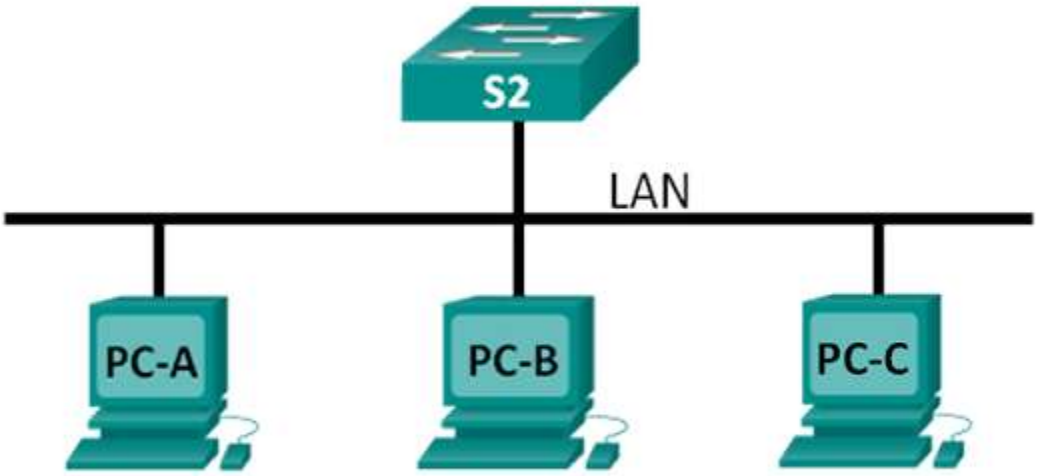
Lab - Using Wireshark to View Network Traffic

This lab has been updated for use on NETLAB+

Topology



Objectives

Capture and Analyze Local 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.

Capture and Analyze Local ICMP Data in Wireshark

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: Configure IP addresses on PC-A, PC-B and PC-C

a. Assign the IP address and subnet mask to the PC's. Use the address's **192.168.1.12**, **192.168.1.13**, **192.168.1.14**. All addresses will use a **24-bit** mask.

1) Click the **Windows Start** icon > **Control Panel**.

2) Click **View By:** > **Category**.

3) Choose **View network status and tasks** > **Change adapter settings**.

4) Right-click **Local Area Network Connection** and select **Properties**.

5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**.

6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

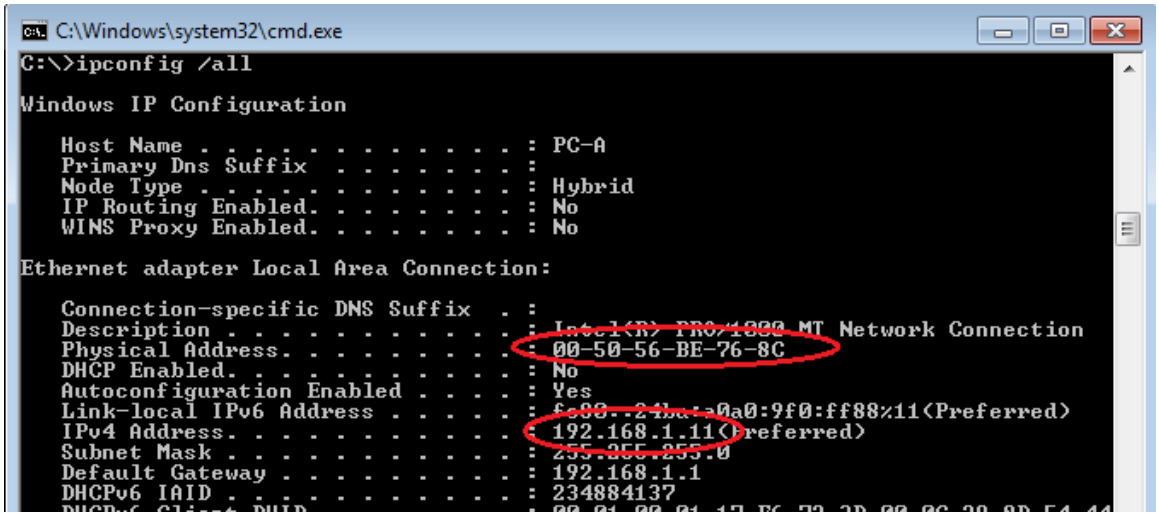
7) Click **OK**.

8) Click **OK** once more.

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

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

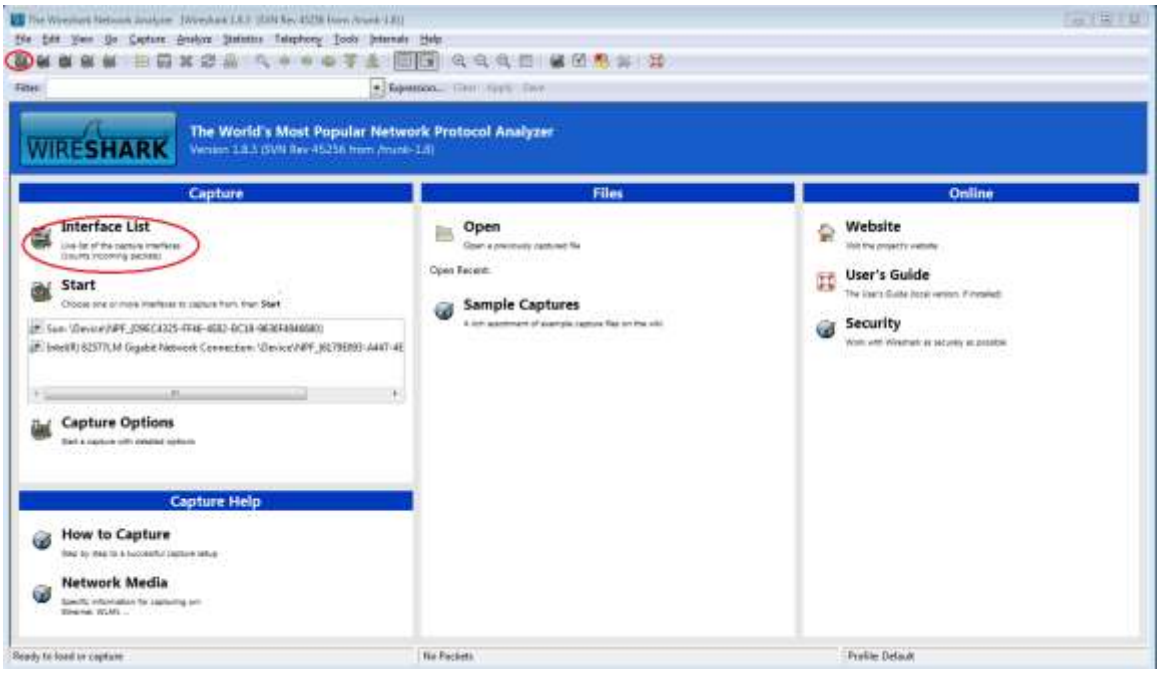
c. Note your PC interface's IP address and MAC (physical) address.



Step 2: Start Wireshark and begin capturing data.

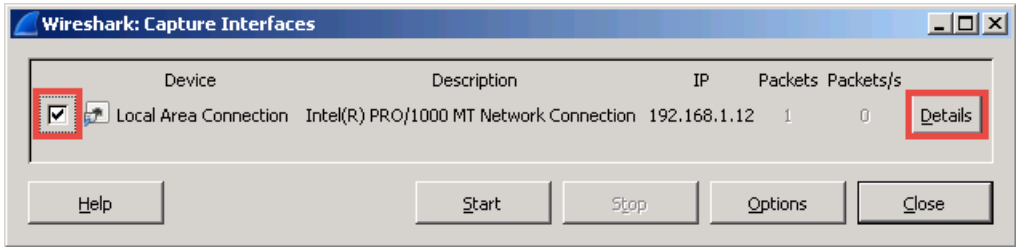
a. On your PC-A, double-click the **Wireshark** icon found on the Desktop.

b. After Wireshark starts, click **Interface List**.

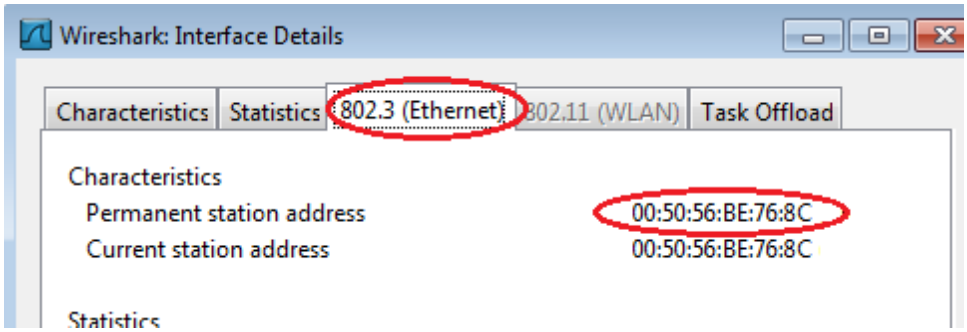


Note: Clicking the first interface icon in the row of icons also opens the Interface List.

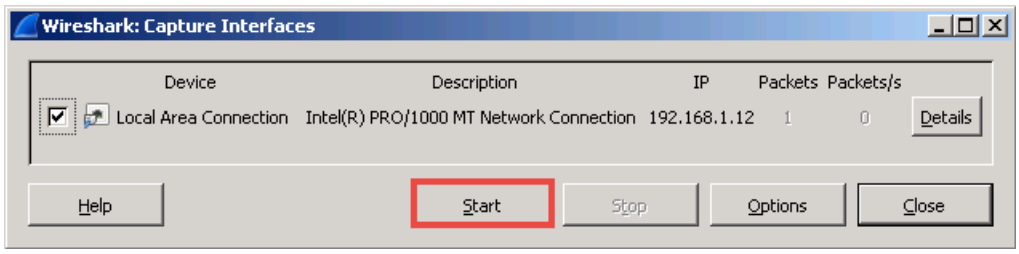
c. On the Wireshark: Capture Interfaces window, make sure the check box next to the interface connected to your LAN is checked.



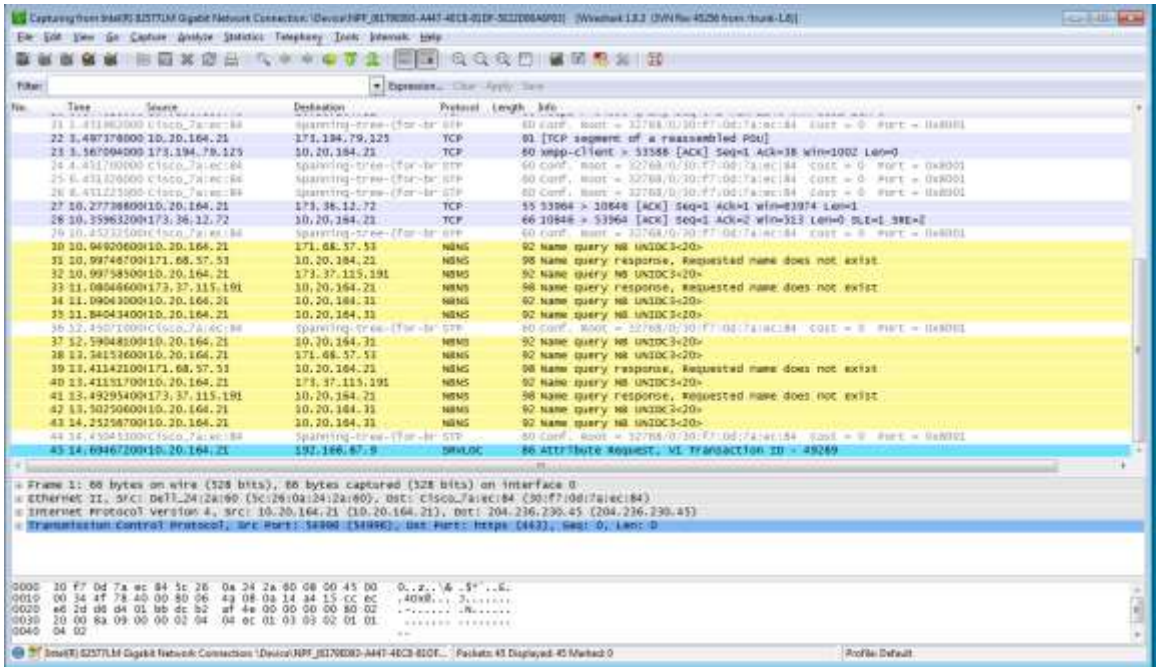
Note: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.



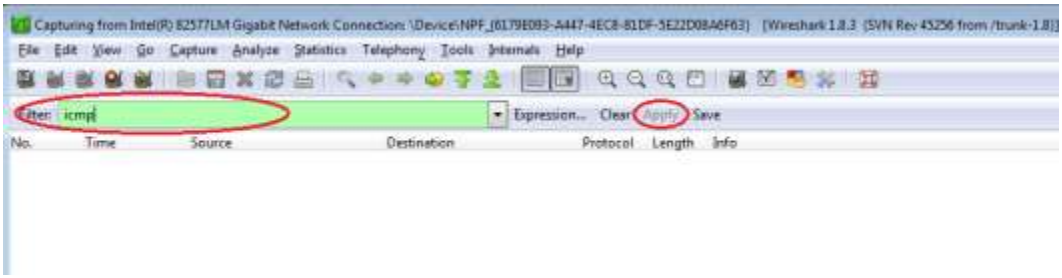
d. After you have checked the correct interface, click **Start** to start the data capture.



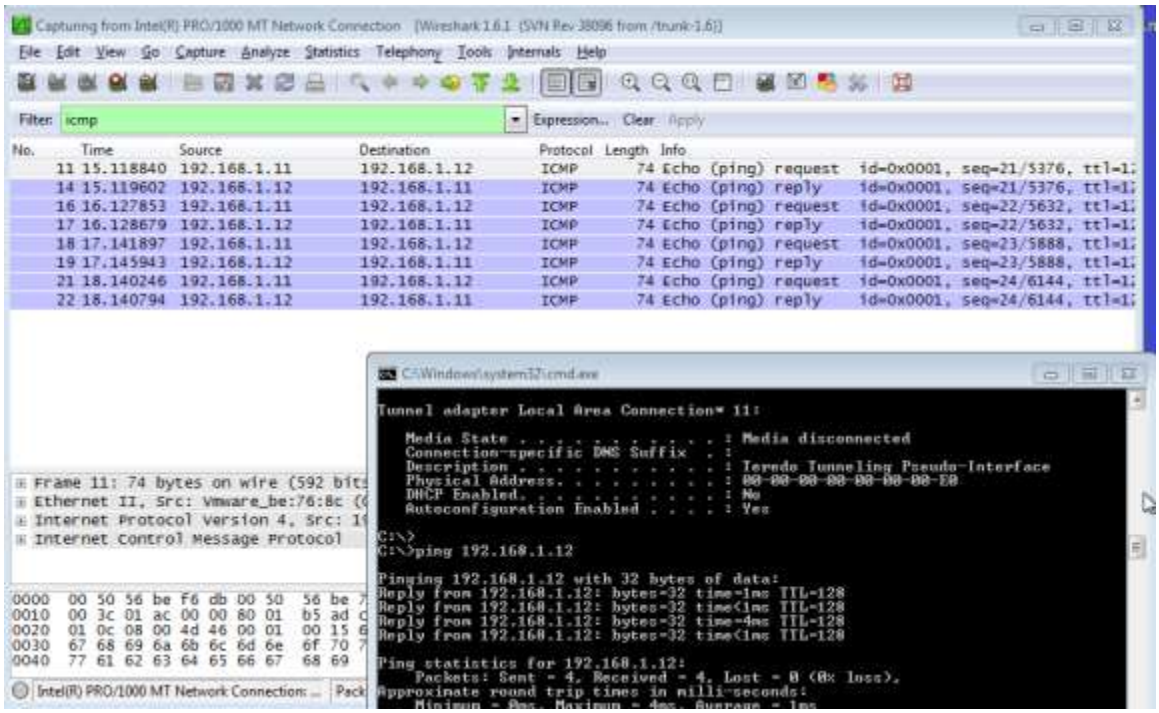
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



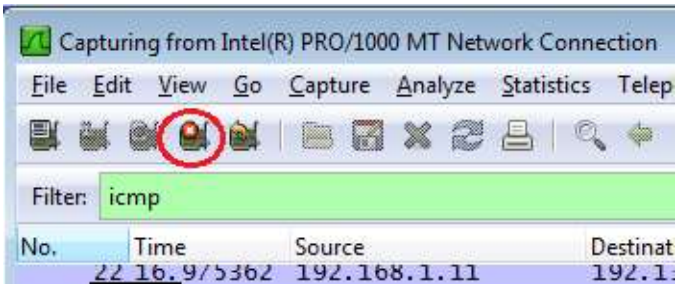
e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the Filter box at the top of Wireshark and press Enter or click on the **Apply** button 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 of PC-B. Notice that you start seeing data appear in the top window of Wireshark again.

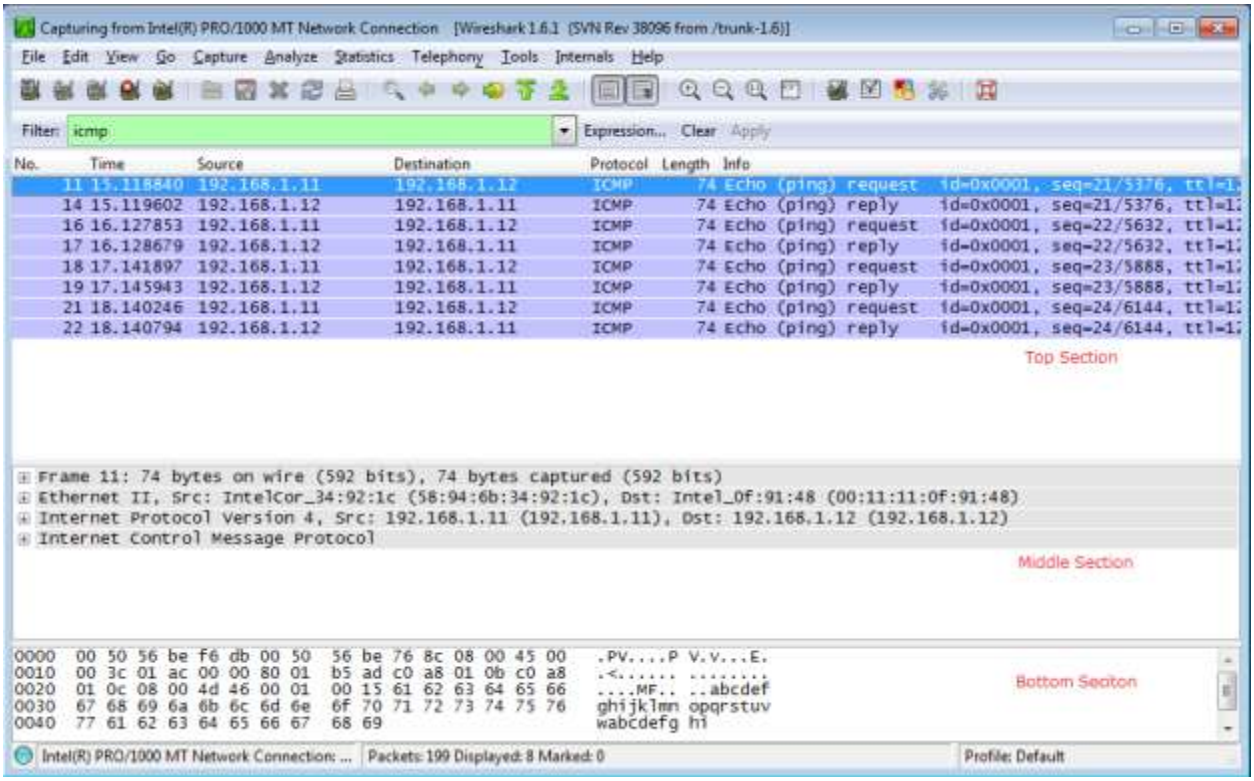


g. Stop capturing data by clicking the **Stop Capture** icon.

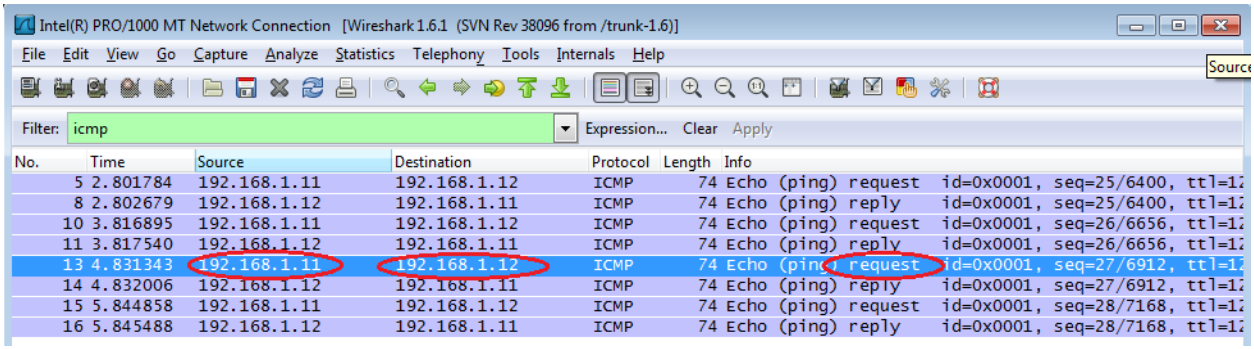


Step 3: Examine the captured data.

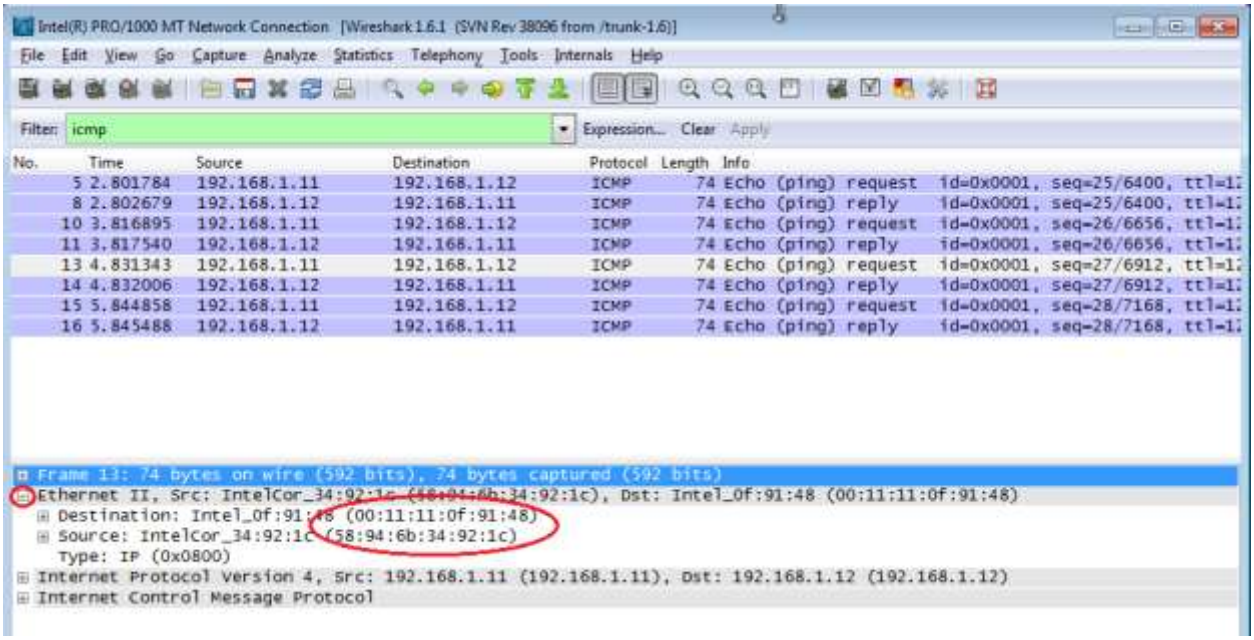
In Step 3, examine the data that was generated by the ping requests of your team member's PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for 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 form.



a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC's IP address, and the Destination contains the IP address of the teammate's PC 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's interface? _____

Does the Destination MAC address in Wireshark match your team member's 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.