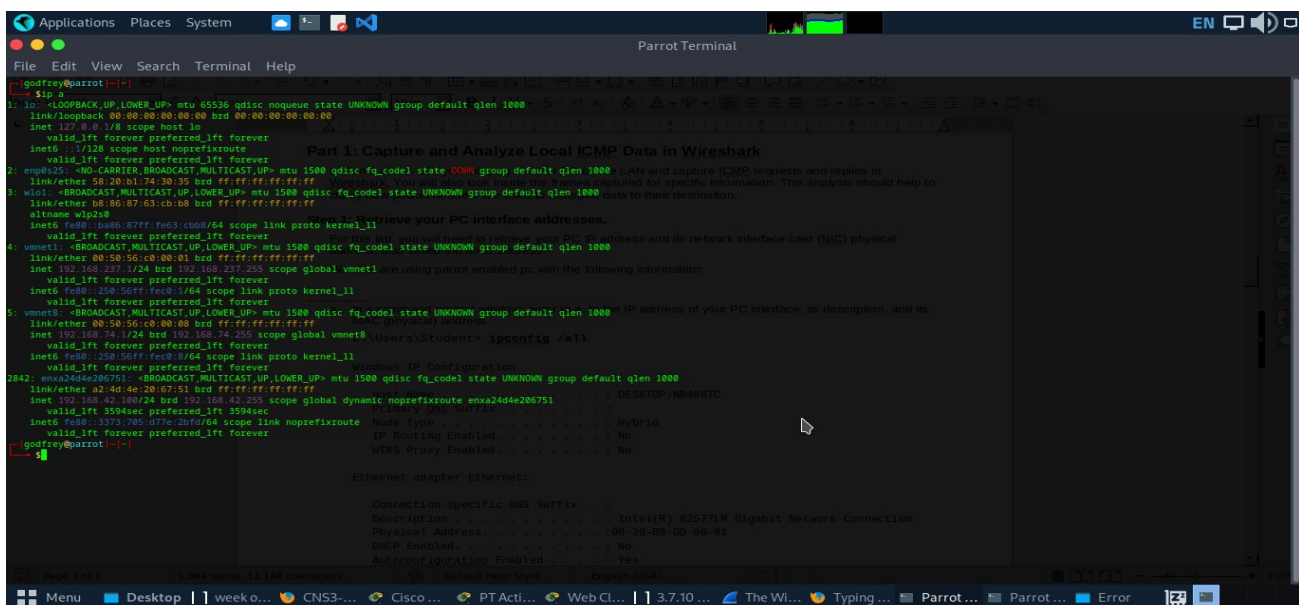
For this lab, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

Here we are using parrot enabled pc with the following information:

as displayed the Ip address is 198.162.42.173 IPv6 8e:f3:c1:dc:34:fd

Open a Windows command prompt.

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



```

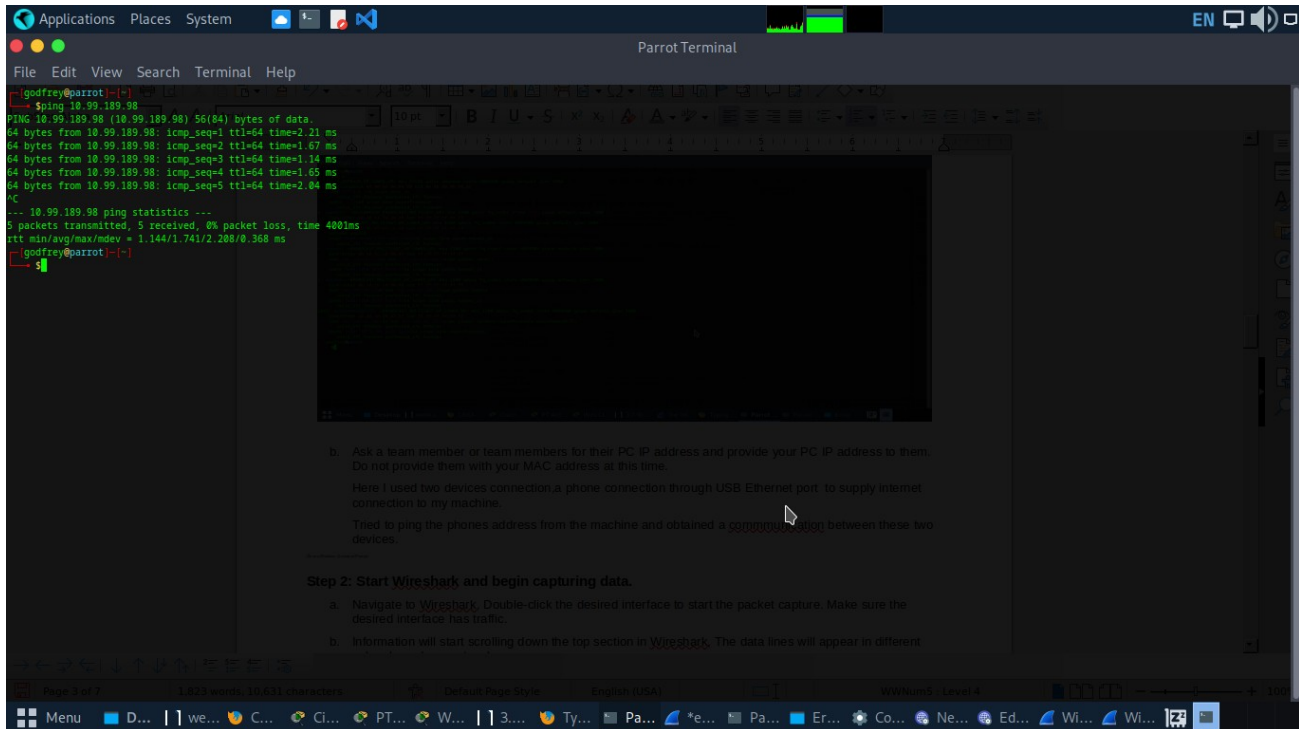
godfrey@parrot:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: empx2: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 56:20:b1:74:30:35 brd ff:ff:ff:ff:ff:ff
3: vnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.237.1/24 brd 192.168.237.255 scope global vnet1
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe00:1/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
4: vnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:50:56:c0:00:08 brd ff:ff:ff:ff:ff:ff
    inet 192.168.74.1/24 brd 192.168.74.255 scope global vnet8
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe00:8/64 scope link proto kernel ll
        valid_lft forever preferred_lft forever
5: vnet9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether a2:4d:4e:20:67:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.42.100/24 brd 192.168.42.255 scope global dynamic noprefixroute enxa24d4e206751
        valid_lft 3594sec preferred_lft 3594sec
    inet6 fe80::3373:705:07fa:20f0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
godfrey@parrot:~$
  
```

- 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.

Here I used two devices, a phone connection through USB Ethernet port to supply internet connection to my machine.

Tried to ping the phone's address from the machine and obtained a communication between these two devices.

## Lab - Use Wireshark to View Network Traffic

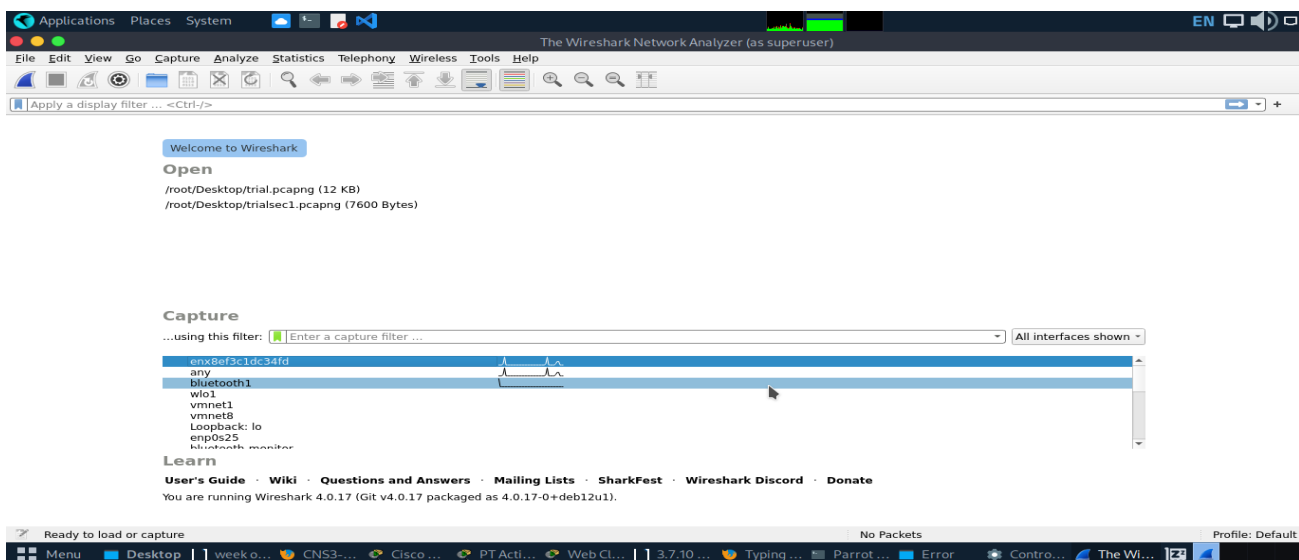


Close a Windows Command Prompt.

### 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.

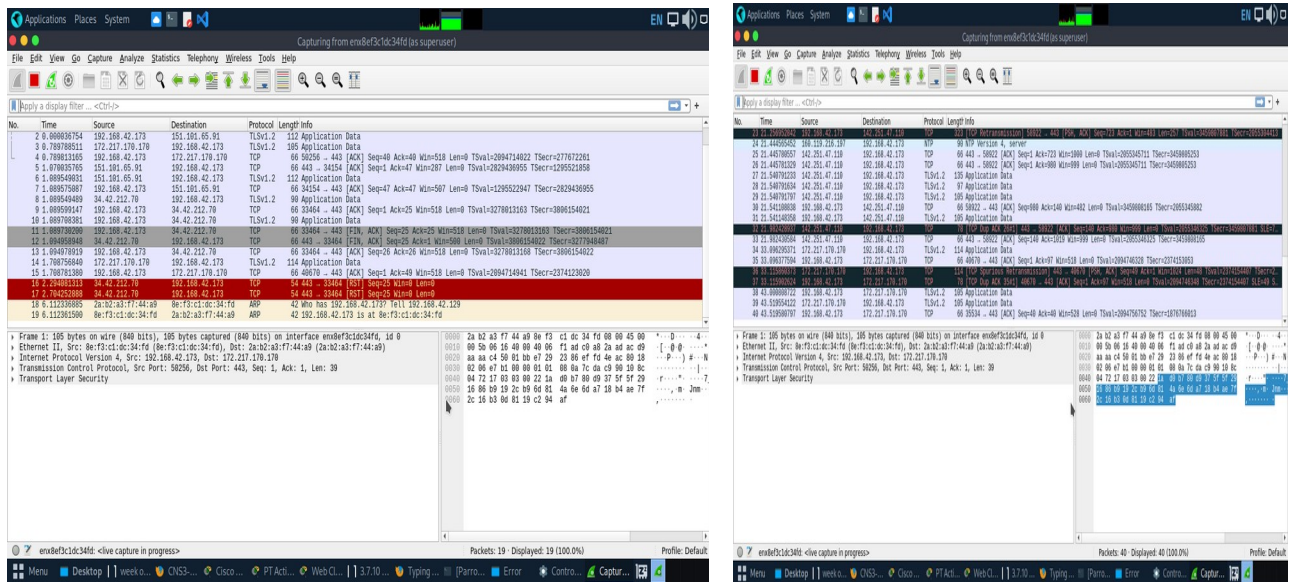
Here we will start the wireshark tool and pick the **enx8ef3c1dc34fd** interface connection for our activity.



## Lab - Use Wireshark to View Network Traffic

- b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

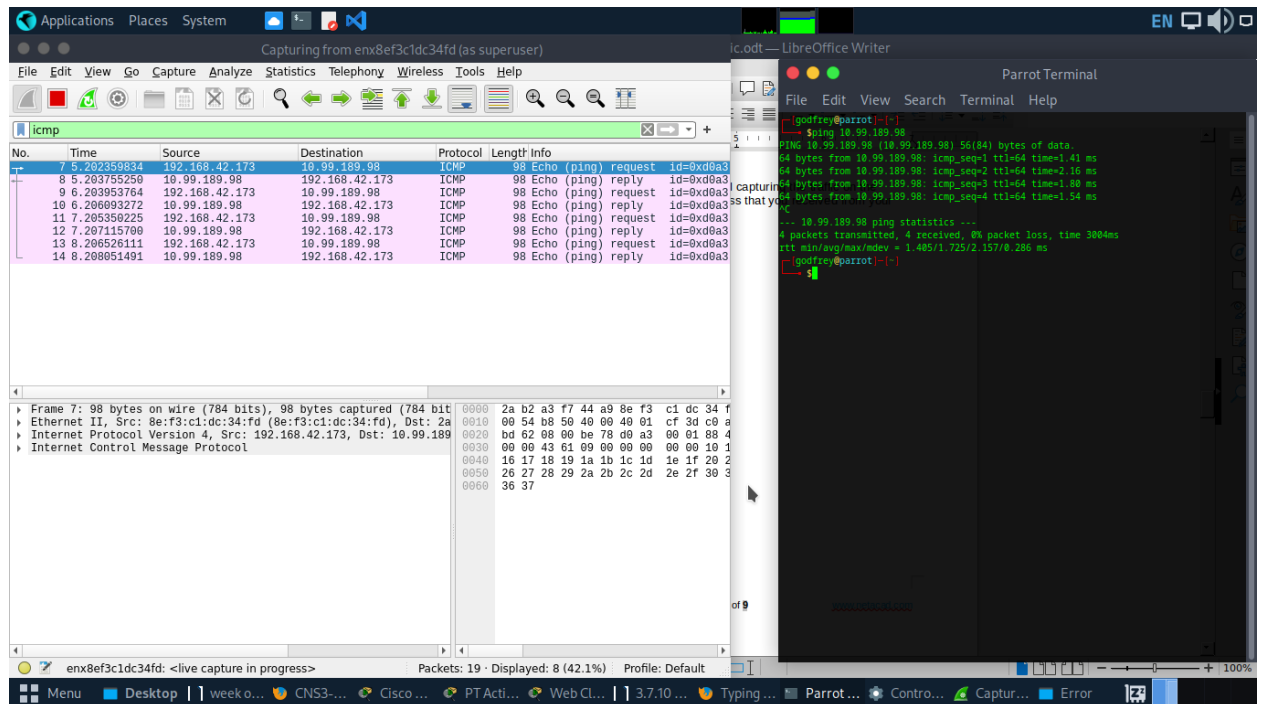
This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark.



Communication capture between the phone and the PC through the USB tethered connection.

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 (In our case we will use the phones IP address).

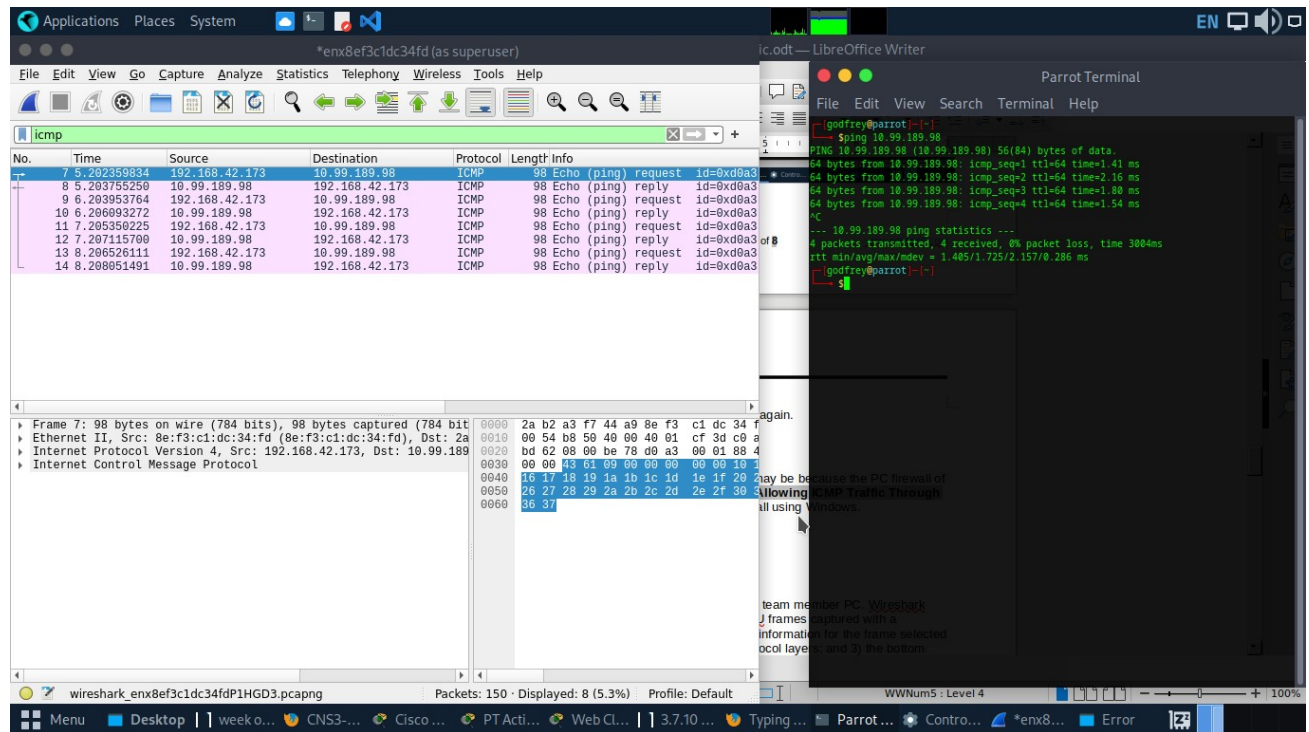


Notice that you start seeing data appear in the top window of Wireshark again.

**Note:** If the PC of your team member does not reply to your pings, this may be because the PC firewall of the team member is blocking these requests. Please see **Appendix A: Allowing ICMP Traffic Through a Firewall** for information on how to allow ICMP traffic through the firewall using Windows.

- d. Stop capturing data by clicking the **Stop Capture** icon.



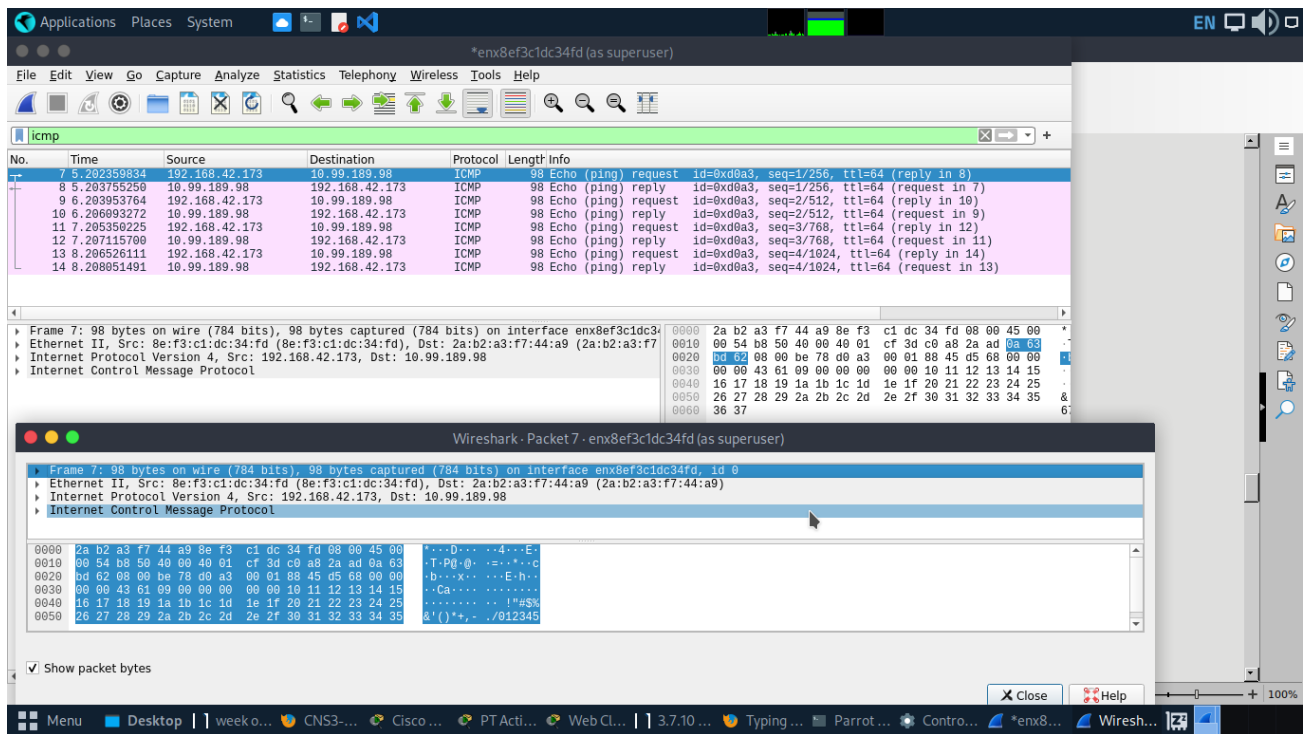


### Step 3: Examine the captured data.

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.

- 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.

## Lab - Use Wireshark to View Network Traffic



- 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.

Questions:

Does the source MAC address match your PC interface?

Yes

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

Yes

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

*The MAC address is obtained through an ARP request*

**Note:** In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

## 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.

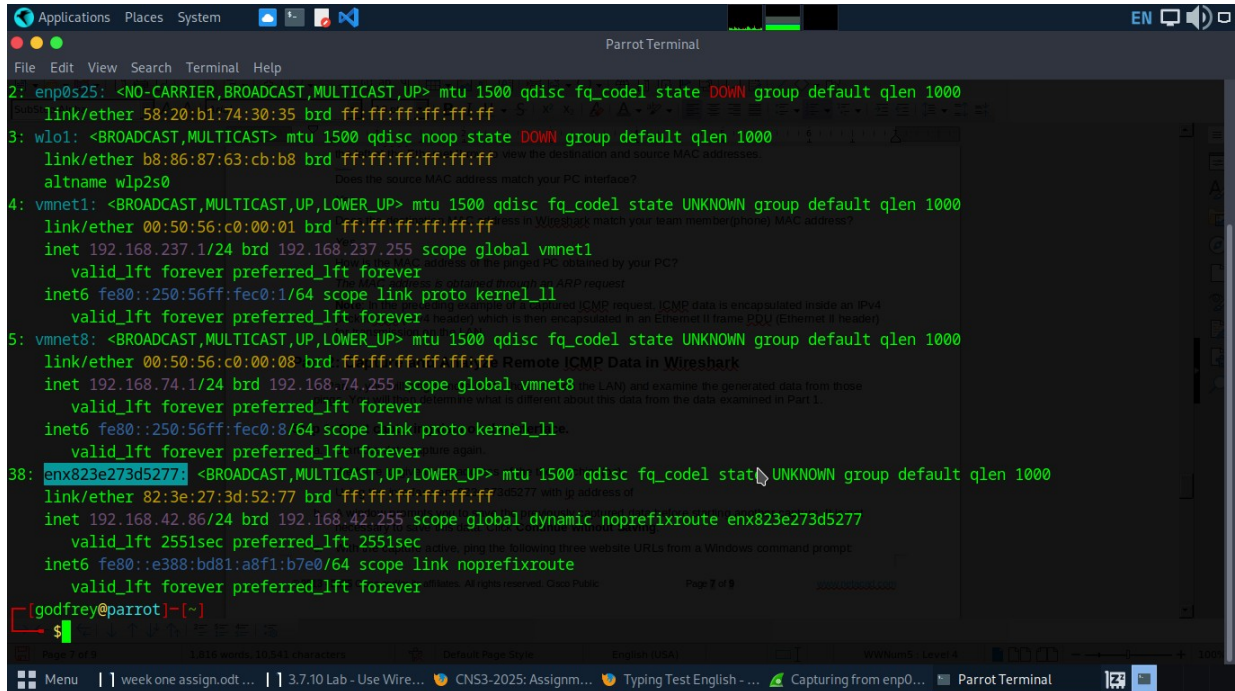


### Step 1: Start capturing data on the interface.

- Start the data capture again.

We have to give the ip address of the the machine(pc).

Using the interface enx823e273d5277 with ip address of 192.168.42.86



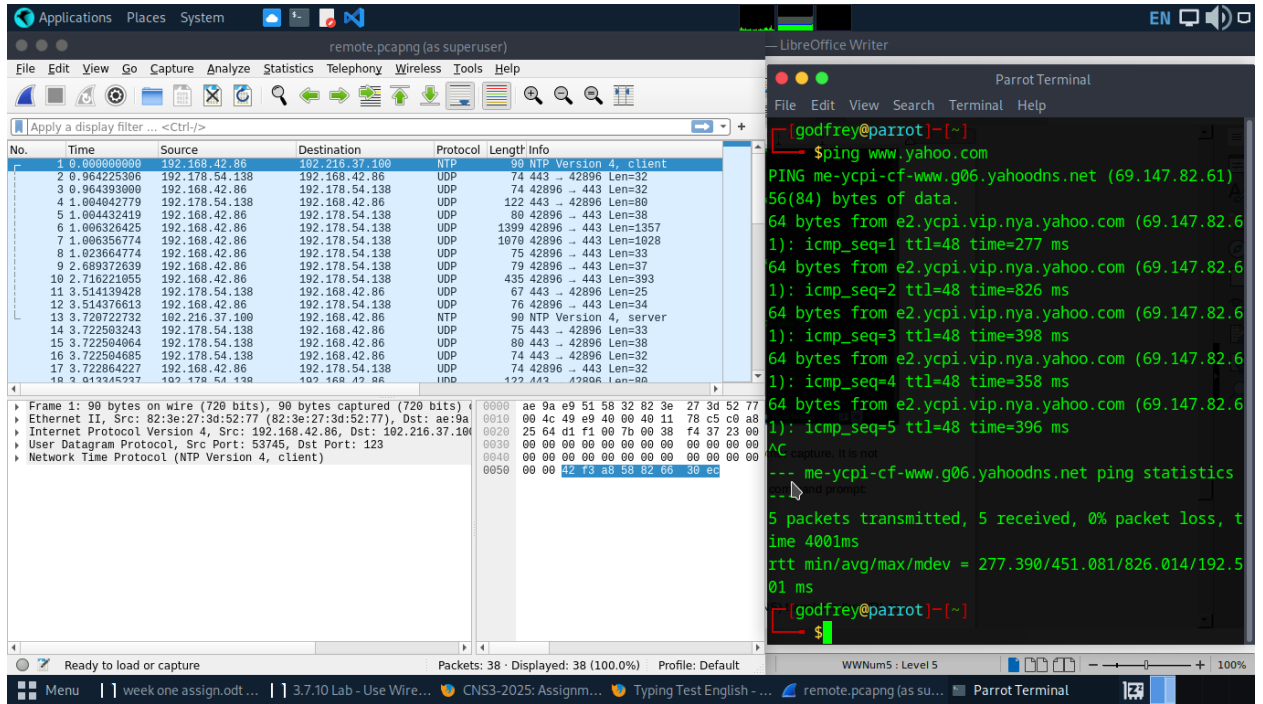
```
2: enp0s25: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
   link/ether 58:20:b1:74:30:35 brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
   link/ether b8:86:87:63:cb:b8 brd ff:ff:ff:ff:ff:ff
   altname wlp2s0
4: vmnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
   link/ether 00:50:56:c0:00:01 brd ff:ff:ff:ff:ff:ff
   inet 192.168.237.1/24 brd 192.168.237.255 scope global vmnet1
     valid_lft forever preferred_lft forever
   inet6 fe80::250:56ff:fec0:1/64 scope link proto kernel llmnr
     valid_lft forever preferred_lft forever
5: vmnet8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
   link/ether 00:50:56:c0:00:08 brd ff:ff:ff:ff:ff:ff
   inet 192.168.74.1/24 brd 192.168.74.255 scope global vmnet8
     valid_lft forever preferred_lft forever
   inet6 fe80::250:56ff:fec0:8/64 scope link proto kernel llmnr
     valid_lft forever preferred_lft forever
38: enx823e273d5277: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
   link/ether 82:3e:27:3d:52:77 brd ff:ff:ff:ff:ff:ff
   inet 192.168.42.86/24 brd 192.168.42.255 scope global dynamic noprefixroute enx823e273d5277
     valid_lft 2551sec preferred_lft 2551sec
   inet6 fe80::e388:bd81:a8f1:b7e0/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
```

- A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.
- With the capture active, ping the following three website URLs from a Windows command prompt:

Open a Windows command prompt

- [www.yahoo.com](http://www.yahoo.com)

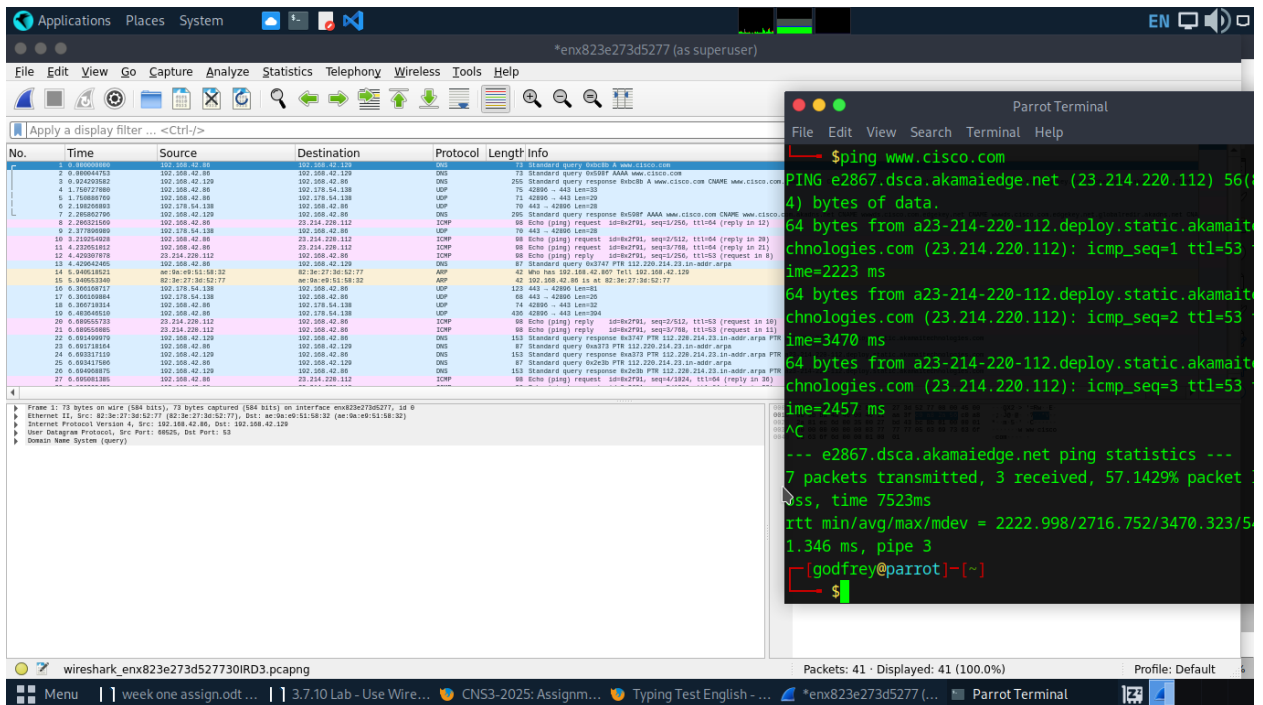
## Lab - Use Wireshark to View Network Traffic



The screenshot shows Wireshark capturing network traffic on the interface 'remote.pcapng (as superuser)'. The packet list displays 19 packets, including ICMP Echo (ping) requests and responses from 192.168.42.86 to 192.178.54.138. The packet details pane shows the selected packet (No. 19) as an ICMP Echo (ping) request. The packet bytes pane shows the raw data. A Parrot Terminal window is open in the foreground, showing the command 'ping www.yahoo.com' and its output, which includes the IP address 69.147.82.61 and various statistics.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.42.86	192.216.37.100	NTP	90	NTP Version 4, client
2	0.064225	192.178.54.138	192.168.42.86	UDP	74	42896 -> 443 Len=32
3	0.064393	192.168.42.86	192.178.54.138	UDP	74	42896 -> 443 Len=32
4	1.004042	192.178.54.138	192.168.42.86	UDP	122	443 -> 42896 Len=80
5	1.004324	192.168.42.86	192.178.54.138	UDP	80	42896 -> 443 Len=38
6	1.006326	192.168.42.86	192.178.54.138	UDP	1399	42896 -> 443 Len=1357
7	1.006356	192.168.42.86	192.178.54.138	UDP	1070	42896 -> 443 Len=1028
8	1.023664	192.168.42.86	192.178.54.138	UDP	75	42896 -> 443 Len=33
9	2.689372	192.168.42.86	192.178.54.138	UDP	79	42896 -> 443 Len=37
10	2.716221	192.168.42.86	192.178.54.138	UDP	435	42896 -> 443 Len=393
11	3.514139	192.178.54.138	192.168.42.86	UDP	67	443 -> 42896 Len=25
12	3.514376	192.168.42.86	192.178.54.138	UDP	76	42896 -> 443 Len=34
13	3.720722	192.216.37.100	192.168.42.86	NTP	90	NTP Version 4, server
14	3.722503	192.178.54.138	192.168.42.86	UDP	75	443 -> 42896 Len=33
15	3.722504	192.178.54.138	192.168.42.86	UDP	80	443 -> 42896 Len=38
16	3.722504	192.178.54.138	192.168.42.86	UDP	74	443 -> 42896 Len=32
17	3.722864	192.168.42.86	192.178.54.138	UDP	74	42896 -> 443 Len=32
18	3.915458	192.178.54.138	192.168.42.86	UDP	122	443 -> 42896 Len=80
19	3.915458	192.168.42.86	192.178.54.138	UDP	80	42896 -> 443 Len=38

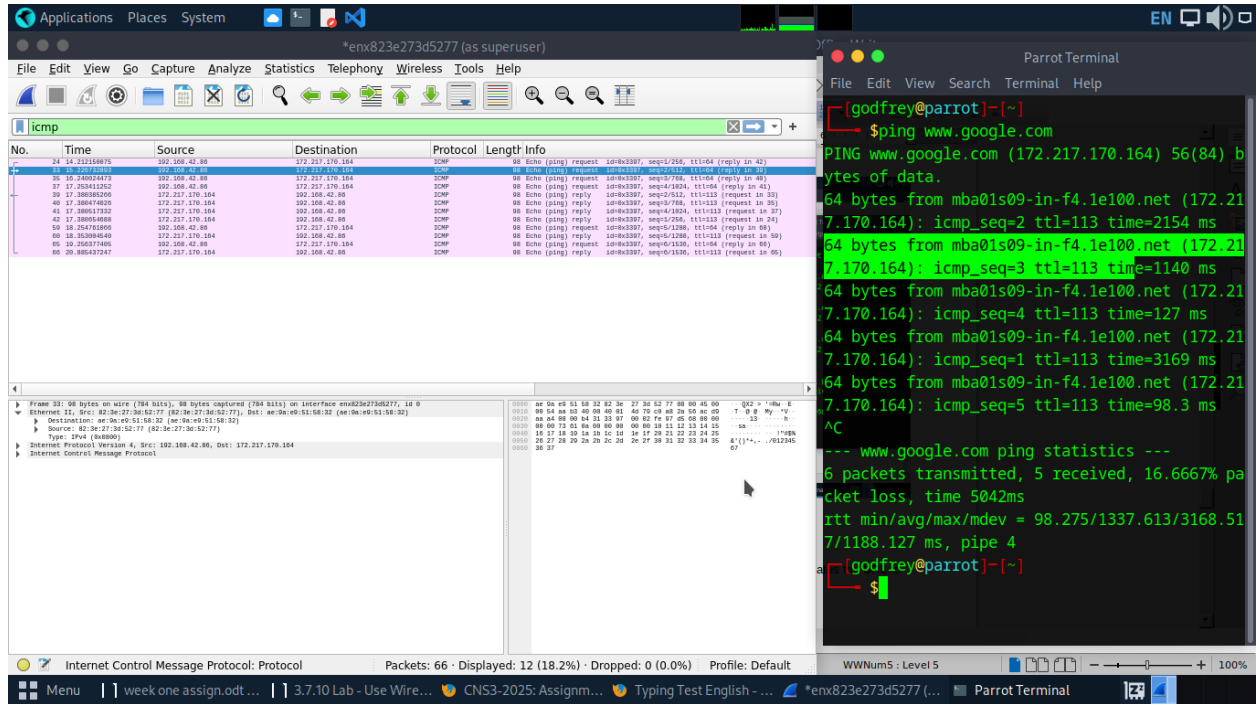
### 2) [www.cisco.com](http://www.cisco.com)



The screenshot shows Wireshark capturing network traffic on the interface '\*enx823e273d5277 (as superuser)'. The packet list displays 27 packets, including ICMP Echo (ping) requests and responses from 192.168.42.86 to 23.214.220.112. The packet details pane shows the selected packet (No. 27) as an ICMP Echo (ping) request. The packet bytes pane shows the raw data. A Parrot Terminal window is open in the foreground, showing the command 'ping www.cisco.com' and its output, which includes the IP address 23.214.220.112 and various statistics.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
2	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
3	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
4	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
5	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
6	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
7	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
8	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
9	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
10	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
11	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
12	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
13	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
14	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
15	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
16	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
17	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
18	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
19	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
20	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
21	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
22	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
23	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
24	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
25	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
26	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com
27	0.000000	192.168.42.86	192.168.42.86	OS	18	Standard query for www.cisco.com

### 3) [www.google.com](http://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.

d. You can stop capturing data by clicking the **Stop Capture** icon.

## 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.

Questions:

IP address for **www.yahoo.com**:

202.165.107.49

MAC address for **www.yahoo.com**:

ae:9a:e9:51:58:32

IP address for **www.cisco.com**:

23.214.228.112

MAC address for **www.cisco.com**:

ae:9a:e9:51:58:32

IP address for **www.google.com**:

172.217.170

MAC address for **www.google.com**:

ae:9a:e9:51:58:32

What is significant about this information?

*The MAC addresses for all three locations are the same.*

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. A ping to a remote host returns the MAC address of the default gateway LAN interface.*

*Close the Windows command prompt*

### 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 remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router. [r answers here](#).*

## Appendix A: Allowing ICMP Traffic Through a Firewall

If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

**Part 1: Create a new inbound rule allowing ICMP**In the System and Security window, click **Windows Defender Firewall** or **Windows Firewall**. traffic through the firewall.

- Navigate to the **Control Panel** and click the **System and Security** option in the Category view.
- 
- In the left pane of the **Windows Defender Firewall** or **Windows Firewall** window, click **Advanced settings**.
- On the **Advanced Security** window, click the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.
- This launches the **New Inbound Rule** wizard. On the **Rule Type** screen, click the **Custom** radio button and click **Next**.

- f. In the left pane, click the **Protocol and Ports** option and using the **Protocol Type** drop-down menu, select **ICMPv4**, and then click **Next**.
- g. Verify that **Any IP address** for both the local and remote IP addresses are selected. Click **Next** to continue.
- h. Select **Allow the connection**. Click **Next** to continue.
- i. By default, this rule applies to all the profiles. Click **Next** to continue.
- j. Name the rule with **Allow ICMP Requests**. Click **Finish** to continue. This new rule should allow your team members to receive ping replies from your PC.

## Part 2: Disabling or deleting the new ICMP rule.

After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of inbound rules.

- a. On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created previously.
  - b. Right-click the ICMP rule and select **Disable Rule** if so desired. You may also select **Delete** if you want to permanently delete it. If you choose this option, you must re-create the rule again to allow ICMP replies.
- End of document