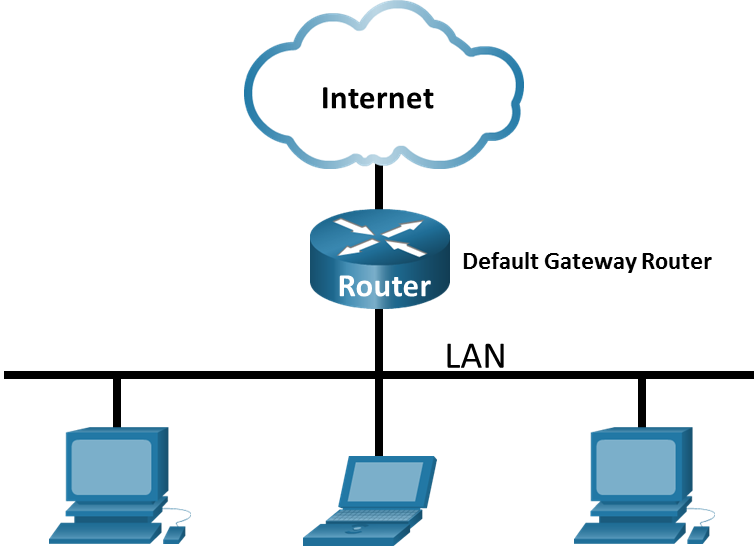
Lab 3.7.10 - Use Wireshark to View Network Traffic – Windows Version

# 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)

# Instructions

* Enter your screenshots/answers below the items highlighted in blue and turn in the completed file without making any changes to the original content.
* This Lab cannot be completed using NetLab. Complete using a computer with Internet Access.
* Once the Lab is graded it cannot be resubmitted for a new grade.

## Capture and Analyze Local ICMP Data in Wireshark

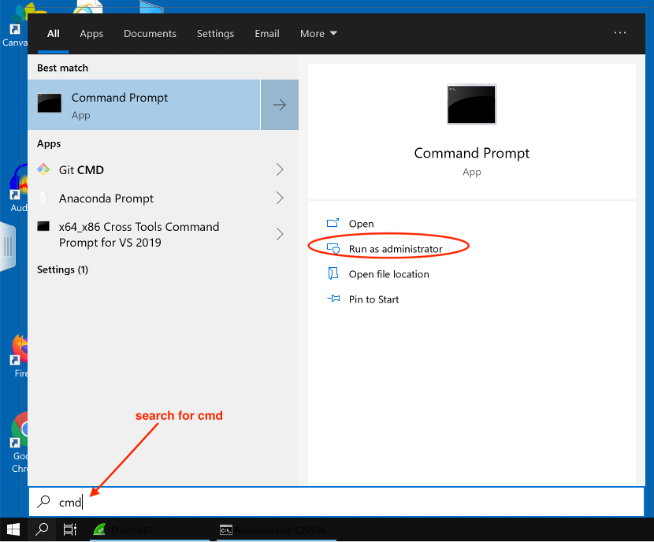
In Part 1 of this lab, you will ping your local default gateway and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

### 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.

Open a Windows command prompt.

* + - 1. Open a command prompt window used to enter commands on your PC, CMD. You may search for the command prompt utility on a Windows 10/11 PC and run it as an administrator as shown in the screenshot below.

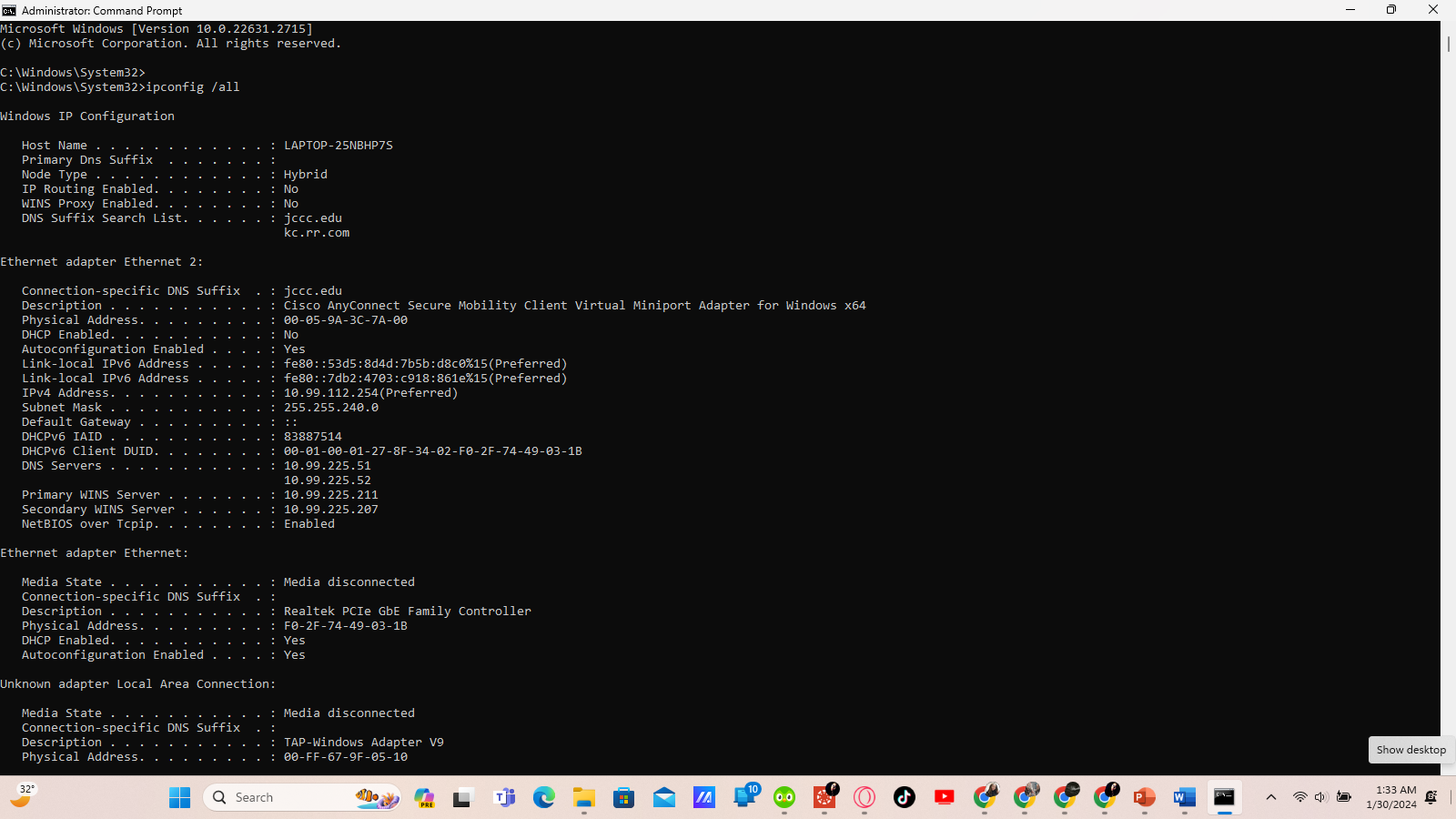


* + - 1. In a command prompt window, enter **ipconfig /all** as shown in the screenshot below:

Text

Description automatically generated with low confidence

Provide a screenshot like the one above. (10 points)



Record the following information from the screenshot (3 points each):

IPv4 address = 192.168.132.1

MAC or Physical address = 00-05-9A-3C-7A-00

IPv4 Default Gateway=; ;

Default Gateway is a router which is a networking device that connects separate networks together. Your home default gateway usually is wireless router that connects your home network to your service provide.

Close a Windows Command Prompt.

### Install Wireshark if it is not installed on your PC.

* + - 1. Go to [www.wireshark.org](http://www.wireshark.org) and click Download.
      2. Choose the Installer appropriate for your computer operating system.

Graphical user interface, website

Description automatically generated

* + - 1. Launch the installer program and follow all the default settings to install Wireshark.

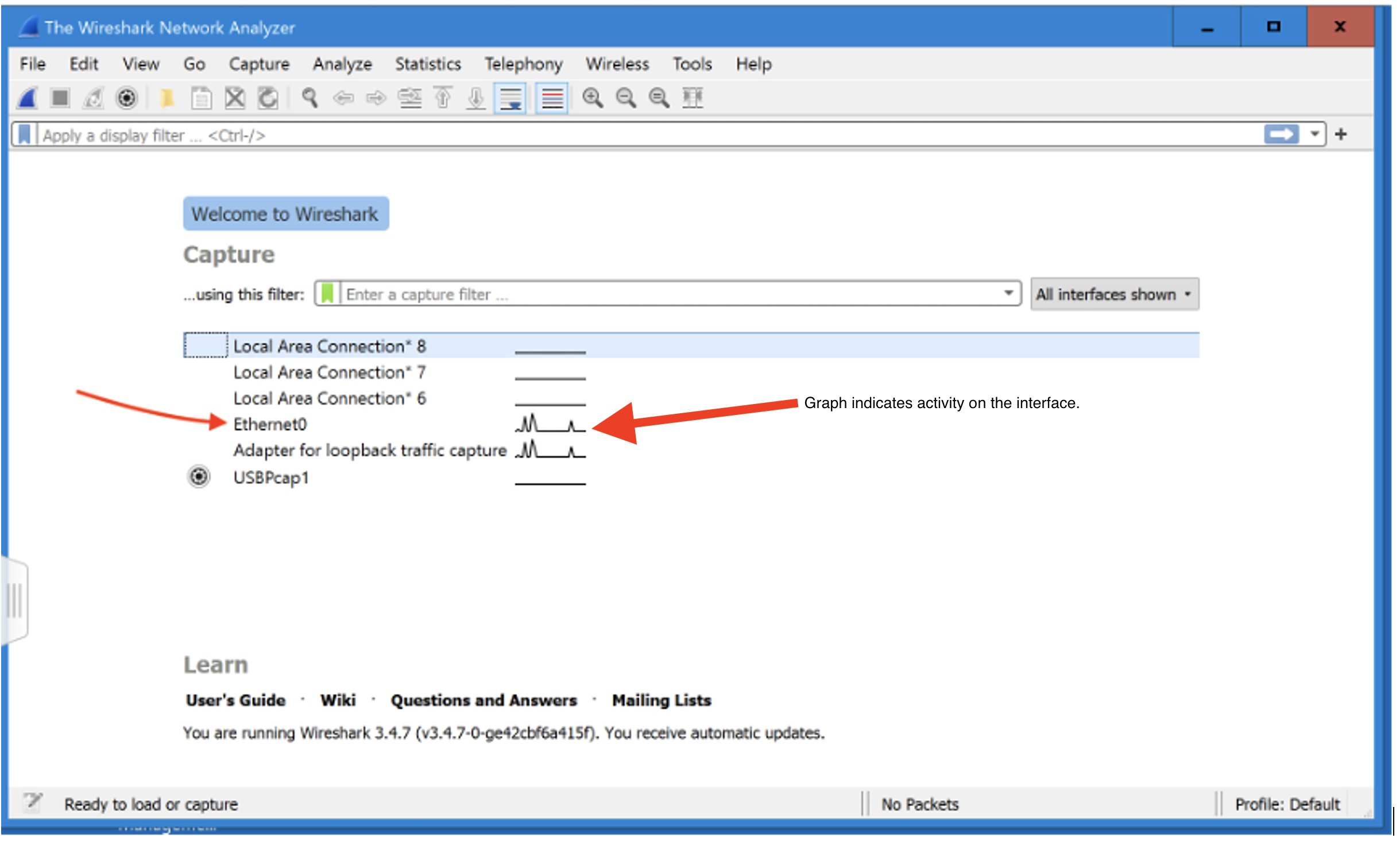
### Start Wireshark and begin capturing data.

* + - 1. Navigate to Wireshark, run it as an administrator:

Graphical user interface, text, application, email

Description automatically generated

* + - 1. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic activity, see Ethernet0 is the example below. It could be a wired or WiFi interface.



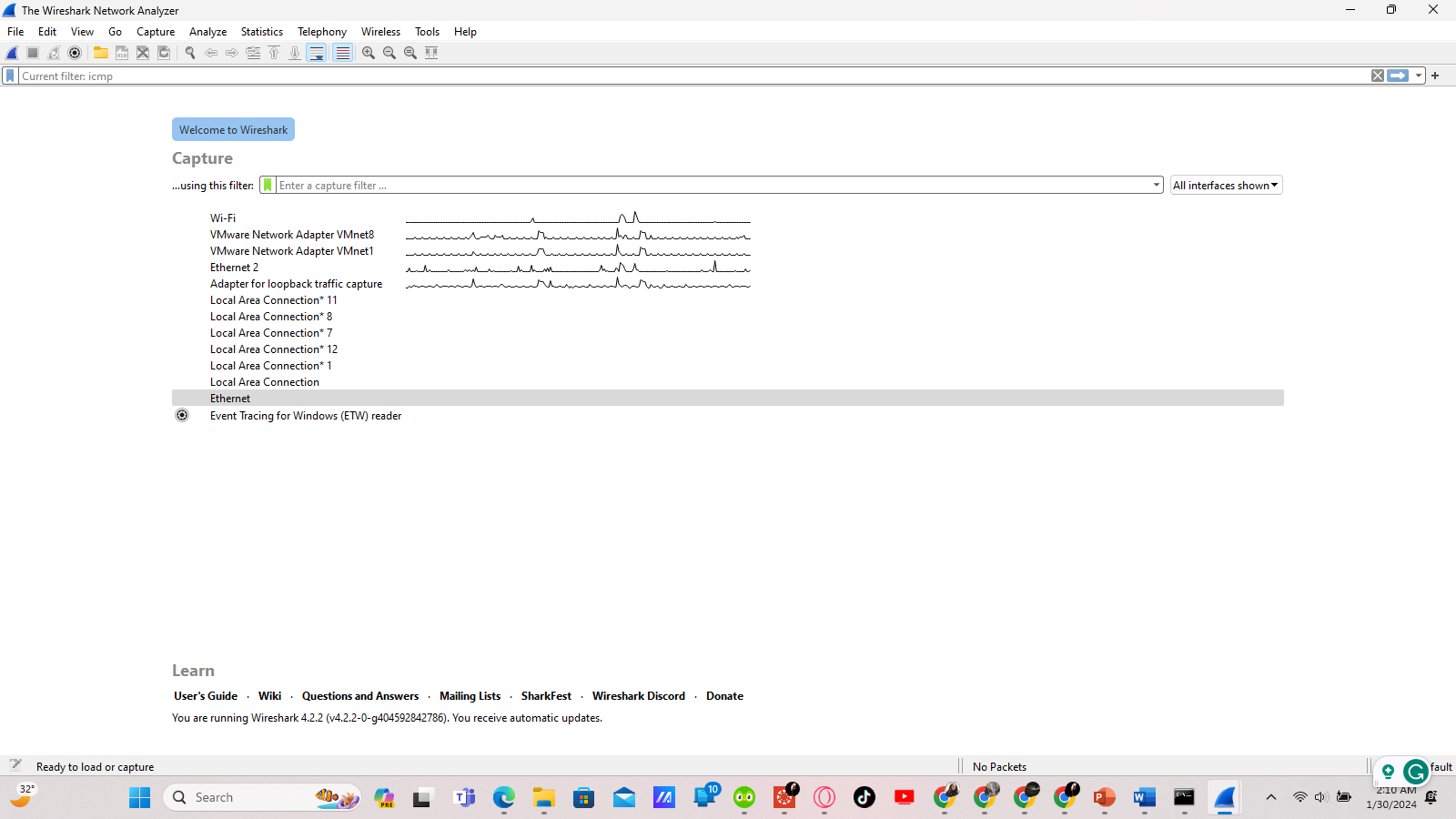
* + - 1. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.

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 being captured by Wireshark.

For this lab, we are only interested in displaying Internet Control Messaging Protocol packets (ICMP) generated because of ping traffic. Type **icmp** in the **Filter** box at the top of Wireshark and press **Enter** and click the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.

* + - 1. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface.
      2. Navigate to a command prompt window and ping the IP address of the default gateway you recorded in step 1 above.

Provide a screenshot showing the result of the **ping**. (10 points)

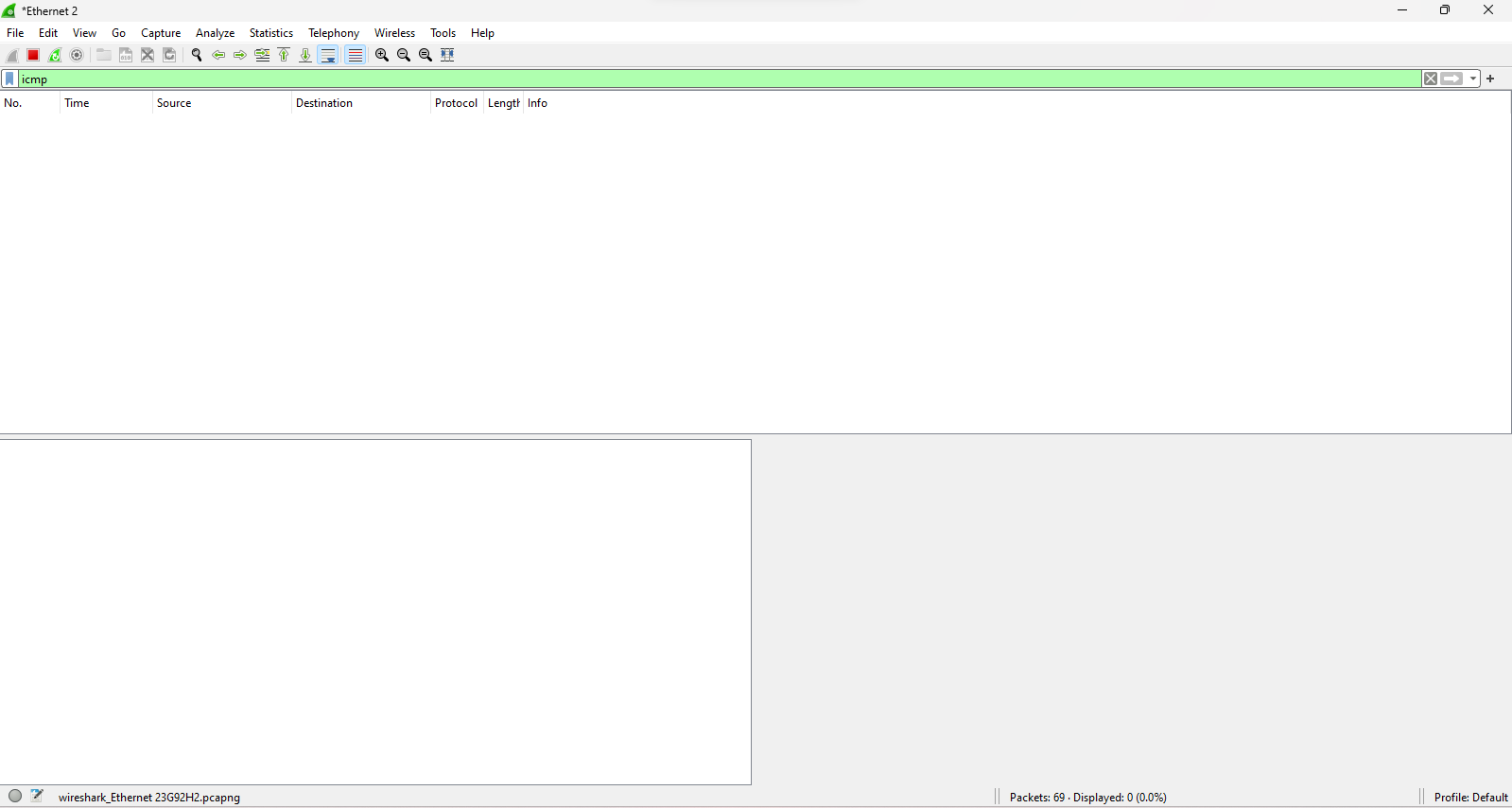


Data will start to appear in the top window of Wireshark again like the screenshot below provided the ping is successful. Note that your Wireshark Window may be arranged slightly differently than the screenshot below depending on the version you are running.

A screenshot of a computer

Description automatically generated

Provide a screenshot like the one above. (10 points)

****

**Note**: If the default gateway you are pinging does not reply to your pings, this may be because the PC firewall 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.

* + - 1. Stop capturing data by clicking the **Stop Capture** icon.

### Examine the captured data.

Wireshark data is displayed in three sections: 1) The top section displays the list of Protocol Data Unit (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 third section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

* + - 1. 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 default gateway that you pinged.
      2. 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? (3 points)

No

What is the destination MAC address, record the value below? (4 points)

192.168.19.1answers here.

How is the MAC address of the pinged default gateway obtained by your PC? (4 points)

It is obtained by C:\ Windows\System32>ipconfig /all your answers here.

**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.

## 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.

**Note: Computers with newer operating systems prefer to use newer IPv6 addressing over older IPv4, so your pings may not show IPv4 addresses. You can change the capture filter to icmpv6 or force the computer to use IPv4 by adding -4 after the target address you are trying to ping from the command prompt.**

### Start capturing data on the interface.

* + - 1. Start the data capture again.
      2. 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**.
      3. With the capture active, ping the following three website URLs from a Windows command prompt:

Open a Windows command prompt

* + - * 1. www.yahoo.com
        2. www.cisco.com
        3. www.google.com

**Note**: When you ping the URLs listed, the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

* + - 1. You can stop capturing data by clicking the **Stop Capture** icon.

### 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**](http://www.yahoo.com)(5 points): 72.30.35.10

Type your answers here.

MAC address for [**www.yahoo.com**](http://www.yahoo.com)(5 points): 84:78:ac: 09:47:c2

Type your answers here.

IP address for [**www.cisco.com**](http://www.cisco.com)(5 points):72.163.4.185

Type your answers here.

MAC address for [**www.cisco.com**](http://www.cisco.com)(5 points): 84:78:ac: 09:47:c2

Type your answers here.

IP address for [**www.google.com**](http://www.google.com)(5 points):216.58.194.174

Type your answers here.

MAC address for [**www.google.com**](http://www.google.com)(5 points): 84:78:ac: 09:47:c2

Type your answers here.

Compare the results of the remote pings above to the results of the local ping to the default gateway in Part 1. What is significant about the addressing information you reported above and how does it differ from the local ping information you received in Part 1? (10 points)

I had results to work with but on a serious note, the results are more detailed. Plus, it’s significant because it has personal information. your answers here.

1. Close the Win
2. 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? (10 points)

The encryption hides addresses that are tied down to the privacy and security of the servers. When it comes to personal information it needs to be secured and this is the best way to do it to prevent hacking.

# 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.

## Create a new inbound rule allowing ICMP traffic through the firewall.

* + - 1. Navigate to the **Control Panel** and click the **System and Security** option in the Category view.
      2. In the **System and Security** window, click **Windows Defender Firewall** or **Windows Firewall**.
      3. In the left pane of the **Windows Defender Firewall** or **Windows Firewall** window, click **Advanced settings**.
      4. On the **Advanced Security** window, click the **Inbound Rules** option on the left sidebar and then click **New Rule…** on the right sidebar.
      5. This launches the **New Inbound Rule** wizard. On the **Rule Type** screen, click the **Custom** radio button and click **Next**.
      6. In the left pane, click the **Protocol and Ports** option and using the **Protocol Type** drop-down menu, select **ICMPv4**, and then click **Next**.
      7. Verify that **Any IP address** for both the local and remote IP addresses are selected. Click **Next** to continue.
      8. Select **Allow the connection**. Click **Next** to continue.
      9. By default, this rule applies to all the profiles. Click **Next** to continue.
      10. 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.

## 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.

* + - 1. On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created previously.
      2. 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