OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Simon Graves

01195419

TASK A

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

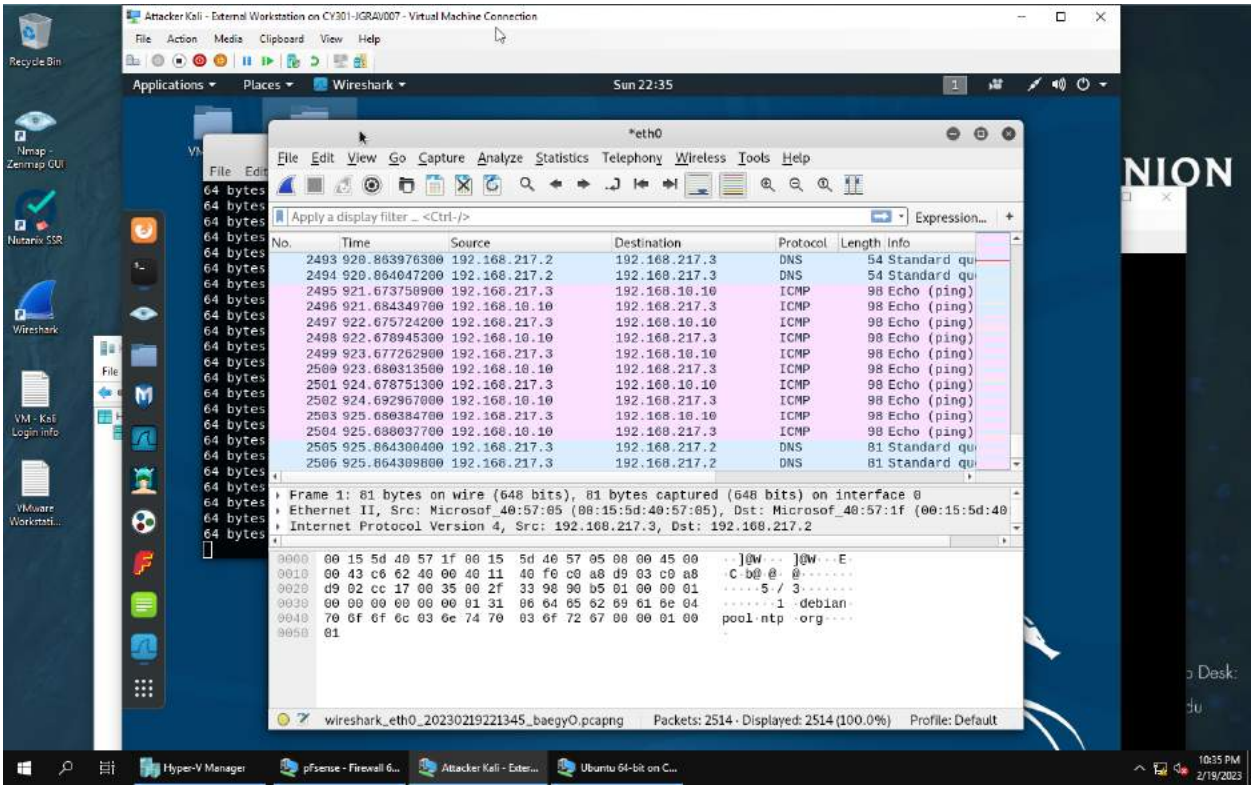

Figure 1 Screenshot of answer to Q.1

There are 2514 packets captured in total and display is 2514.

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

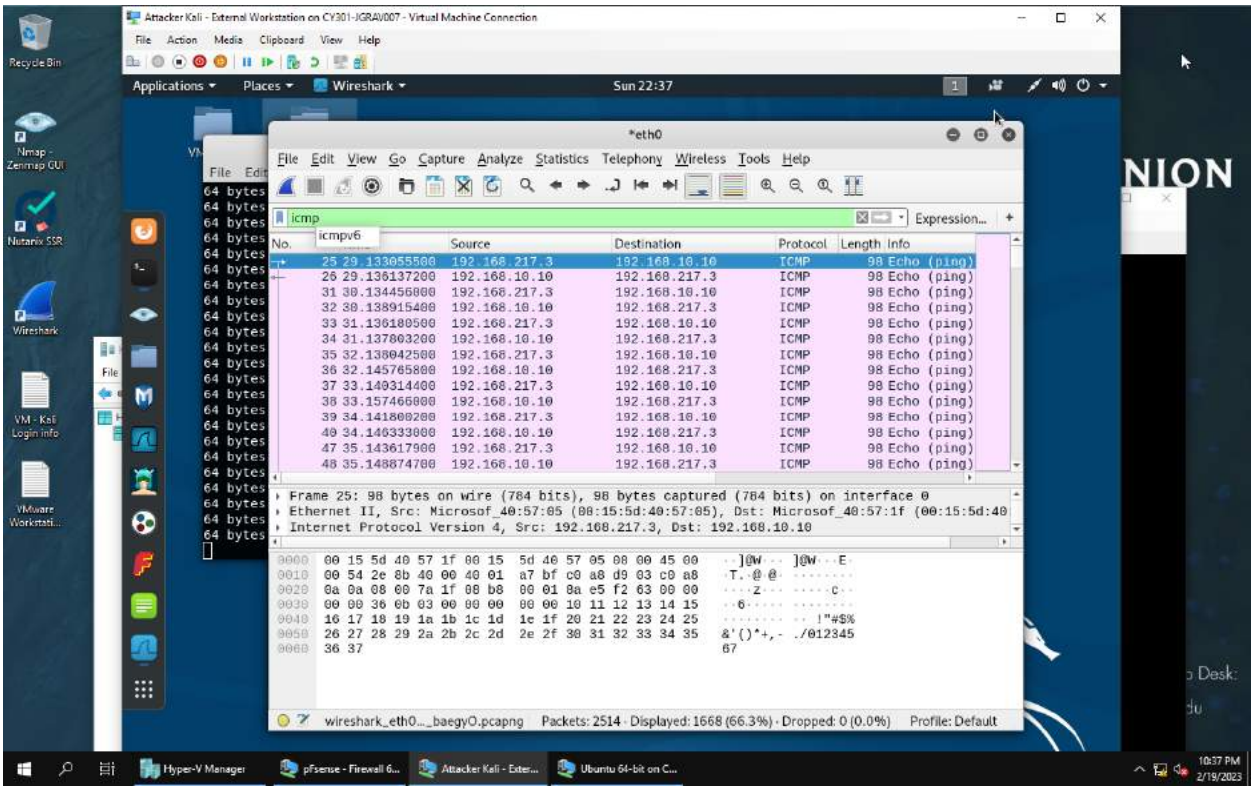

Figure 2 Q.2

They have 2514 packets on this one. And display is 1668.

3. Select an Echo (replay) 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?

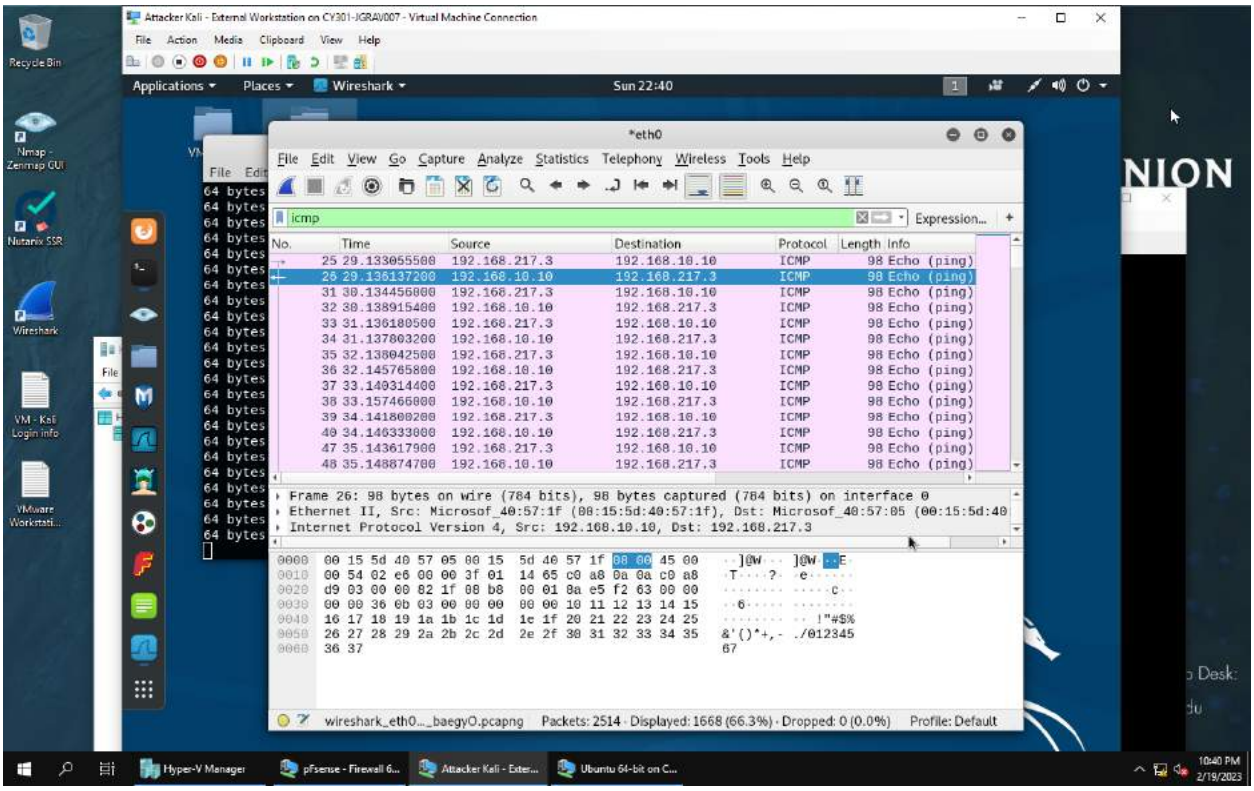

Figure 3 Q.3

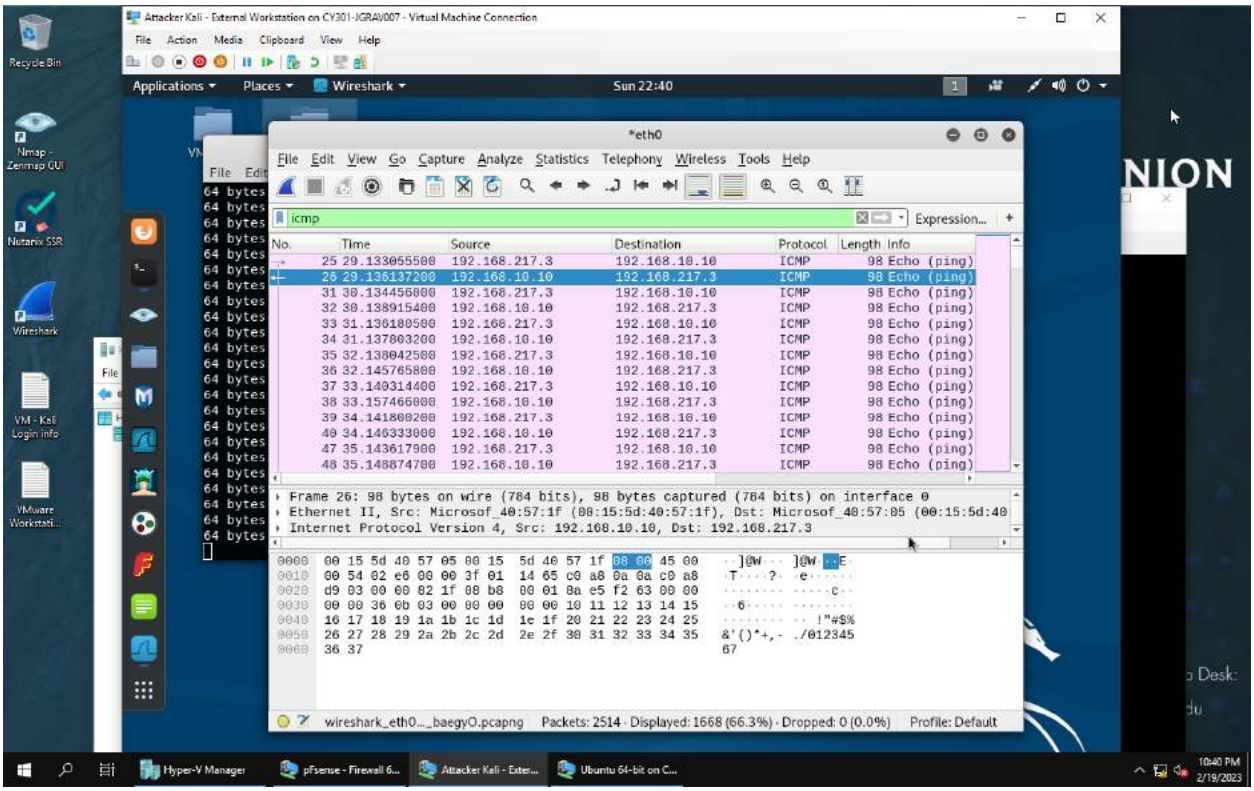

Figure 4 Q.3

What are the source and destination IPs of thispacket? The source is 192.168.217.3 the destination is 192.168.10.10. What are the sequence number and the size of the data? The data size is 98 byte and sequence number are 721/53506. What is the response time? The time is 29.136.

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

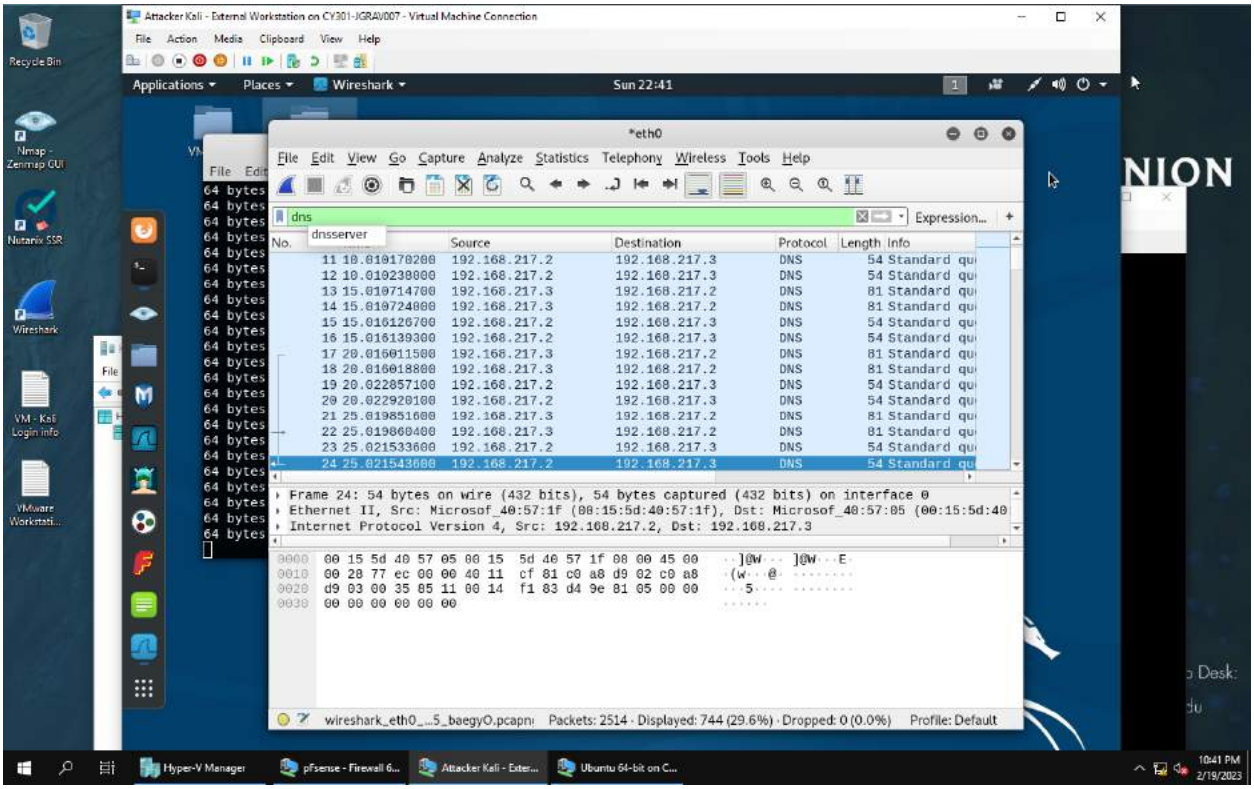

Figure 5 Q.4

How many packets are displayed? The display is 744.

5. 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.**

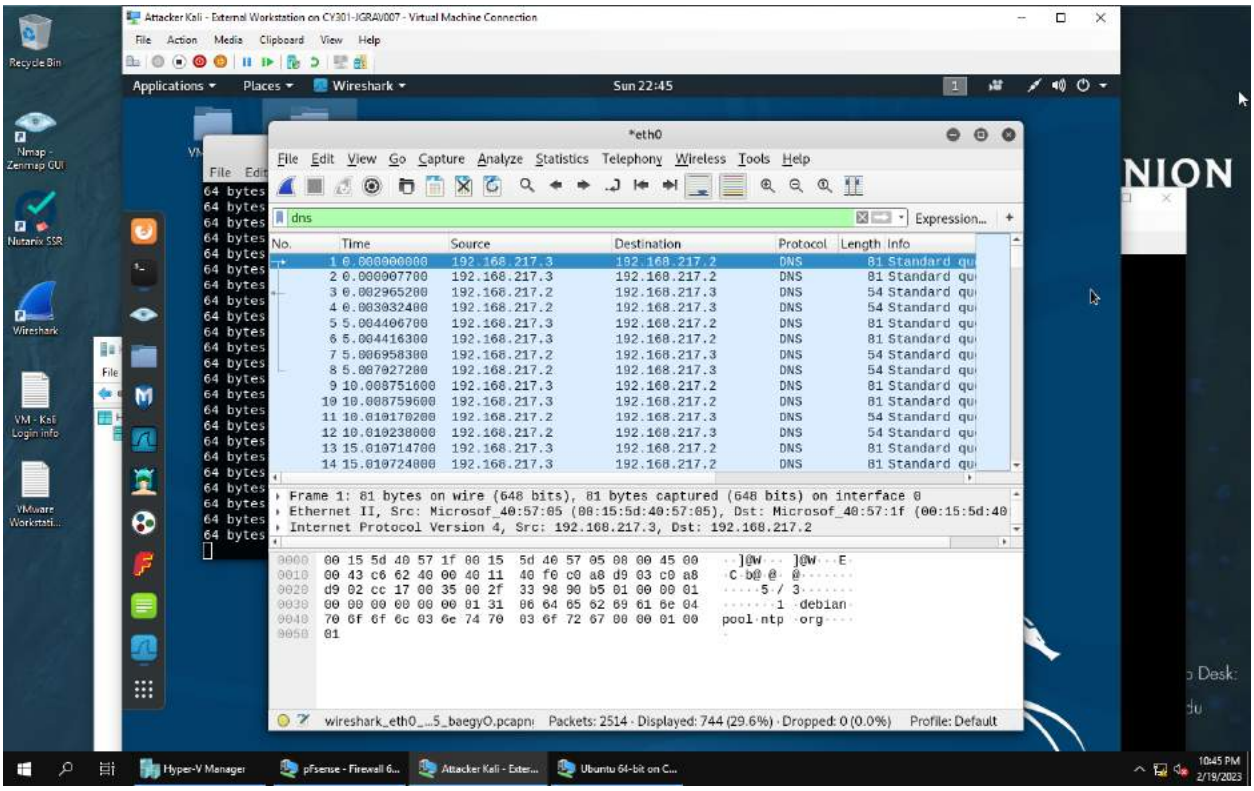

Figure 6 Q.5

What is the domain name this host is trying to resolve? The domain name Internet protocol v 4. What is the source IP and port number, destination IP and port number? The source 192.168.217.3:81. The destination 192.168.10.10:81.

6. 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?

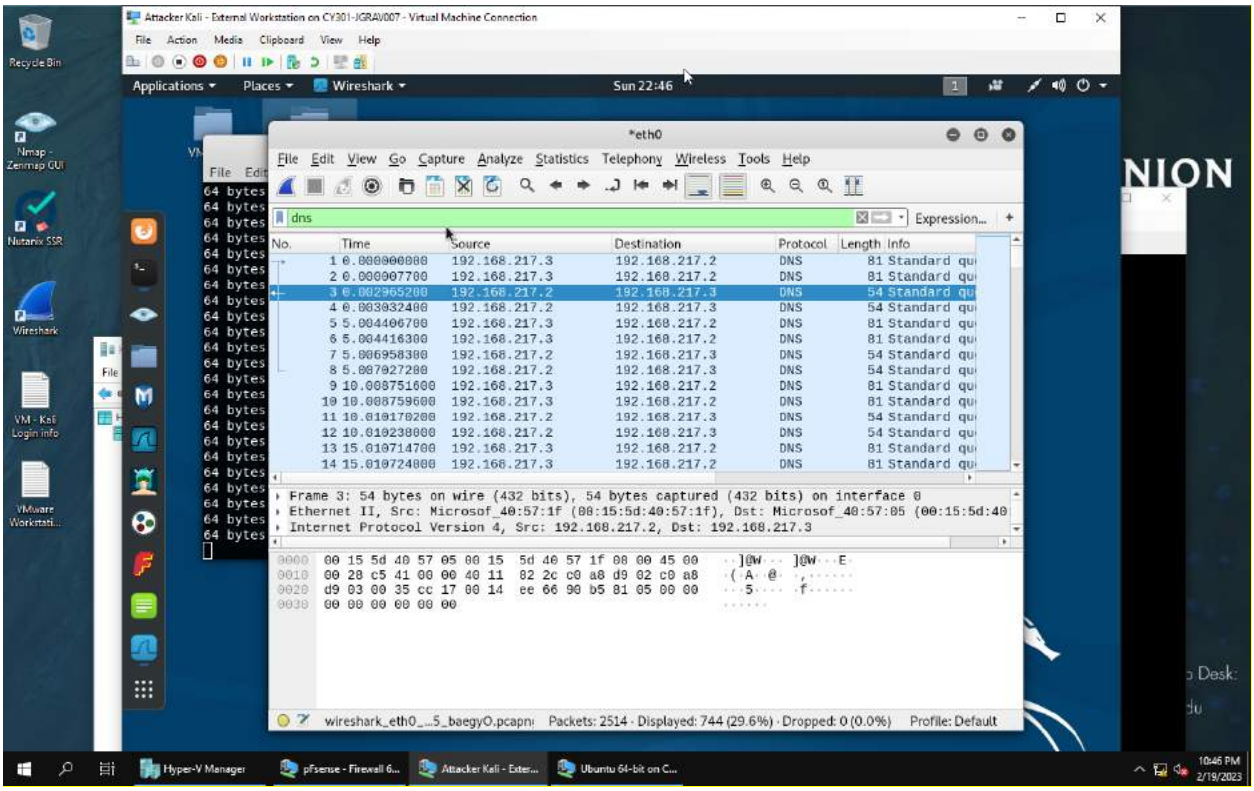

Figure 7 Q6.

what is the source IP and port number, destination IP and port number? Source 192.168.217.3:81 Destination 192.168.217.2:54. What is the message replied from the DNS server?

TASK B

1. Sniff ICMP traffic

Open two terminals on External Kali VM. Use one ping Ubuntu VM, and use the other ping

Internal Kali.

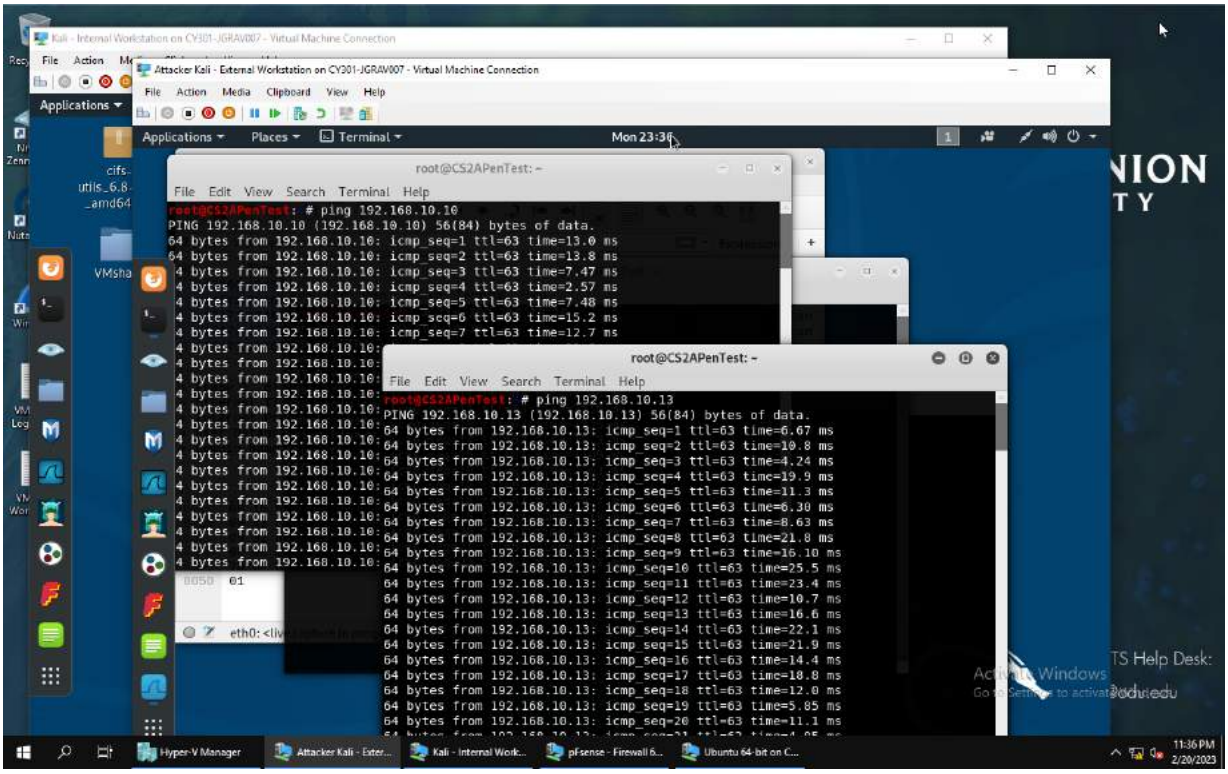

Figure 8 B.Q.1

a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic.

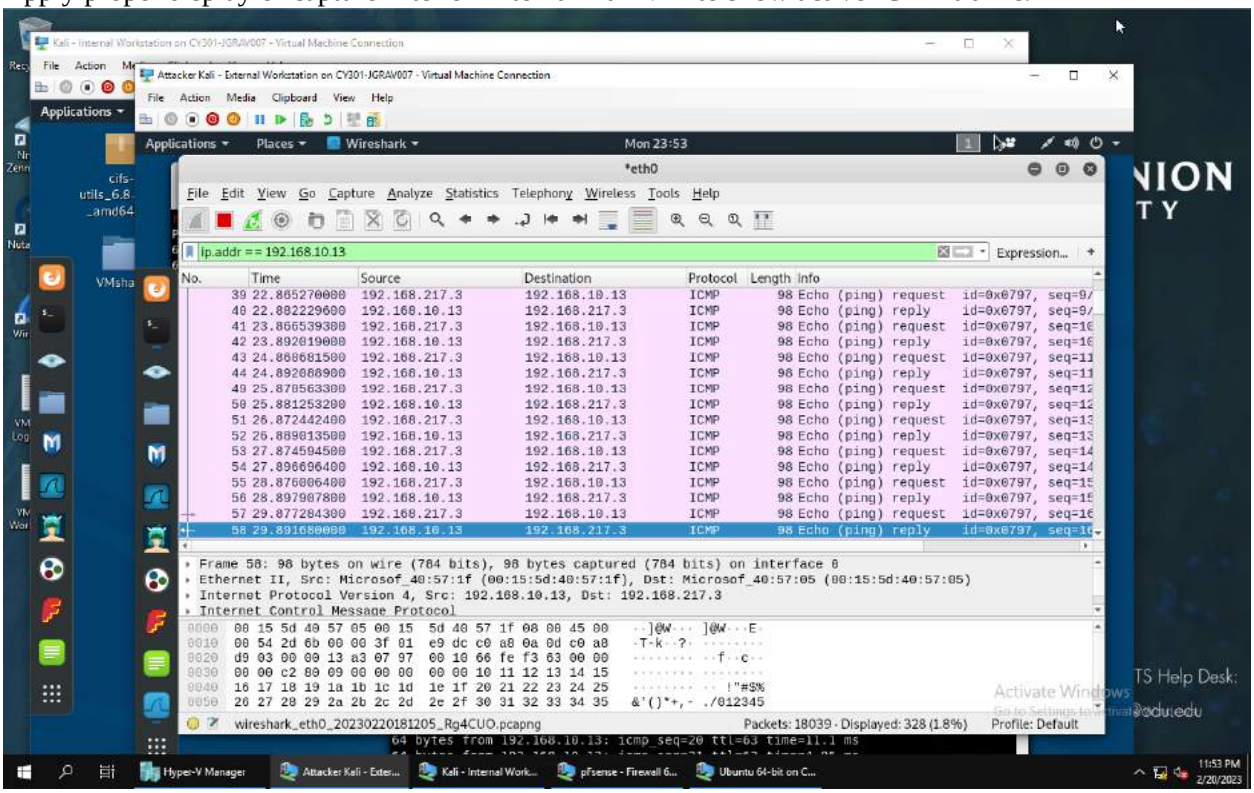

Figure 9 1.A.

b. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM.

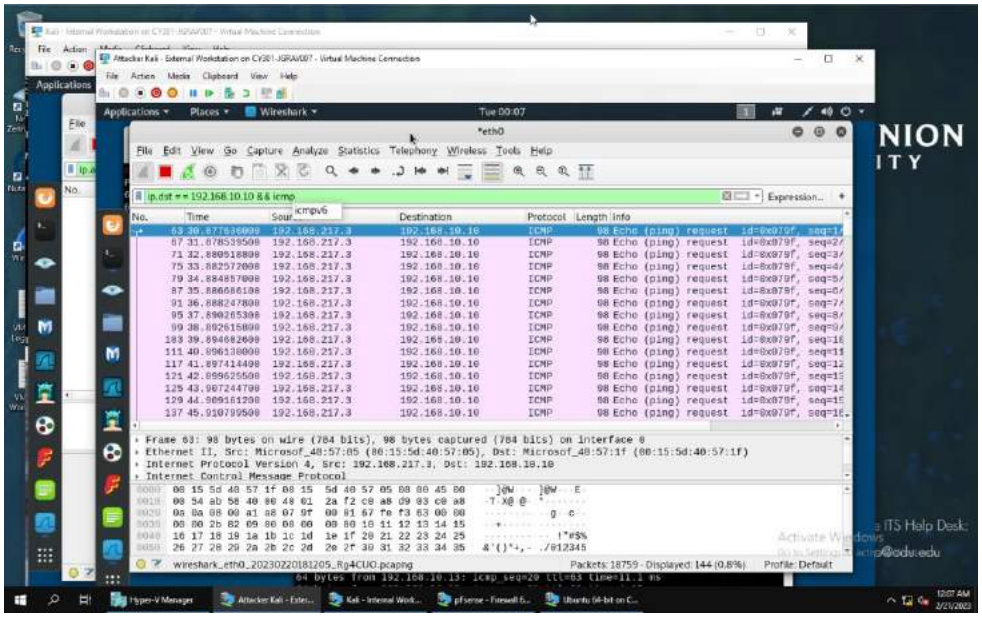

Figure 10 Q1.B.

2. Sniff FTP traffic

a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server.

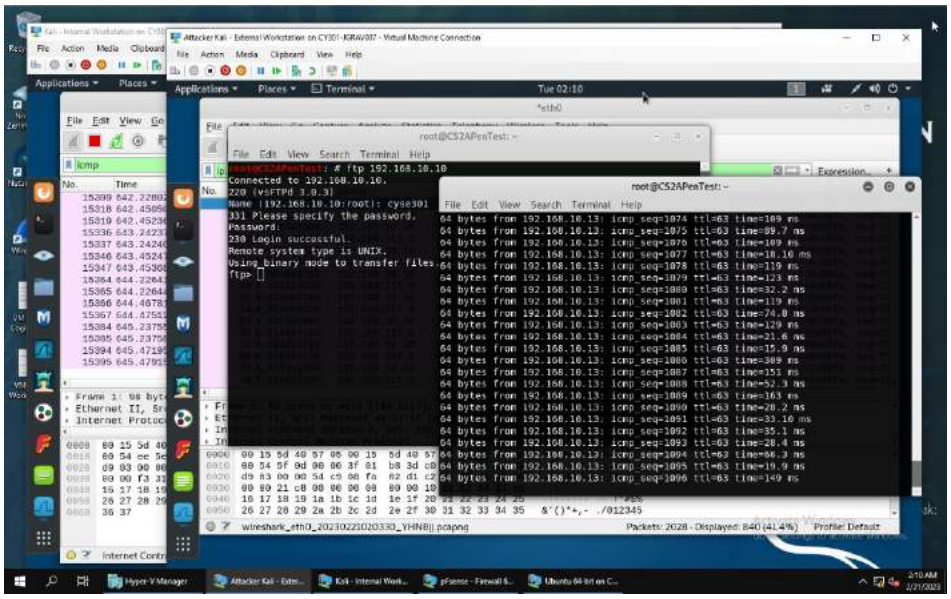

Figure 11 Q2.A.

b. Unfortunately, Internal Kali, the attacker, is also sniffing to the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to screenshot and explain how you find the password.

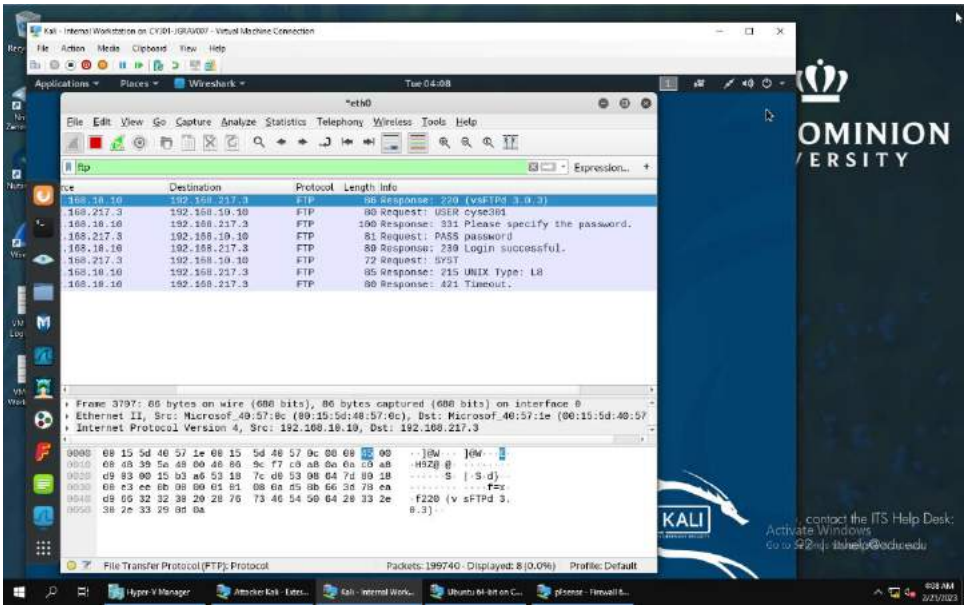

Figure 12 Q.2.B.

c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to

reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these “secrets” from the attacker VM, which is Internal Kali.

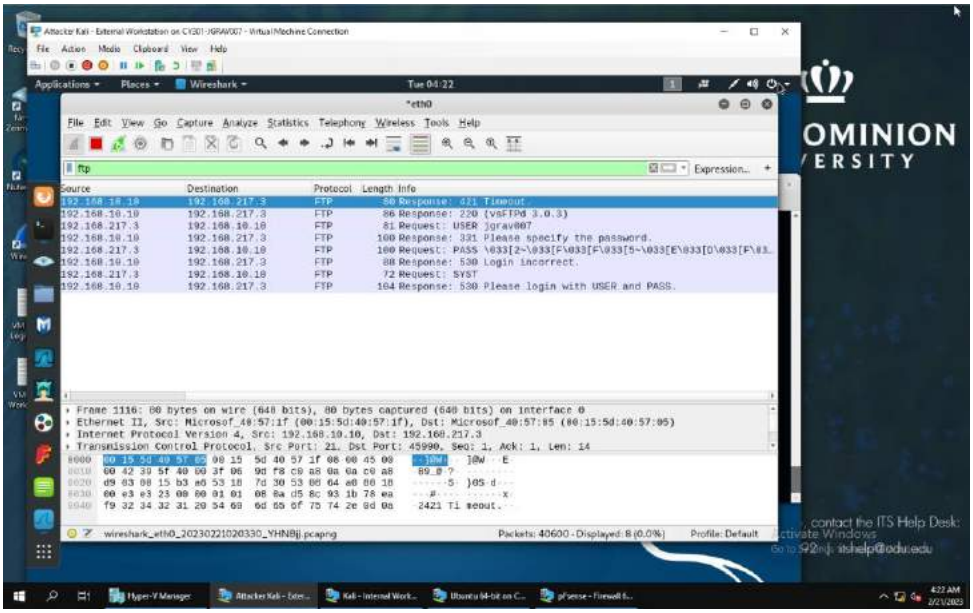

Figure 13 Q.2.B.