Course: Cloud and Network Security
Name: Neville Ngothe Iregi
Student No.: CS-CNS10-25054
Date: Tuesday, 16 September 2025

Week 1: Using Wireshark to Examine Network Traffic

Introduction

Wireshark is a software protocol analyzer or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. A network sniffer—sometimes referred to as a packet sniffer, packet analyzer, protocol analyzer, or network traffic analyzer—can intercept and analyze network traffic that traverses a digital network. 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. Thus, Wireshark is a useful tool for anyone working with networks; it can be invaluable to a network or security engineer, forensic investigator, or even a hacker.

In this lab, I used Wireshark to capture ICMP(Internet Control Message Protocol) data packet IP addresses and Ethernet frame MAC addresses. ICMP operates at the network layer as a supporting protocol to IP (Internet Protocol). ICMP is used for reporting errors and management queries since IP lacks an error-reporting or error-correcting mechanism. ICMP also uses **traceroute** and **ping** to perform network diagnosis. **Ping** issues a series of ICMP echo request packets to the destination to test network connectivity and measure latency.

Objectives

1. Capture and analyze local ICMP data in Wireshark
2. Capture and analyze remote ICMP data in Wireshark

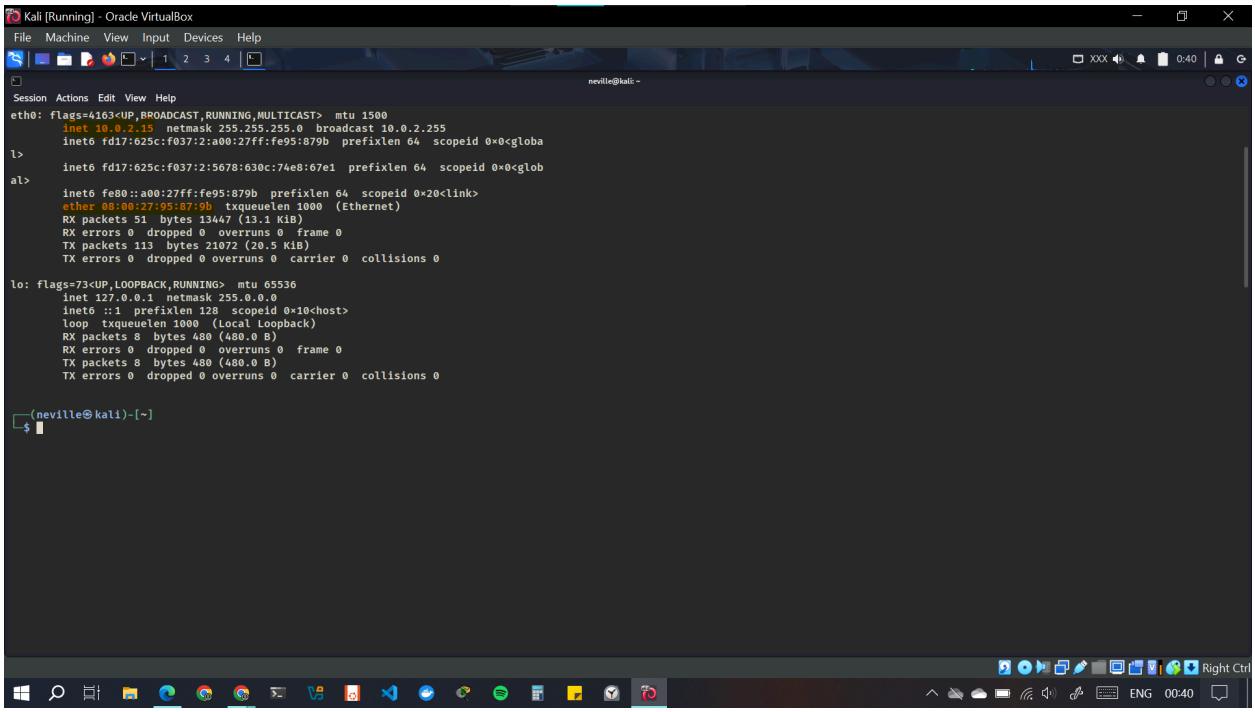
Part 1: Capture and Analyze Local ICMP Data in Wireshark

In part 1 of this lab, I pinged my default gateway/router on the LAN and captured ICMP requests and replies in Wireshark. I also looked inside the frames captured for specific information. This analysis helped me to clarify how packet headers are used to transport data to their destination.

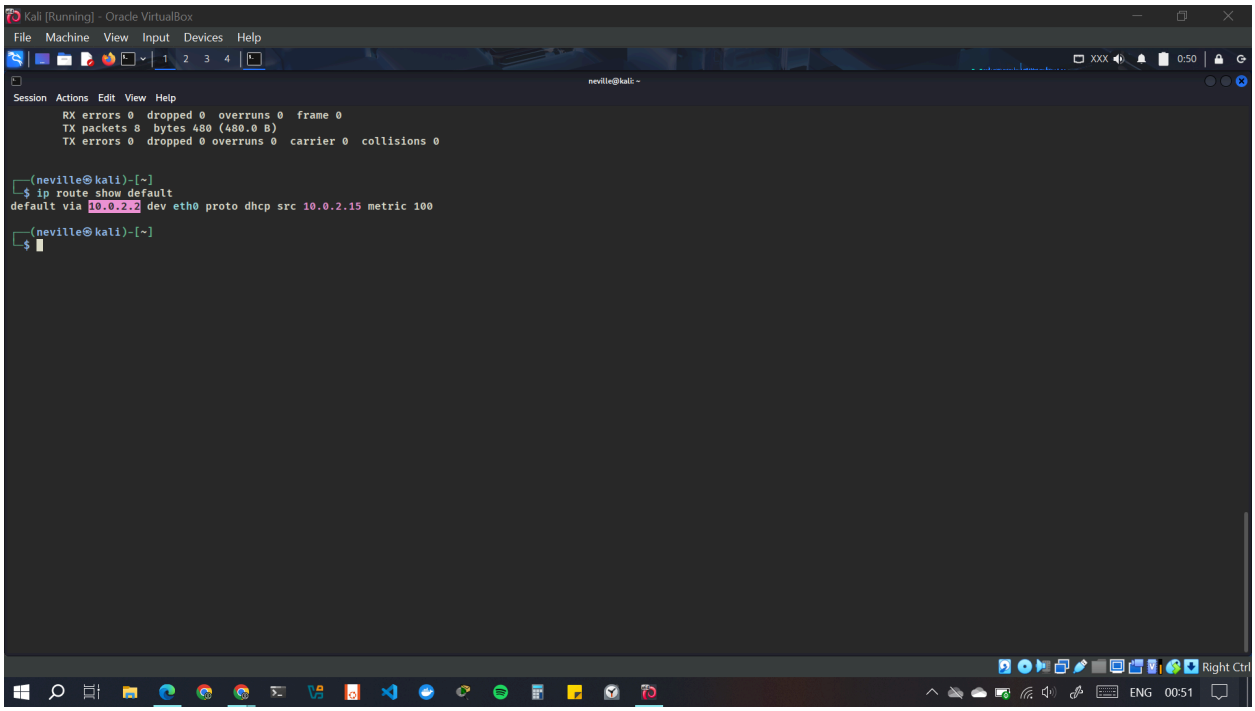
Step 1: Retrieve my PC interface addresses

For this lab, I needed to retrieve my PC IP address and its network interface card(NIC) physical address, also called the MAC address.

a. In a terminal window, I entered **ifconfig** to get the IP address of my PC interface, its description and MAC address and **ip route show default** to get the address of the default gateway.



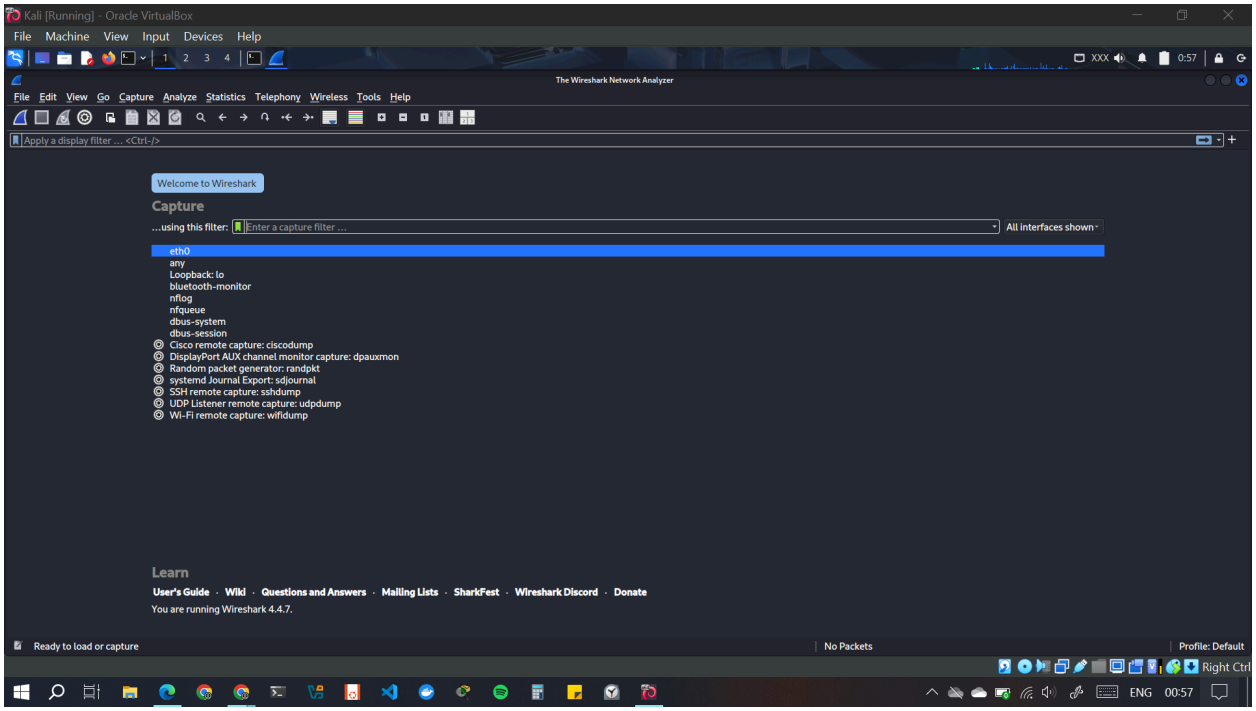
- My IP address is **10.0.2.15** and my MAC address is **08:00:27:95:87:9b.**

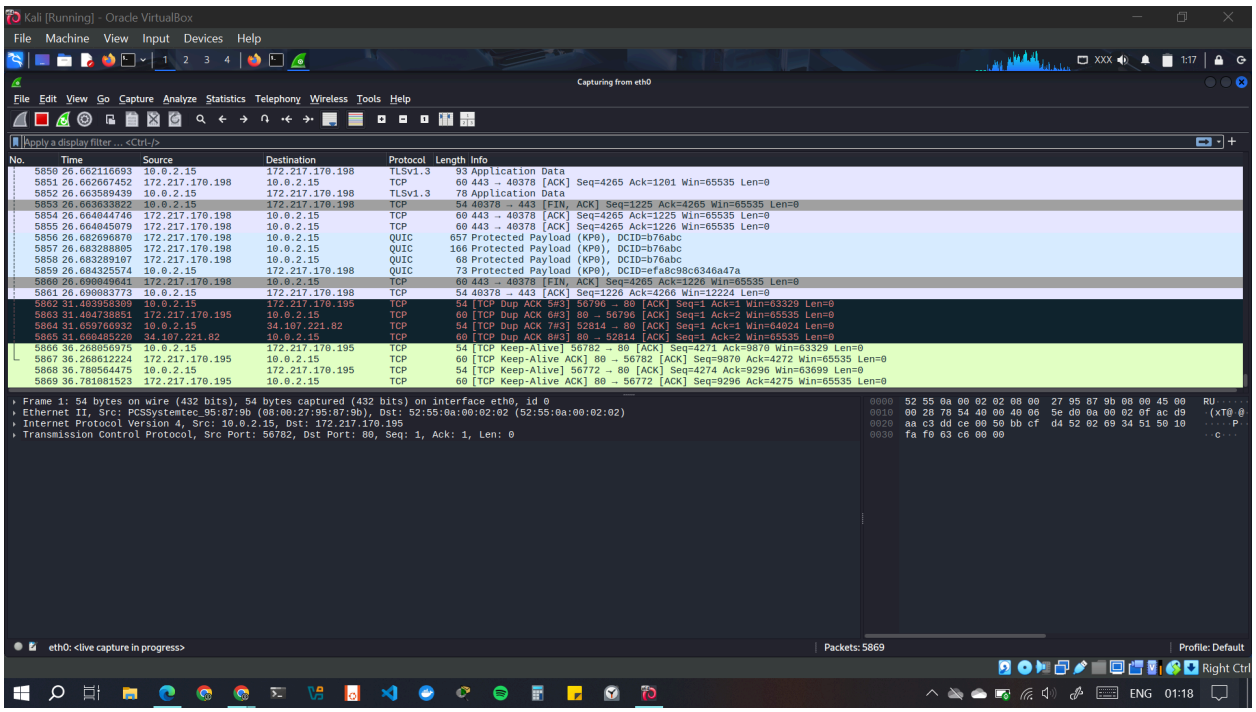


- The address of the default gateway is **10.0.2.2.**

Step 2: Start Wireshark and begin capturing data.

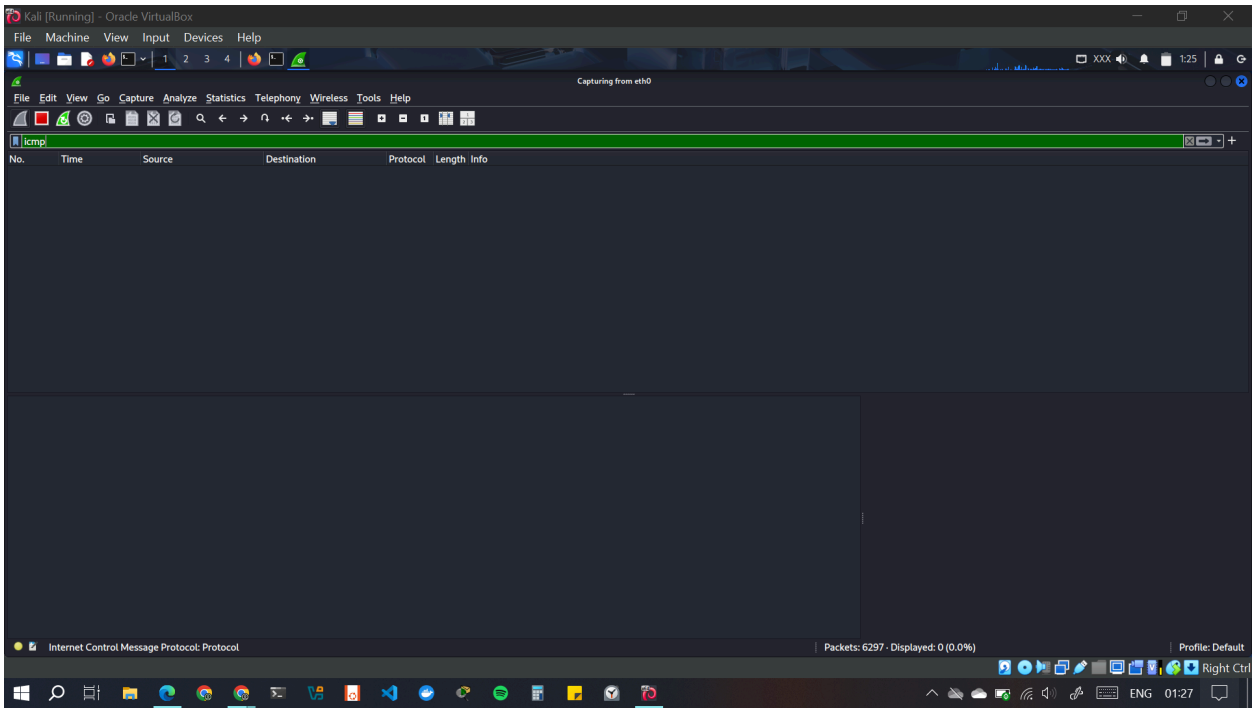
a. I navigated to Wireshark, double-clicked on the desired interface(eth0) to start the packet capture while making sure the desired interface had traffic.
b. Information started scrolling down the top section in Wireshark. Data lines appear in different colors based on protocol.



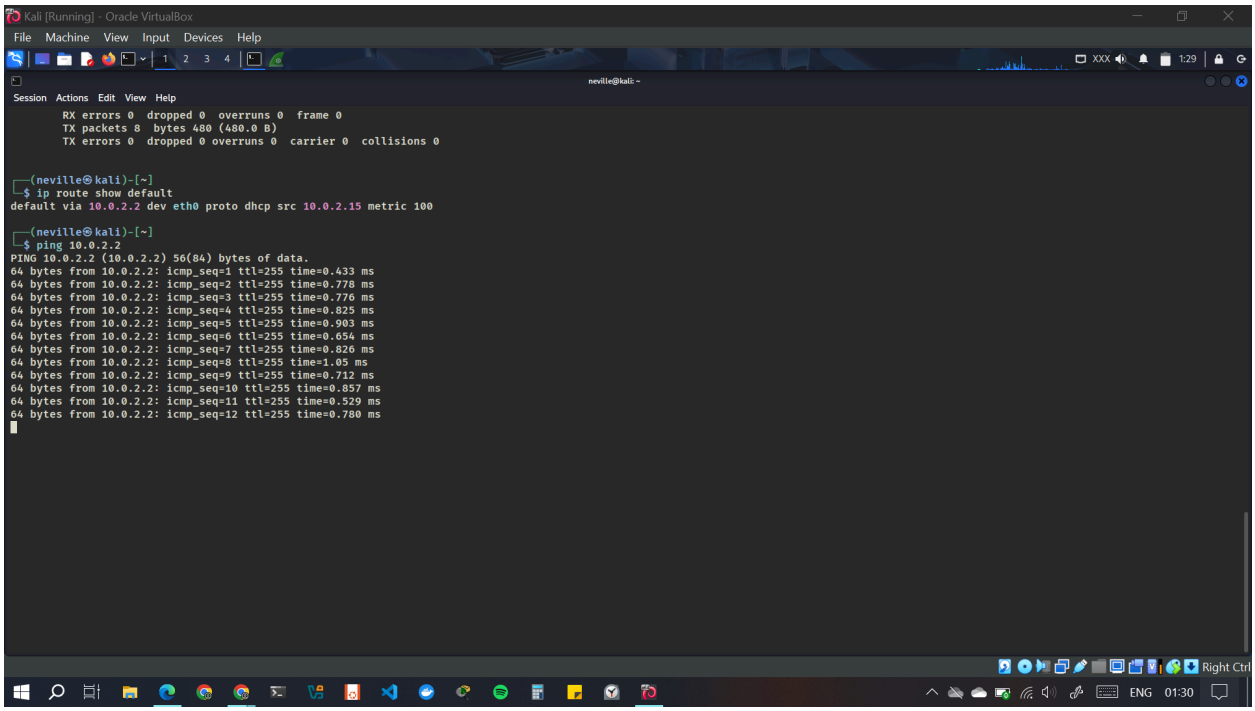


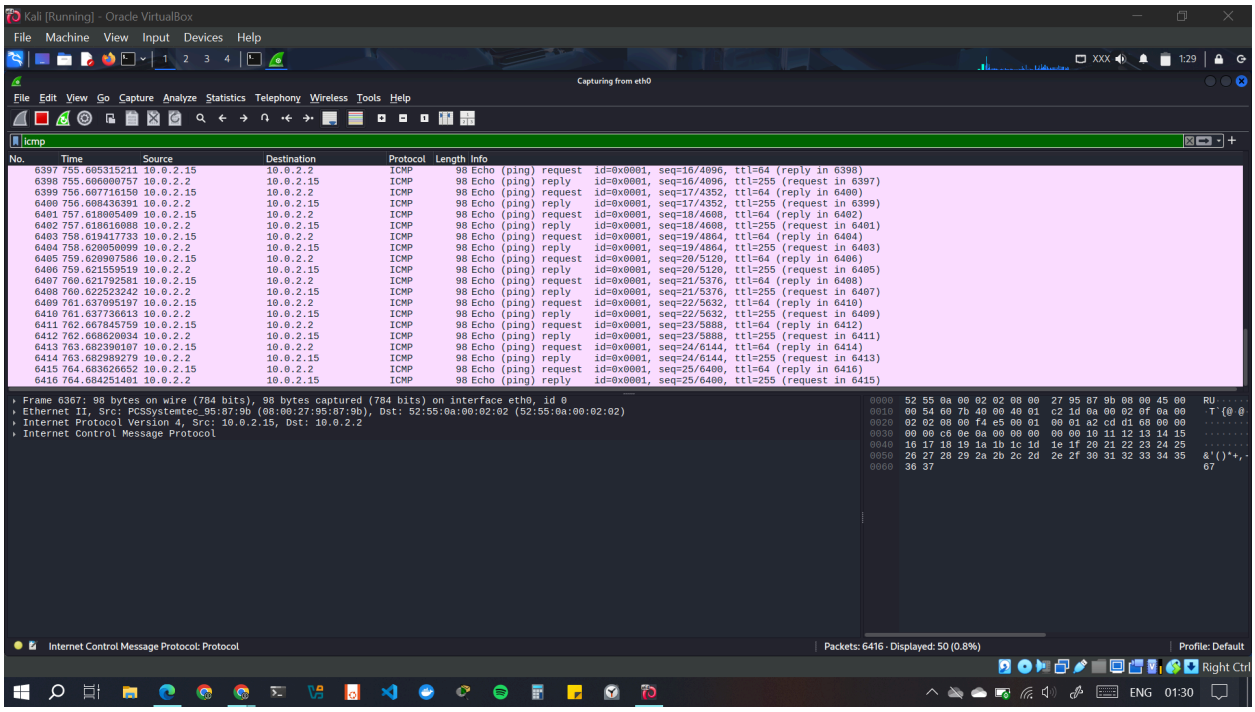
- One can apply a filter to make it easier to view and work with the data being captured by

wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. I typed **icmp** in the **Filter** box at the top of Wireshark and pressed Enter to view only ICMP (ping) PDUs.



c. The icmp filter caused all data in the top window to disappear, but I was still capturing the traffic on the eth0 interface. I navigated to the terminal and pinged the default gateway IP address and at some point, I clicked the **Stop Capture** icon to stop capturing the data.





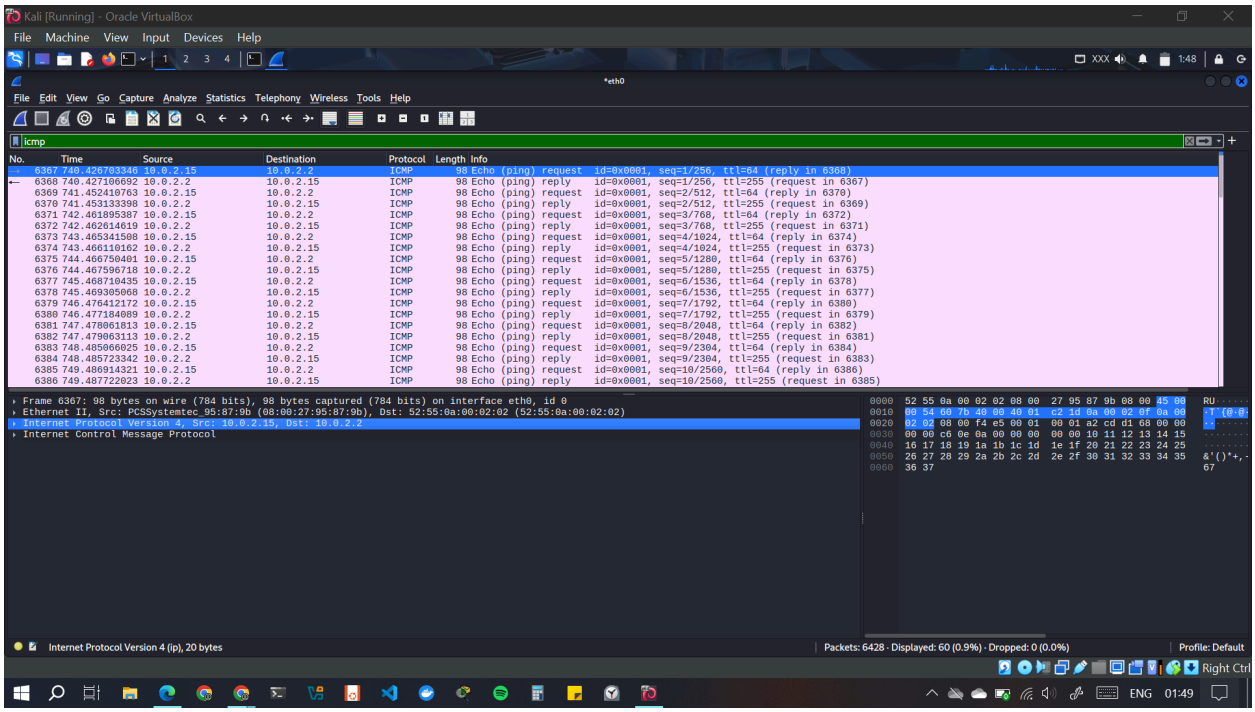
Step 3: Examine the captured data

I examined the data that was generated by the ping requests to the default gateway.

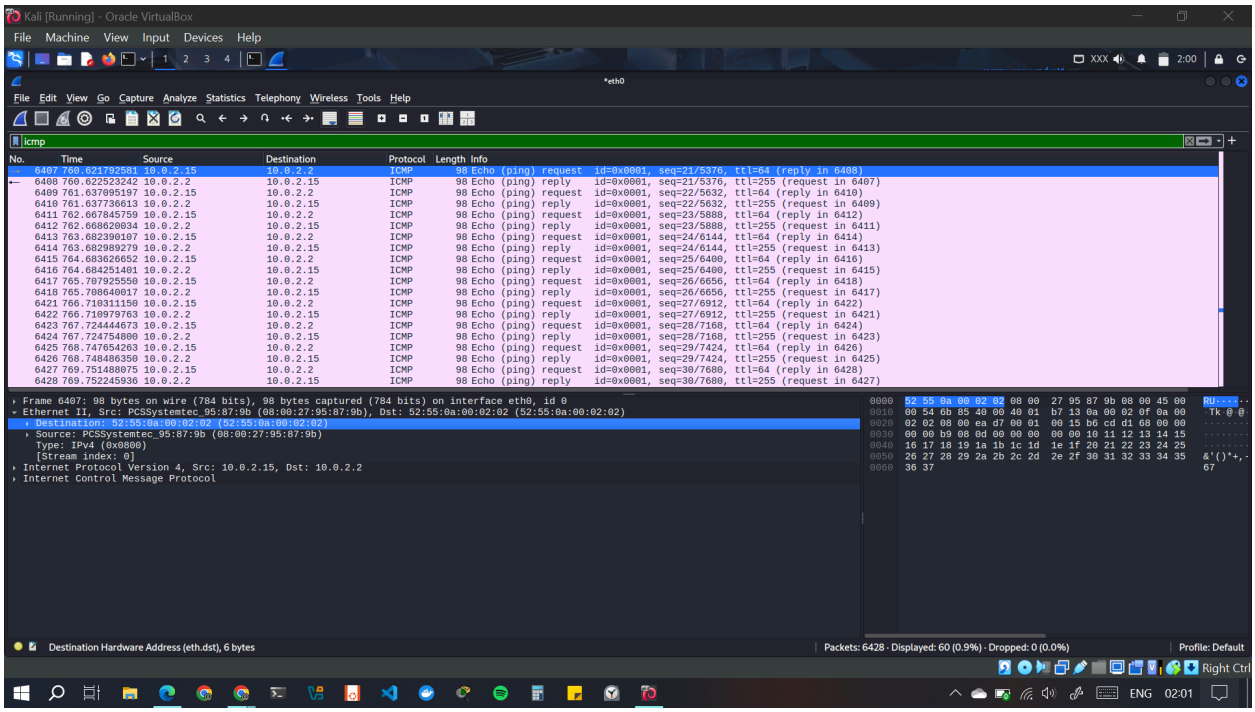
Wireshark data is displayed in three sections:

1. The top section displayed 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.

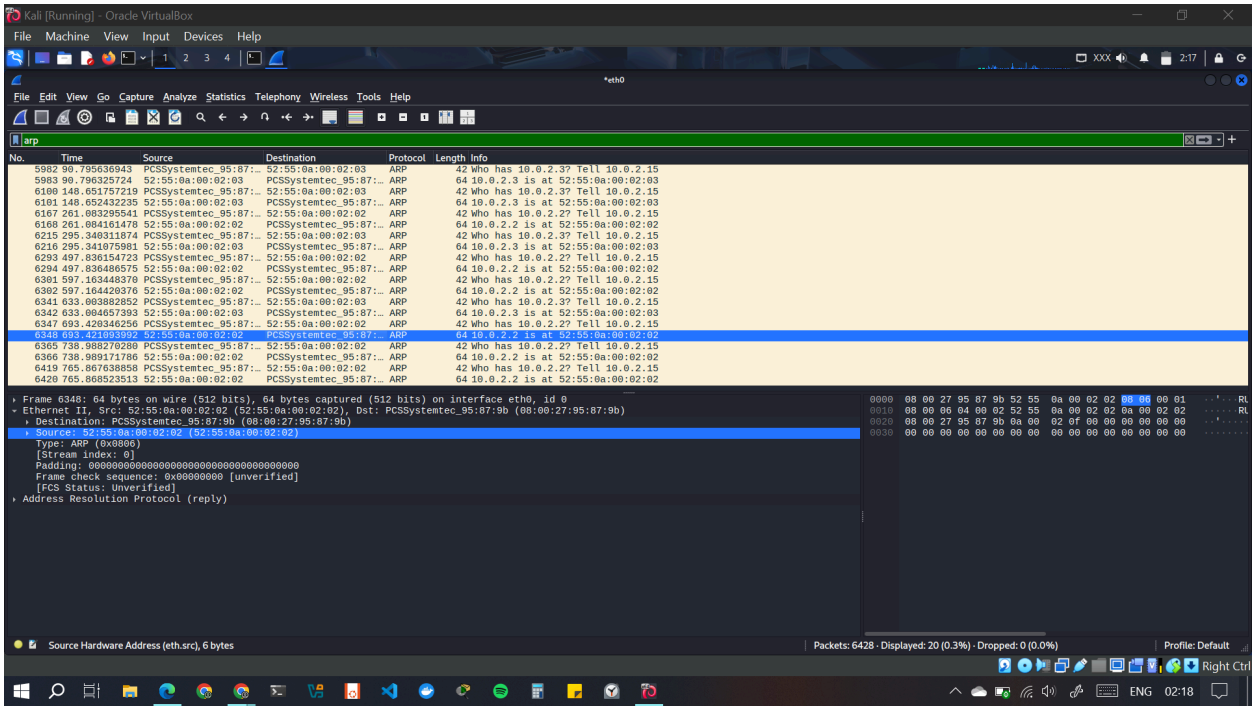
a. I clicked on the first ICMP request PDU frames in the top section of Wireshark. I noticed that the **Source** column has my PC IP address(10.0.2.15) and the **Destination** column contains the IP address of the default gateway that I pinged.

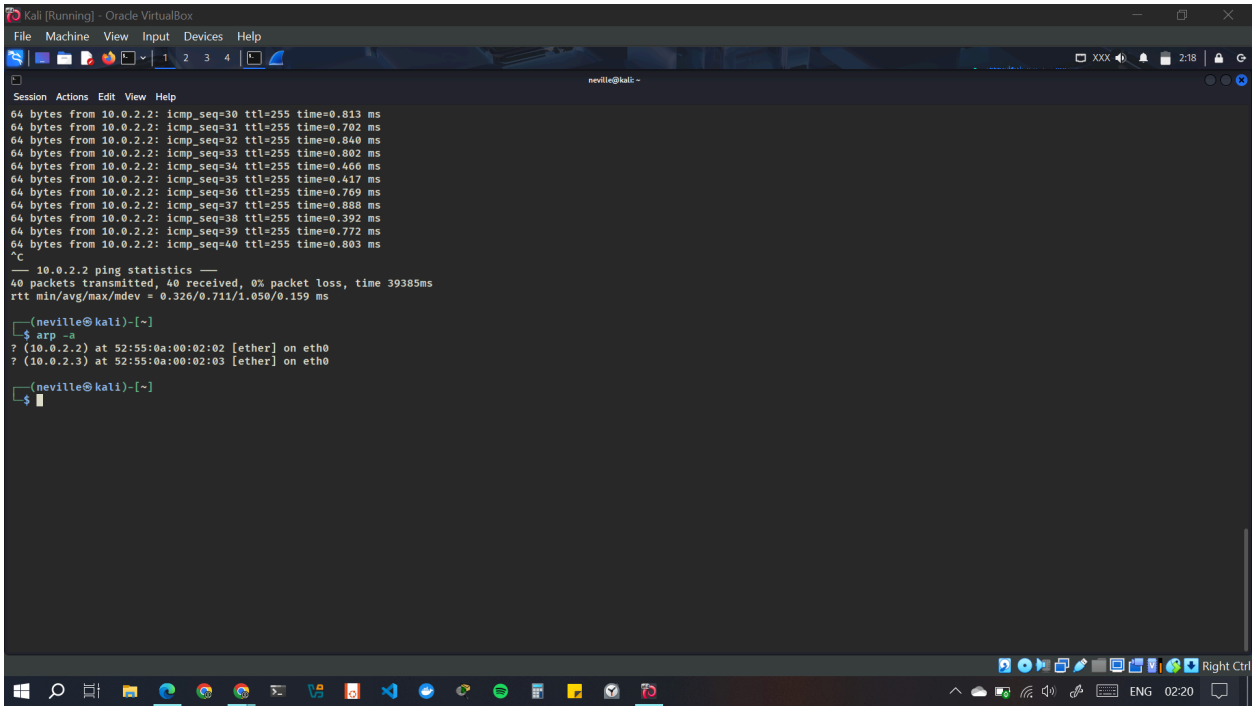


b. With the PDU frame still selected in the top section, I navigated to the middle section, clicked the arrow to the left of the Ethernet II row to view the destination and source MAC address.



- The source MAC address matched that of my PC interface(**08:00:27:95:87:9b**)
- The MAC address of the destination which is the pinged default gateway is obtained by my PC using an **ARP(Address Resolution Protocol) request** which sends out a broadcast message on LAN to discover the associated MAC address; basically, the ARP request is saying, “Whoever is 10.0.2.2, I need your MAC address”.





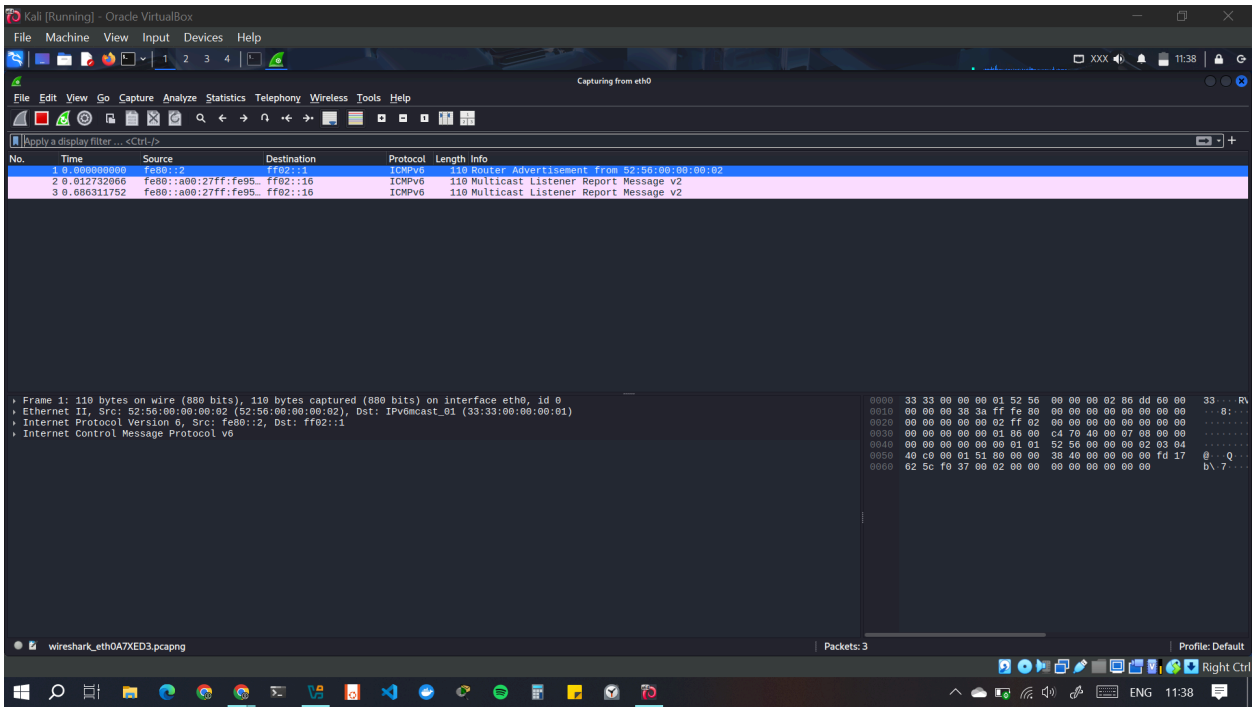
- Using an arp filter in Wireshark, I saw how arp requests for the MAC address of the default gateway. Similarly, using command **arp -a,** I was able to view the ARP table on my system to confirm the default gateway's MAC address, which is **52:55:0a:00:02:02.**

Part 2: Capture and Analyze Remote ICMP Data In Wireshark

In this part, I pinged remote hosts(hosts not on the LAN) and examined the generated data from those pings. I then determined what is different about this data from the data examined in Part 1.

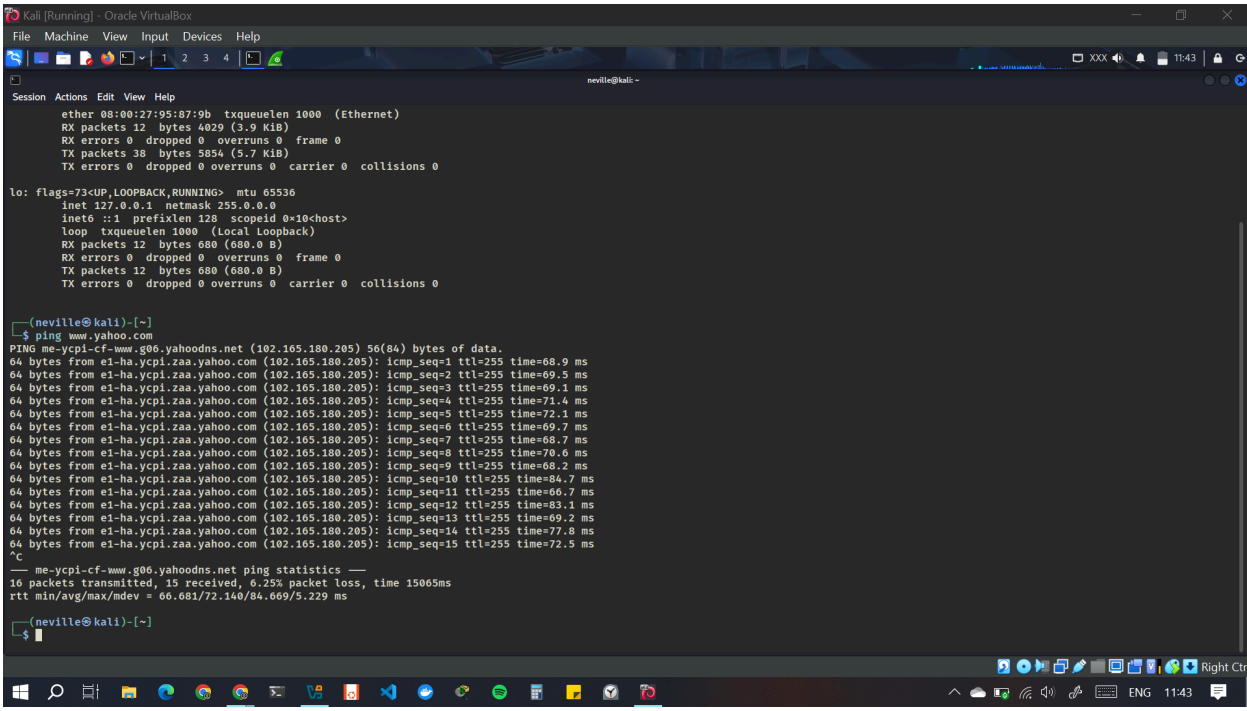
Step 1: Start capturing data on the interface

a. I started the data capture again.

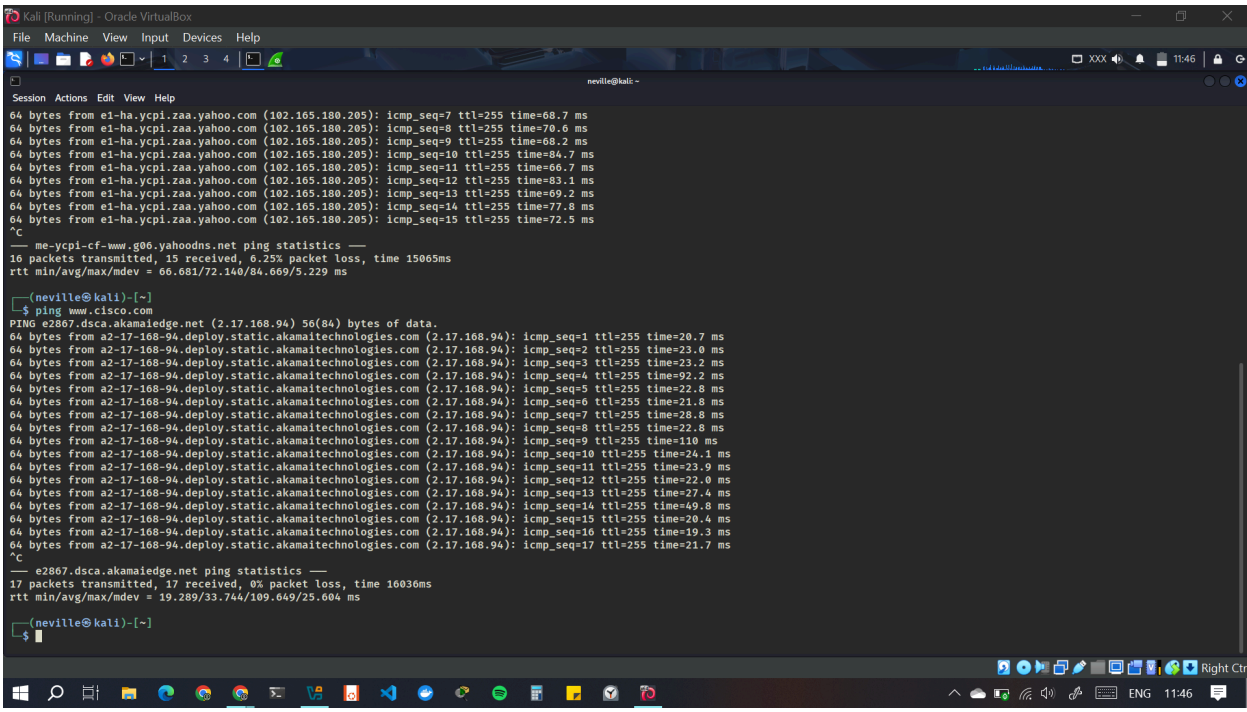


b. With the capture active, I pinged the following 3 website URLs from the terminal.

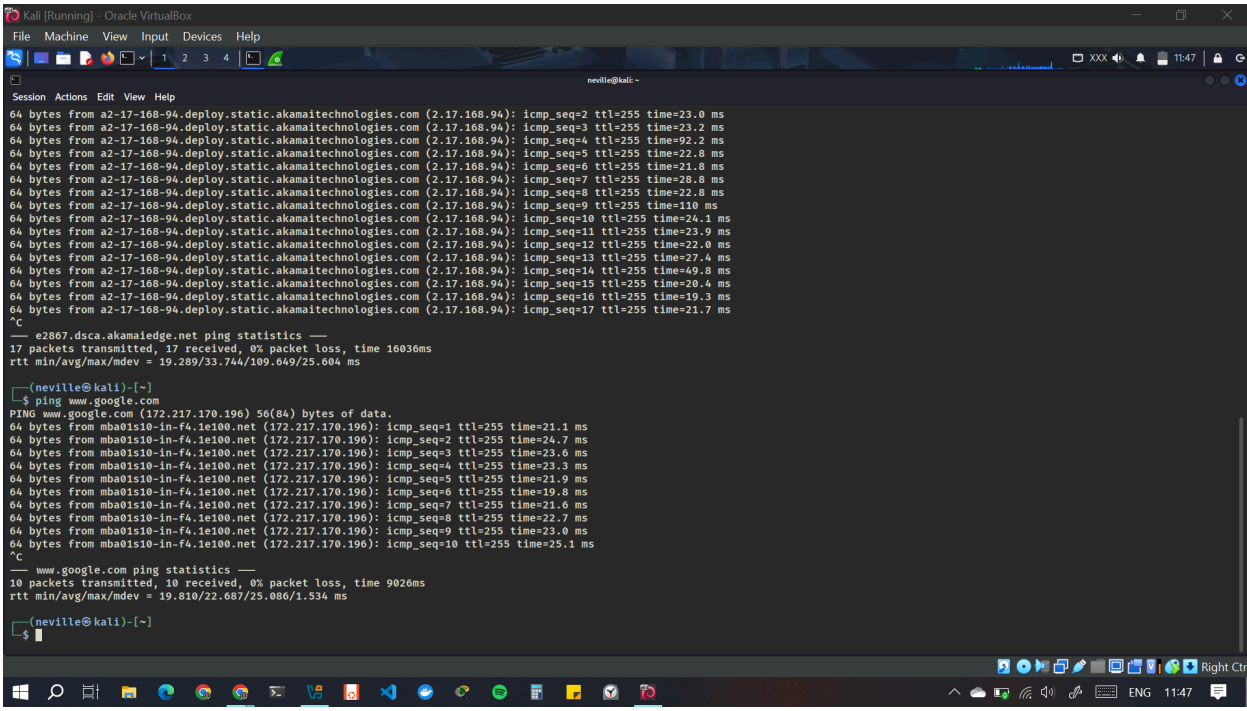
1. www.yahoo.com



2. www.cisco.com



3. www.google.com



- When I pinged the URLs listed, I noticed that the Domain Name Server(DNS) translates the URL to an IP address.

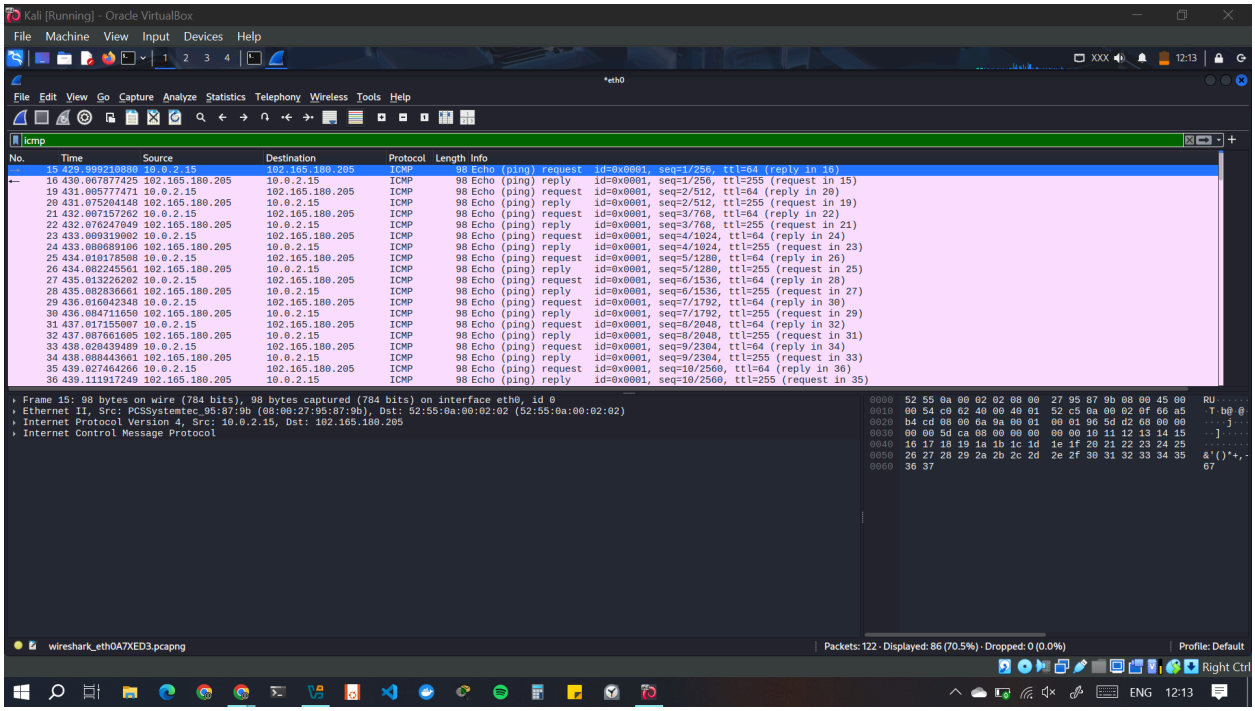
c. In Wireshark, I stopped capturing data by clicking the **Stop Capture** icon.

Step 2: Examining and analyzing the data from the remote hosts

I reviewed the captured data in Wireshark and examined the IP and MAC addresses of the three locations that I pinged.

- IP address for www.yahoo.com

  102.165.180.205



- MAC address for www.yahoo.com

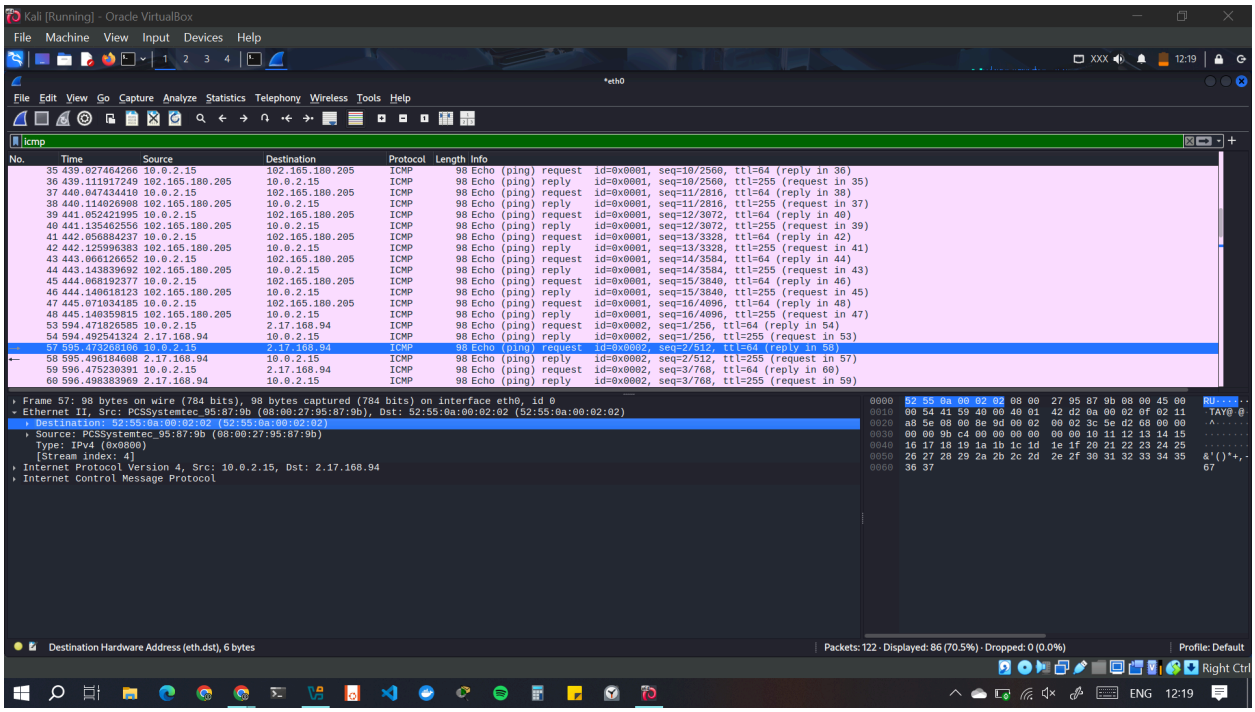
  52:55:0a:00:02:02

- IP address for www.cisco.com

  2.17.168.94

- MAC address for www.cisco.com

  52:55:0a:00:02:02

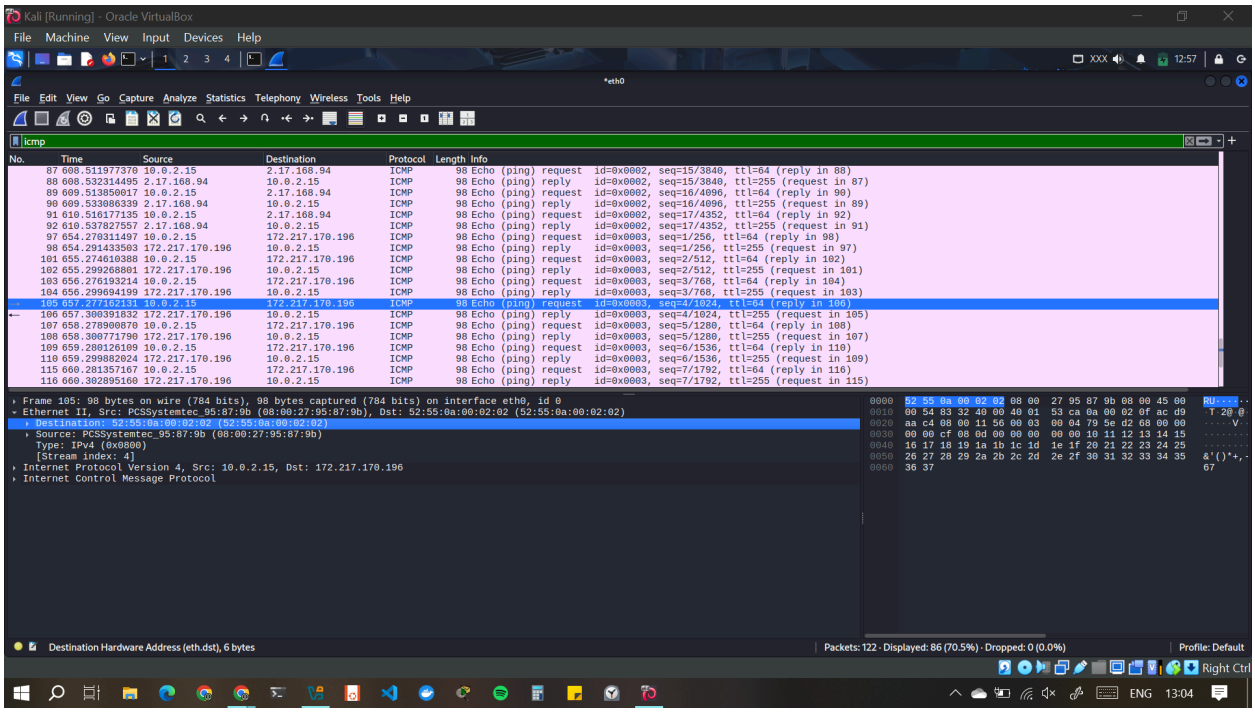


- IP address for www.google.com

  172.217.170.196

- MAC address for www.google.com

  52:55:0a:00:02:02



Question: What is significant about this information?

Answer: The MAC address is the same for the 3 locations

Question: How does this information differ from the local ping information you received in Part 1?

Answer: The information in Part 2 uses one MAC address for the different remote IP addresses meaning that the MAC address belongs to the default gateway through which the remote ping information passes through.

REFLECTION QUESTION

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

Answer:

MAC addresses are only meaningful within a local network segment (Layer 2 domain). When you send traffic to a remote host, your packet is first sent to your default gateway (router). That router deencapsulates the Ethernet header (with your MAC + router's MAC) and forwards the packet at Layer 3 (IP). Each hop along the path builds a new

Ethernet frame with its own source and next-hop destination MAC addresses. By the time your traffic reaches the remote host, your machine has no visibility of its MAC address — only of your local router's MAC.

Wireshark shows actual MAC addresses for local hosts because those Ethernet frames are on your LAN. For remote hosts, you only see the MAC of your local gateway/router, since that's the last device your machine directly communicates with at Layer 2. The remote host's actual MAC never leaves its own LAN.

Conclusion

This lab demonstrated how Wireshark can be used to capture and analyze ICMP traffic at both the local and remote levels. By examining local pings, I confirmed that my system communicates directly with other devices on the LAN using their actual MAC addresses, which are resolved through ARP. However, when pinging remote hosts, Wireshark showed that all ICMP packets shared the same MAC address — that of the default gateway — because MAC addressing is only relevant within a local network segment. Beyond the LAN, packets are forwarded at the IP layer, and new Ethernet frames are created at each hop. This assignment helped to practically show the difference between Layer 2 (MAC) and Layer 3 (IP) addressing, and highlighted the important role of the default gateway in connecting local devices to remote networks.