

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #1 Traffic Tracing and Sniffing

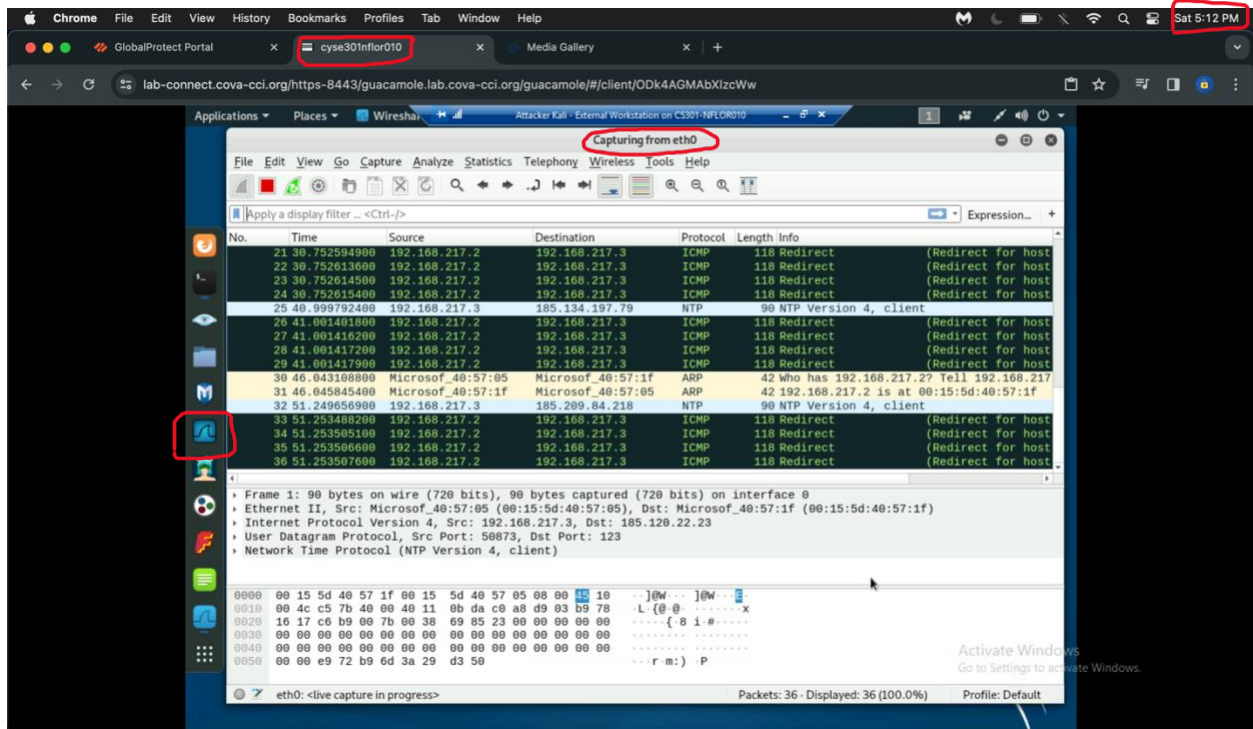
Niko Florido

01227364

TASK A: GET STARTED WITH WIRESHARK

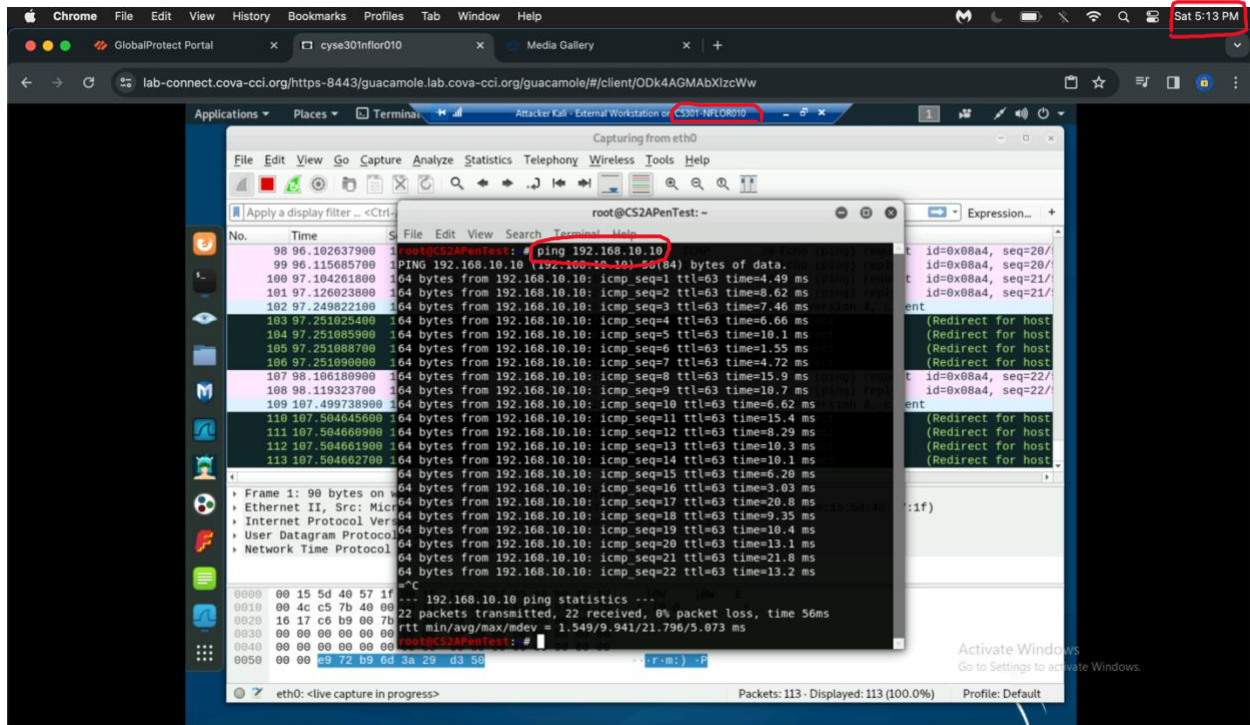
In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other. **(5 point each x 6 questions = 30 points)**

1. Open Wireshark on External Kali and listen on interface “eth0”.



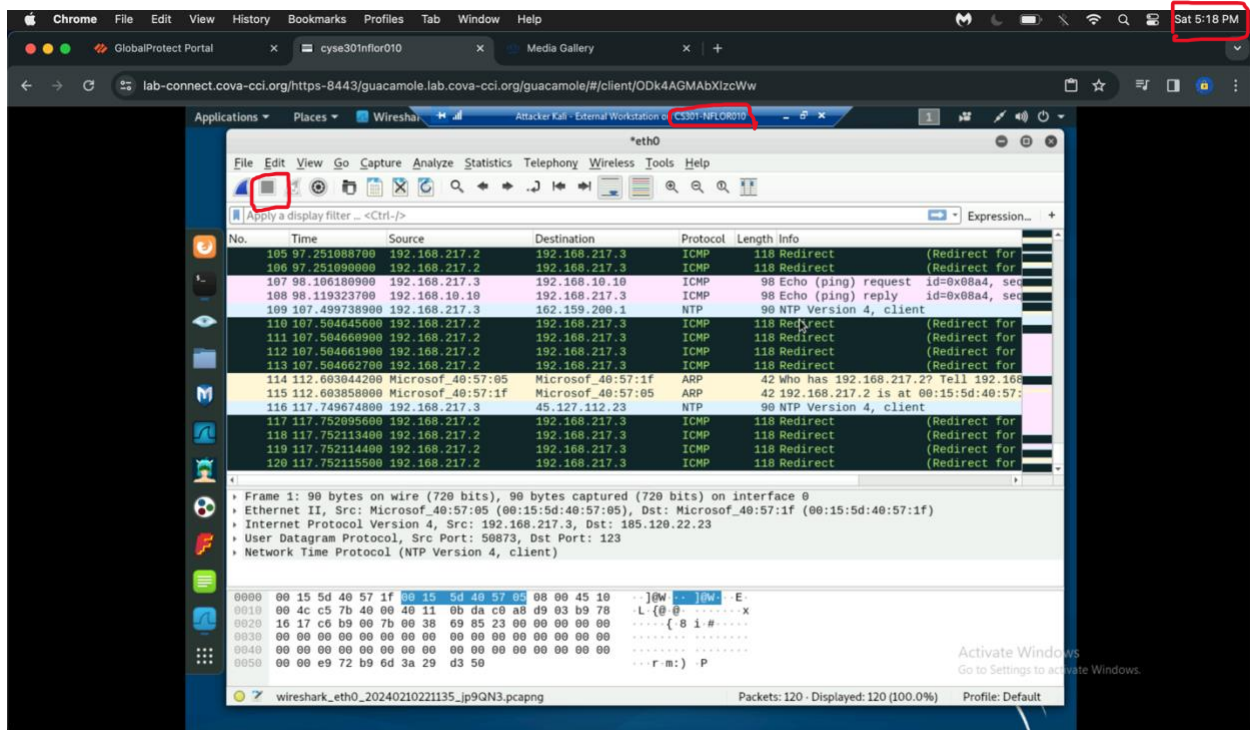
I connected the External Kali Attack Station using the Hyper-V Manager. I opened Wireshark, then started capturing from “eth0.”

2. Open a new terminal then ping Ubuntu VM for 5 – 10 seconds.



I opened the Terminal in External Kali, then typed, "ping 192.168.10.10" to ping to Ubuntu VM. I had the terminal running for 10 seconds. I pressed CTRL, +, C to end the ping.

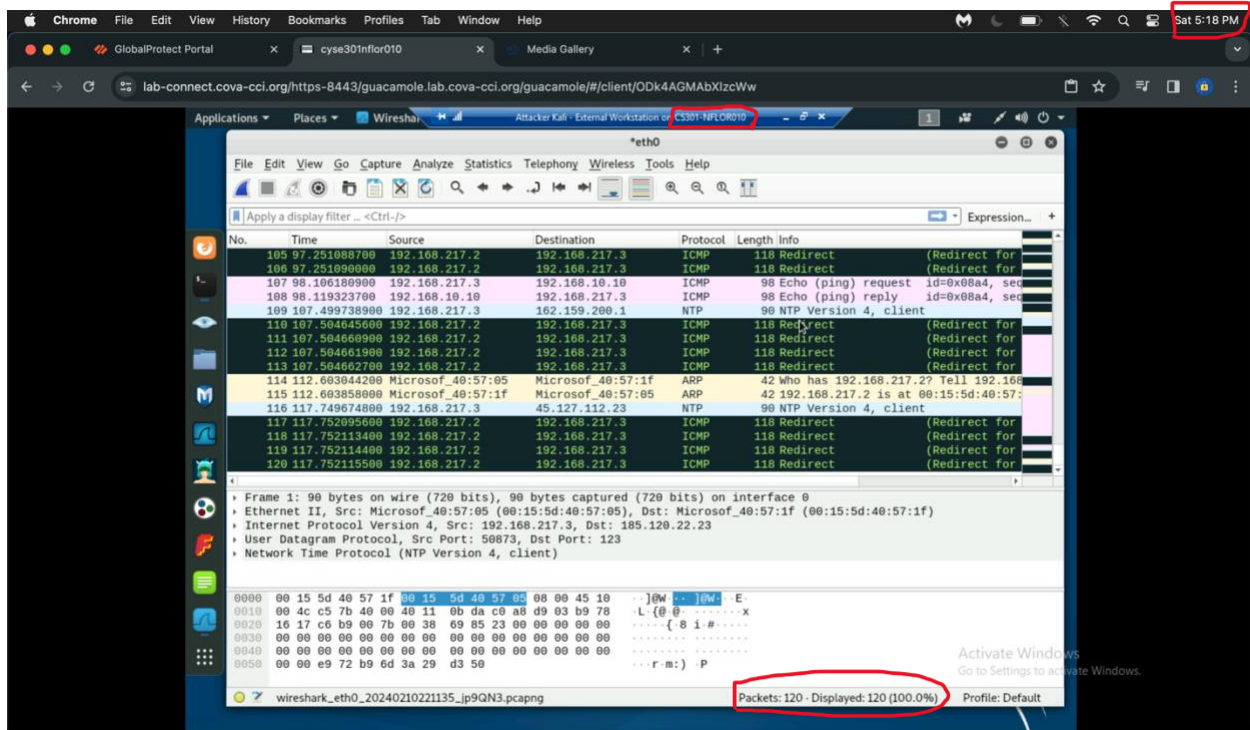
3. Stop capturing (the red button on the tool bar).



After I ended the ping, I stopped capturing on Wireshark by clicking the red button on the tool bar.

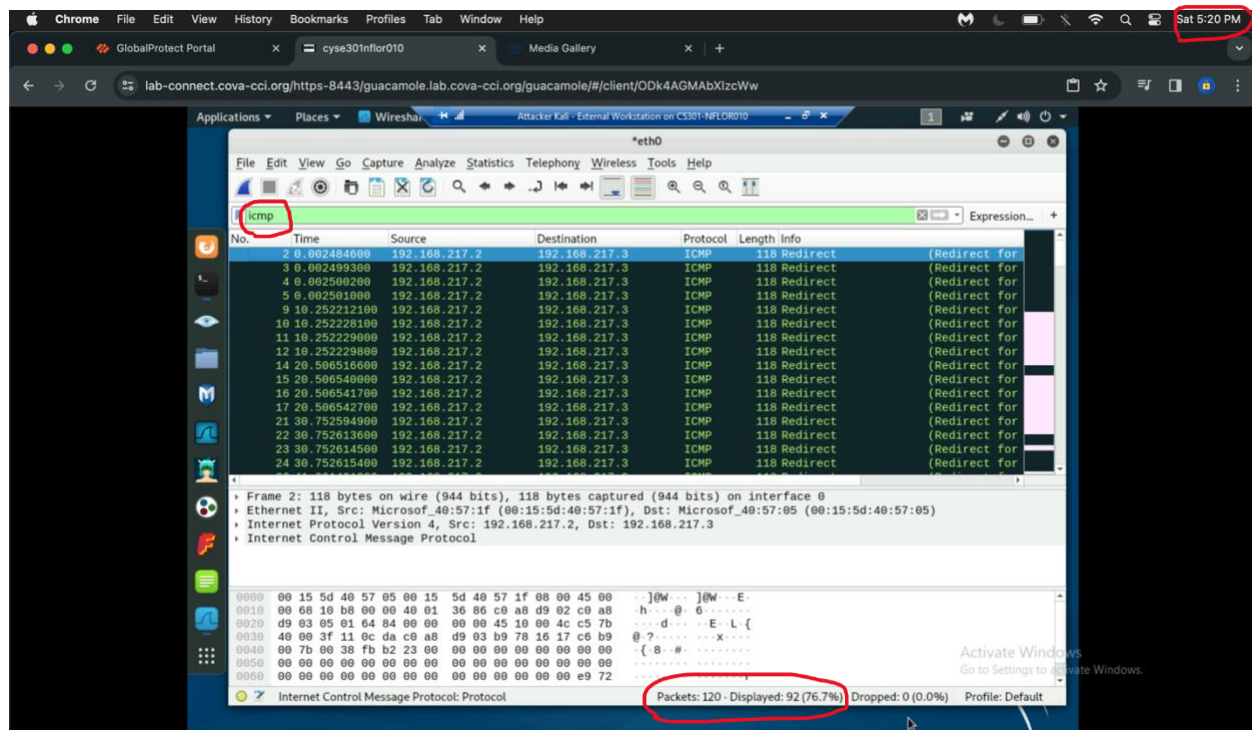
Now, answer the following questions. You need to provide a screenshot that contains the answers to each question.

Q1. How many packets are captured in total? How many packets are displayed?



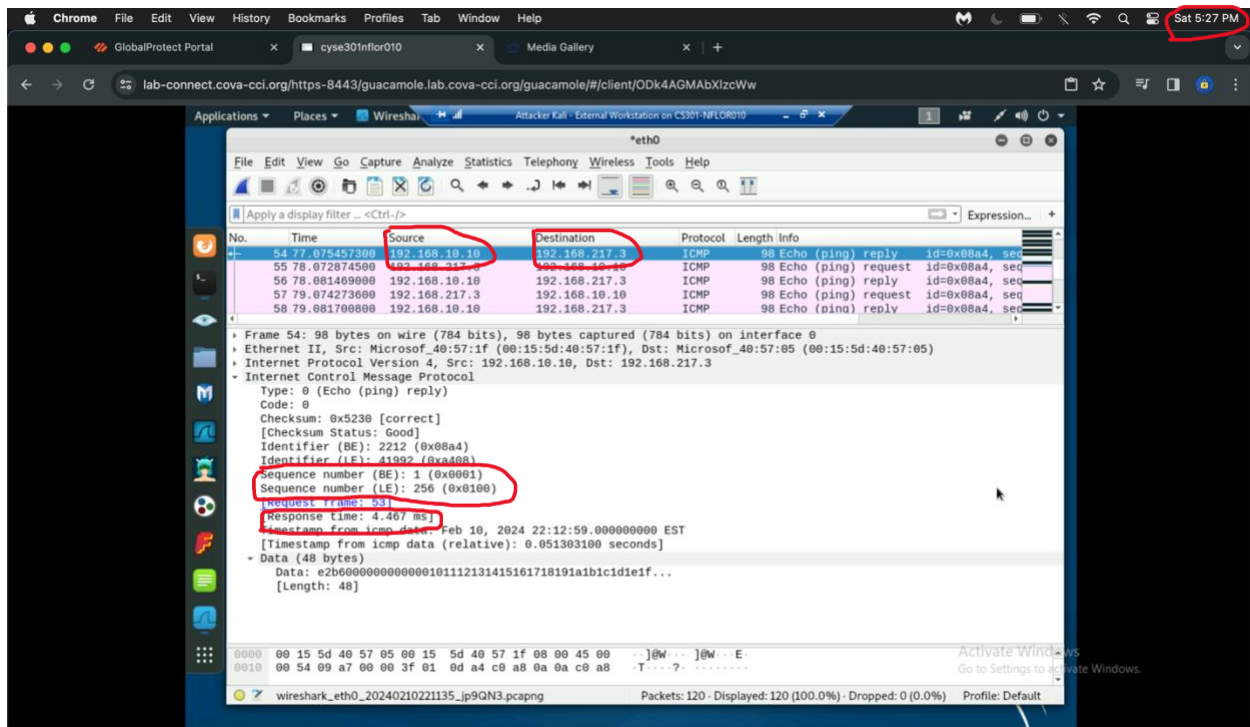
There are 120 Packets captured in total and 120 packets displayed. (100.0% displayed).

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).



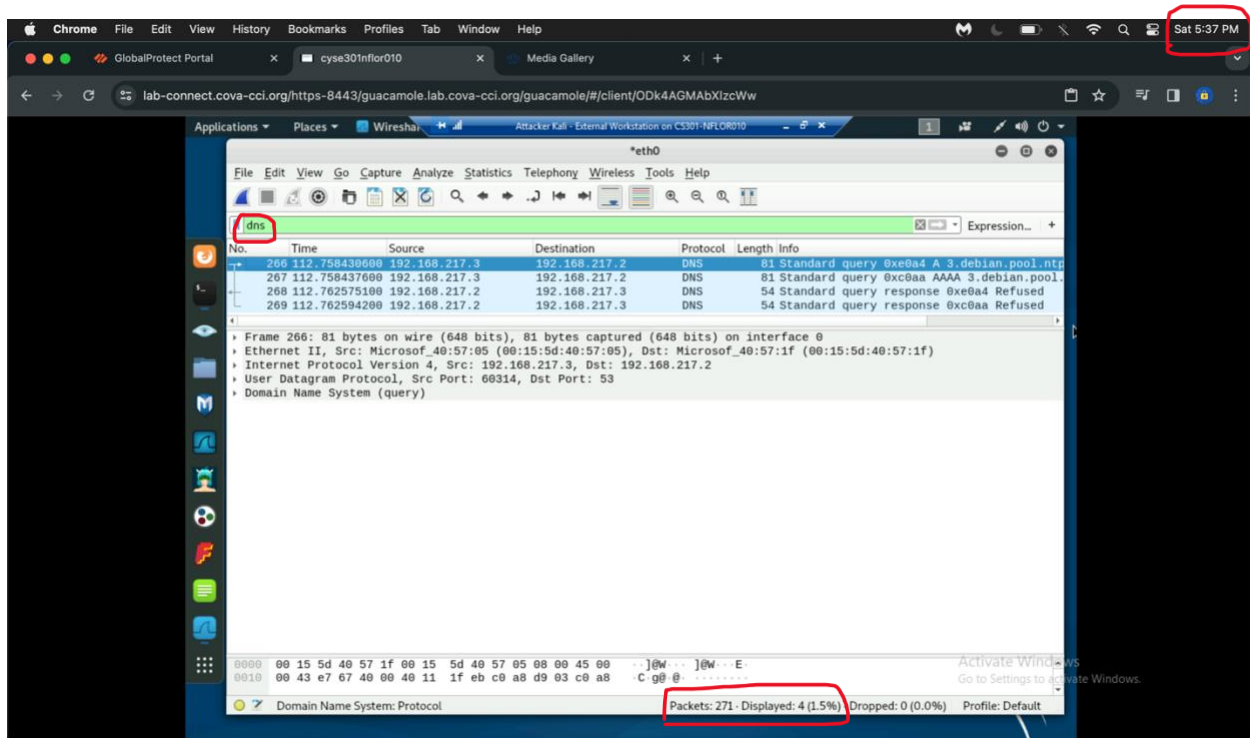
After applying the “ICMP” as the display filter, 120 packets were captured but 92 packets were displayed. 76.7% of the packets were displayed.

Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



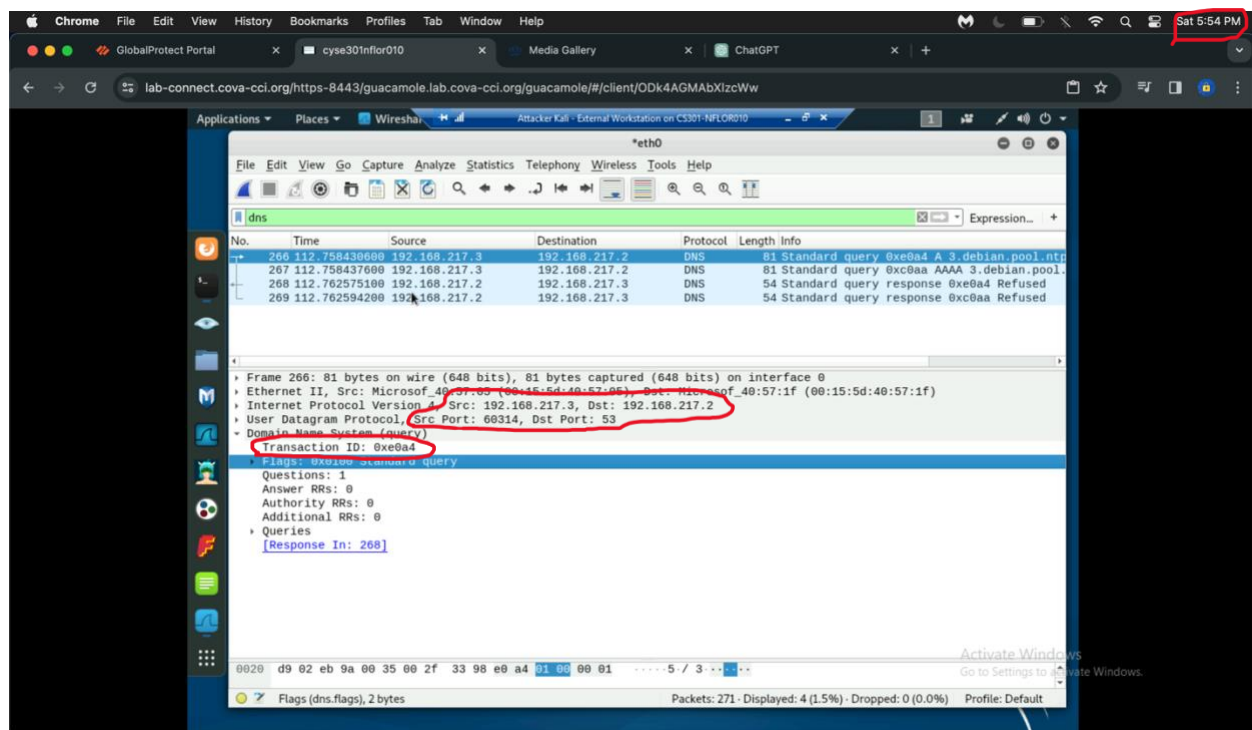
The source IP is 192.168.10.10 and the destination IP is 192.168.217.3. The BE sequence number is 1 and the LE sequence number is 256. The data size is 48 bytes, and the response time is 4.467 milliseconds.

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



I didn't see any DNS packets when I applied the filter, so I began capturing more packets. I waited 30 seconds and then stopped capturing. After applying the “DNS” as a display filter, I now have 271 packets captured and only 4 packets displayed. (1.5% of packets were displayed).

Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: **IP:port.**



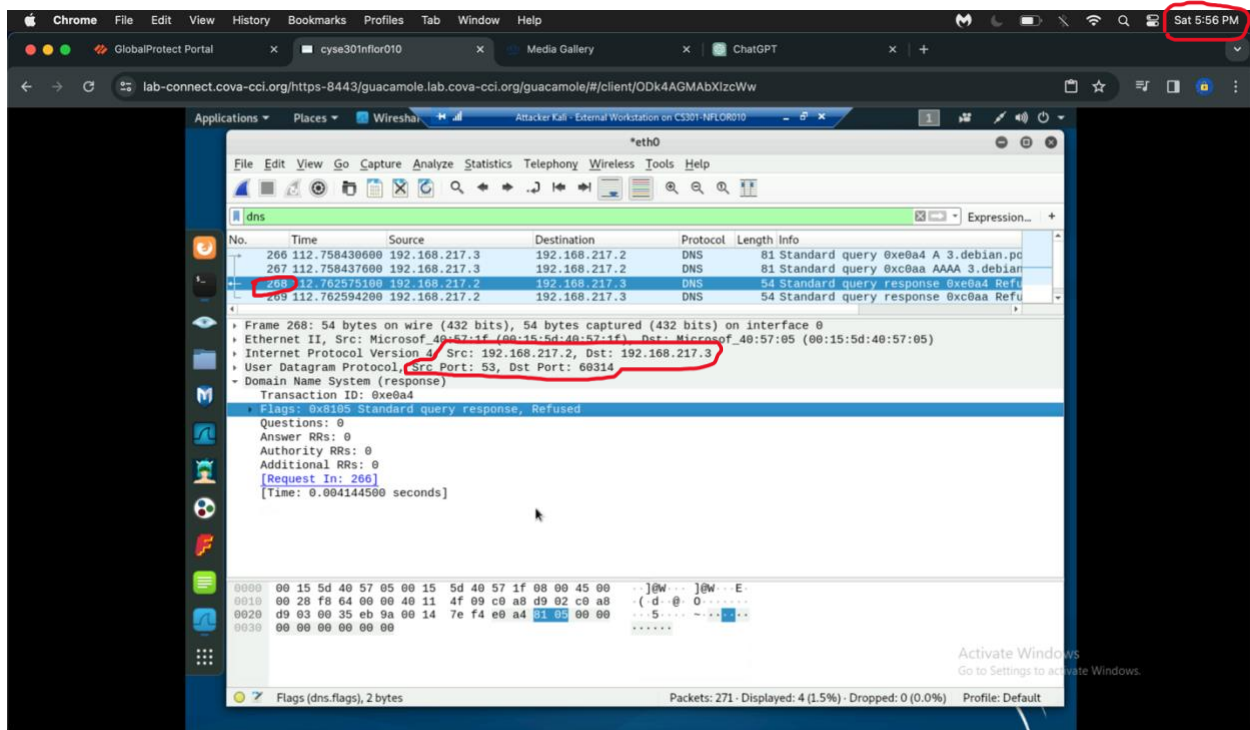
The DNS query packet I chose is number 266.

The Domain name for the DNS query packet is 0xe0a4.

The Source IP:192.168.217.3: Src Port: 60314

The Destination IP: 192.168.217.2: Dst Port: 53

Q6. Find the **corresponding** DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?



The corresponding DNS response to the query is number 268.

The Source IP: 192.168.217.2: Src Port: 53

The Destination IP: 192.268.217.3: Dst Port: 60314