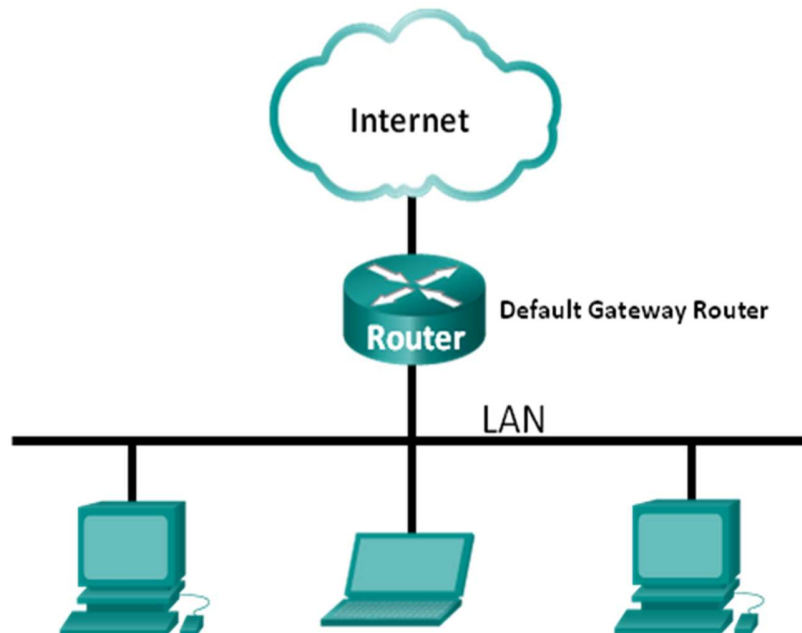


Lab - Using Wireshark to View Network Traffic

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.

Lab - Using Wireshark to View Network Traffic

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.

- Open a command window, type **ipconfig /all**, and then press Enter.
- 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::d009: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
```

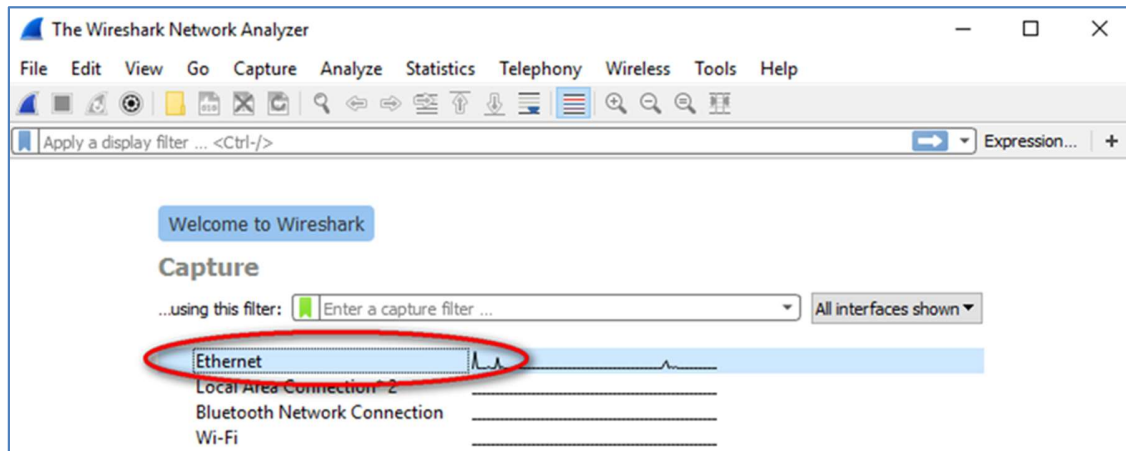
- Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

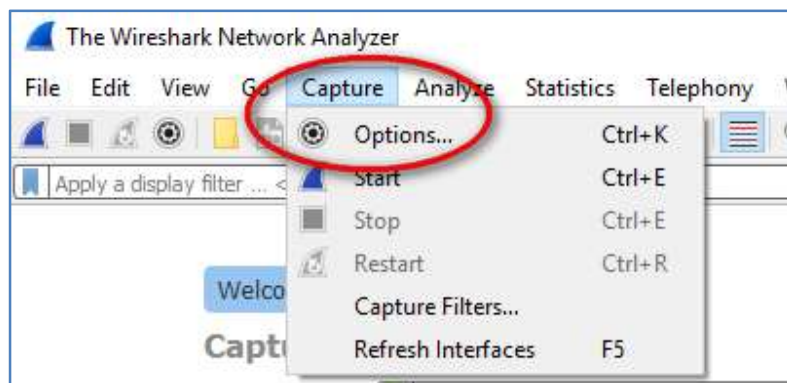
- On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

Lab - Using Wireshark to View Network Traffic

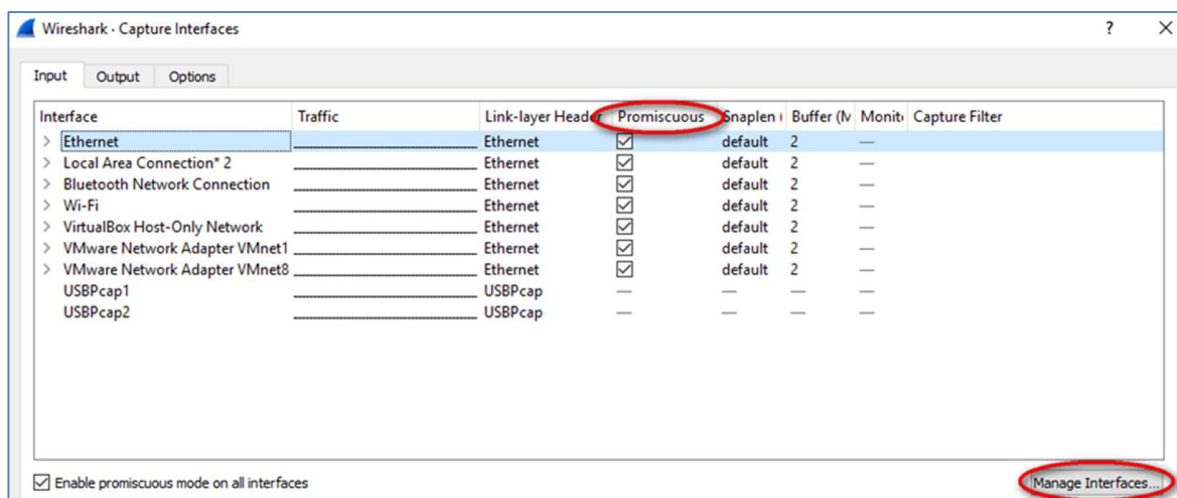
- b. After Wireshark starts, click the capture interface to be used. Because we are using the wired Ethernet connection on the PC, make sure the Ethernet option is on the top of the list.



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

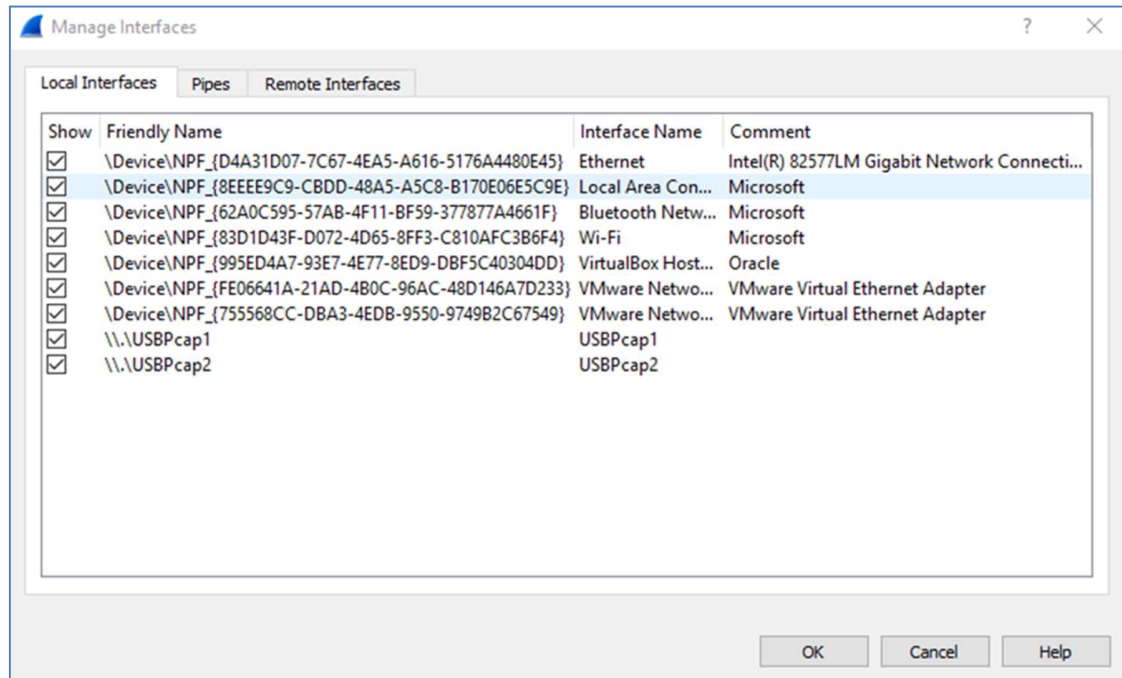


- c. A list of interfaces will display. Make sure the capture interface is checked under **Promiscuous**.

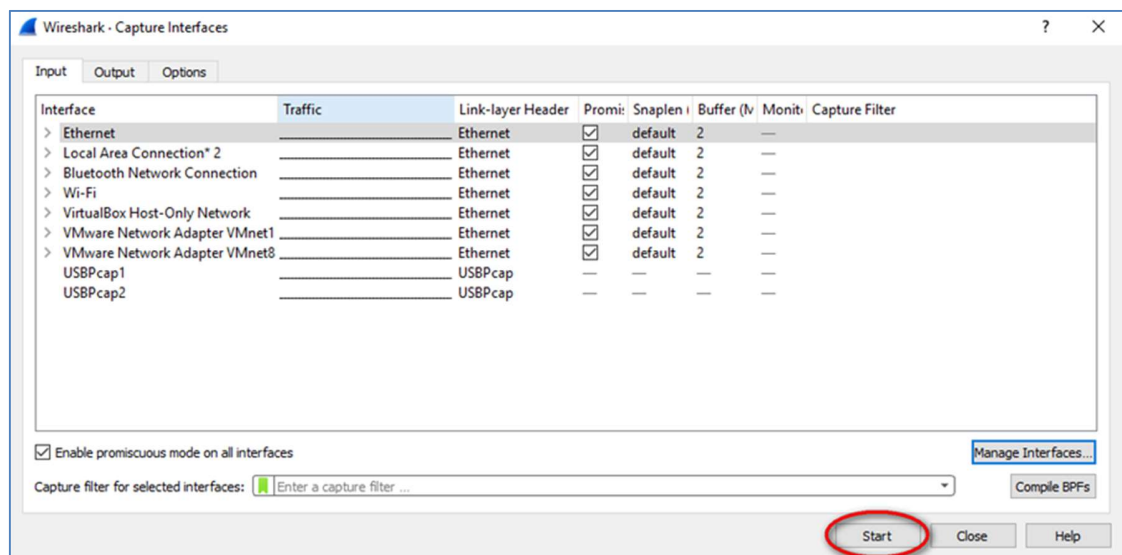


Lab - Using Wireshark to View Network Traffic

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.

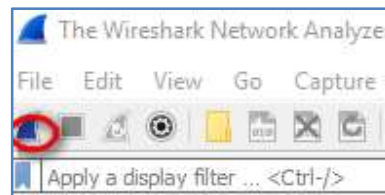


- d. After you have checked the correct interface, click **Start** to start the data capture.

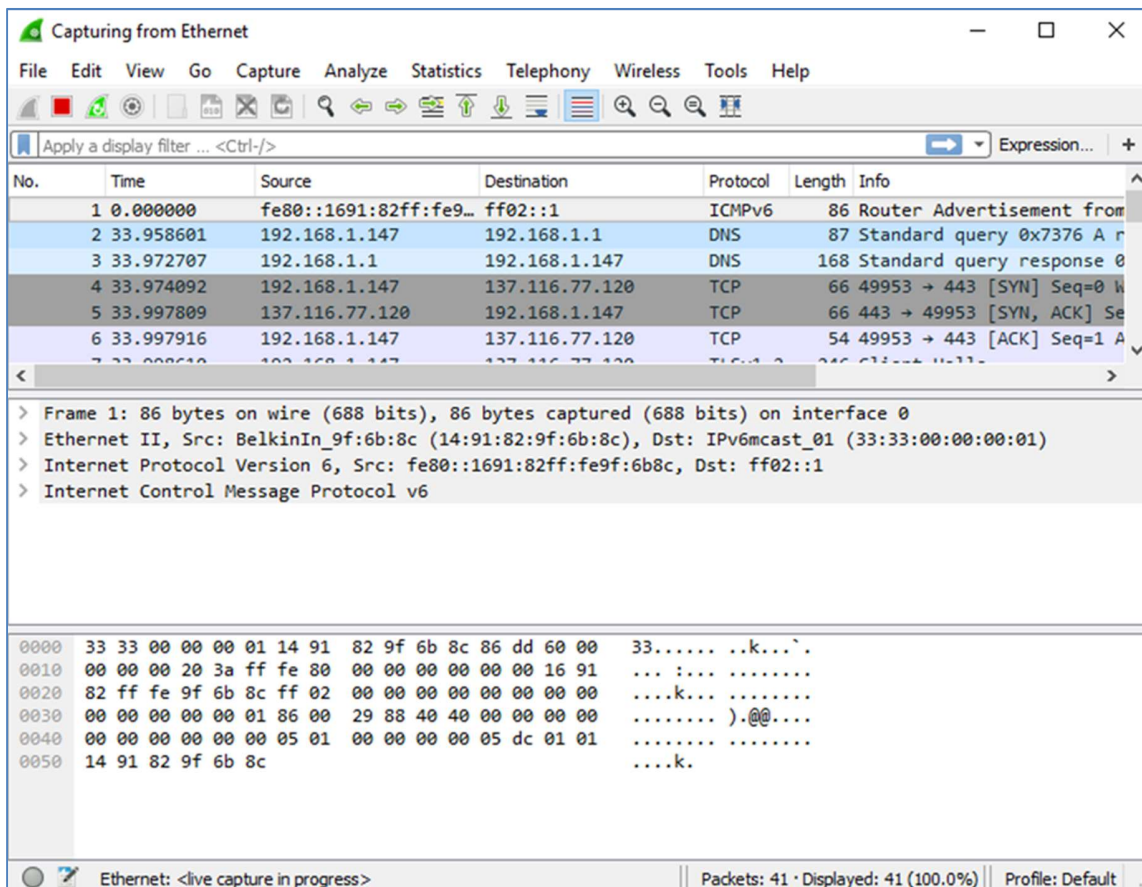


Lab - Using Wireshark to View Network Traffic

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



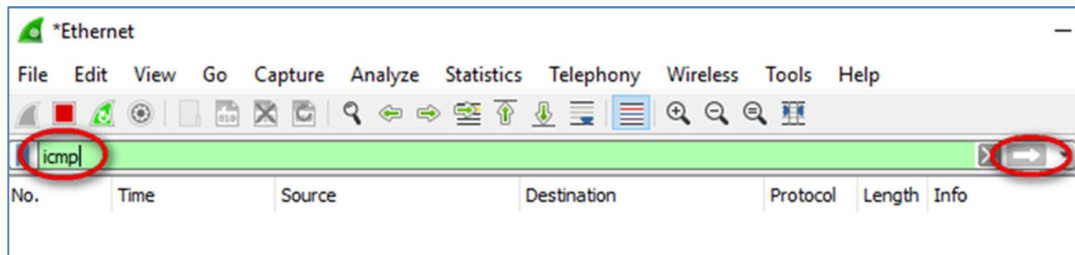
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



- 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

Lab - Using Wireshark to View Network Traffic

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.

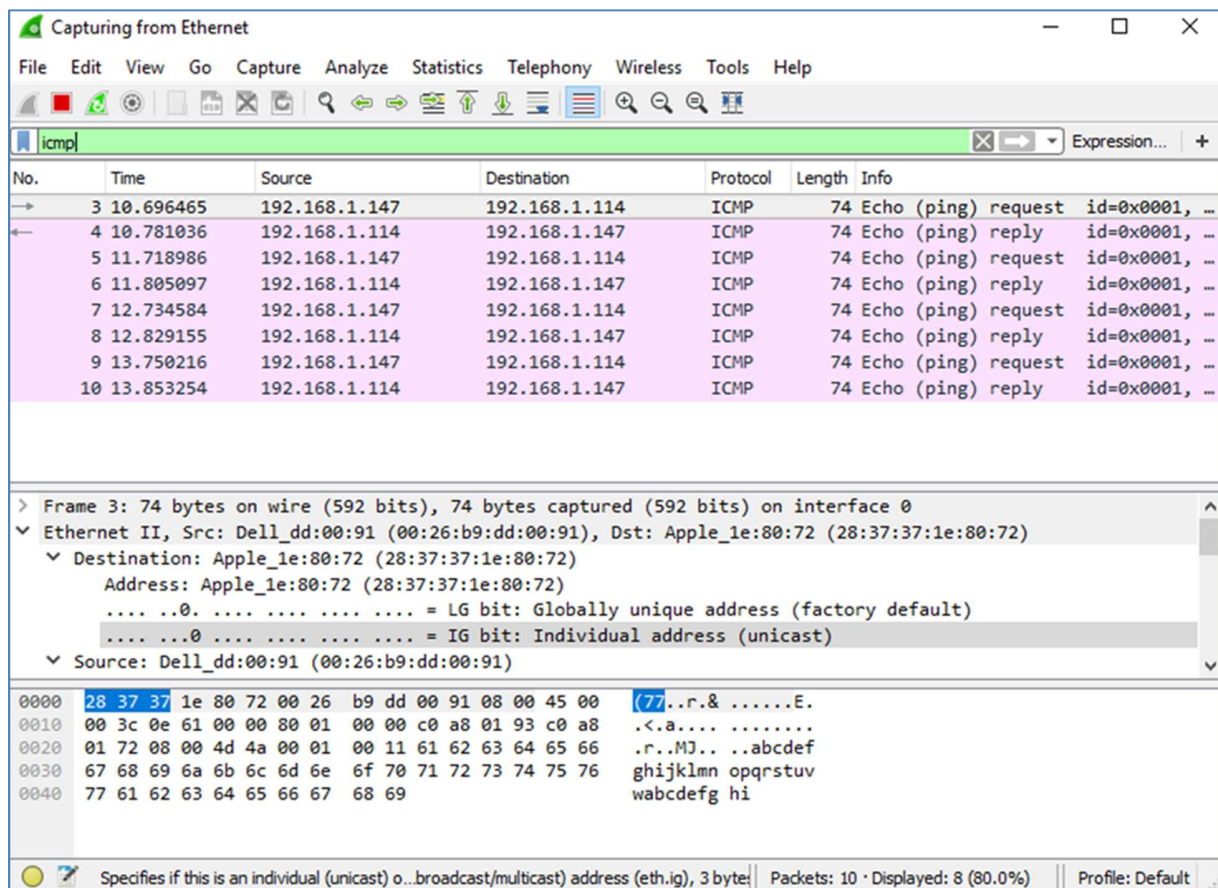
C:\> ping 192.168.1.114

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
```

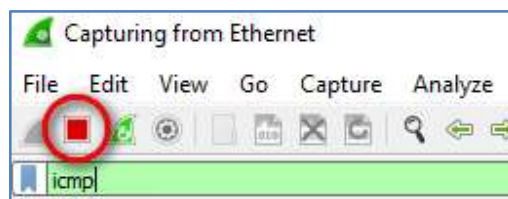

Lab - Using Wireshark to View Network Traffic

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.

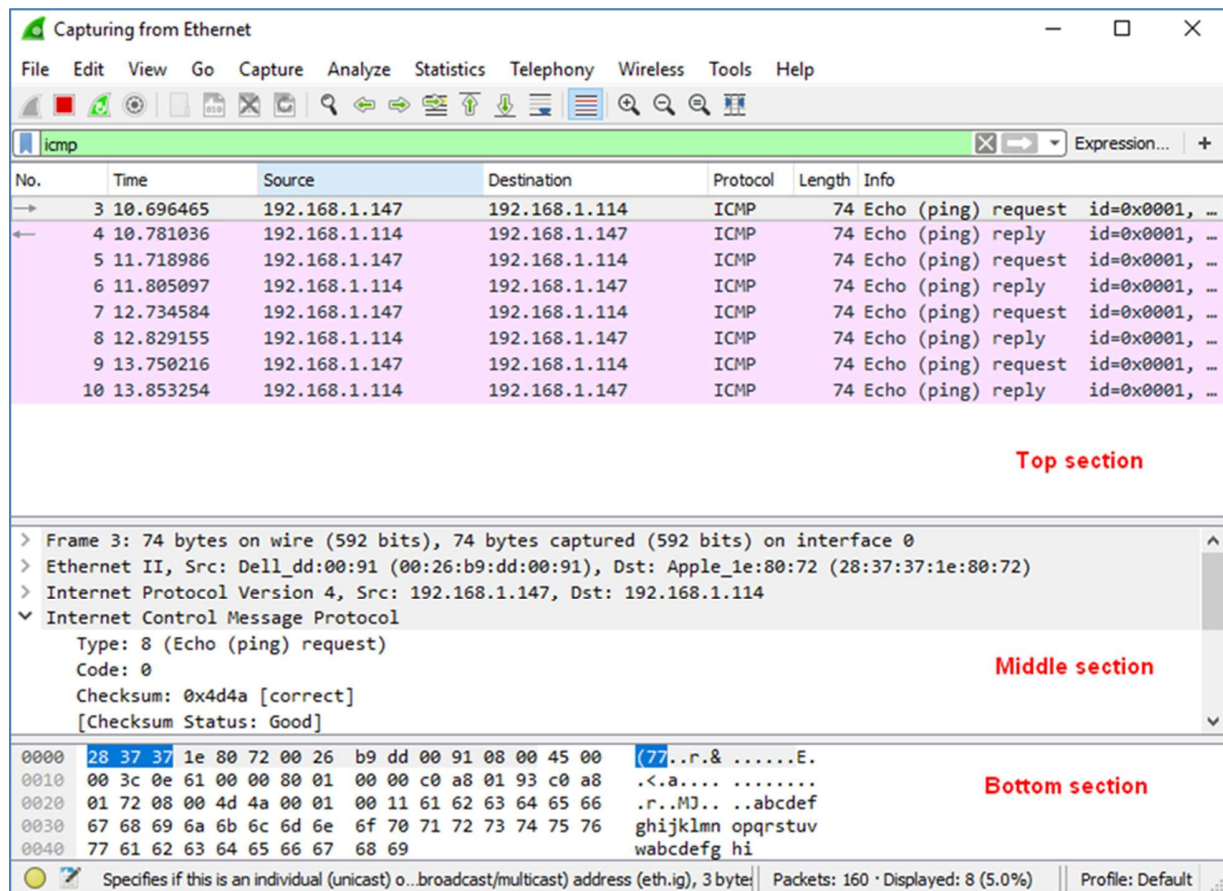


Step 3: Examine the captured data.

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

Lab - Using Wireshark to View Network Traffic

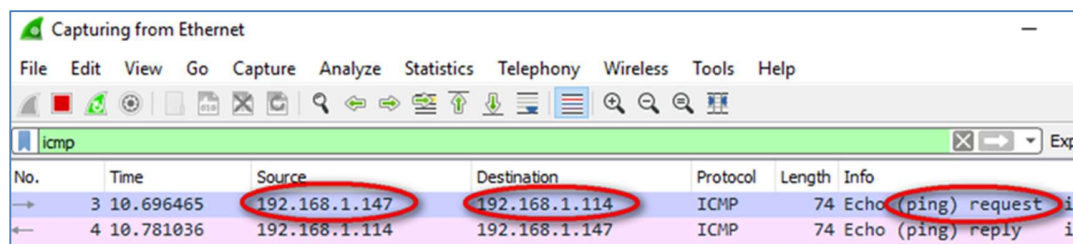
in the top part of the screen and separates a captured PDU frame by its protocol layers; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.



The screenshot shows the Wireshark interface with the following sections:

- Top section:** A list of captured packets. The first packet (No. 3) is selected, showing it is an ICMP Echo (ping) request from 192.168.1.147 to 192.168.1.114.
- Middle section:** The details pane for the selected packet (Frame 3). It shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) details, including the type (Echo (ping) request), code (0), and checksum (0x4d4a).
- Bottom section:** The raw data of the packet, displayed in hexadecimal and decimal form. The decimal data shows the ASCII string "77..r.&.....E."

- 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.

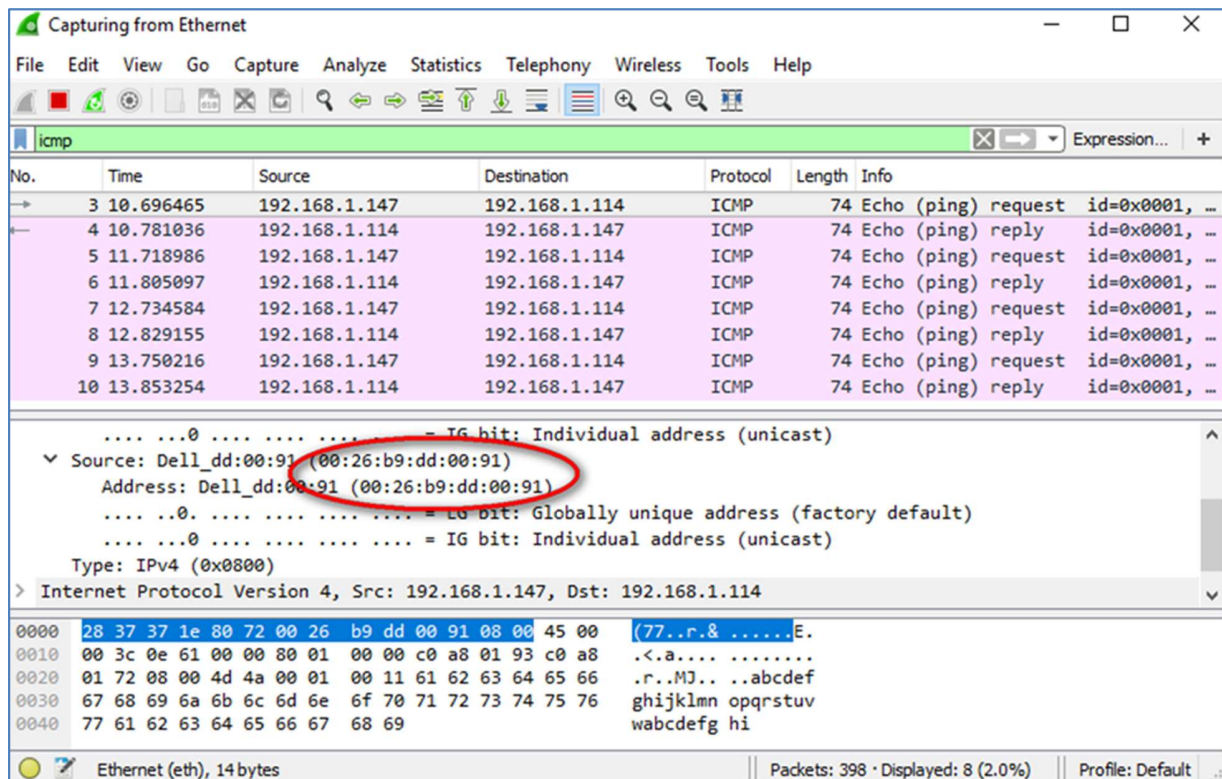


The screenshot shows the Wireshark interface with the following sections:

- Top section:** A list of captured packets. The first packet (No. 3) is selected, showing it is an ICMP Echo (ping) request from 192.168.1.147 to 192.168.1.114.

Lab - Using 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.



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? _____

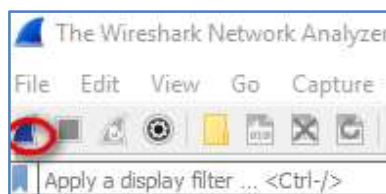
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

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.

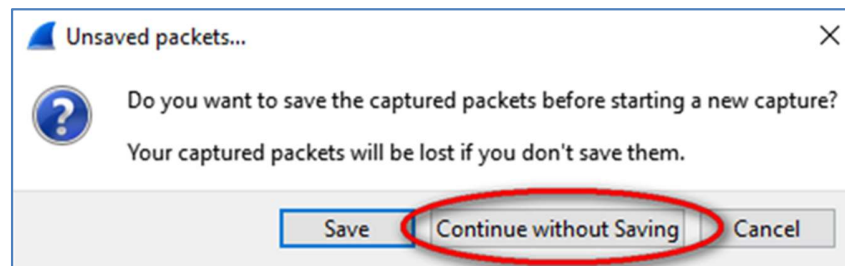
Step 1: Start capturing data on the interface.

- a. Start the data capture again.



Lab - Using Wireshark to View Network Traffic

- 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

Lab - Using Wireshark to View Network Traffic

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

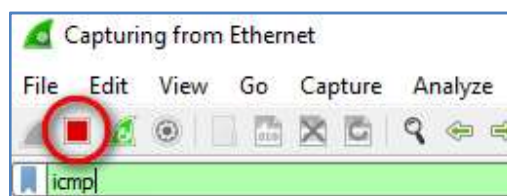
Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

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.



Lab - Using Wireshark to View Network Traffic

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.

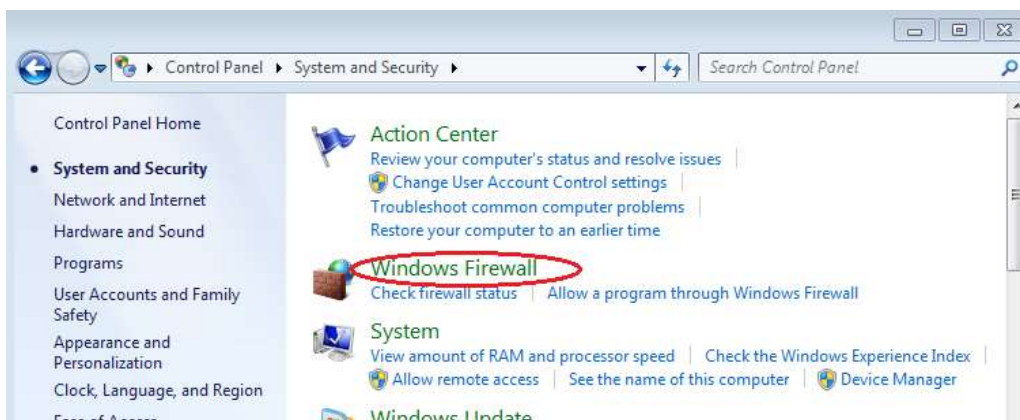
Step 1: Create a new inbound rule allowing ICMP traffic through the firewall.

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



Lab - Using Wireshark to View Network Traffic

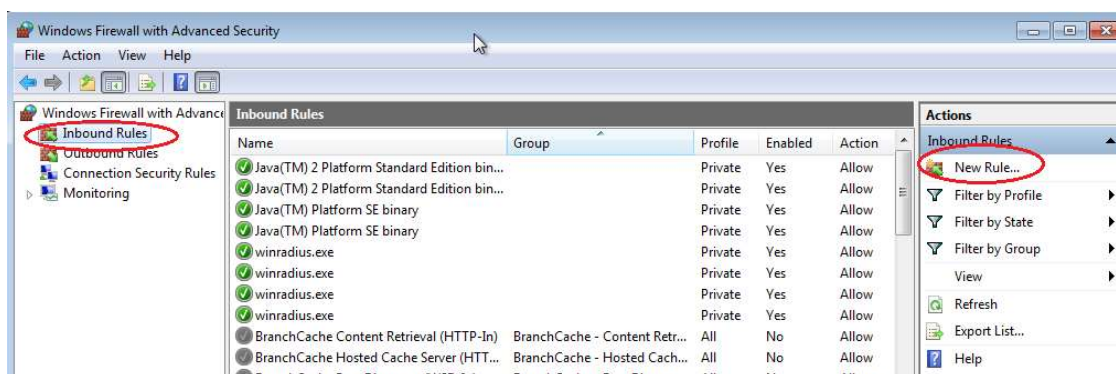
- b. From the **System and Security** window, click **Windows Firewall**.



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

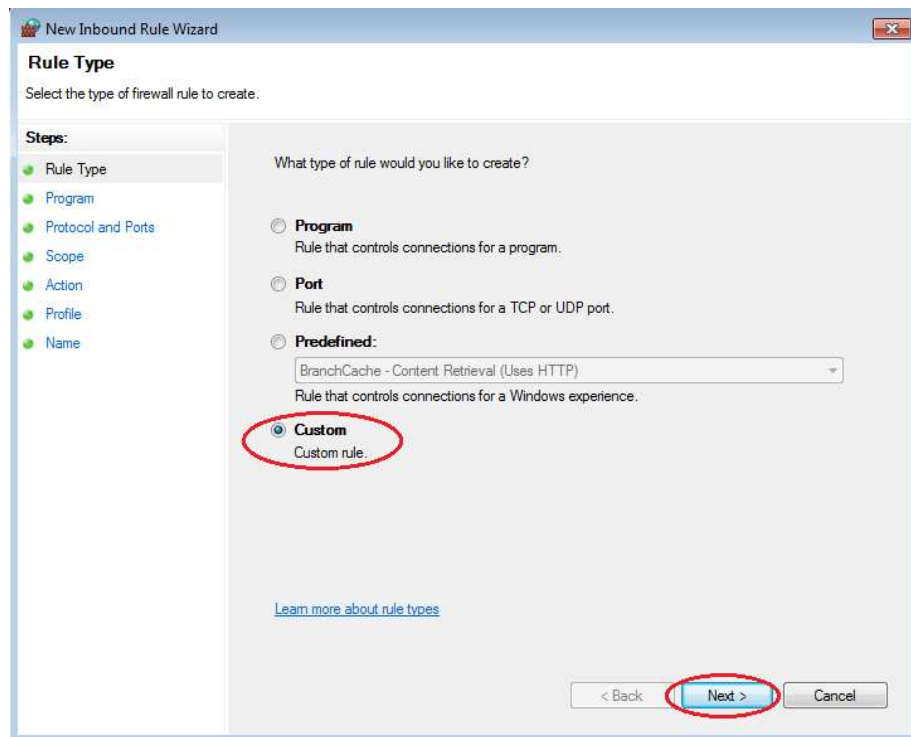


- d. On the **Advanced Security** window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.

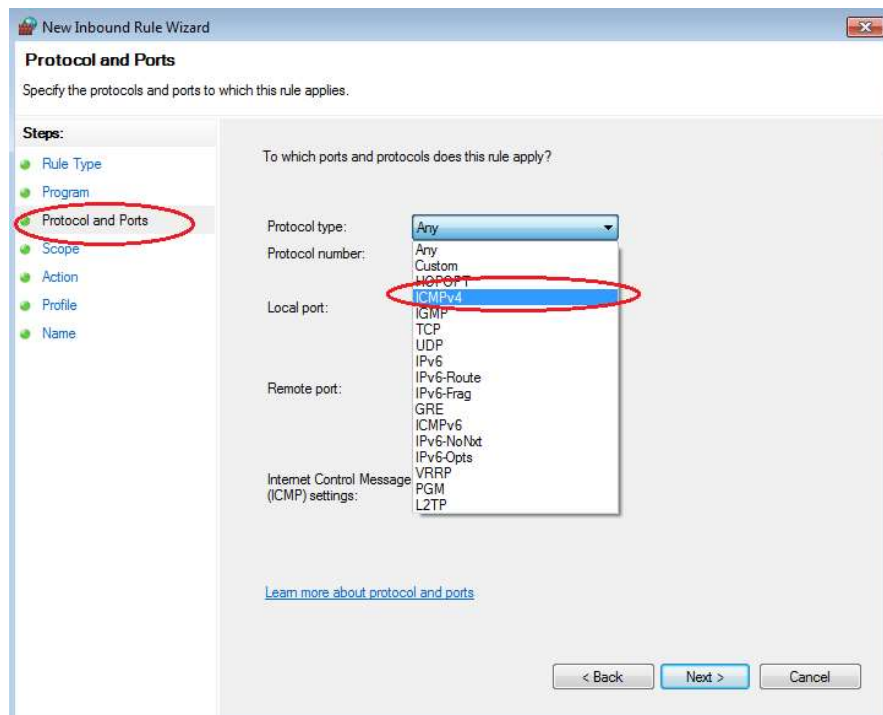


Lab - Using Wireshark to View Network Traffic

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

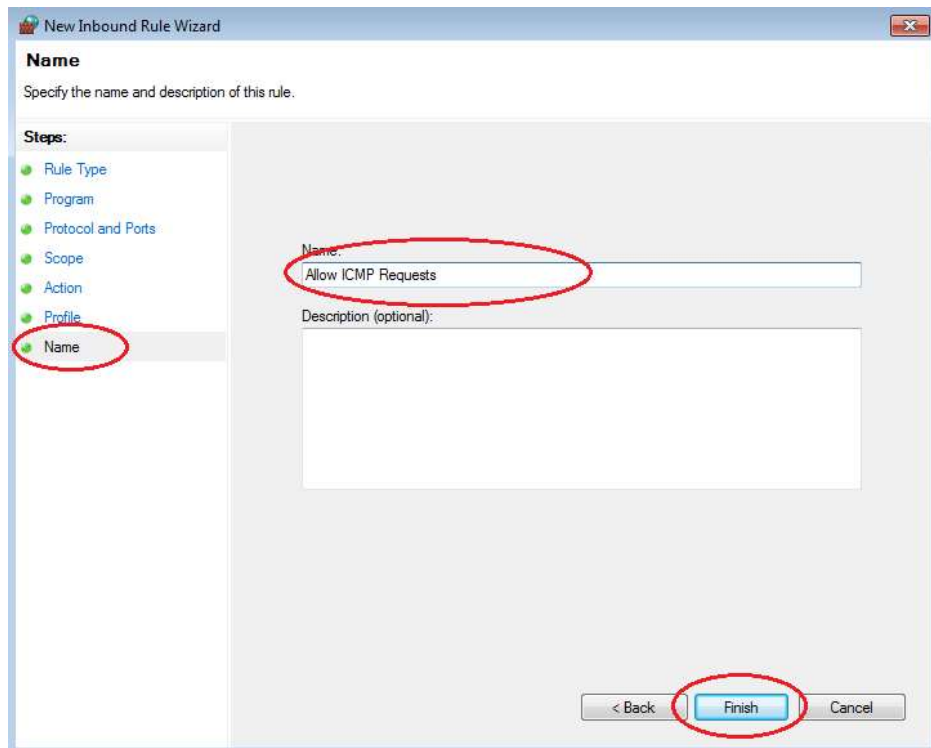


- f. In the left pane, click the **Protocol and Ports** option and using the **Protocol Type** drop-down menu, select **ICMPv4**, and then click **Next**.



Lab - Using Wireshark to View Network Traffic

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

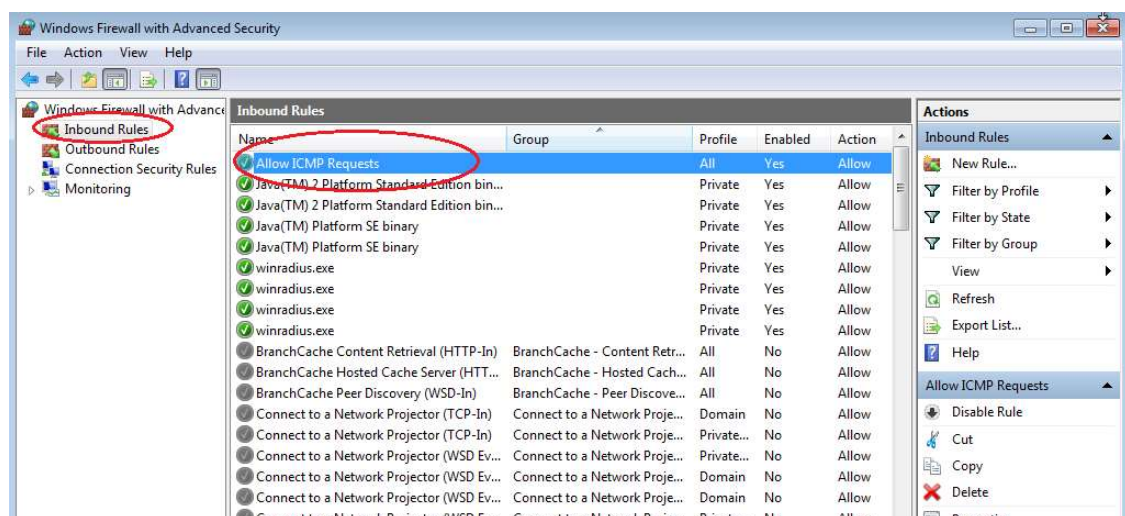


This new rule should allow your team members to receive ping replies from your PC.

Step 2: Disabling or deleting the new ICMP rule.

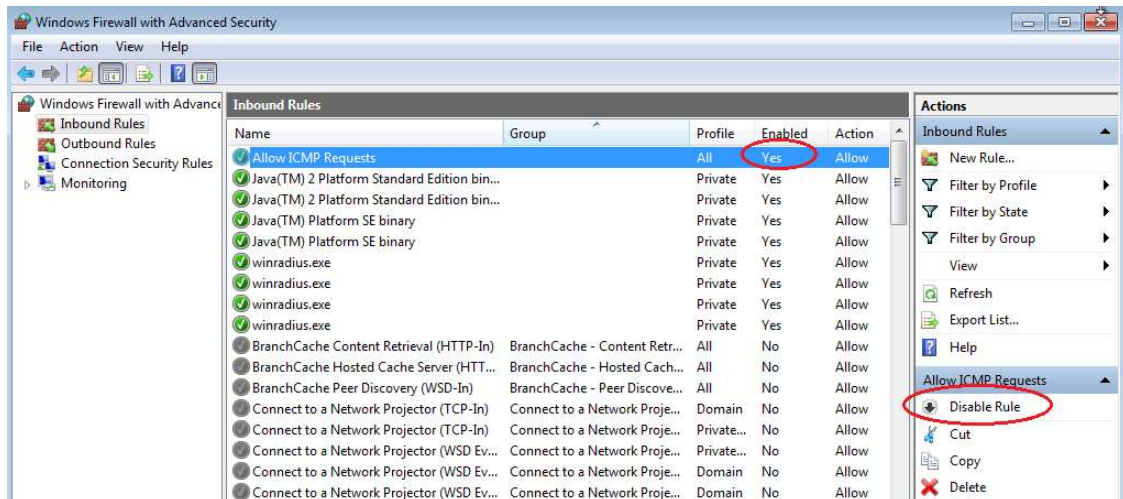
After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of inbound rules.

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



Lab - Using Wireshark to View Network Traffic

- 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.

