Lab – Installing Wireshark

Objectives

Download and Install 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. This lab provides instructions for downloading and installing Wireshark.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access)

Download and Install Wireshark

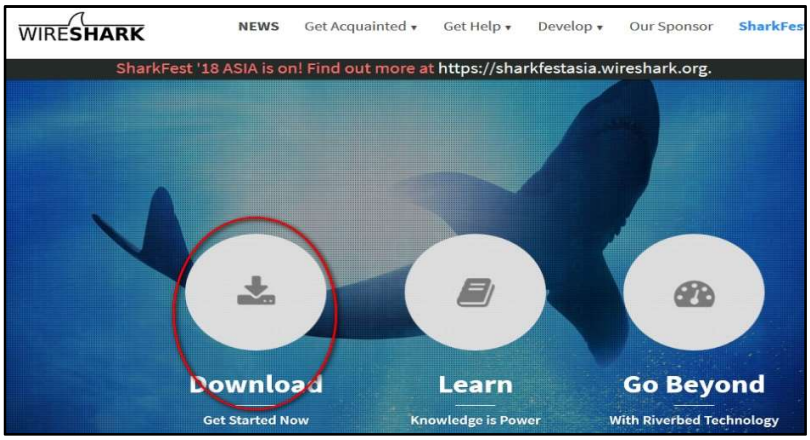
Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In this lab, you will download and install the Wireshark software program on your PC.

Note: Before downloading Wireshark, check with your instructor about the software download policy of your academy.

Step 1: Download Wireshark.

a. Wireshark can be downloaded from www.wireshark.org.

b. Click the icon above **Download**.



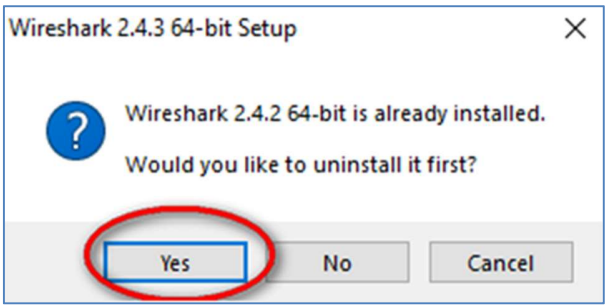
c. Choose the software version you need based on your PC architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.

After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

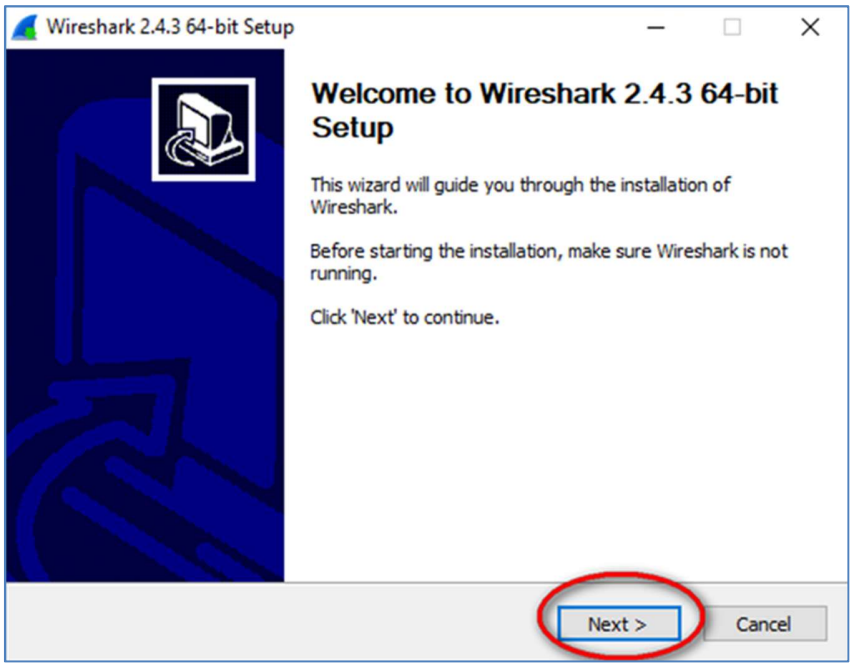
Step 2: Install Wireshark.

a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.

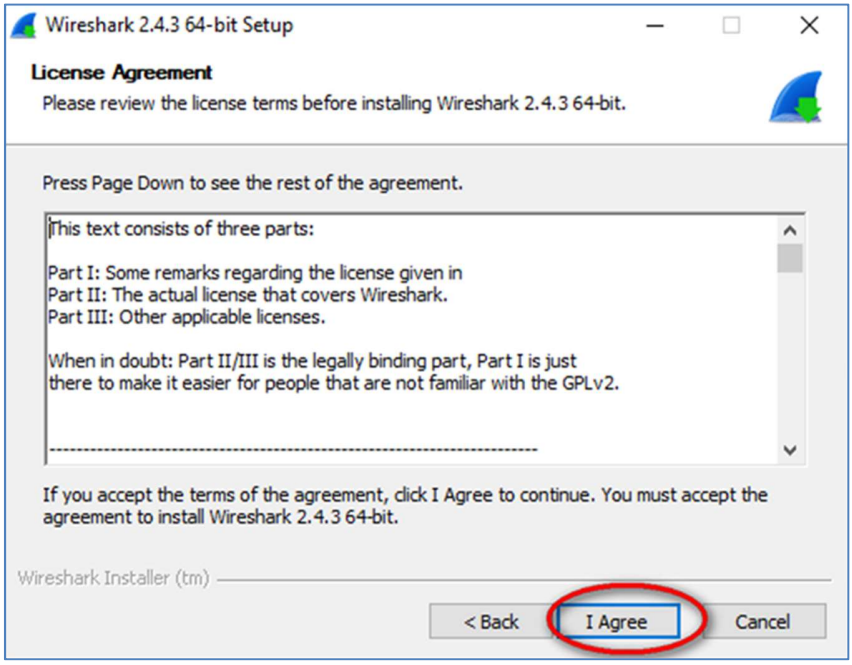
b. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.



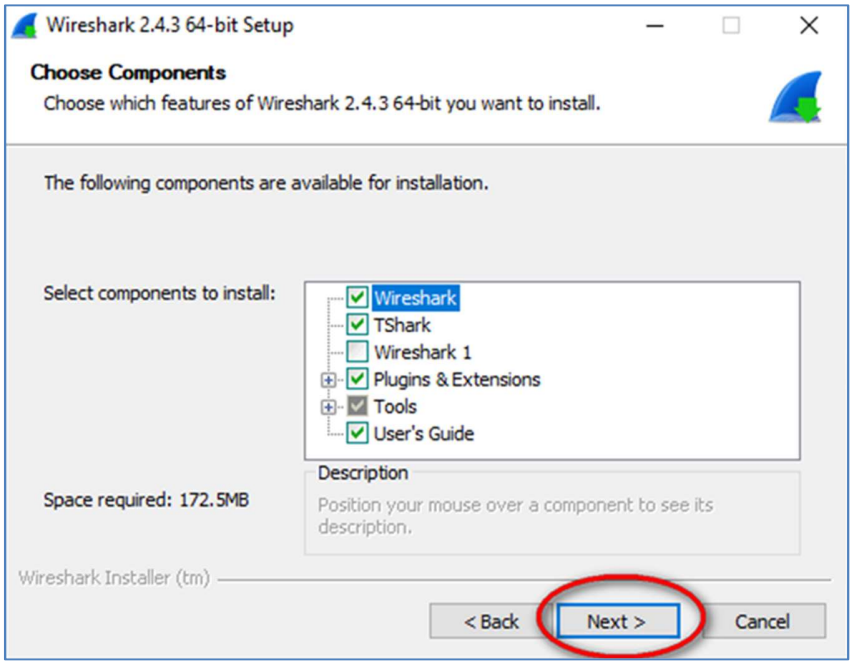
c. If this is the first time that you have installed Wireshark, or after you have completed the uninstall process, you will navigate to the **Wireshark Setup** wizard. Click **Next**.



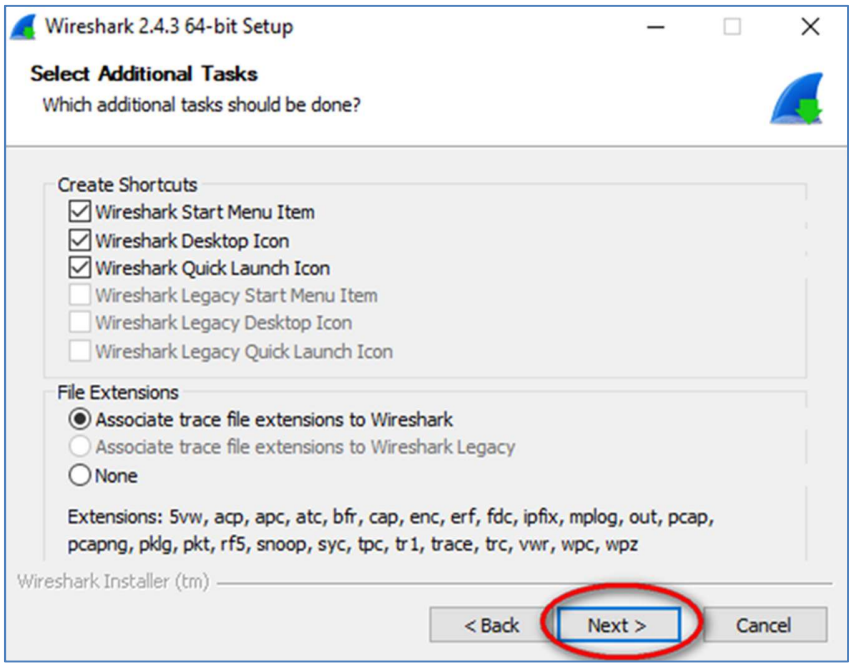
d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.



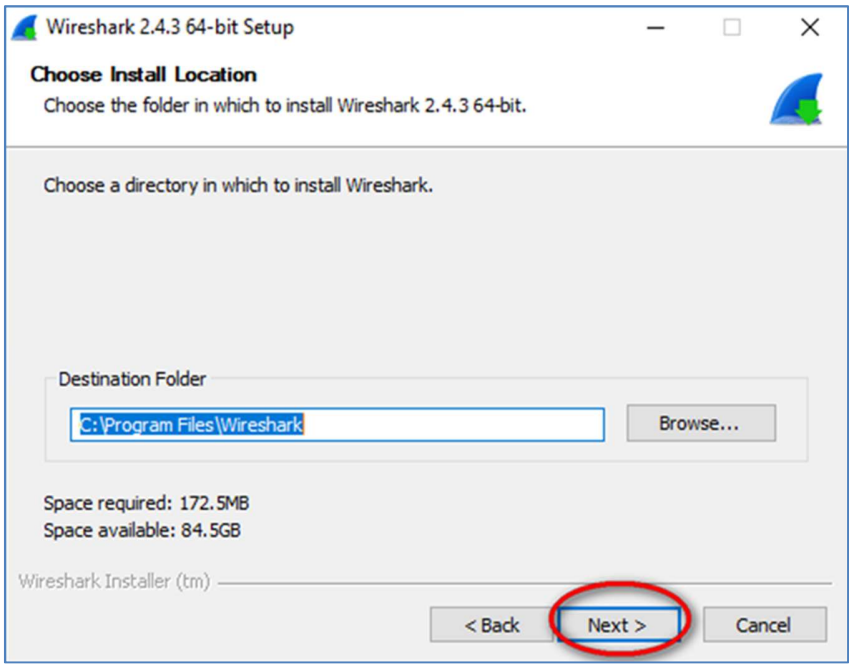
e. Keep the default settings on the **Choose Components** window and click **Next**.



f. Choose your desired shortcut options and click **Next**.

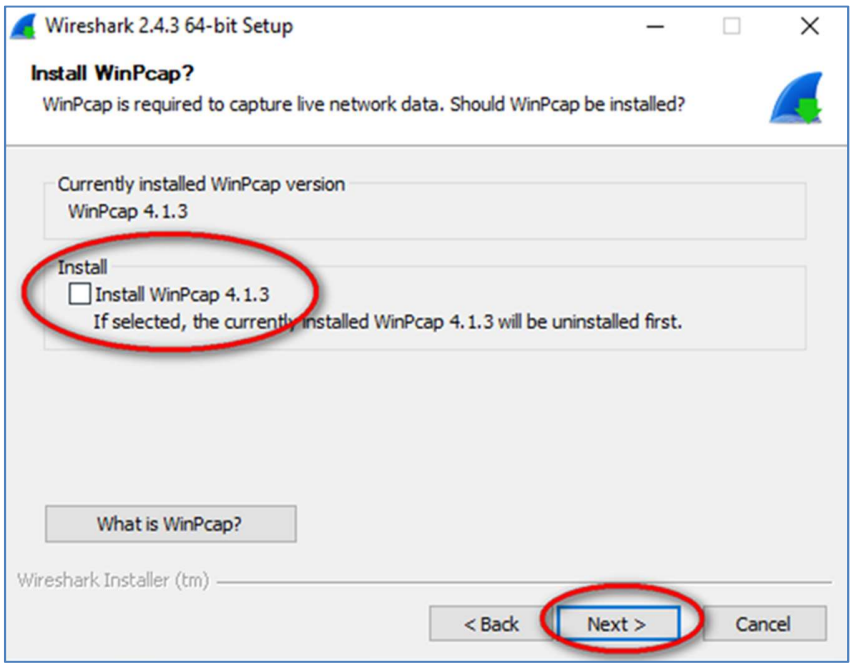


g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.



h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.

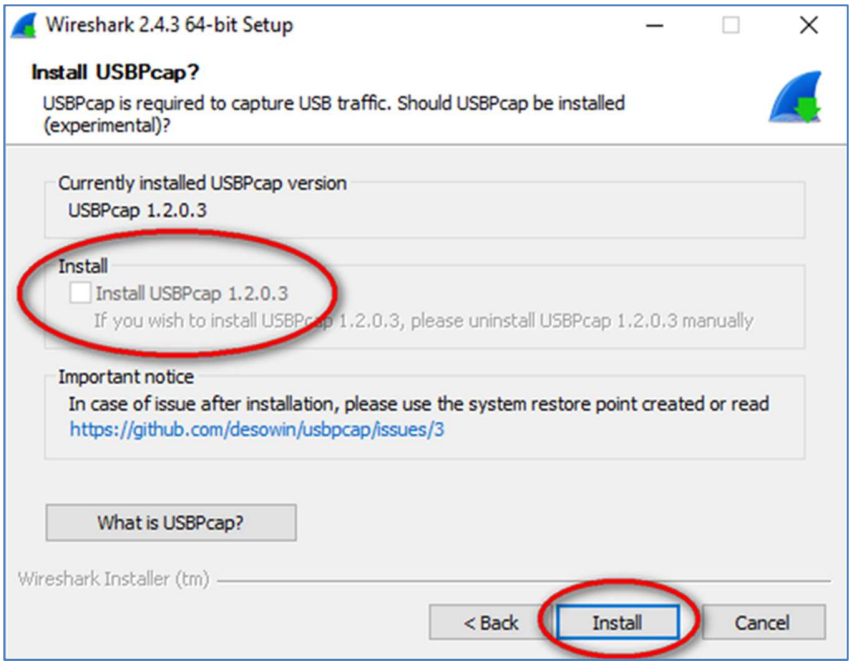
i. Finish the **WinPcap Setup** wizard if installing WinPcap.



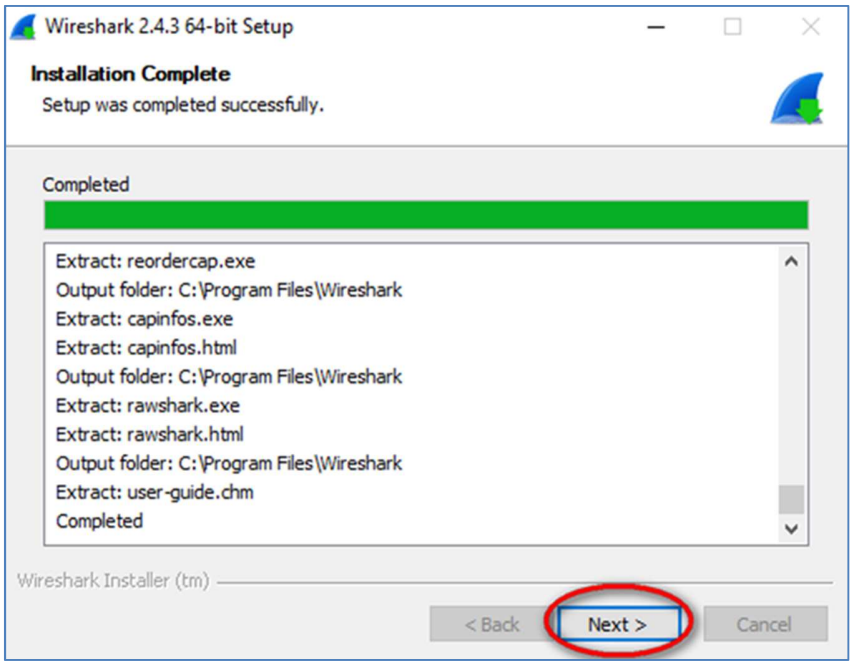
j. In addition, USBPcap can be installed on your PC. If USBPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of USBPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install USBPcap x.x.x** (version number) check box.

Note: Because USBcap is still experimental, it is recommended that you **DO NOT** install USBcap unless you need to capture USB traffic.

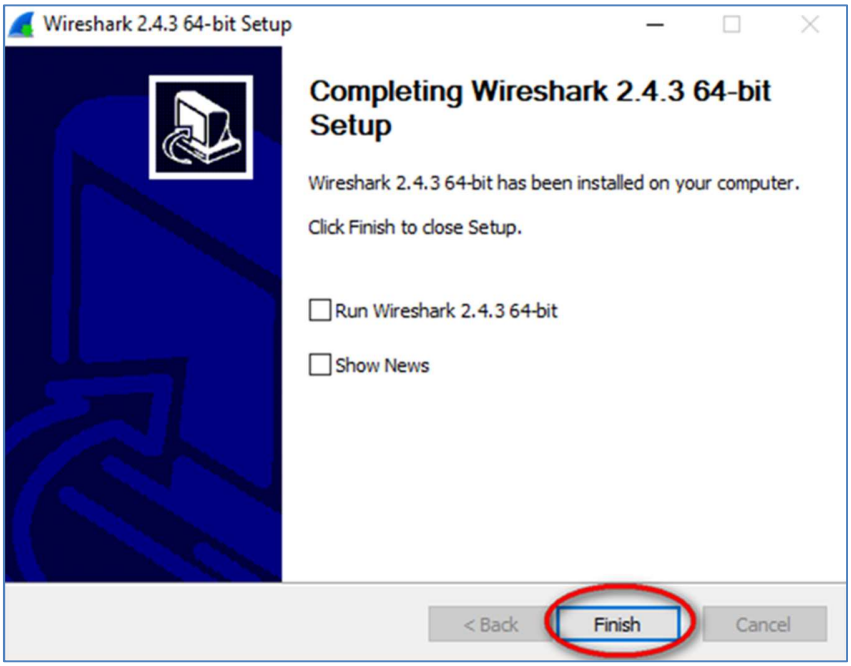
k. Finish the **USBPcap Setup** wizard if installing USBPcap.



l. Wireshark starts installing its files, and a separate window displays with the status of the installation. Click **Next** when the installation is complete.

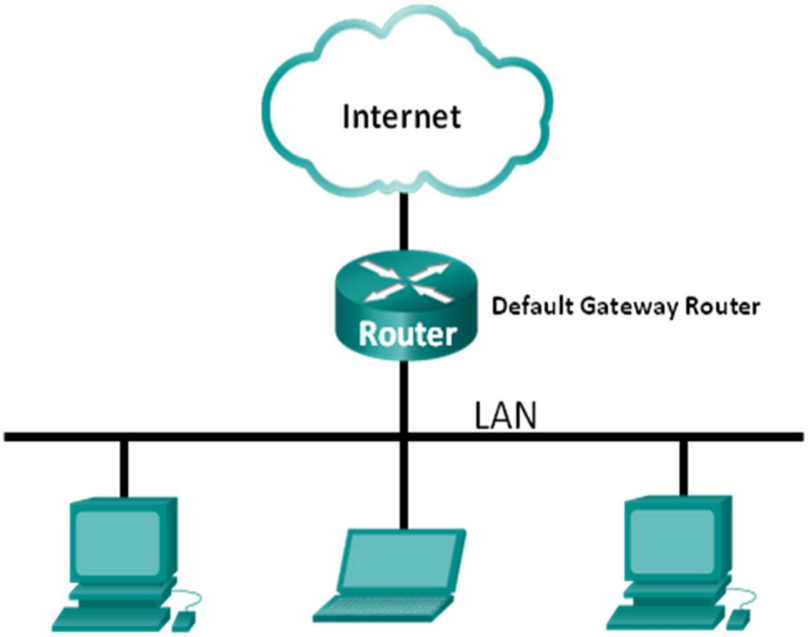


m. Click **Finish** to complete the Wireshark install process.



Lab - Using Wireshark to View Network Traffic

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 7, 8, or 10 with internet access)
- Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

Part 1: Capture and Analyze Local ICMP Data in Wireshark

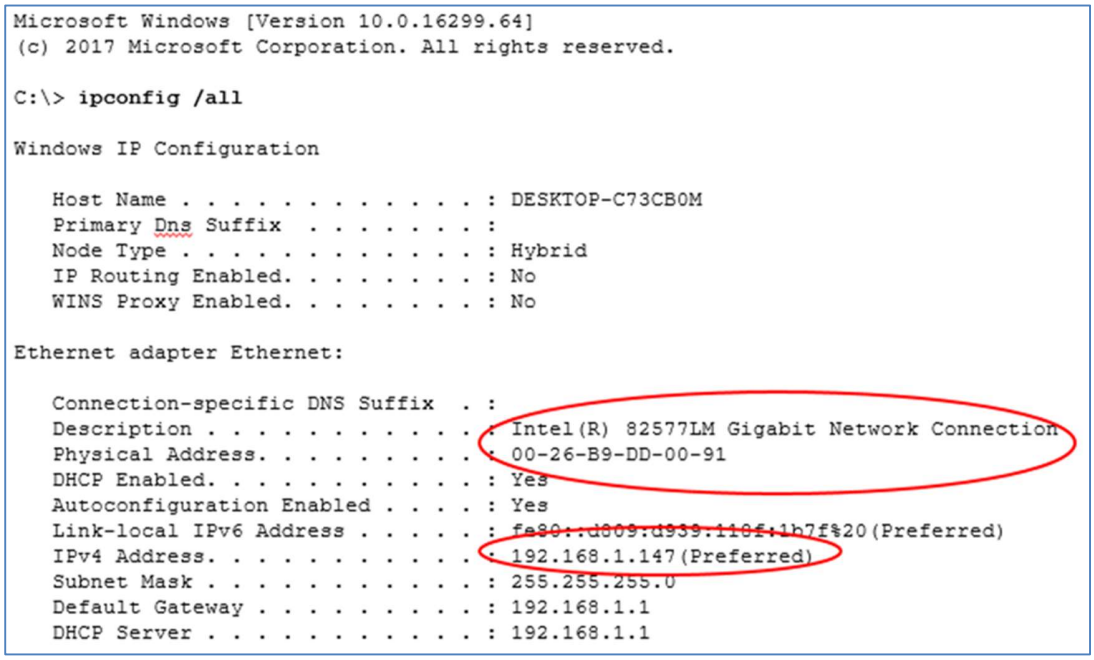
In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

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.

a. Open a command window, type **ipconfig /all**, and then press Enter.

b. Note the IP address of your PC interface, its description, and its MAC (physical) address.



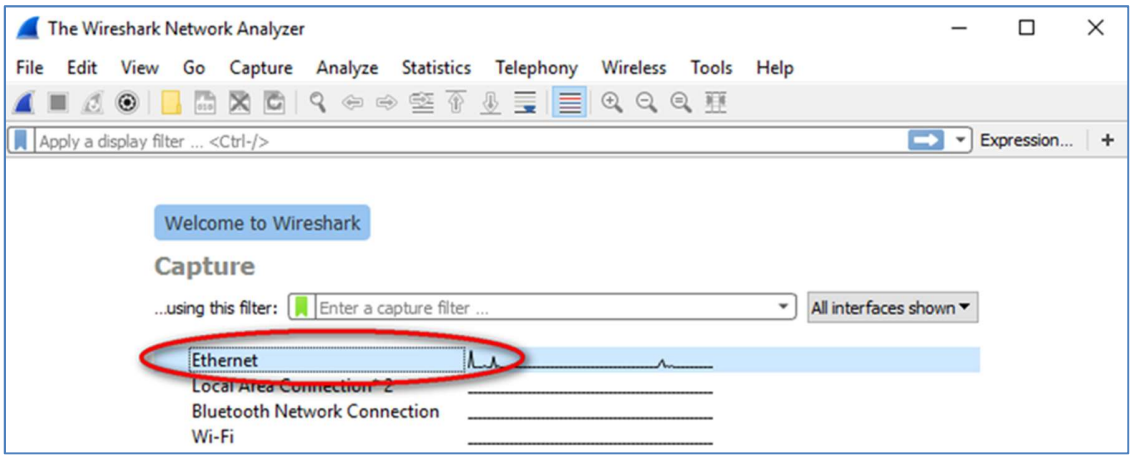
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

c. 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.

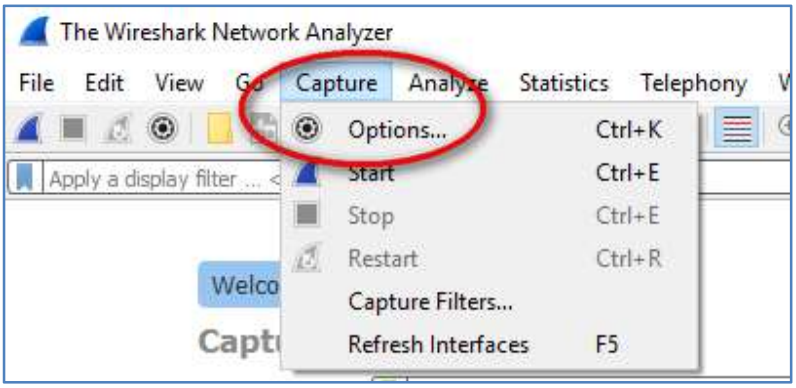
Step 2: Start Wireshark and begin capturing data.

a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

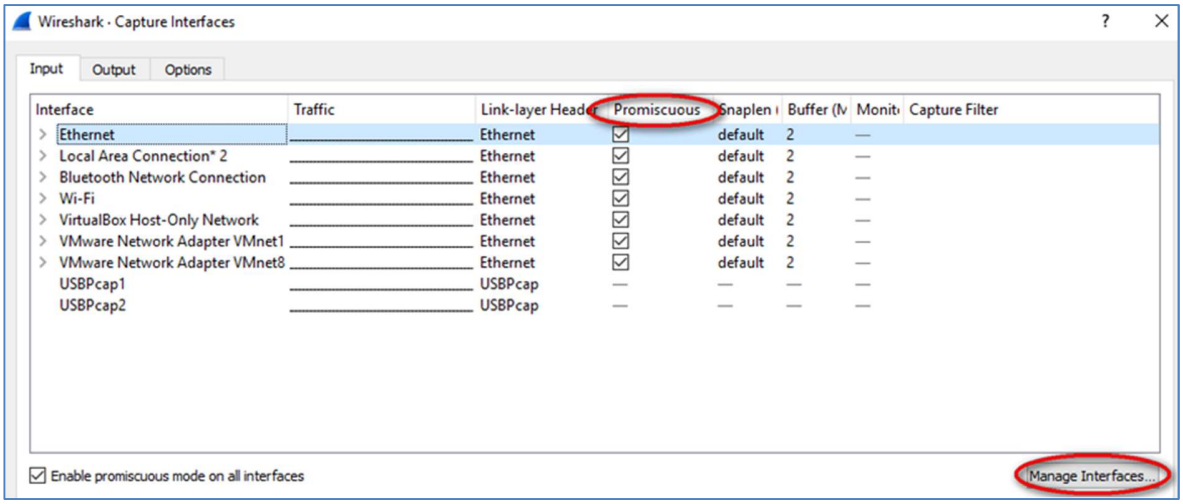
b. After Wireshark starts, click the capture interface to be used. Because we are using the wired Ethernet connection on the PC, make sure the Ethernet option is on the top of the list.



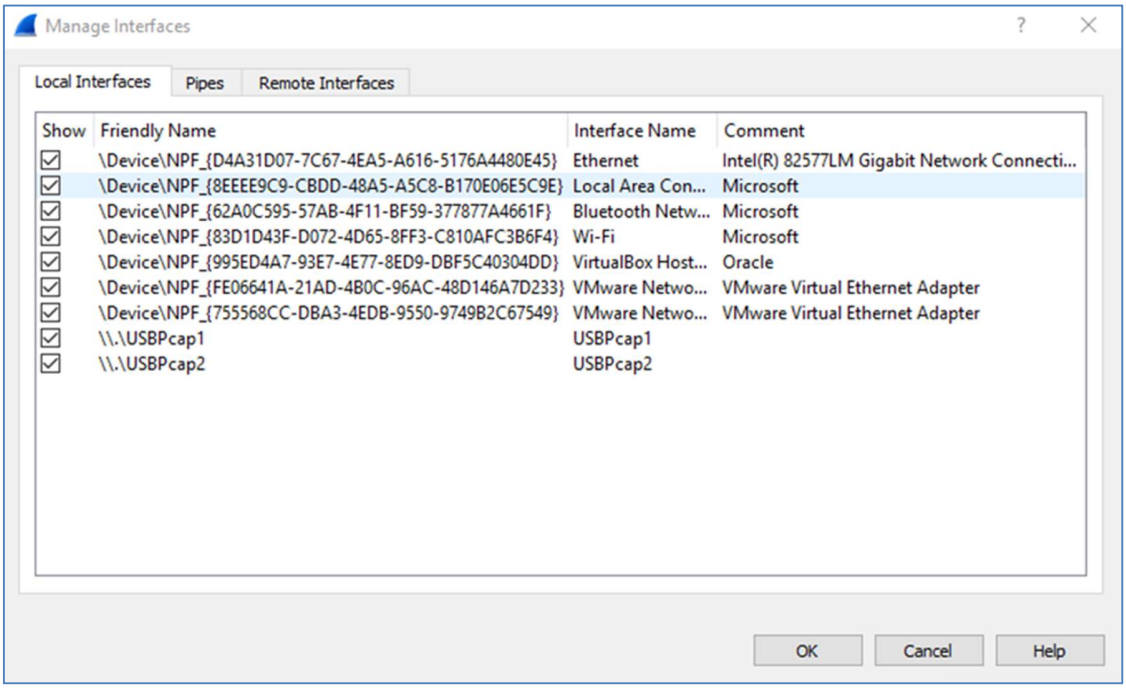
You can manage the capture interface by clicking **Capture** and **Options**:



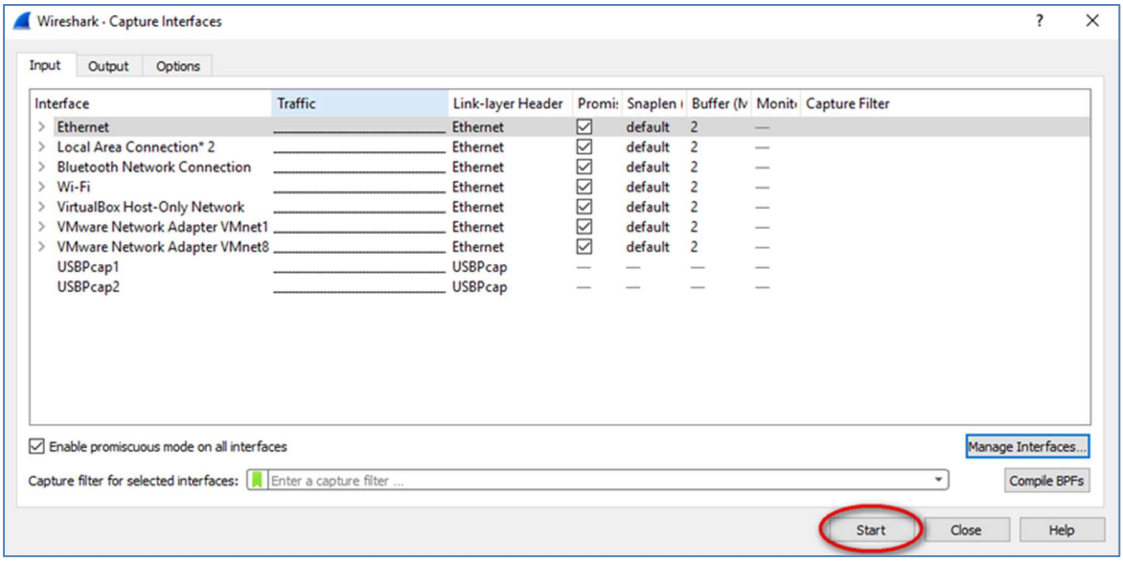
c. A list of interfaces will display. Make sure the capture interface is checked under **Promiscuous**.



Note: We can further manage the interfaces on the PC by clicking **Manage Interfaces**. Verify that the description matches what you noted in Step 1b. Close the **Manage Interfaces** window after verifying the correct interface.

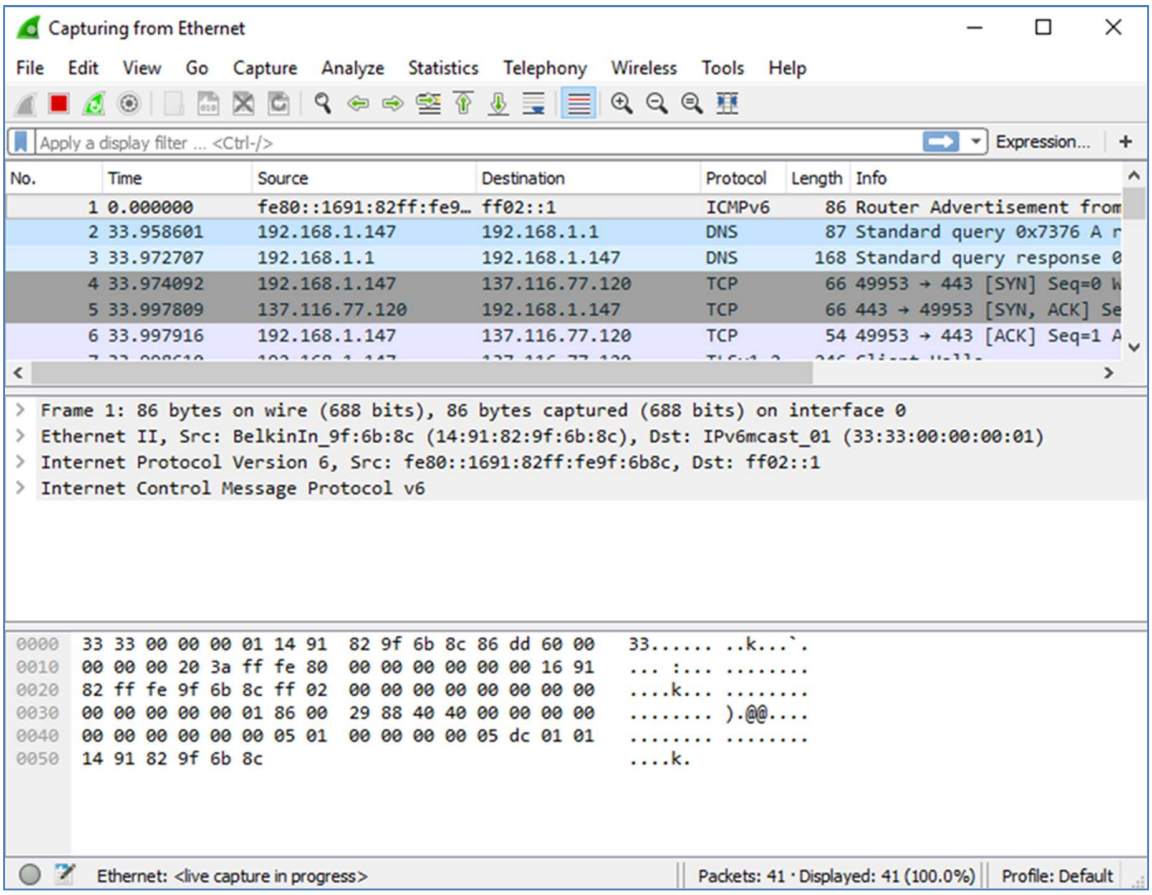


d. After you have checked the correct interface, click **Start** to start the data capture.



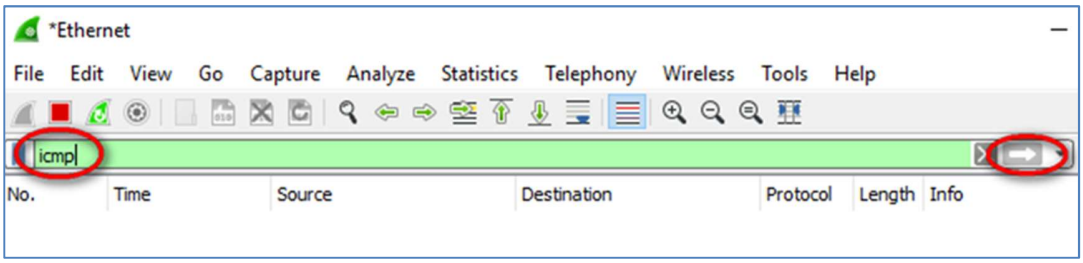
Note: You can also start the data capture by clicking the **Wireshark** icon in the main interface.

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



e. 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. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in

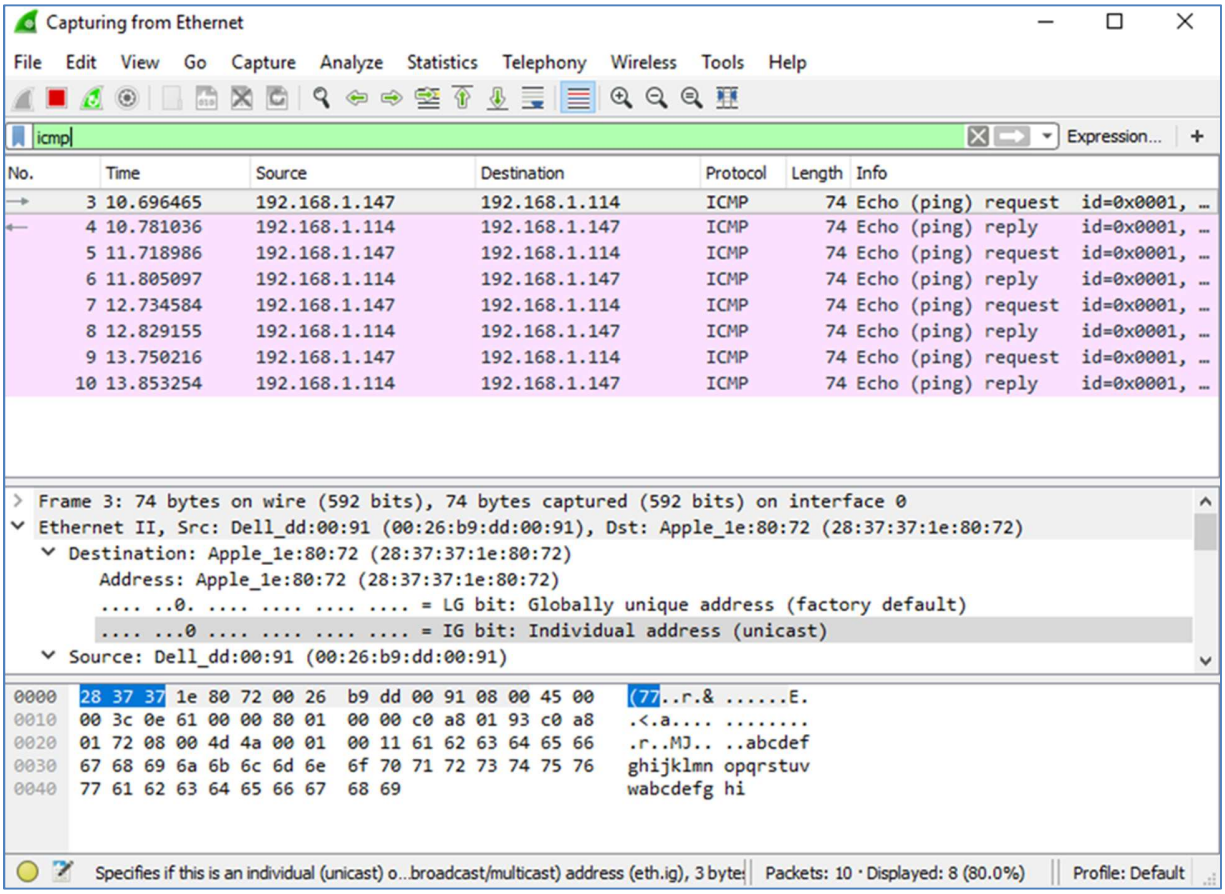
the **Filter** box at the top of Wireshark and press **Enter** or click on the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.



f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member.

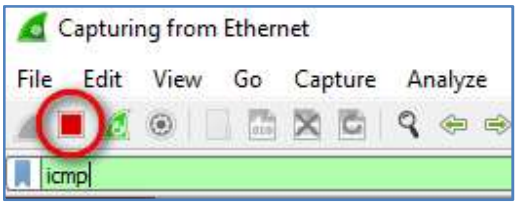
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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 7.

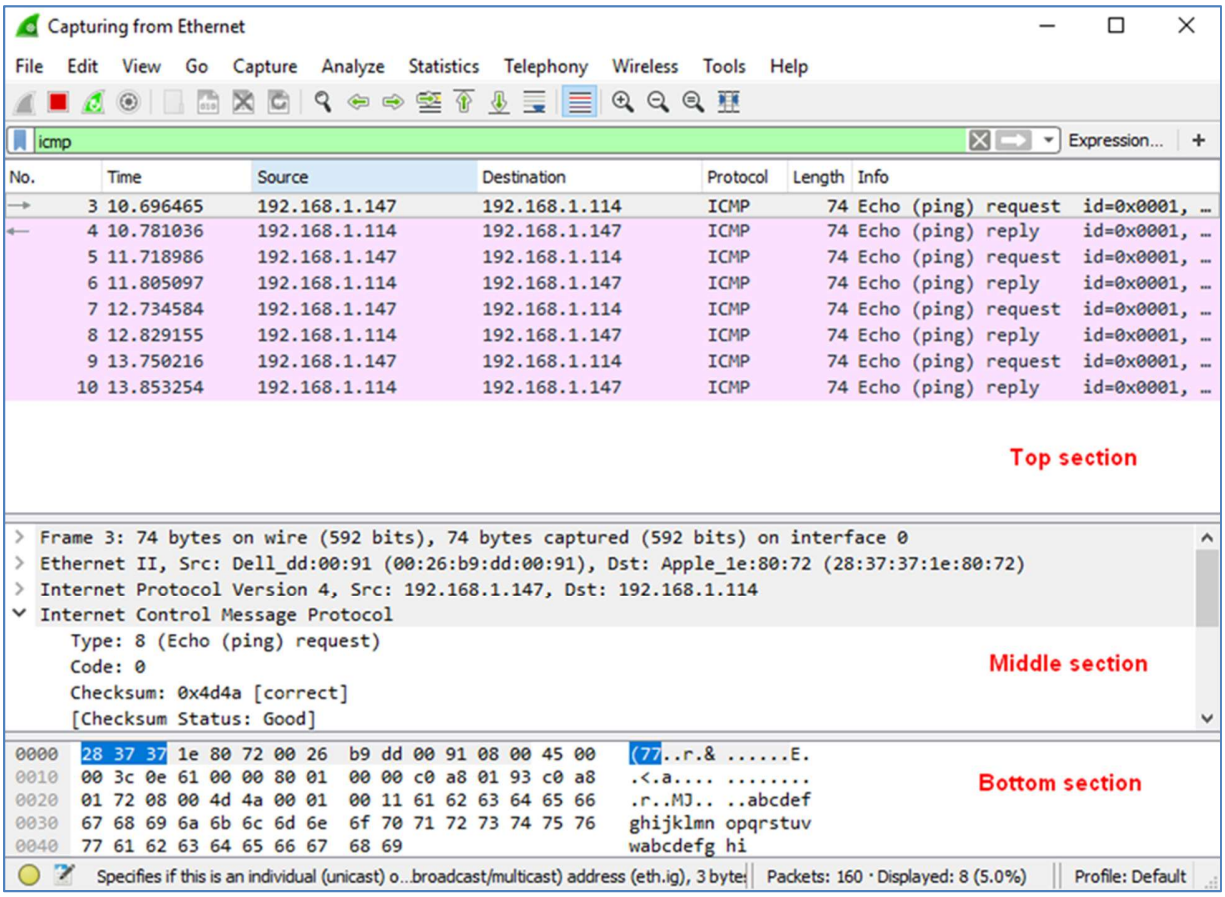
g. Stop capturing data by clicking the **Stop Capture** icon.



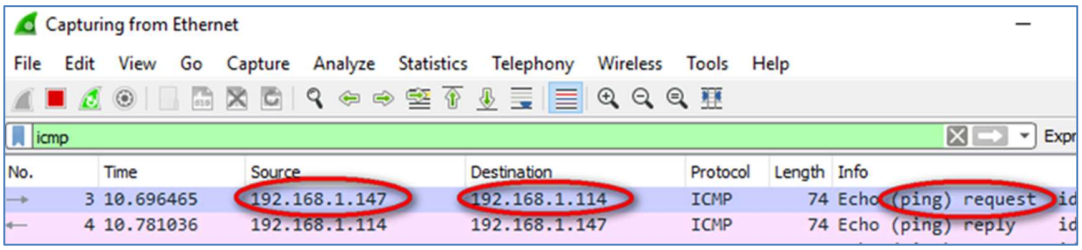
Step 3: Examine the captured data.

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

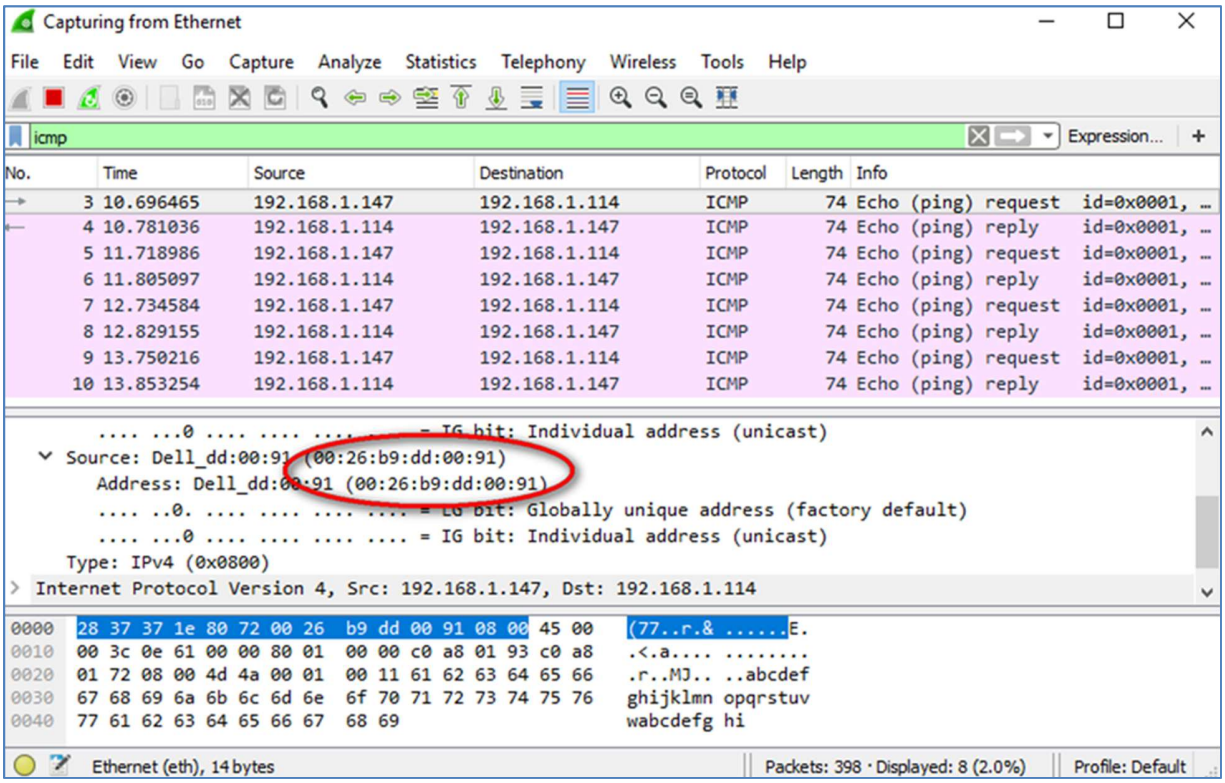
in the top part of the screen and separates a captured PDU frame by its protocol layers; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.



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.



Does the source MAC address match your PC interface (shown in Step 1.b)? _____

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

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

_____

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.

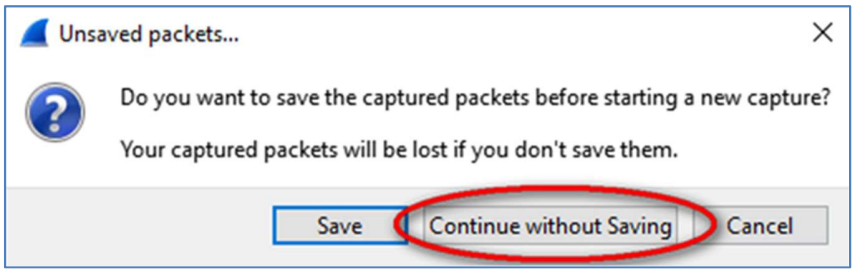
Part 2: Capture and Analyze Remote ICMP Data in Wireshark

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.

a. Start the data capture again.

b. 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**.



c. With the capture active, ping the following three website URLs:

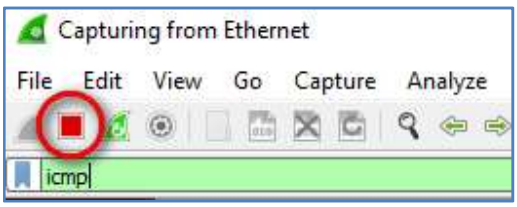
1) www.yahoo.com
2) www.cisco.com

3) www.google.com

```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

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.

a. 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.

1st Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2nd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3rd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

b. What is significant about this information?

_____

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

_____

_____

Reflection

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

_____

_____

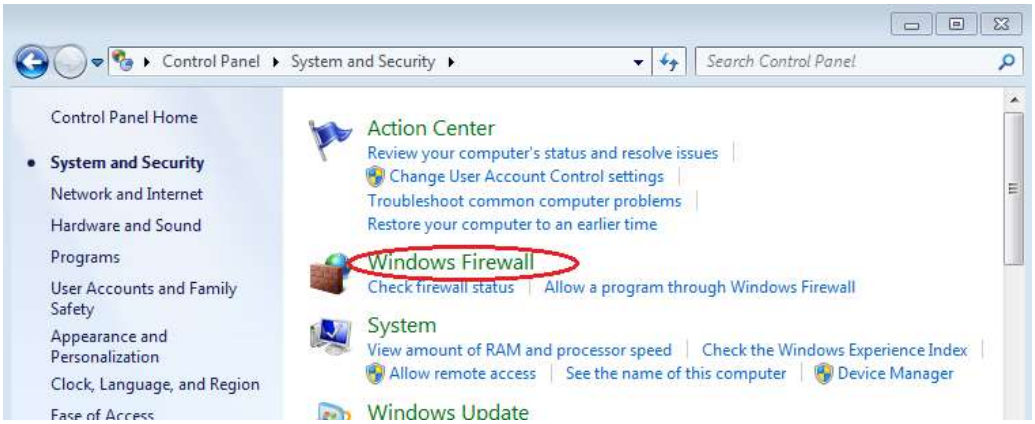
Appendix A: Allowing ICMP Traffic Through a Firewall

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.

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

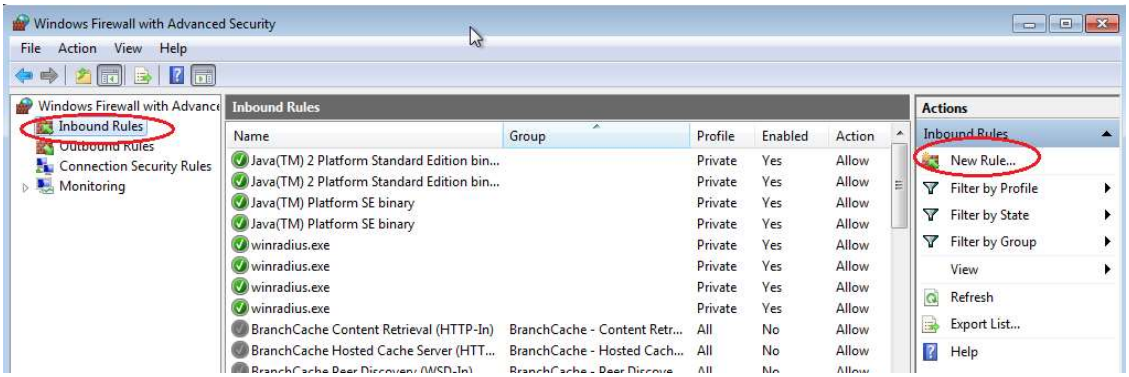
a. From the **Control Panel**, click the **System and Security** option.

b. From the **System and Security** window, click **Windows Firewall**.

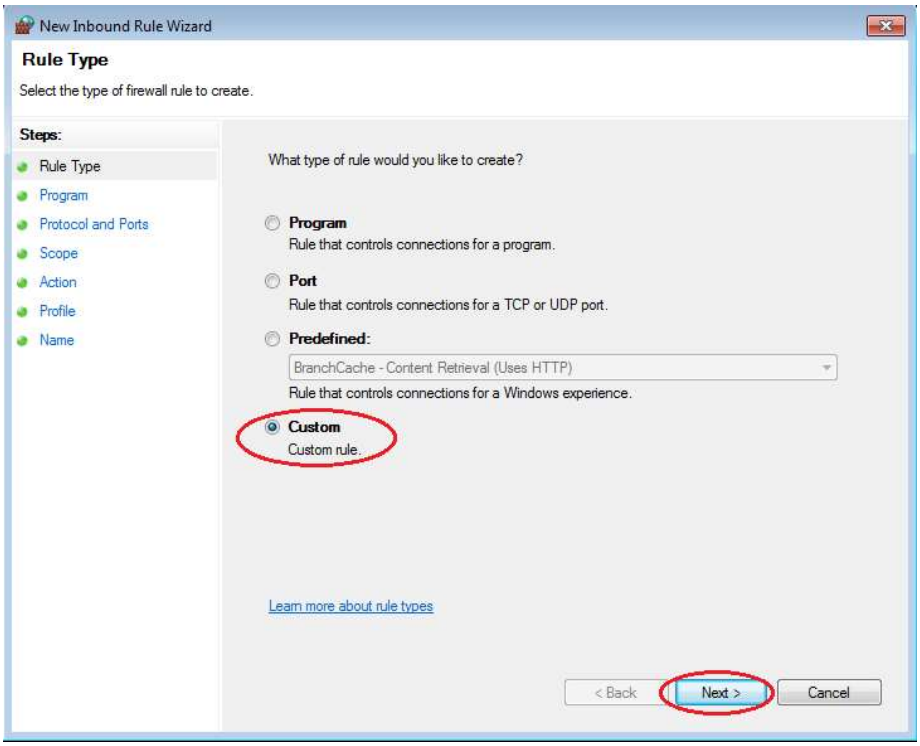


c. In the left pane of the **Windows Firewall** window, click **Advanced settings**.

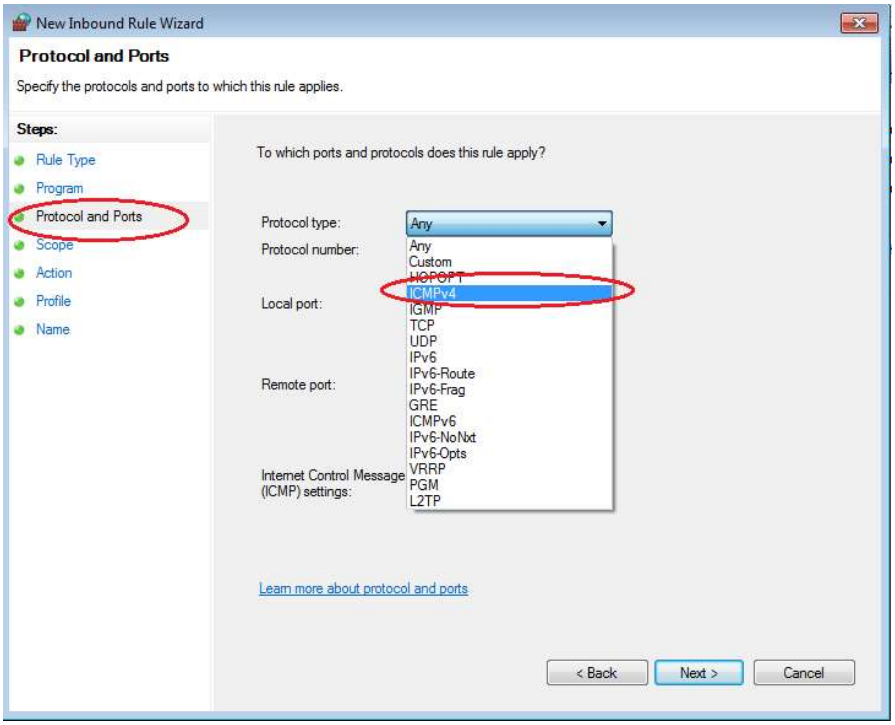
d. On the **Advanced Security** window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule…** on the right sidebar.



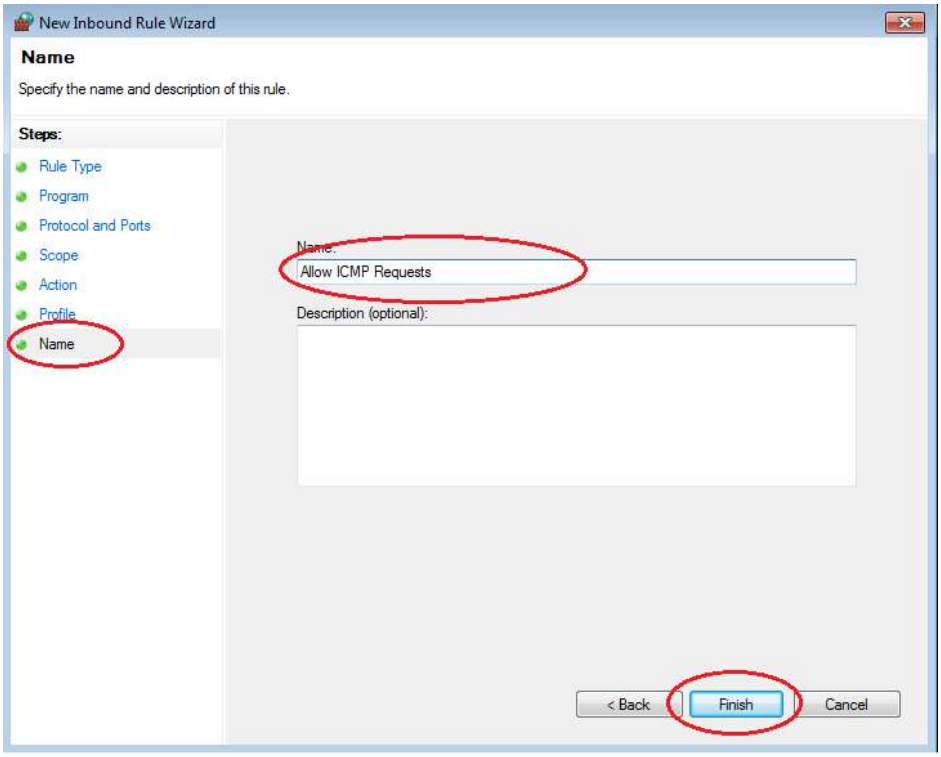
e. This launches the **New Inbound Rule** wizard. On the **Rule Type** screen, click the **Custom** radio button and click **Next**



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. In the left pane, click the **Name** option and in the **Name** field, type **Allow ICMP Requests**. Click **Finish**.

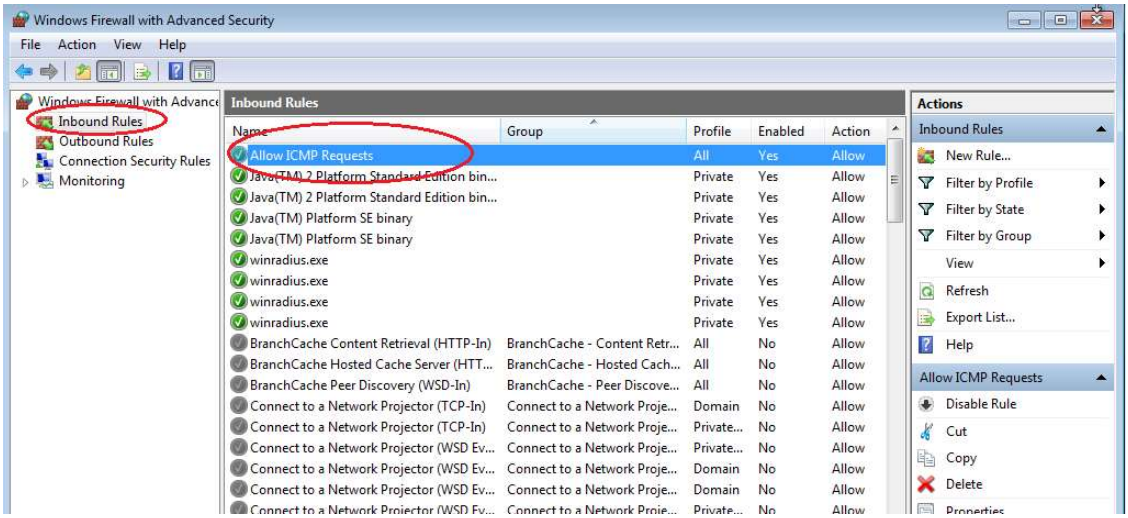


This new rule should allow your team members to receive ping replies from your PC.

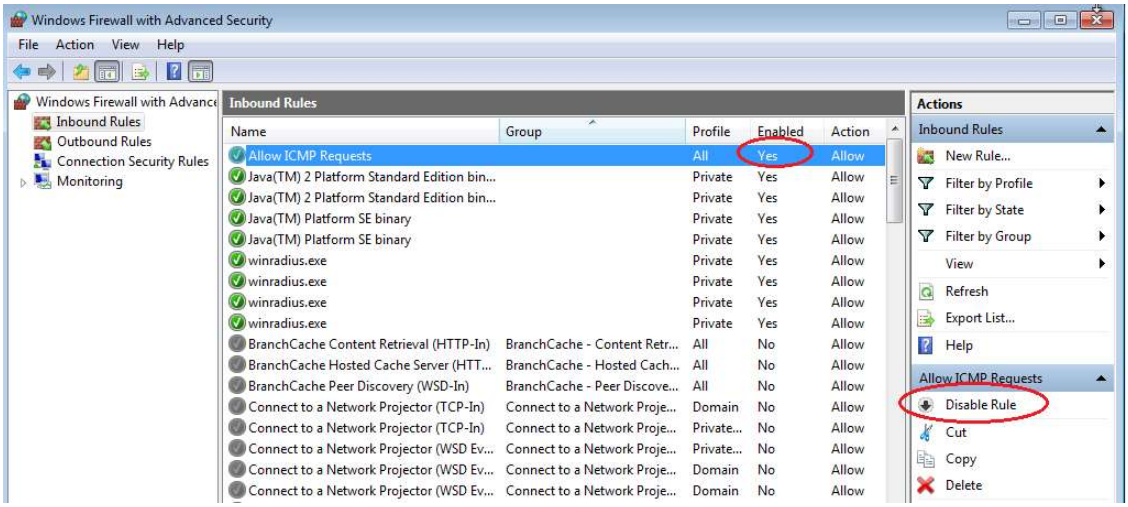
Step 2: Disabling or deleting the new ICMP rule.

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.

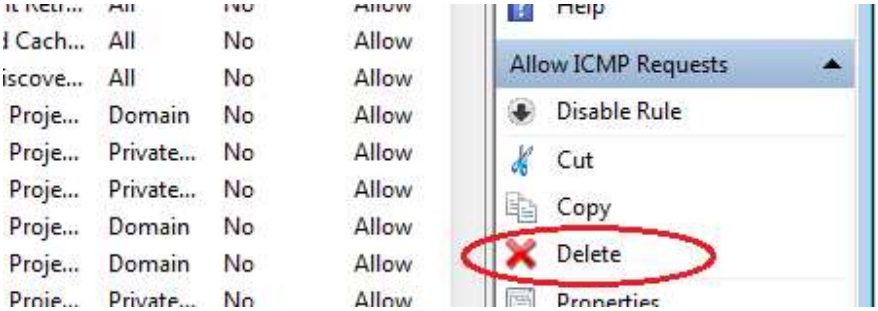
a. On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created in Step 1.



b. To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between **Disable Rule** and **Enable Rule**; the status of the rule also shows in the **Enabled** column of the **Inbound Rules** list.

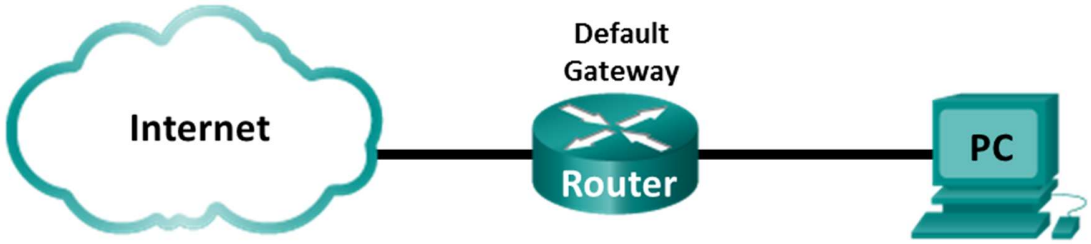


c. To permanently delete the ICMP rule, click **Delete**. If you choose this option, you must re-create the rule again to allow ICMP replies.



Lab – Using Wireshark to Examine Ethernet Frames

Topology



Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access with Wireshark installed)

Part 1: Examine the Header Fields in an Ethernet II Frame

In Part 1, you will examine the header fields and content in an Ethernet II frame. A Wireshark capture will be used to examine the contents in those fields.

Step 1: Review the Ethernet II header field descriptions and lengths.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Step 2: Examine the network configuration of the PC.

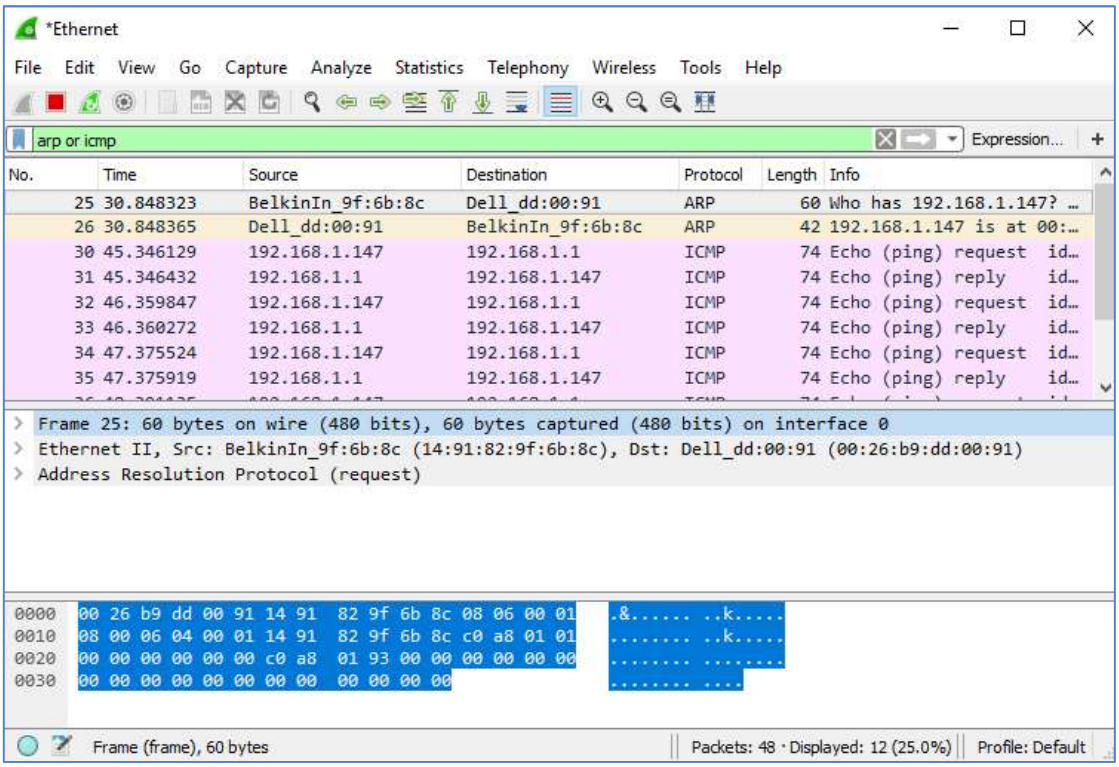
This PC host IP address is 192.168.1.147 and the default gateway has an IP address of 192.168.1.1.

```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C73CB0M
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82577LM Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-26-B9-DD-00-91
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

Step 3: Examine Ethernet frames in a Wireshark capture.

The Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The

session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.



Step 4: Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, `0-9,A-F`. A common format is `12:34:56:78:9A:BC`. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Source Address	BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are these: Value Description `0x0800` IPv4 Protocol `0x0806` Address Resolution Protocol (ARP)
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver.

What is significant about the contents of the destination address field?

_____

_____

Why does the PC send out a broadcast ARP prior to sending the first ping request?

_____

_____

_____

What is the MAC address of the source in the first frame? _____

What is the Vendor ID (OUI) of the Source NIC? _____

What portion of the MAC address is the OUI?

_____

What is the NIC serial number of the source? _____

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

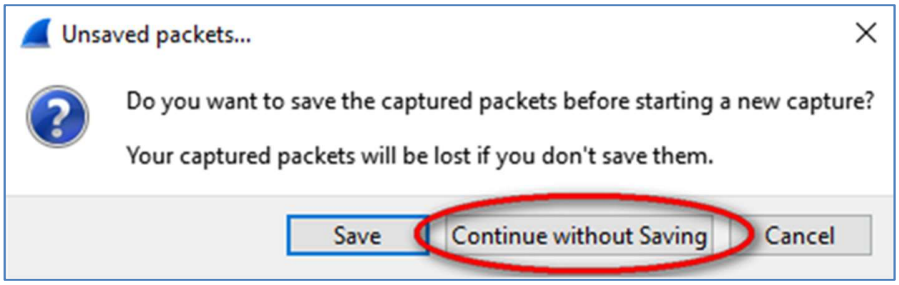
Step 1: Determine the IP address of the default gateway on your PC.

Open a command prompt window and issue the **ipconfig** command.

What is the IP address of the PC default gateway? _____

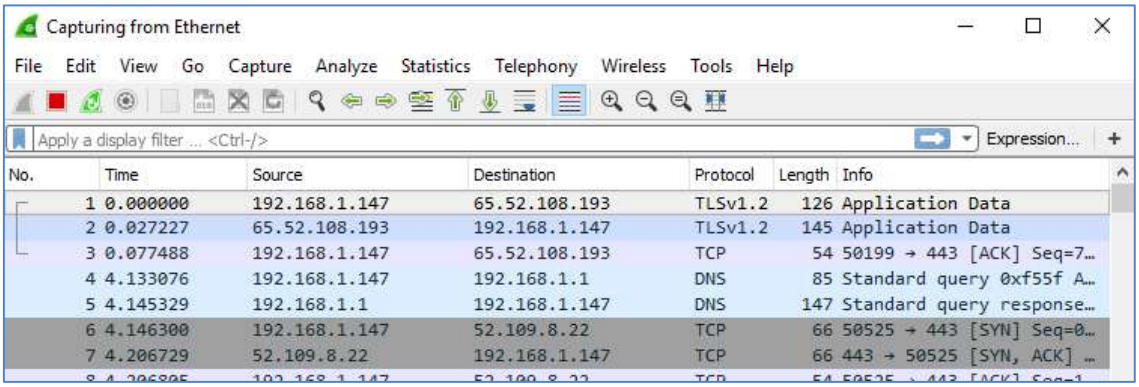
Step 2: Start capturing traffic on your PC NIC.

a. Close Wireshark. No need to save the captured data.



b. Open Wireshark, start data capture.

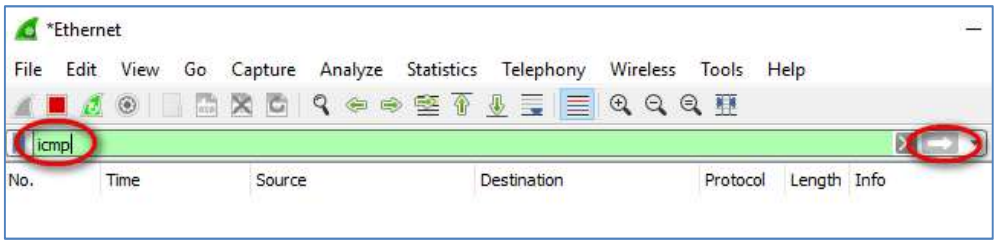
c. Observe the traffic that appears in the packet list window.



Step 3: Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** (the right arrow) to apply the filter.

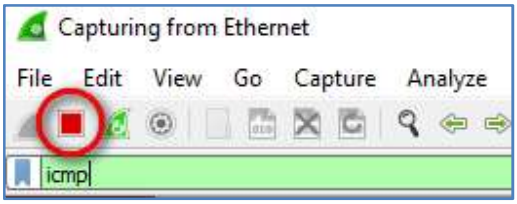


Step 4: From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

Step 5: Stop capturing traffic on the NIC.

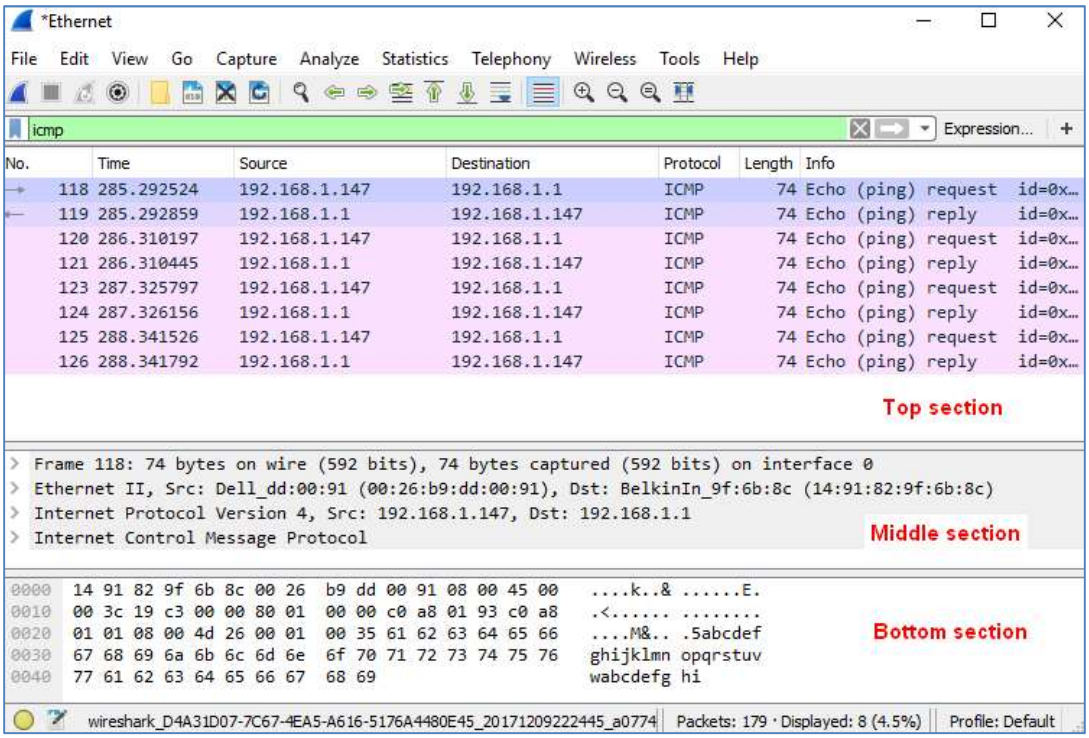
Click the **Stop Capture** icon to stop capturing traffic.



Step 6: Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the packet list pane (top), the **Packet Details** pane (middle), and the **Packet Bytes** pane (bottom). If you selected the correct interface for packet capturing in

Step 3, Wireshark should display the ICMP information in the packet list pane of Wireshark, similar to the following example.



a. In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.

b. Examine the first line in the packet details pane (middle section). This line displays the length of the frame; 74 bytes in this example.

c. The second line in the packet details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC NIC? _____

What is the default gateway's MAC address? _____

d. You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

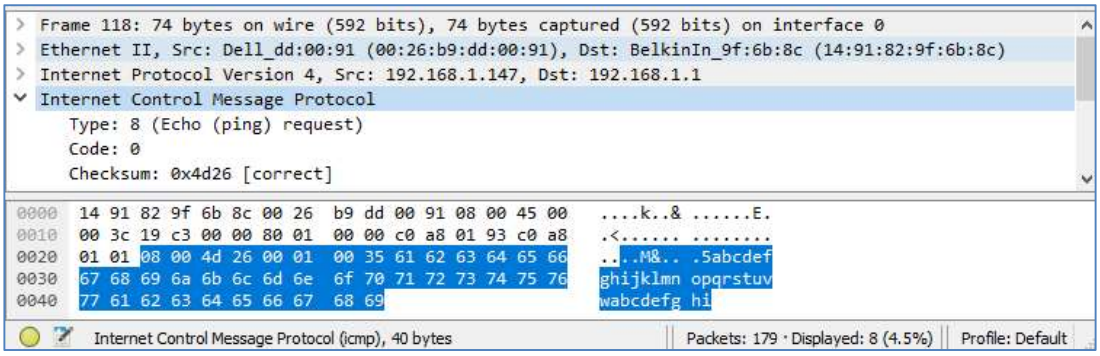
What type of frame is displayed? _____

e. The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address? _____

What is the destination IP address? _____

f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the **Packet Bytes** pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the **Packet Bytes** pane.



What do the last two highlighted octets spell? _____

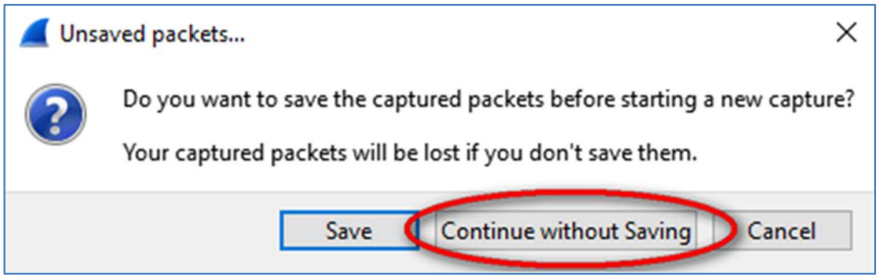
g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?

_____

Step 7: Restart packet capture in Wireshark.

Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.



Step 8: In the command prompt window, ping www.cisco.com.

Step 9: Stop capturing packets.

Step 10: Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source: _____

Destination: _____

What are the source and destination IP addresses contained in the data field of the frame?

Source: _____

Destination: _____

Compare these addresses to the addresses you received in Step 6. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

_____

_____

_____

_____

Reflection

Wireshark does not display the preamble field of a frame header. What does the preamble contain?

_____

_____

_____