OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

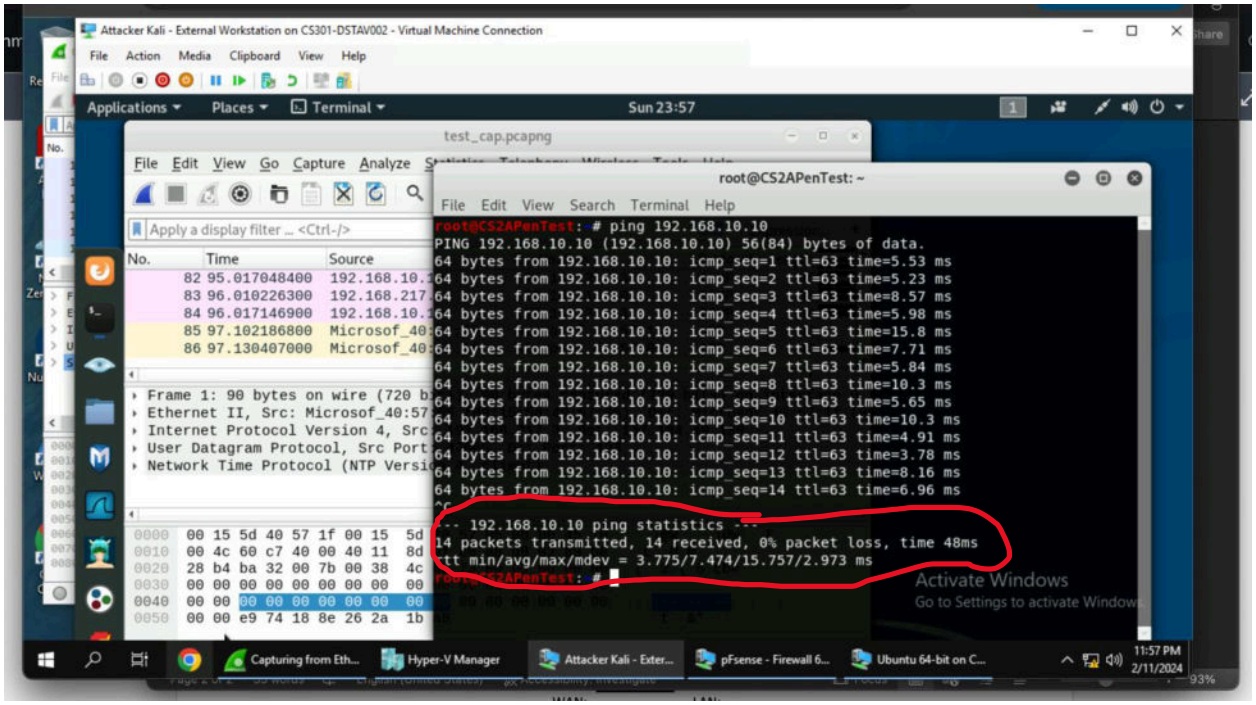
# Assignment #2 Traffic Tracing and Sniffing

Donte Staves

01171770

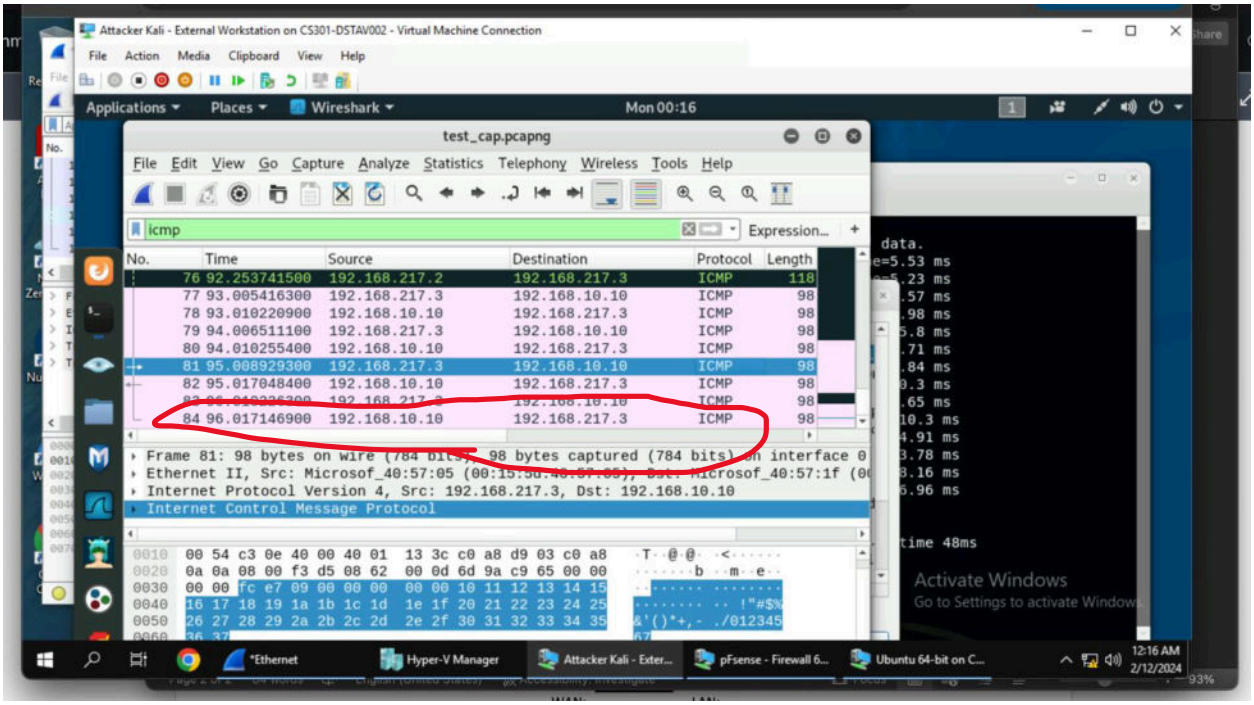
# TASK A

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



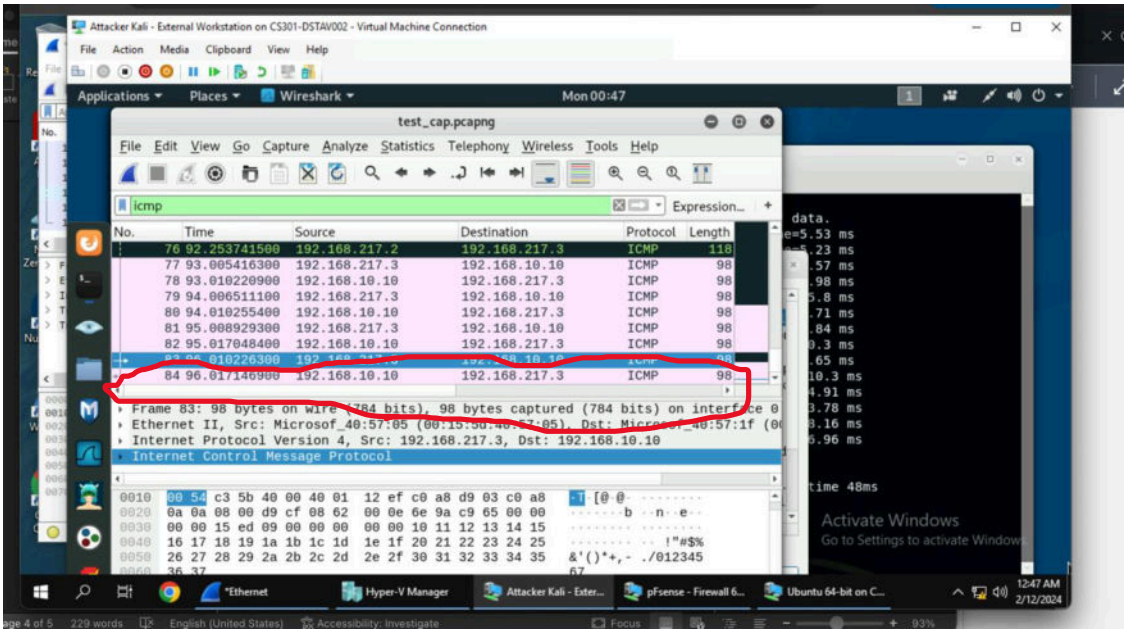

In this screenshot, I used the “ping” command to ping the Ubuntu VM and it shows that 14 packets were captured in total. This also shows that 14 packets are displayed

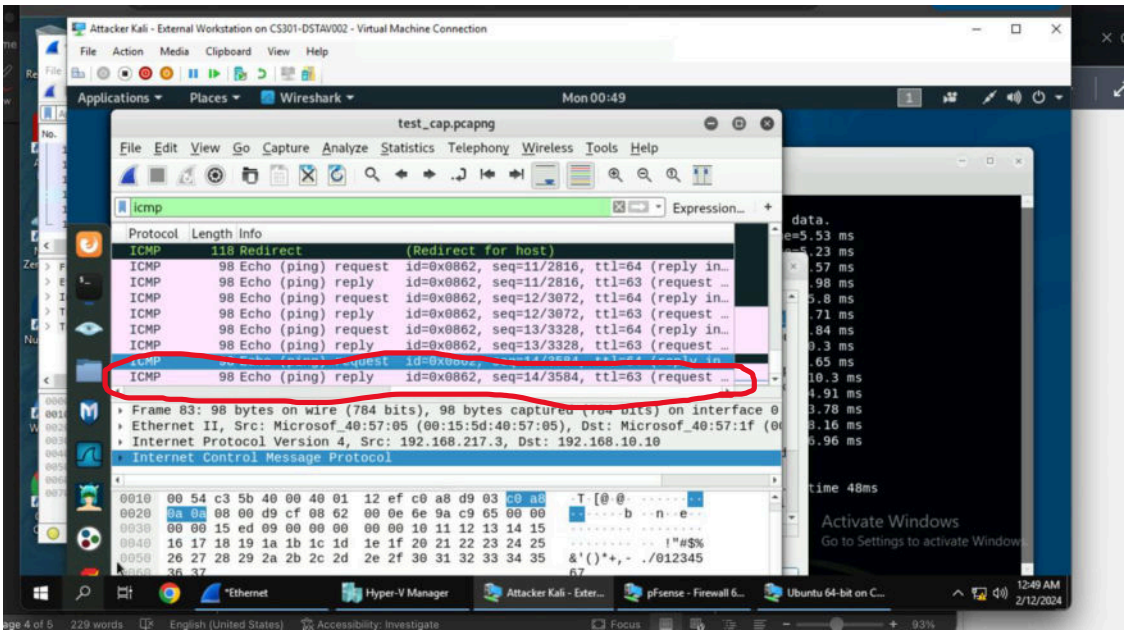
2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).




In this screenshot, this shows “ICMP” displayed as a filter in Wireshark and showing that 84 packets had been capture. There were also 84 packets displayed.

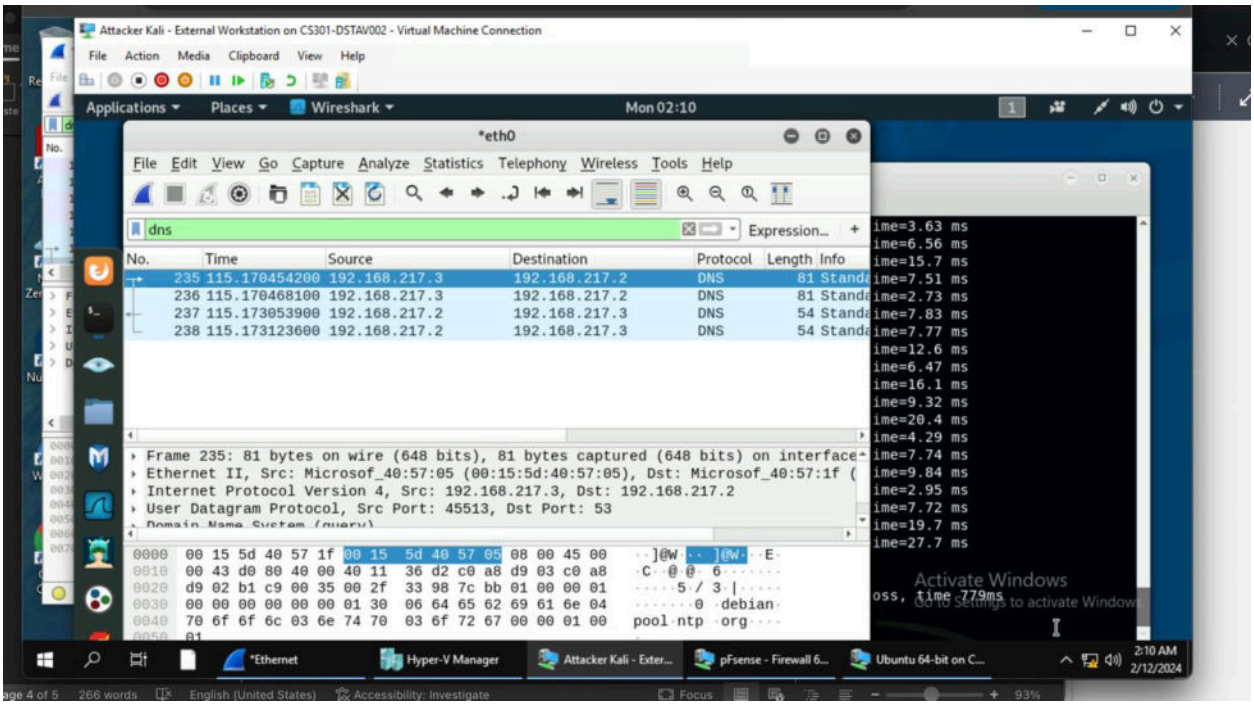
3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



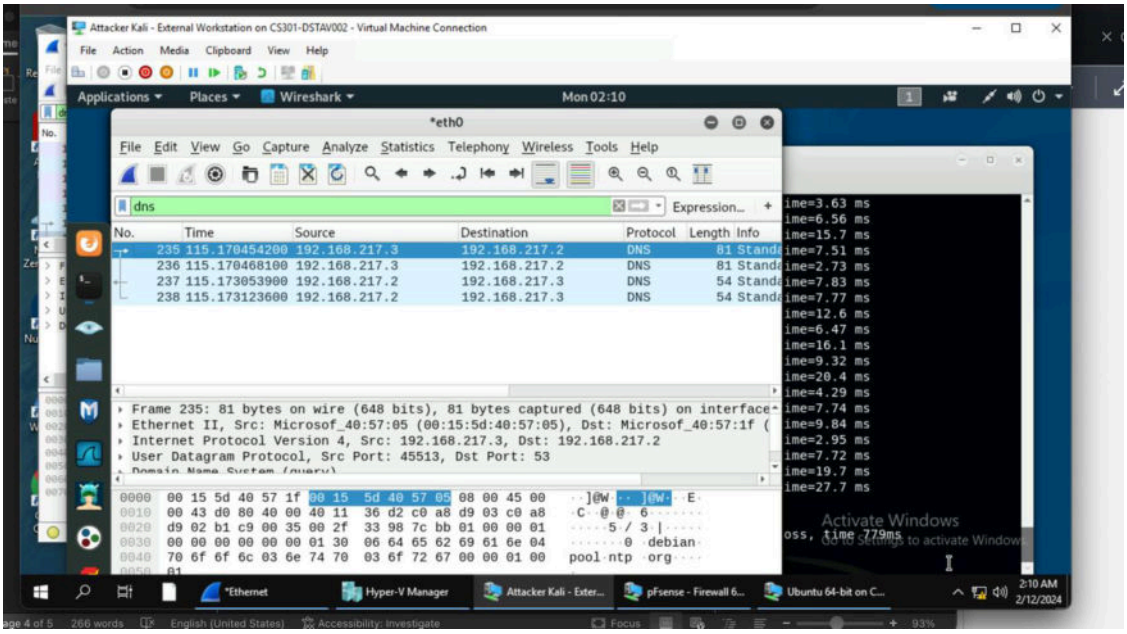

In these screenshots, you can see an Echo (replay) message. The source destination IP is “192.168.10.10” and the destination IP is “192.168.217.3”. The sequence number and size of the data is “14/3584”. The response time is “96.017146900”.

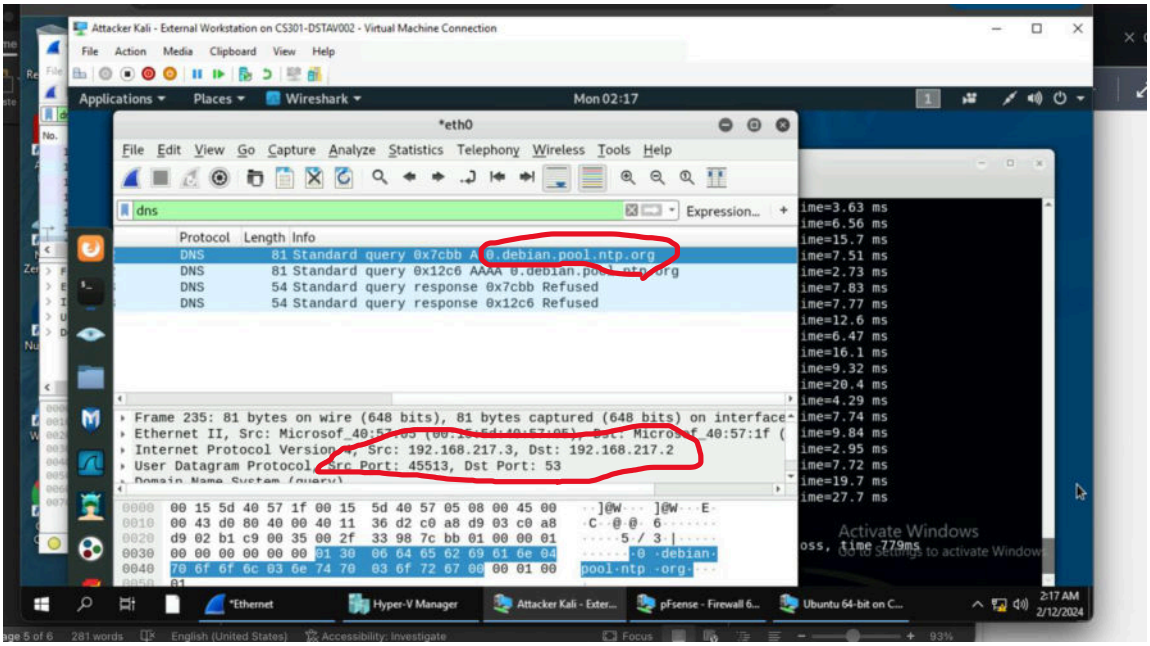
4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed.




In this screenshot, “DNS” was applied as a display filter and 4 packets were displayed

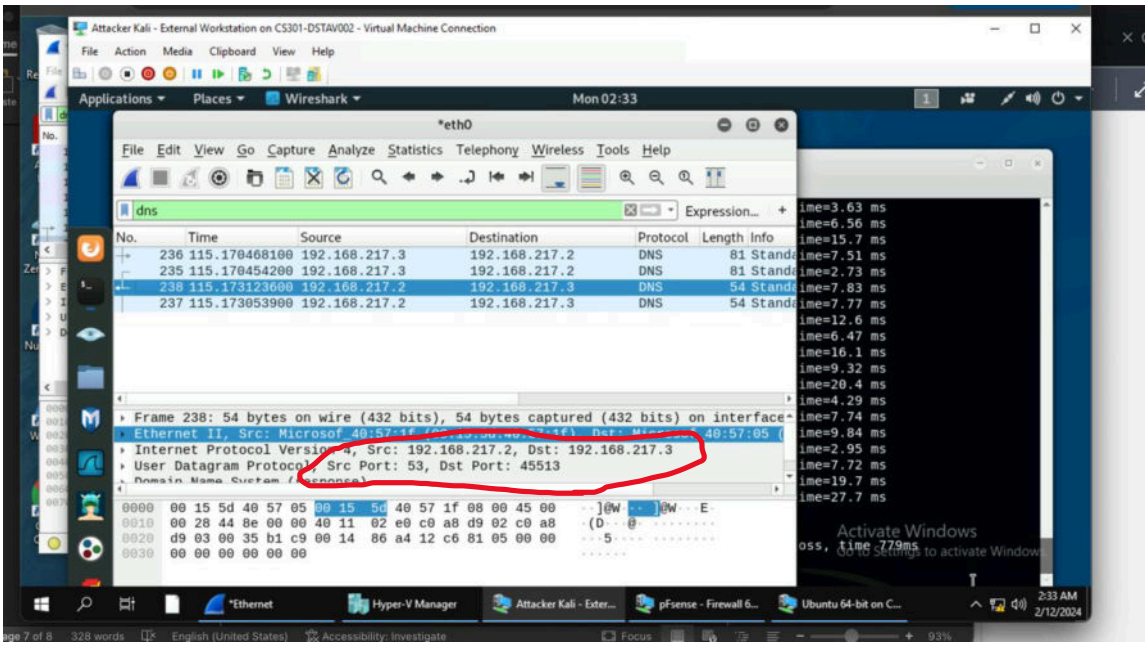
5. Find a DNS query packet. What is the domain name is this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format IP:port.

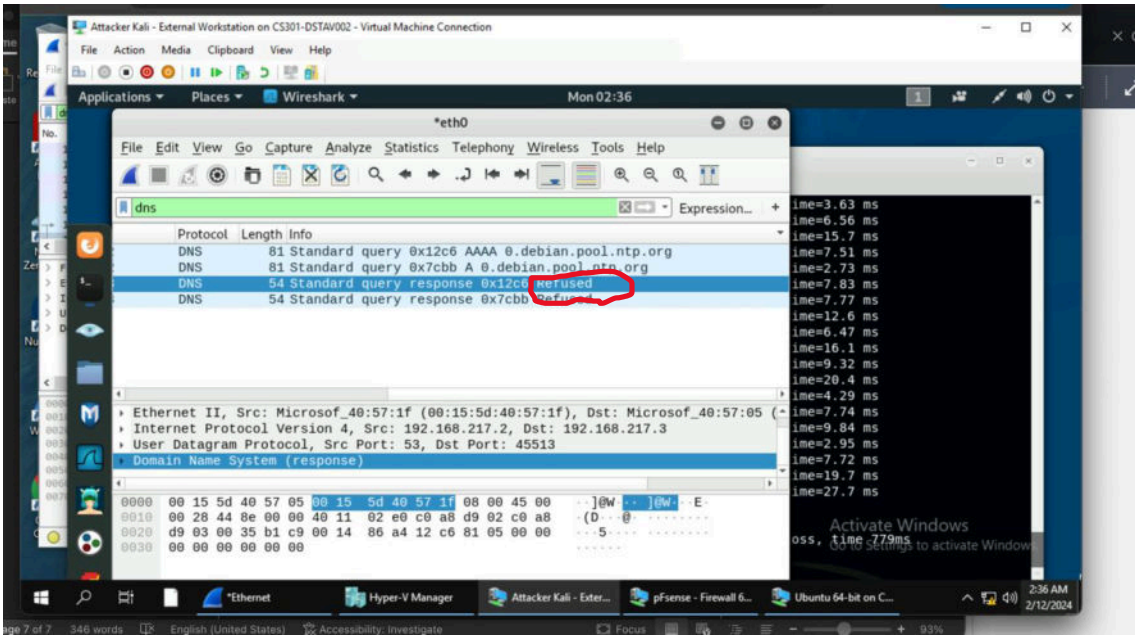



In these screenshots, the domain name the host is trying to resolve is “0.debian.pool.ntp.org”. The source IP and port number is “192.168.217.3:45513” and the source destination IP and port number is “192.168.217.2:53”.

6. Find the corresponding DNS response in 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?

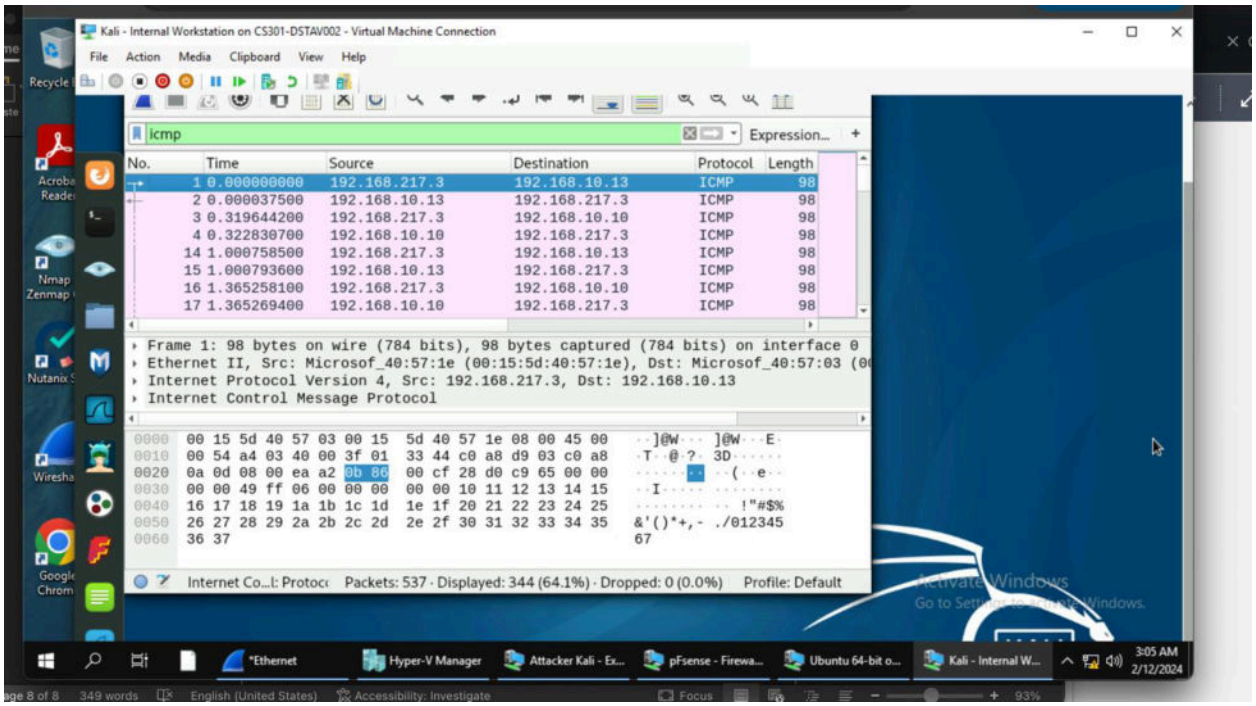



In this screenshot, The source IP and port number for the corresponding DNS response is “192.168.217.2:53” and the destination IP and port number is “192.168.217.3:45513”. The message replied from the DNS server is “Refused”.

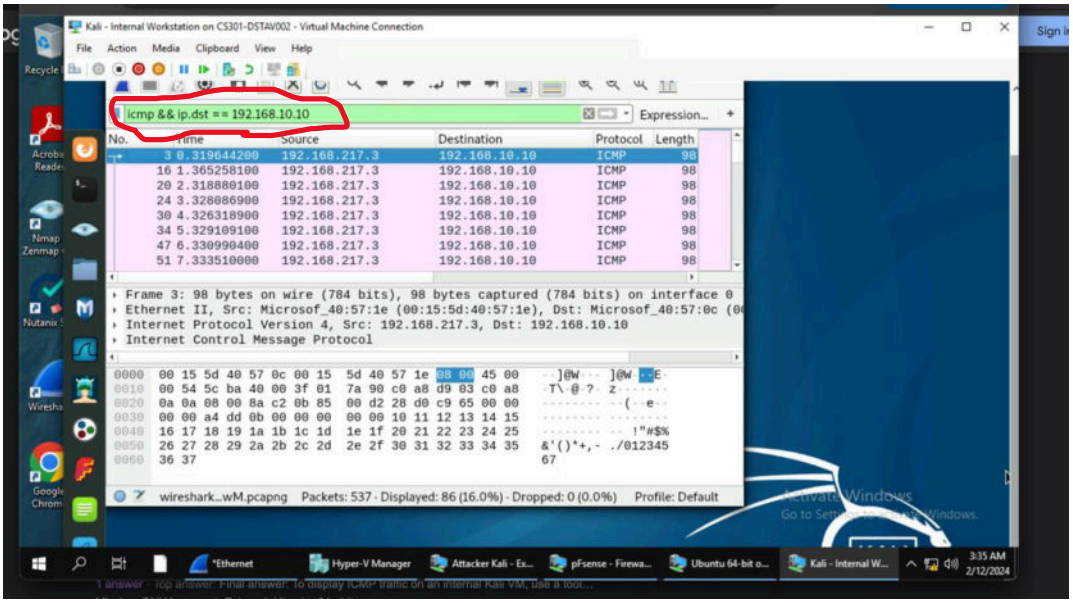
# Task B

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



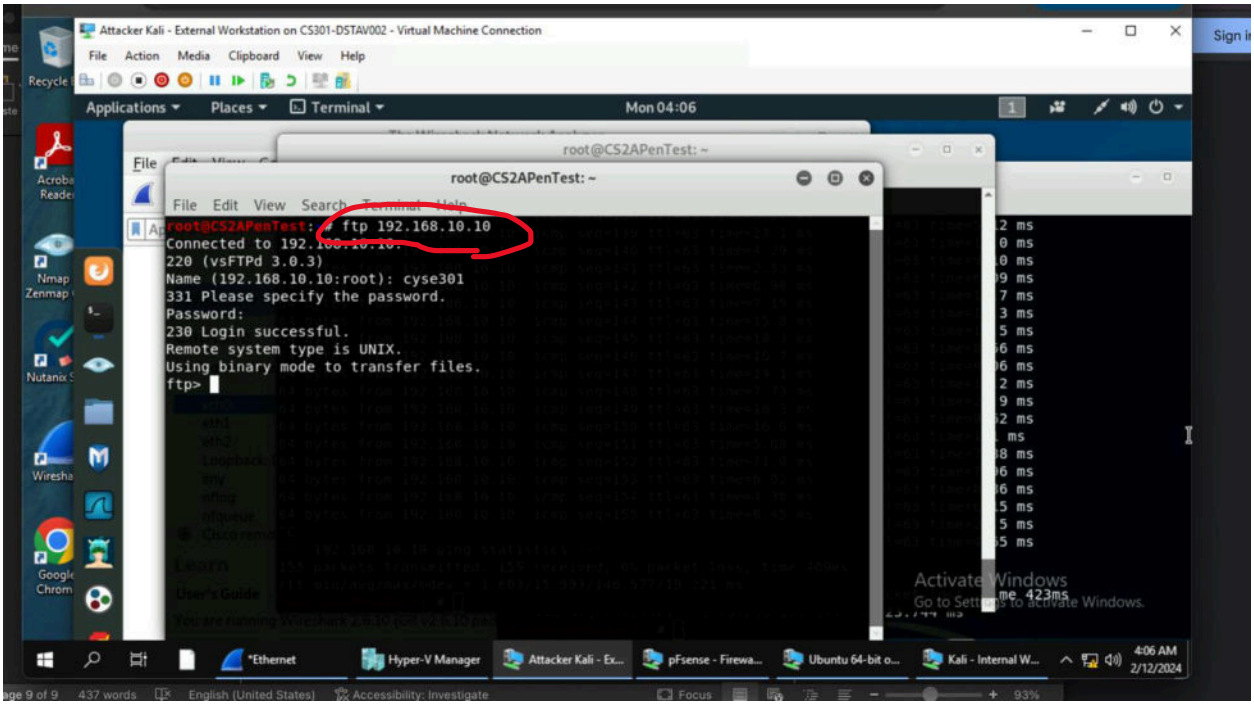

In this screenshot, I used “ICMP” to properly display ICMP traffic on Internal Kali VM.

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.

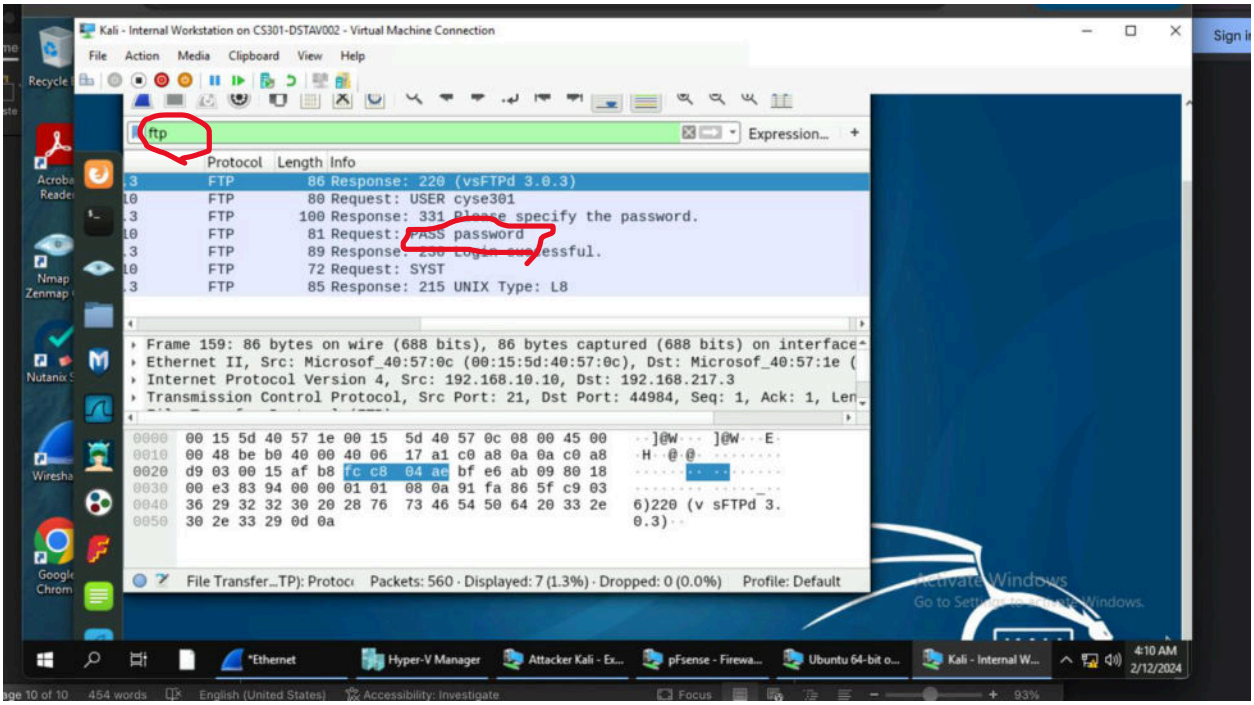



In this screenshot, I used “icmp && ip.dst == 192.168.10.10” to only display ICMP request that originated from External Kali VM and goes to Ubuntu 64-bit VM.

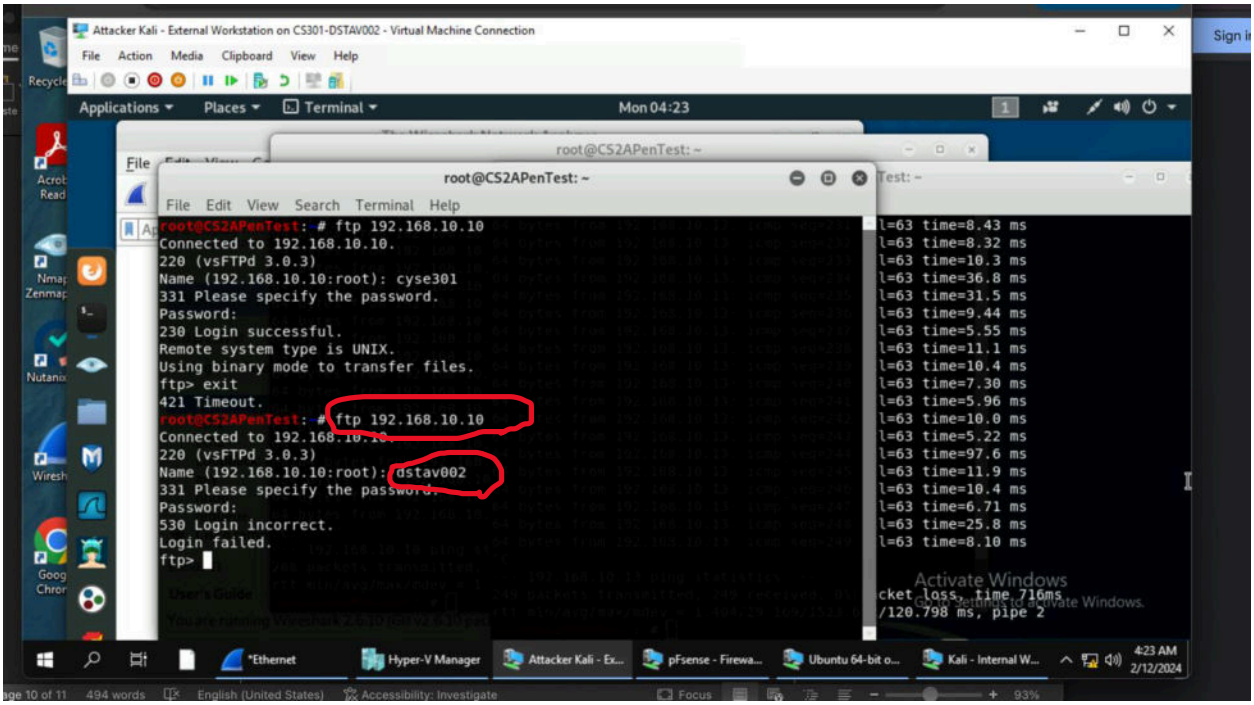
2. Sniff FTP traffic

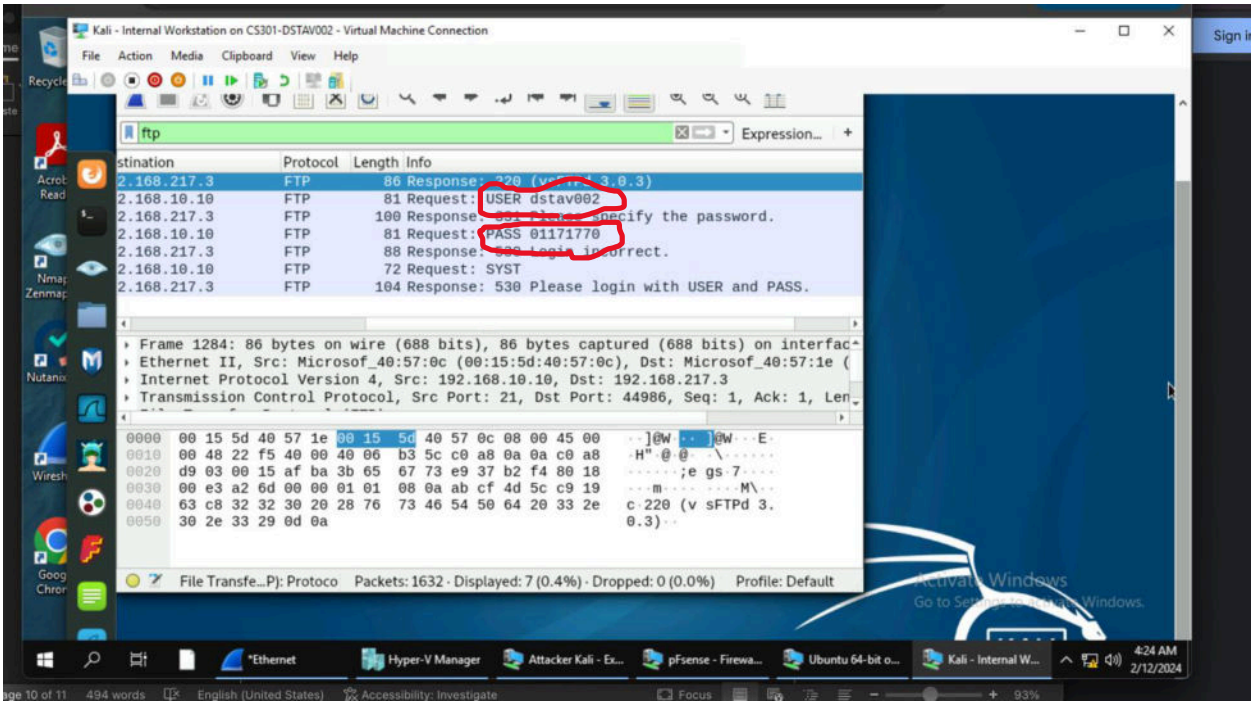
a. 


In this screenshot, I used the command “ftp 192.168.10.10” to connect to the Ubuntu 64-bit VM.

b. 


In this screenshot, I filtered the traffic on the Internal Kali VM using “ftp” in the search bar and scrolled right to see the information between the External Kali VM and the Ubuntu 64-bit VM to get the password.

c. 


In these screenshots, I used the command “ftp 192.168.10.10” to connect to the Ubuntu 64-bit VM. I then used my MIDAS ID for the username and my UIN for the password. I then went to the Internal Kali VM and typed into the filter “ftp” and scrolled over to see the packets containing the “secrets” with my MIDAS ID and UIN.