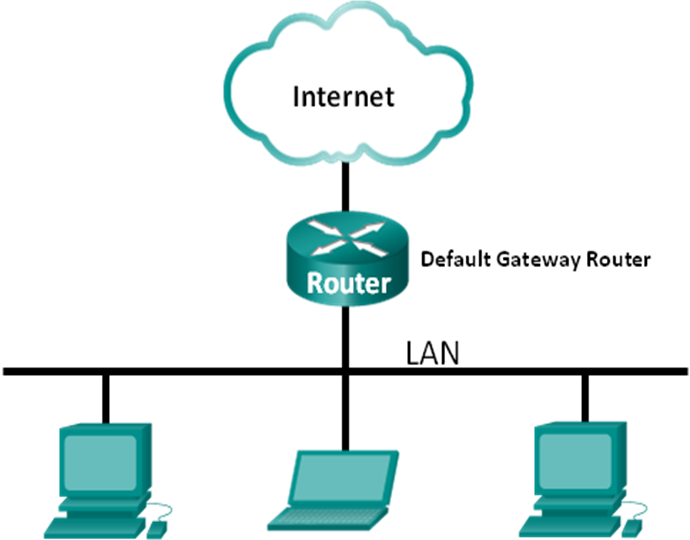
Lab 3.4.1.2 Using Wireshark to View Network Traffic

1. Topology



1. Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

1. 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.

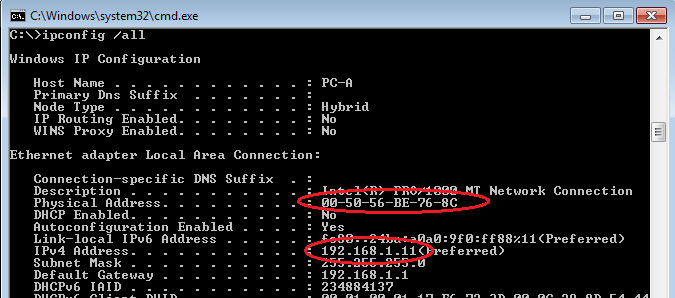
1. Capture and Analyze Local ICMP Data in Wireshark

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.

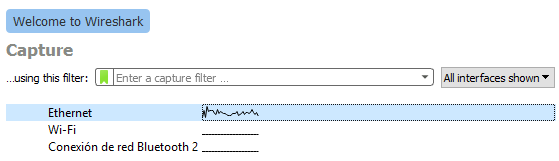
* 1. Retrieve your PC’s interface addresses.

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.

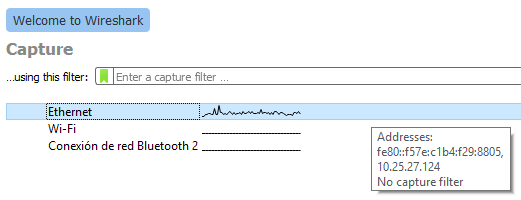
* + 1. Open a command window (**Window + R > cmd**), type **ipconfig /all**, and then press Enter.
    2. Note your PC interface’s **IPv4** address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
    3. Note your PC **MAC** (physical) address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



* + 1. Ask a team member for their PC’s IP address and provide your PC’s IP address to them.
  1. Start Wireshark and select the appropriate interface.
     1. Start **Wireshark**.
     2. In the **Wireshark: Capture Interfaces** window, click to the interface that is connected to your LAN.

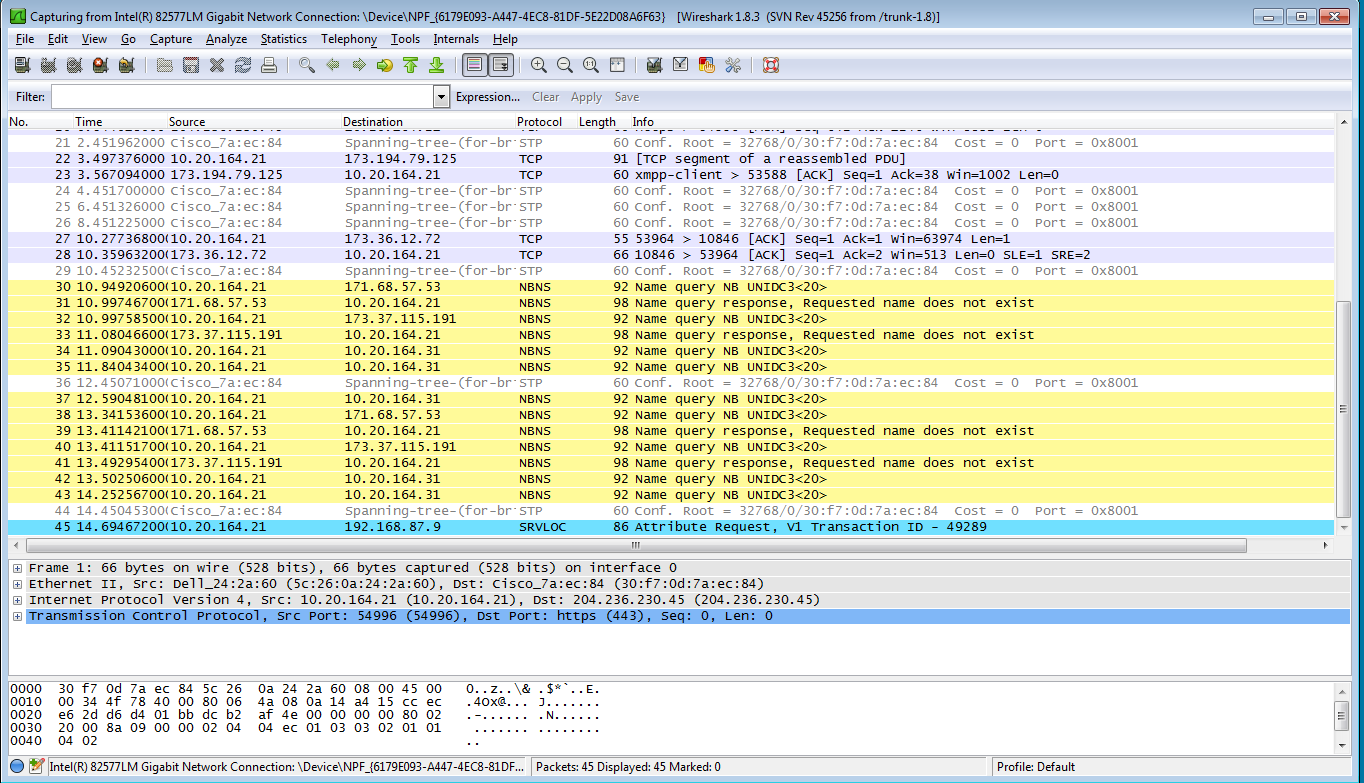


* 1. Verify the addresses and begin capturing data.
     1. Verify that the **IPv4** and **IPv6** addresses match what you noted in Step 1b.

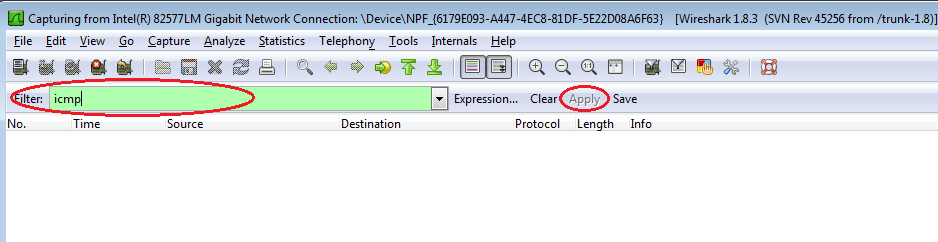


* + 1. Double click on the **Ethernet** interface.

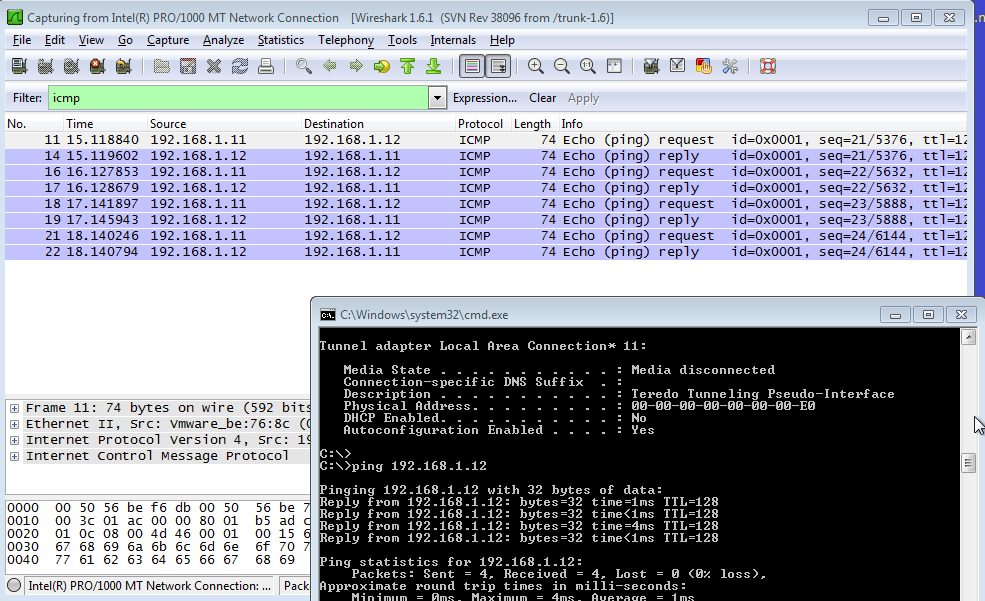
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



* + 1. 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.

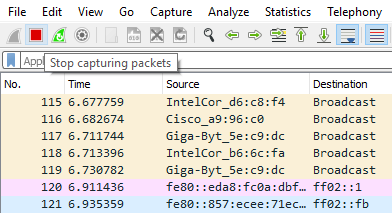


* + 1. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and **ping the IP address** that you received from your team member. Notice that you start seeing data appear in the top window of Wireshark again.



**Note**: If your team member’s PC does not reply to your pings, this may be because their PC firewall is blocking these requests

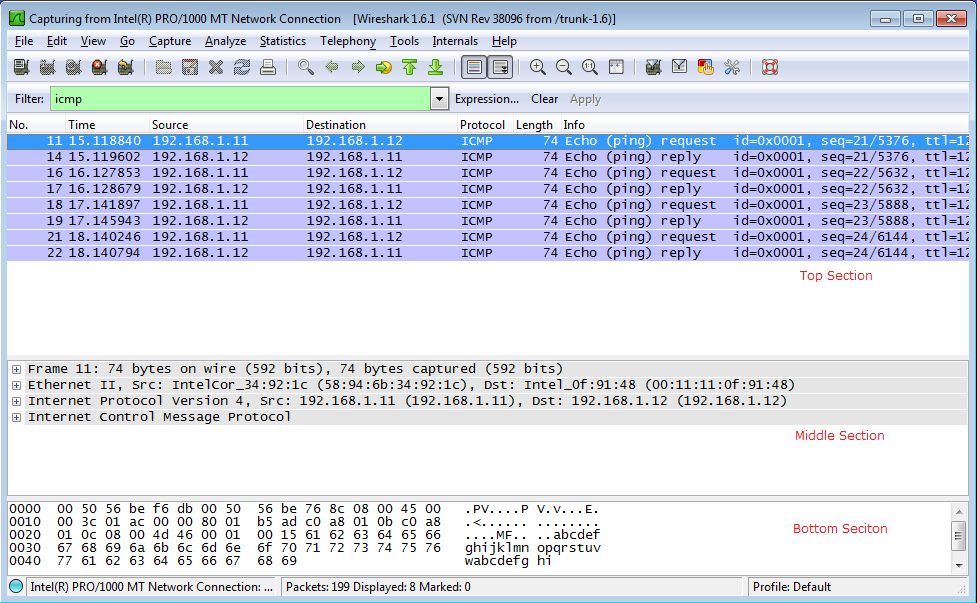
* + 1. Stop capturing data by clicking the **Stop Capture** icon.



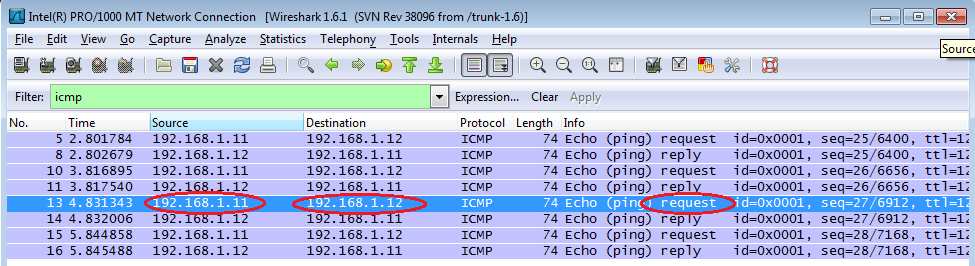
* 1. Examine the captured data.

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:

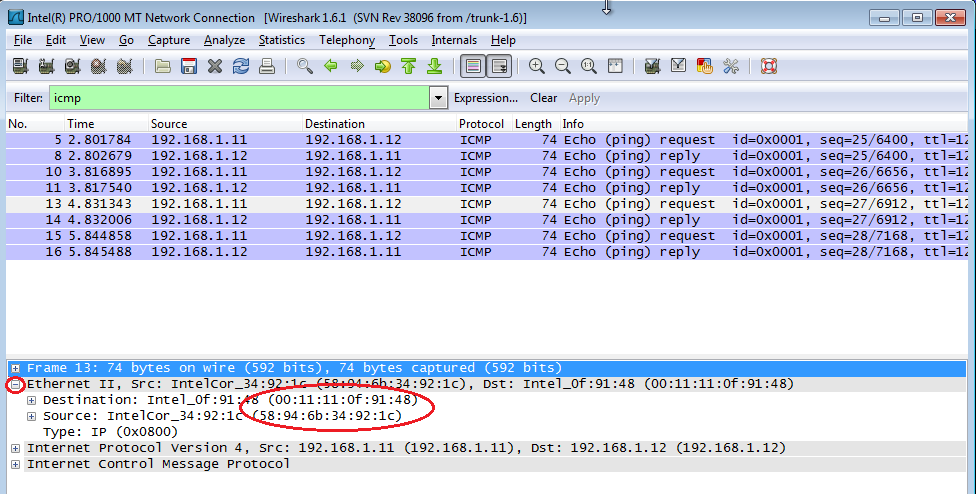
* + 1. The **top section** displays the list of PDU frames captured with a summary of the IP packet information listed.
    2. The **middle section** lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers**.**
    3. The **bottom 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’s IP address, and the Destination contains the IP address of the teammate’s PC you pinged.



* + 1. 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?

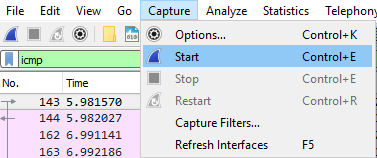
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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.

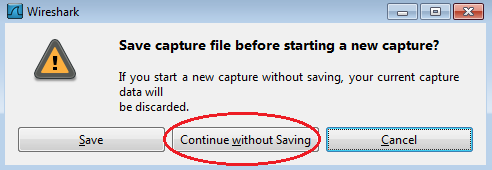
1. Capture and Analyze Remote ICMP Data in Wireshark

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.

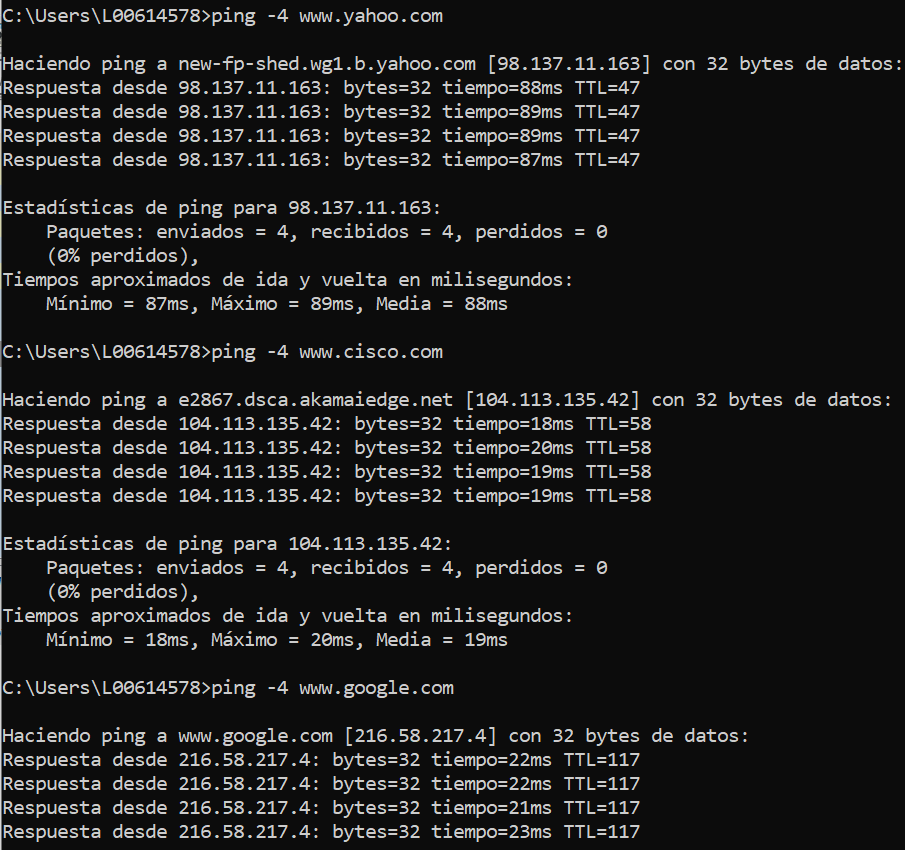
* 1. Start capturing data on the interface.
     1. Click from the menu **Capture** the option to **Start**.



* + 1. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.

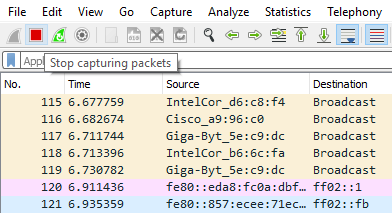


* + 1. With the capture active, ping the following three website URLs:
       1. www.yahoo.com
       2. www.cisco.com
       3. www.google.com



**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.

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



* 1. Examining and analyzing the data from the remote hosts.
     1. Review the captured data in Wireshark, 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: \_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

* + 1. What is significant about this information?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Reflection

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_