**Computer Networks**

**Problem-solving session 3**

**Install and Use Wireshark to View Network Traffic**

**Objectives:**

Part 1: Download and Install Wireshark

Part 2: Capture and Analyze Local ICMP Data in Wireshark

Part 3: 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 Requests for Comment (RFC), or other specifications. *UCA’s Information Security Manager has already approved the usage of this network listening program* *in the class*.

First, students download and install Wireshark. Then, students capture and analyze ICMP (Internet Control Message Protocol) Data in Wireshark.

**Required resources:**

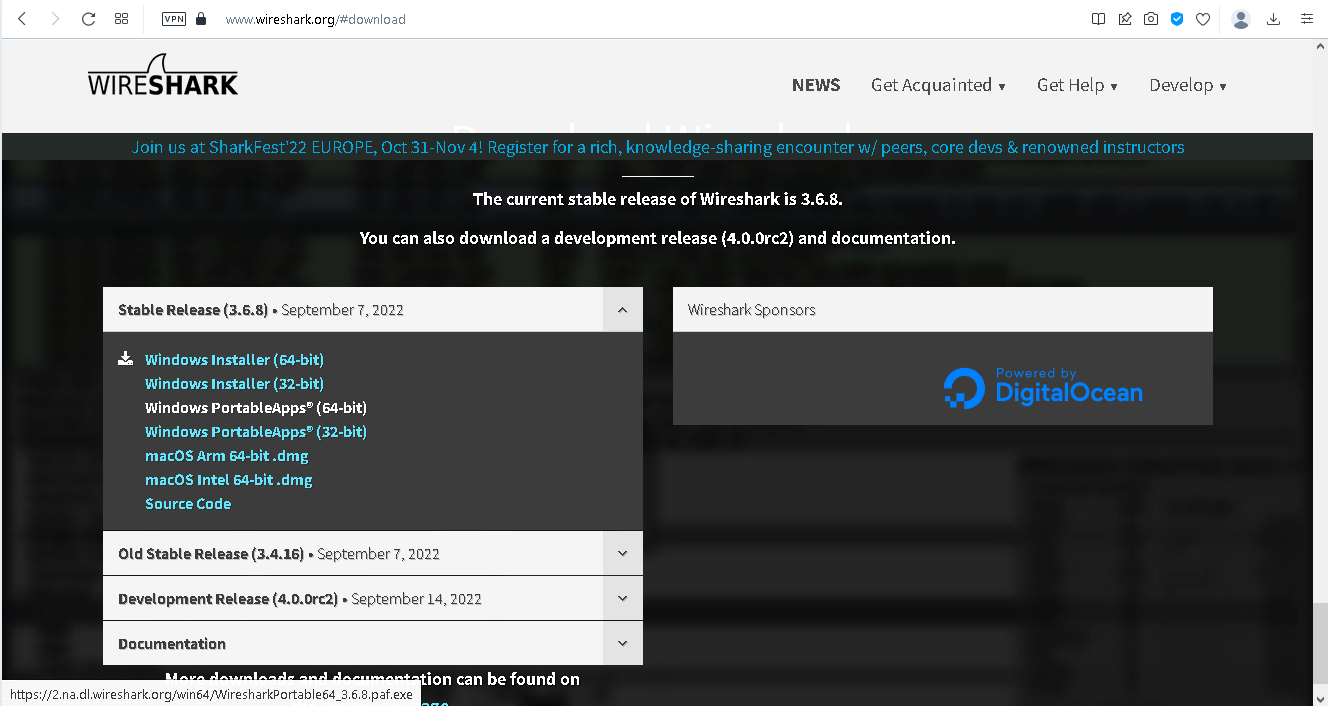
• 1 PC (Windows with internet access)

• Additional PC (the instructor will provide the IP address in the class) on a local-area network (LAN) will be used to reply to ping requests.

**Part 1: Download and Install Wireshark**

**Step 1: Download Wireshark**

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



b. Choose the software version you need based on your PC’s architecture and operating system (it is recommended to use the portable version). 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 if you downloaded the 64bit version. Double-click the file to start the installation process.

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.

b. If this is your first time to install Wireshark, or after you have completed the uninstall process, you will navigate to the Wireshark Setup wizard. Click Next.

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

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

e. Choose your desired shortcut options and click Next.

f. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location. Click Next to continue.

g. To capture live network data, Npcap must be installed on your PC. If Npcap is already installed on your PC, the Install check box will be unchecked. If your installed version of Npcap 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 Npcap x.x.x (version number) check box. Click Next to continue.

h. Do NOT install USBPcap for normal traffic capture. Do NOT select the checkbox to install USBPcap. USBPcap is experimental, and it could cause USB problems on your PC. Click Install to continue.

i. Wireshark starts installing its files and displays the status of the installation.

j. In a separate window, accept the license agreement in the Npcap Setup Wizard if installing Npcap. Click I Agree to continue. Click Install to install Npcap. Click Next to finish the Npcap installation and click Finish to exit the Npcap installation.

k. Click Next when the Wireshark installation is complete.

l. Click Finish to complete the Wireshark install process. Reboot the computer if necessary.

**Part 2: Capture and Analyze Local ICMP Data in Wireshark**

In Part 1 of this work, 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 work, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

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

C:\Users\Student> ipconfig /all

Windows IP Configuration

Host Name . . . . . . . . . . . . : DESKTOP-NB48BTC

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. . . . . . . . . . . : No

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

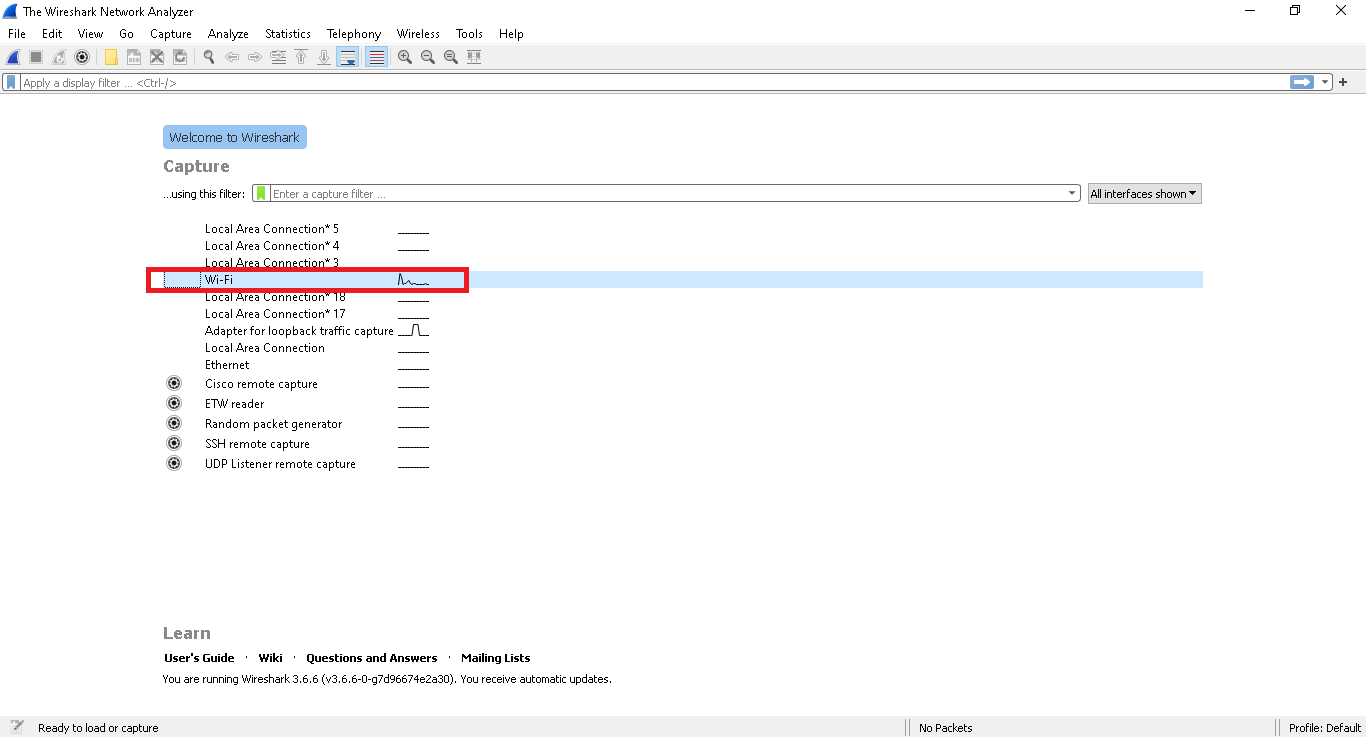
Default Gateway . . . . . . . . . : 192.168.1.1

<output omitted>

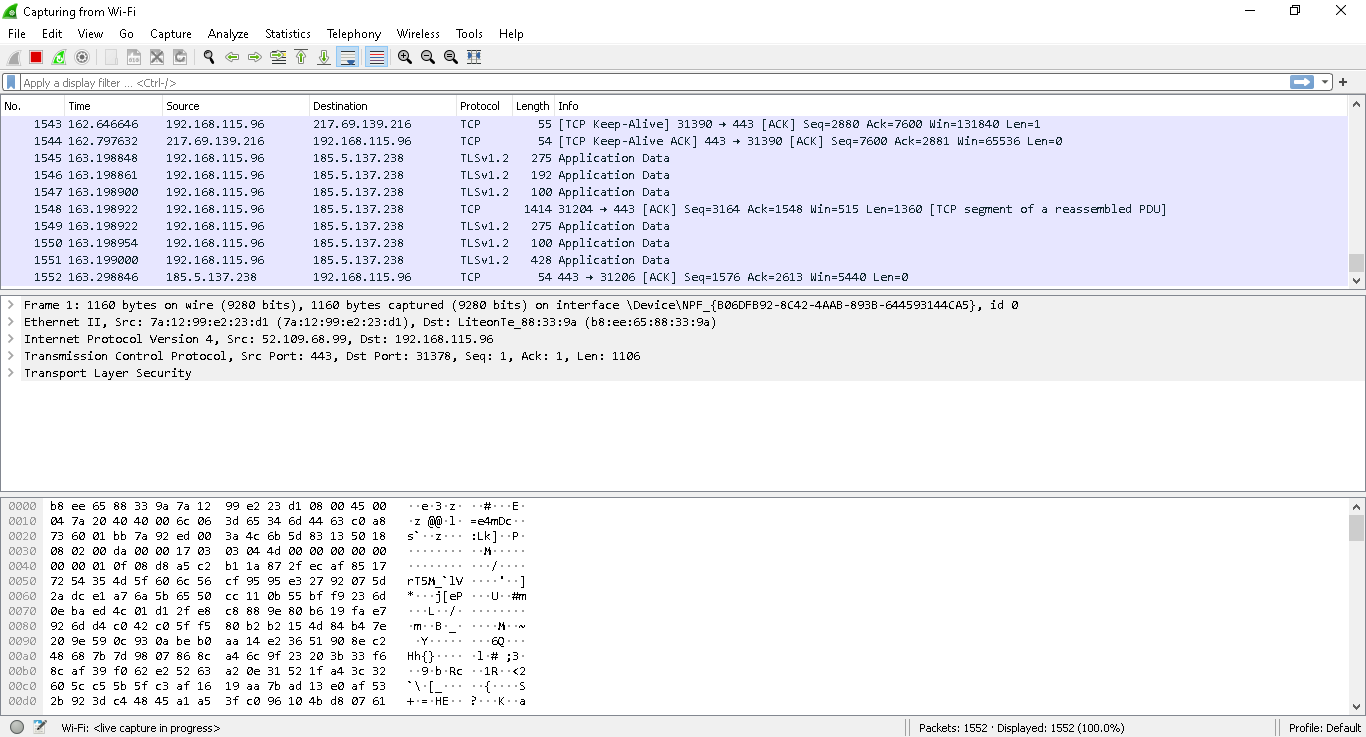
b. Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

**Step 2: Start Wireshark and begin capturing data**

a. Navigate to Wireshark. Double-click the desired interface to start the packet capture. Make sure the desired interface has traffic.

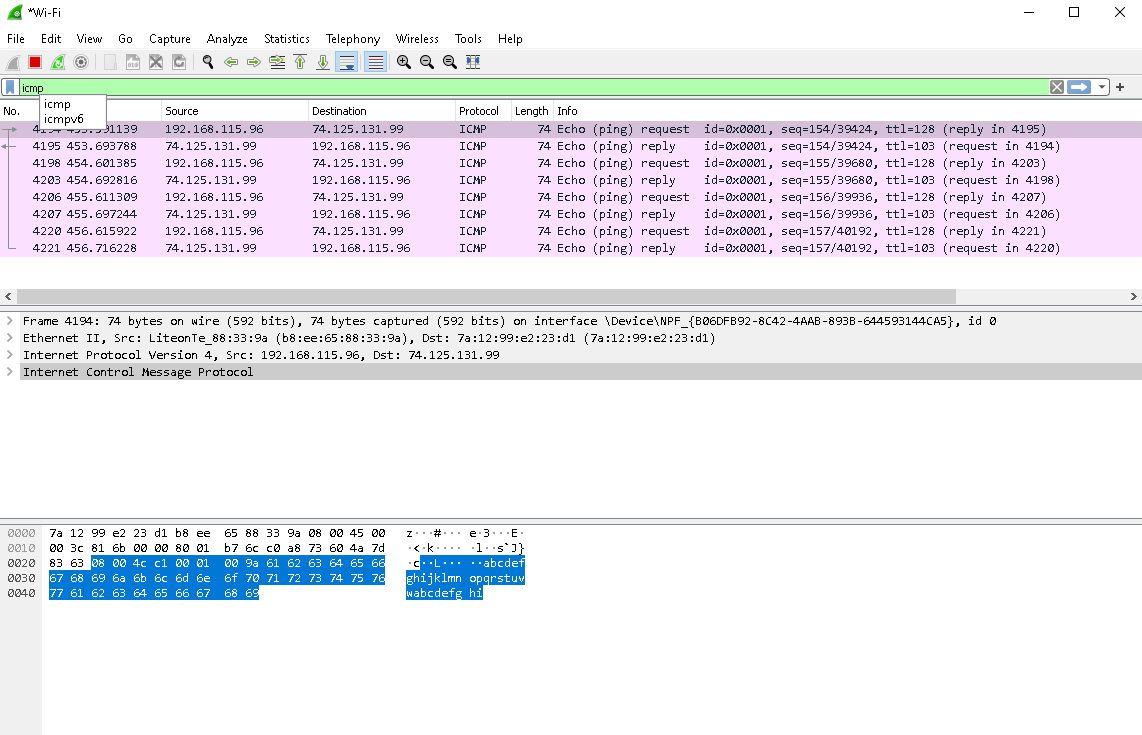


b. Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



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.

For this work, 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 instructor/team member.

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=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

Reply from 192.168.1.114: bytes=32 time<1ms TTL=128

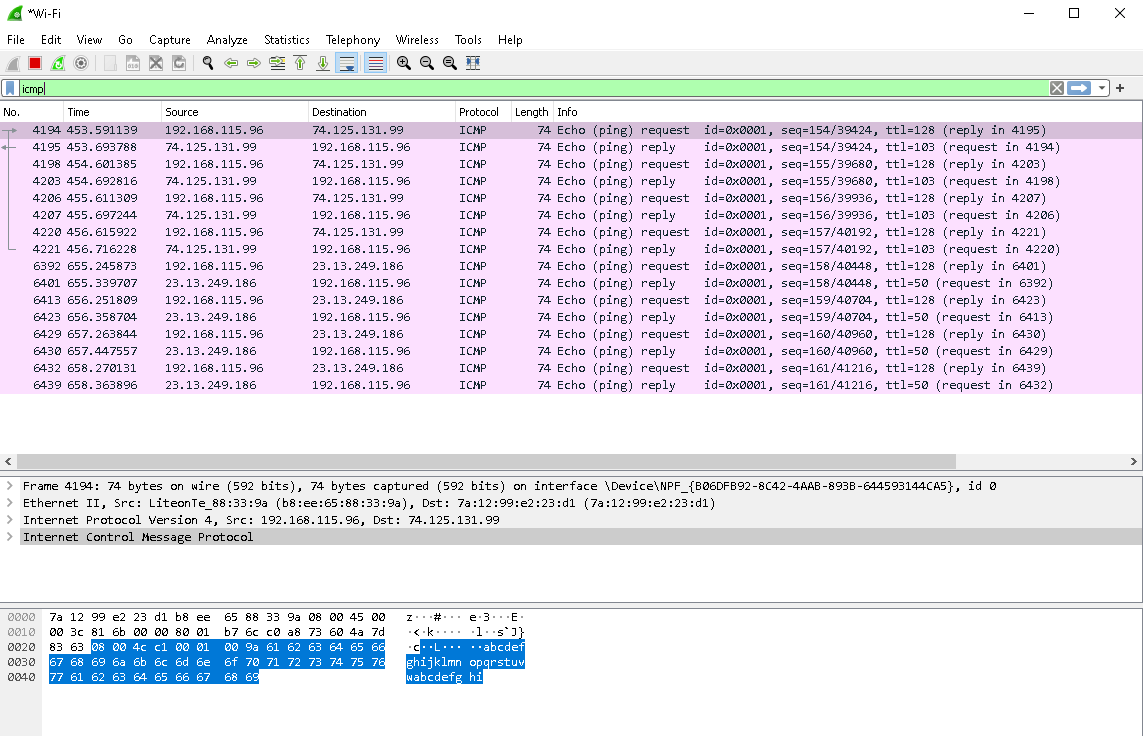
Ping statistics for 192.168.1.114:

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.

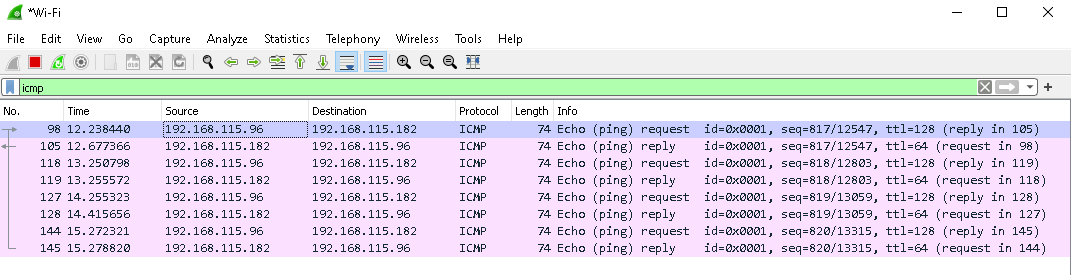


d. Stop capturing data by clicking the Stop Capture icon.

**Step 3: Examine the captured data**

In Step 3, examine the data that was generated by the ping requests of your team member’s 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 forms.

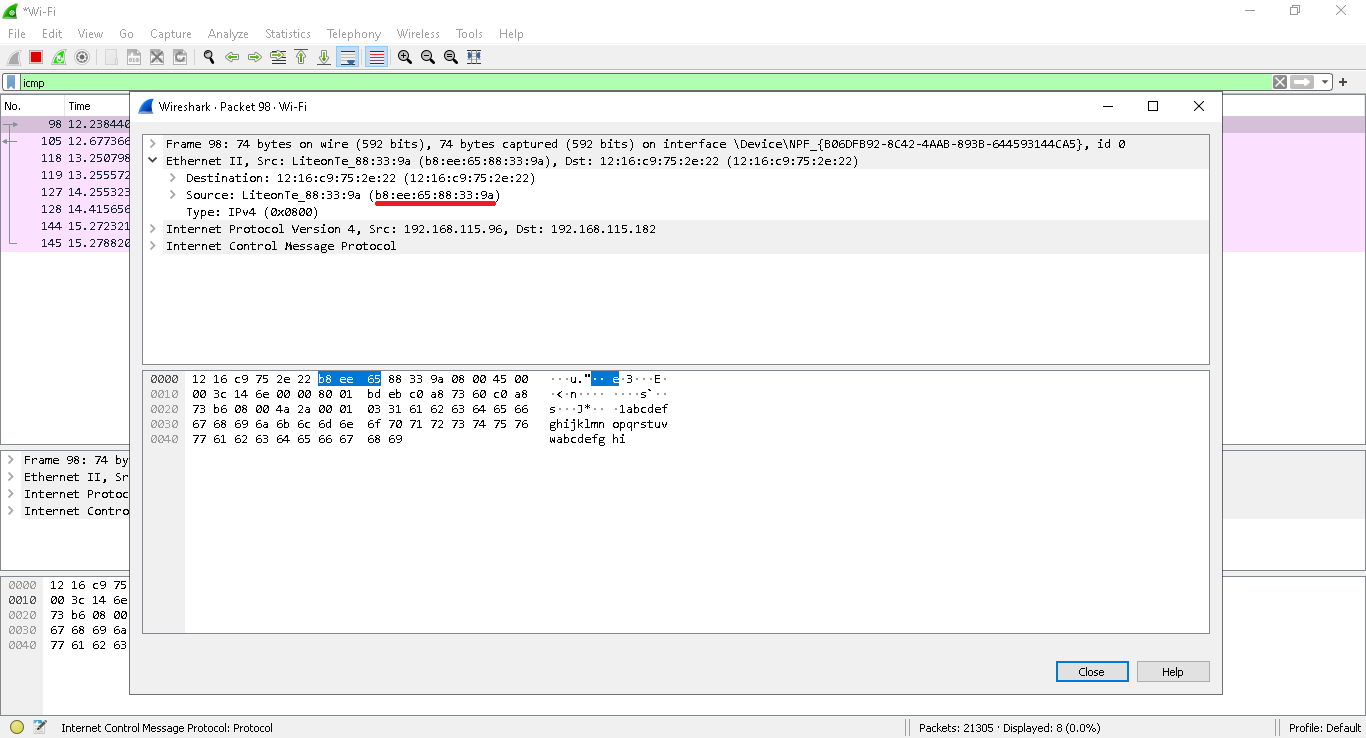
a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC IP address, and the Destination column contains the IP address of the team mate’s PC that you pinged.



If you don’t know the IP address of the teammate, how you can find this IP address? Assume that you are the only two who are connected to the same switch.

Ans: if I have requested then in the destination part I can find the ip address of my teammate. In the source part my ip address will be visible and in destination my teammate’s.

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? **Yes**



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

Ans: Yes

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

Ans: In order to get the MAC address of the PC you're intending to ping, your PC will first check its own ARP cache based on its IP address and see if there are any entries that would indicate a connection to the device that has the correct private IP.

**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 3: Capture and Analyze Remote ICMP Data in Wireshark**

In Part 3, 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 2.

**Step 1: Start capturing data on the interface**

a. Start the data capture again.

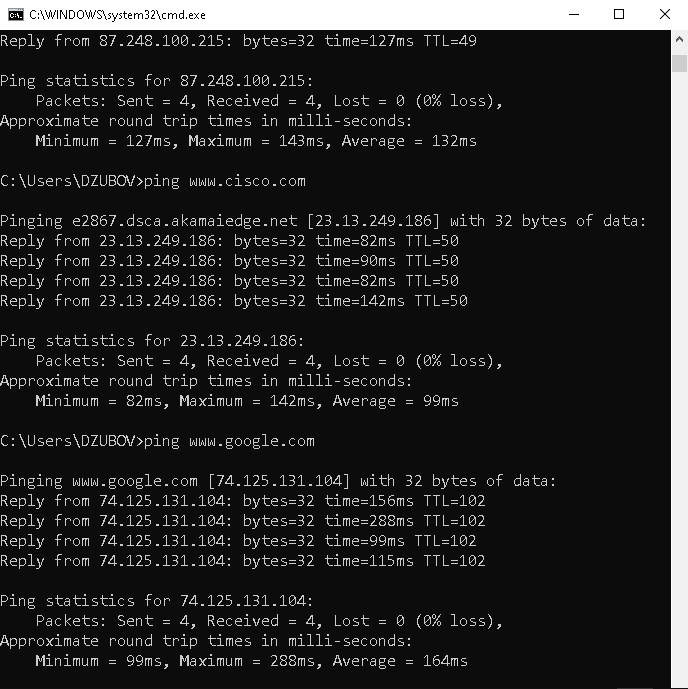
b. A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving.**

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

1) www.yahoo.com

2) www.cisco.com

3) 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.

IP address for **www.yahoo.com:**

Ans: 87.248.100.216

MAC address for **www.yahoo.com:**

Ans: 00:56:2b:35:0e:57

IP address for **www.cisco.com:**

Ans: 23.43.131.231

MAC address for **www.cisco.com:**

Ans: 00:56:2b:35:0e:57

IP address for **www.google.com:**

Ans: 74.125.131.104

MAC address for **www.google.com:**

Ans: Ans: 00:56:2b:35:0e:57

Please describe IP addresses:

Ans: An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network

Please describe MAC addresses:

Ans: A media access control address (MAC address) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

What is significant about this information?

Ans: The MAC addresses for all three locations are the same.

How does this information differ from the local ping information you received in Part 2?

Ans: 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.

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

Ans: 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.