OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

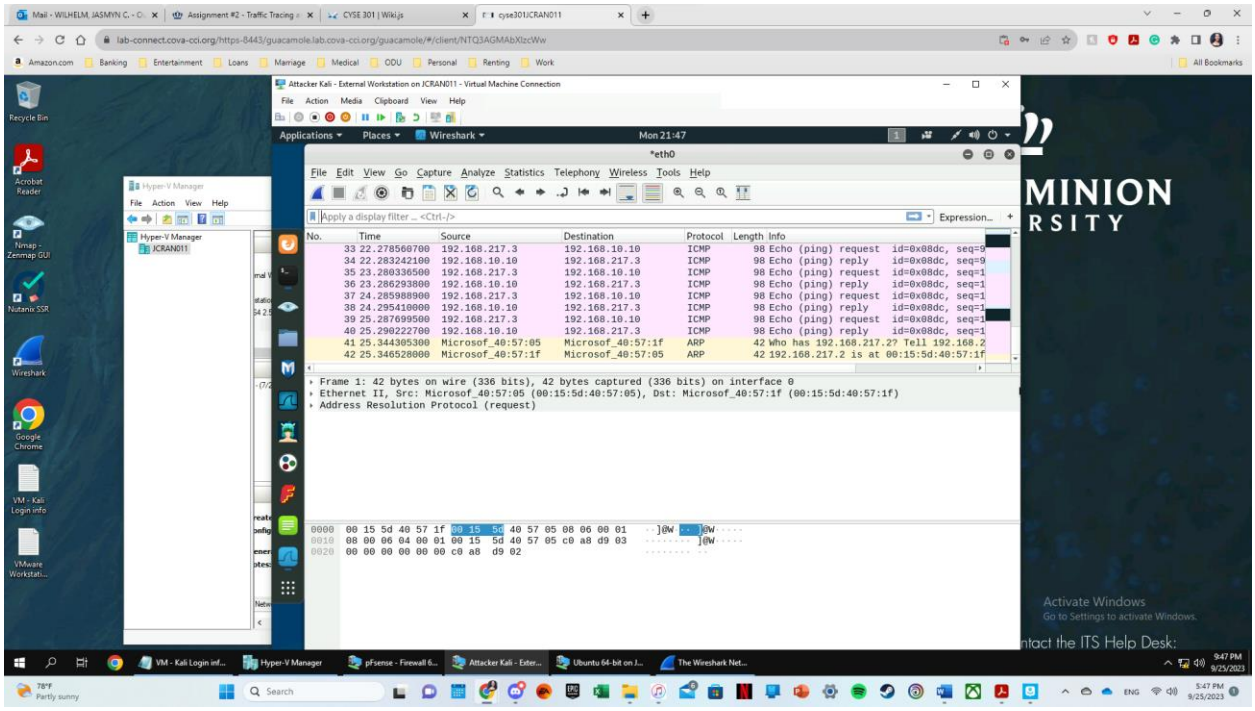
Jasmyn Wilhelm

01155323

Task A: Get started with Wireshark

Question 1:

In 5-10 seconds of capturing the ping to Ubuntu, 42 bytes were captured in total and 42 are displayed as no filters are applied.

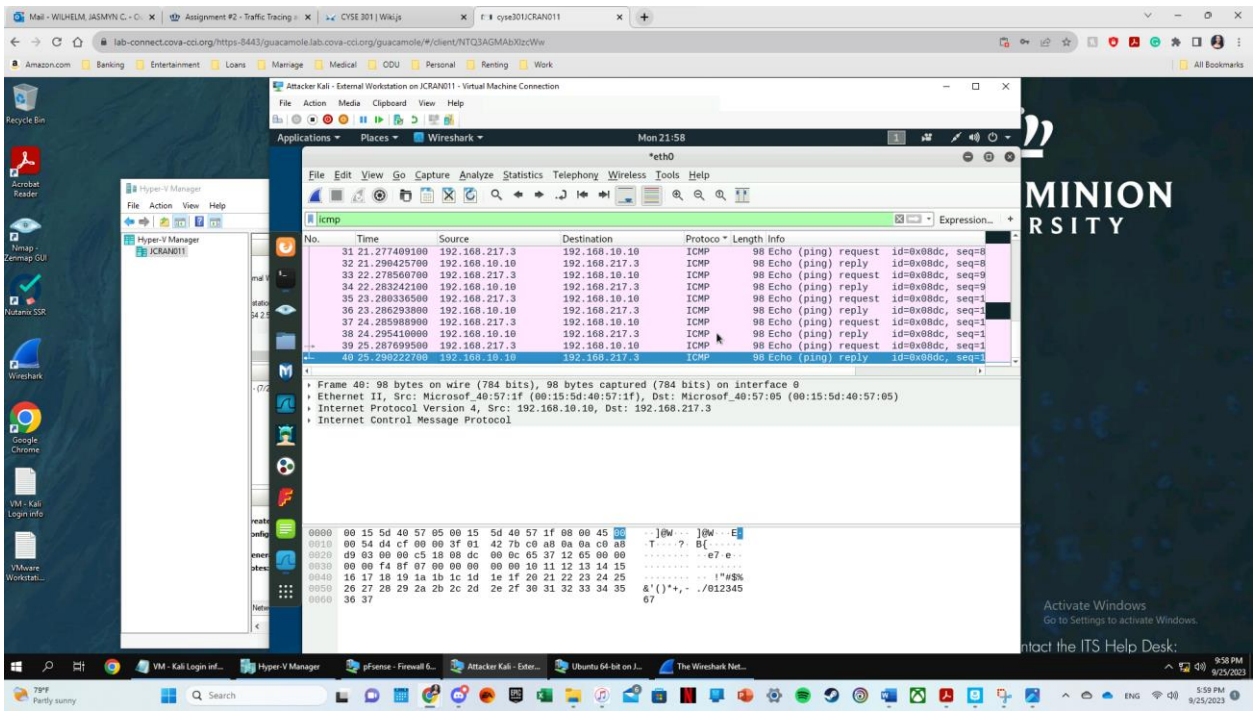


Question 2:

When filtering the protocol to only show ICMP 42 were captured overall, but only 40 (37) frames were displayed.

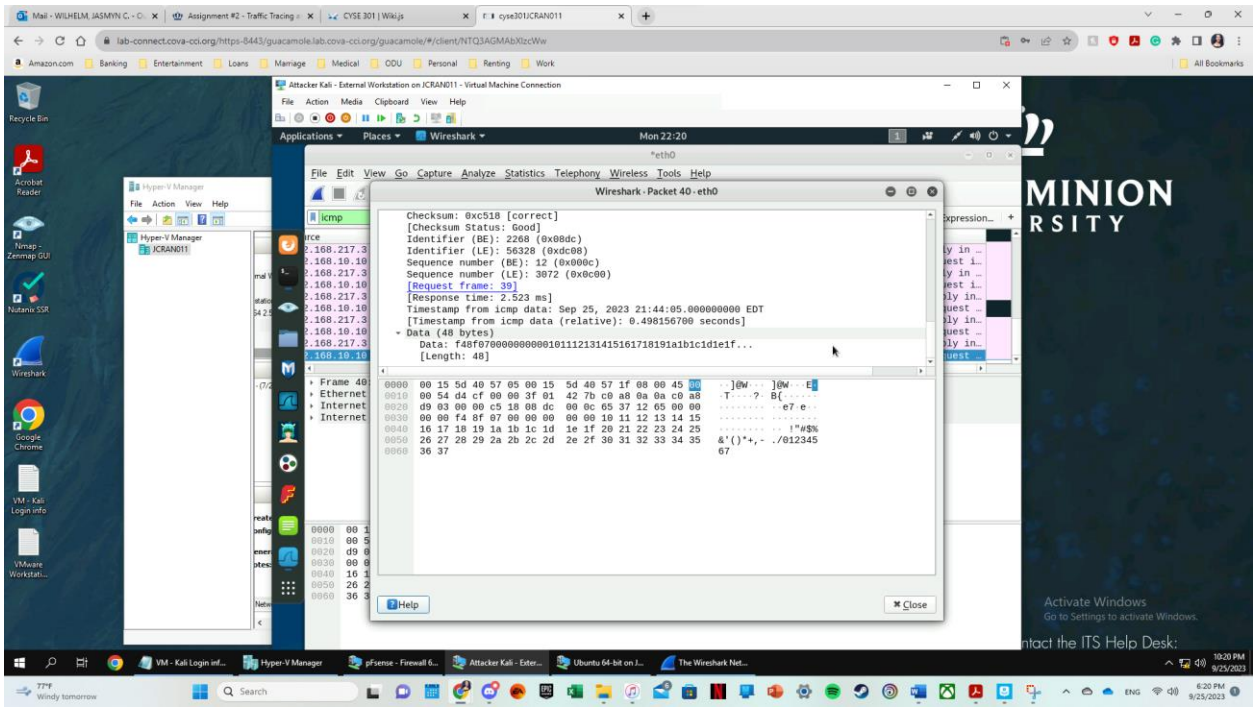
Question 3 part 1:

After selecting an echo reply message from the list, the source IP address is 192.168.10.10 with the destination address listed as 192.168.217.3



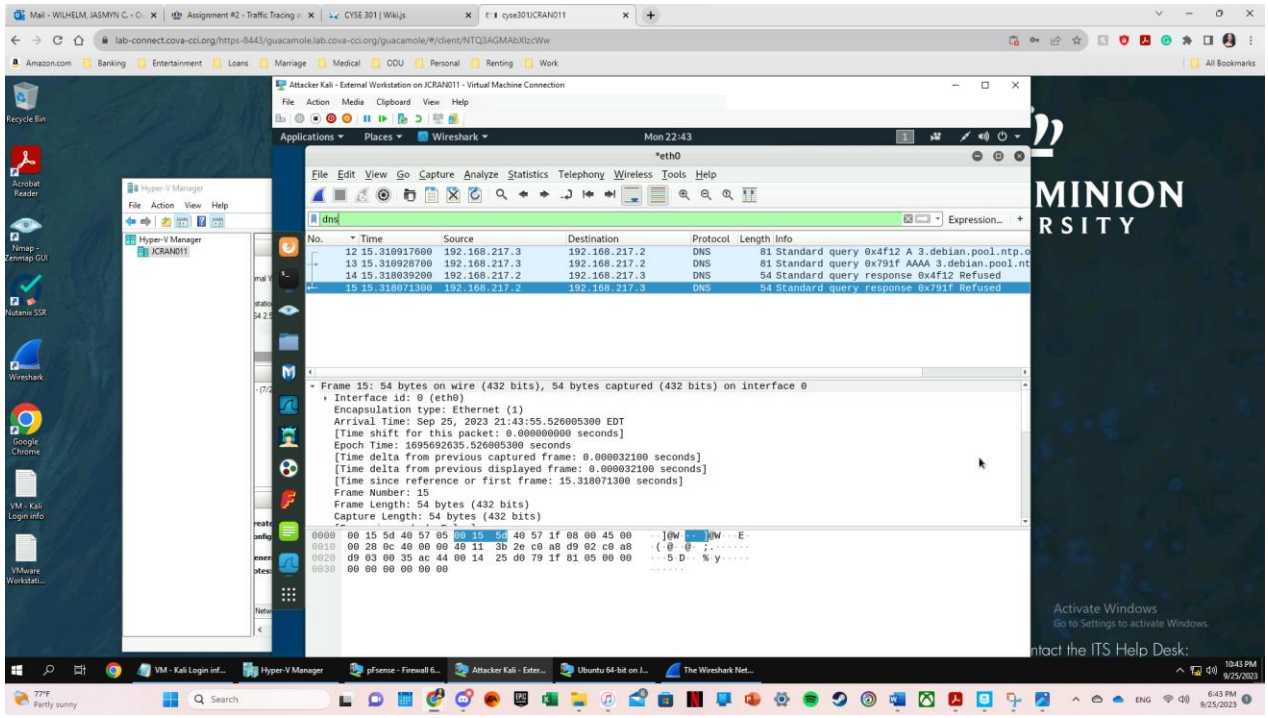
Question 3 part 2:

The sequence number is 12 (BE) or 3072 (LE). The size of the data itself is 48 bytes with a response time of 2.523 ns.



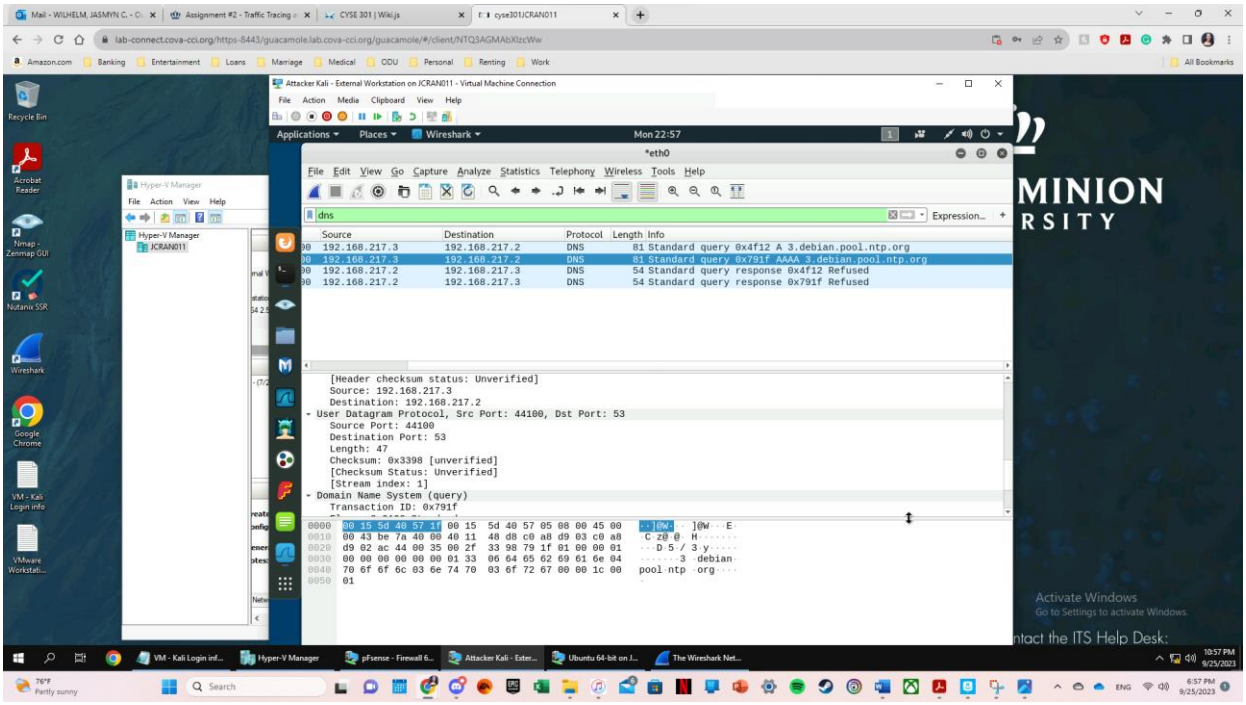
Question 4:

Only 4 packets are displayed while filtering to only show DNS packets.



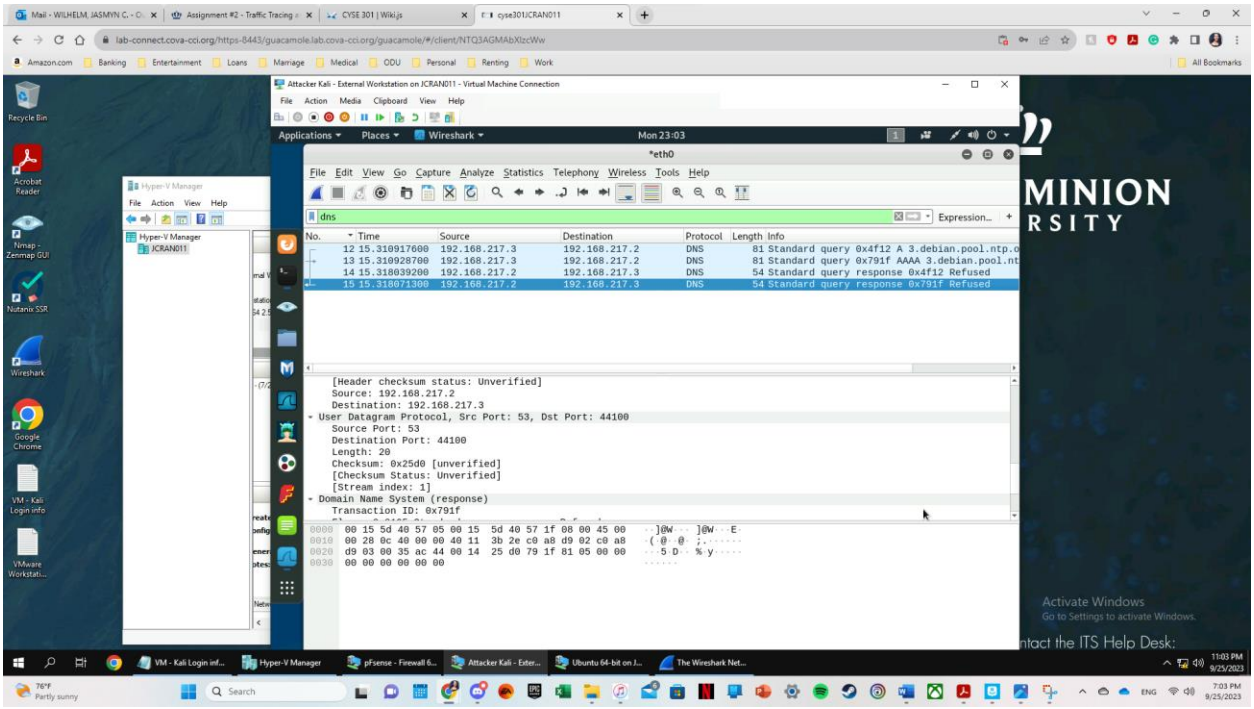
Question 5:

The domain name trying to be resolved is "3.debian.pool.ntp.org". The source IP and port is 192.168.217.3:44100 and the destination IP and port is 192.168.217.2:53.



Question 6:

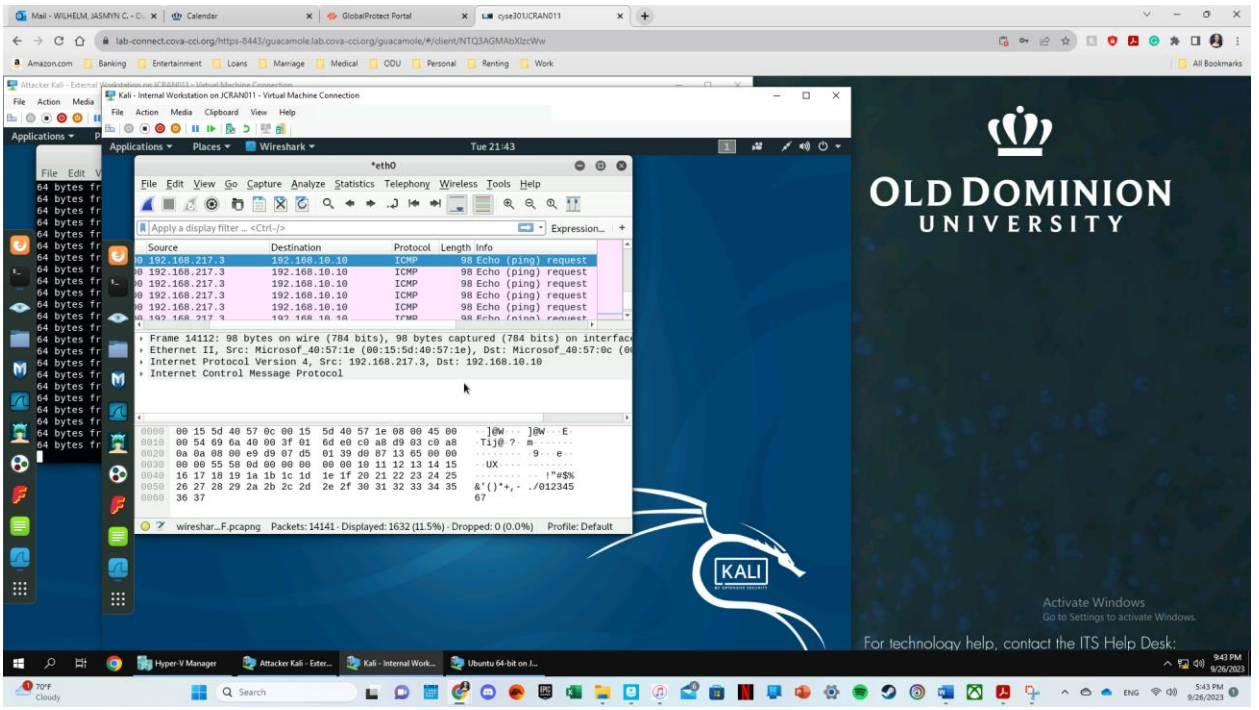
The response query from the question above is that it is Refused. The source IP and port is 192.168.217.2:53 and the destination IP and port is 192.168.217.3:44100 for this query.



Task B: Sniff LAN Traffic

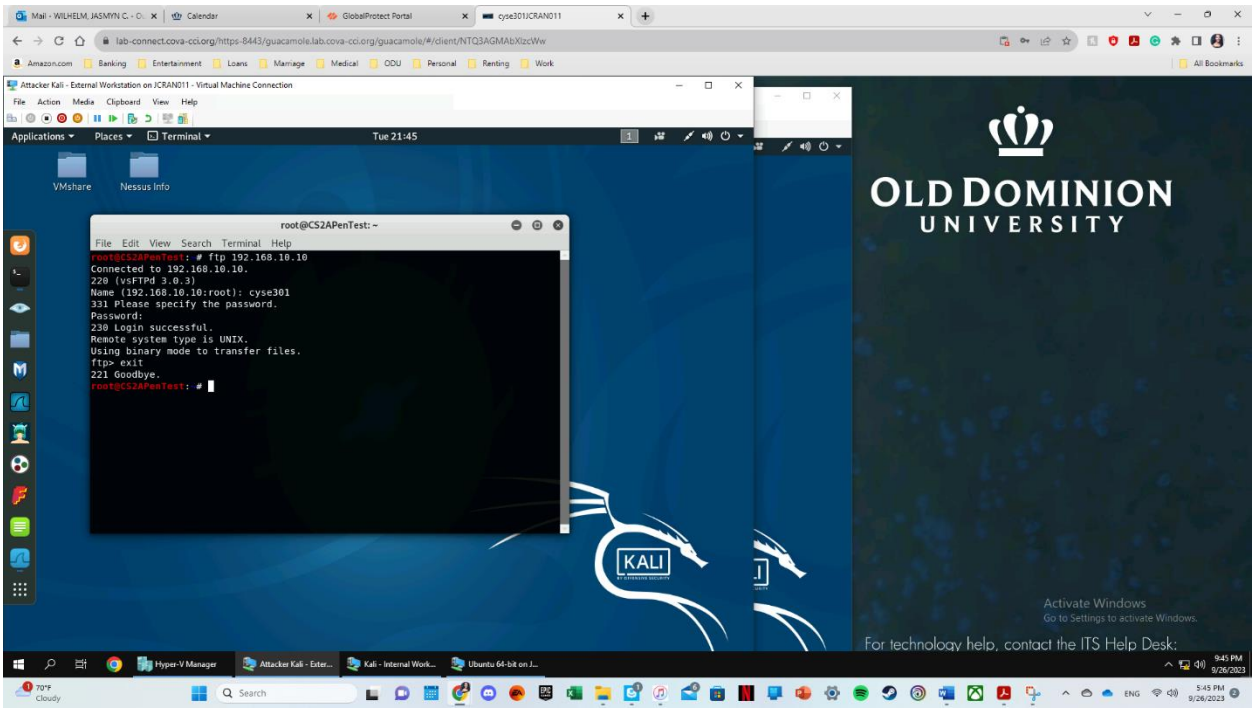
Question 1 A&B:

By on the box above the packets you can search for only ICMP traffic, and you can also change the display to only show ICMP requests.



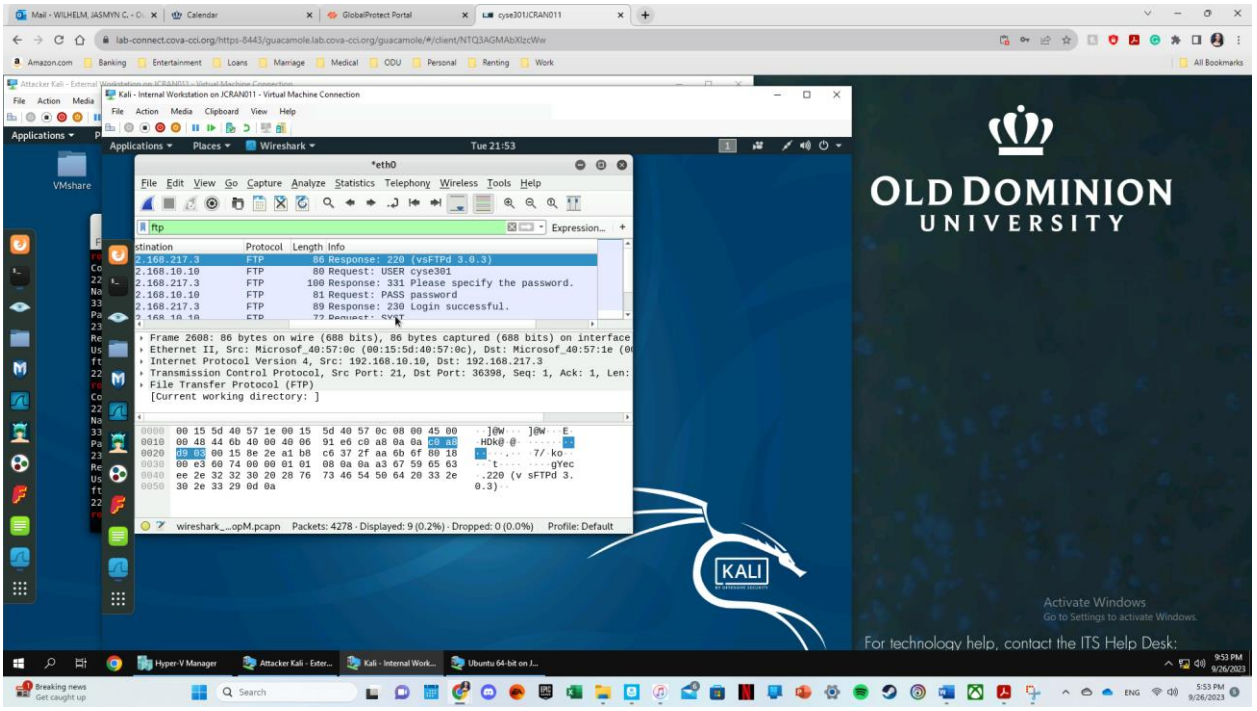
Question 2.A:

The screenshot displays how to use External Kali to gain access to Ubuntu using an FTP server.



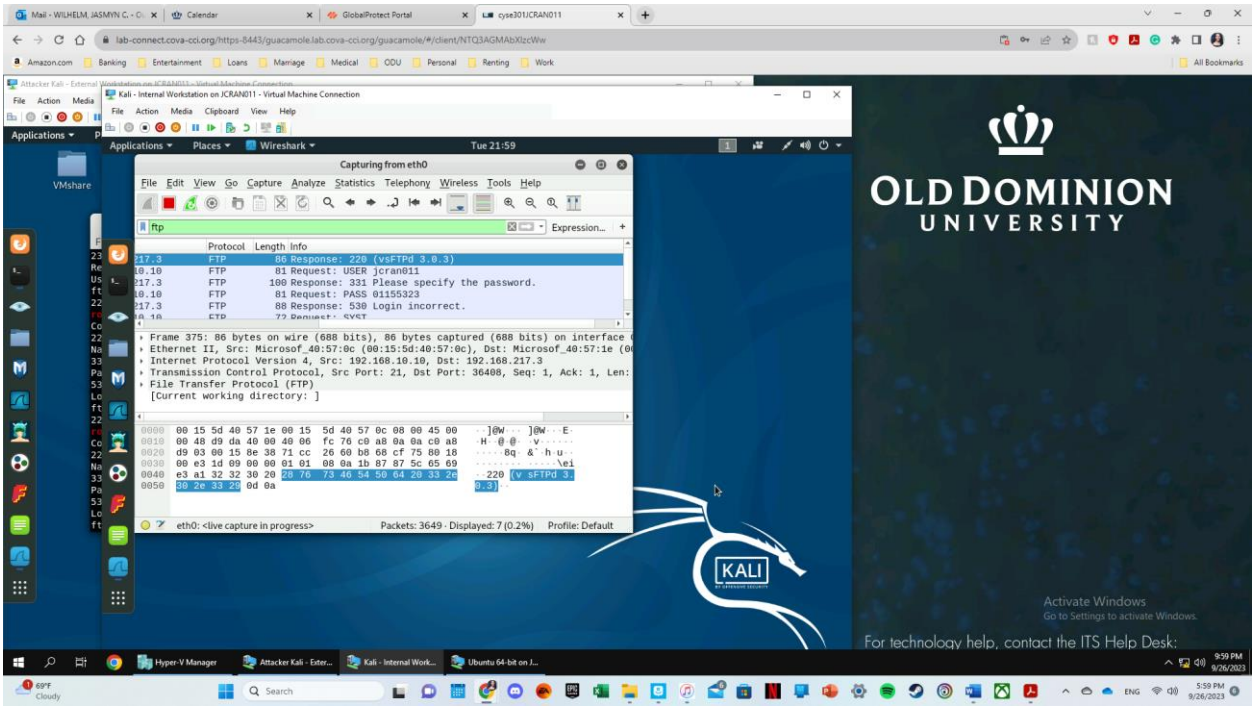
Question 2.B:

To find the intercepted information using the attacker (Internal Kali) you can filter the Wireshark to only show ftp packets which displays the same prompts and information used.



Question 2.C:

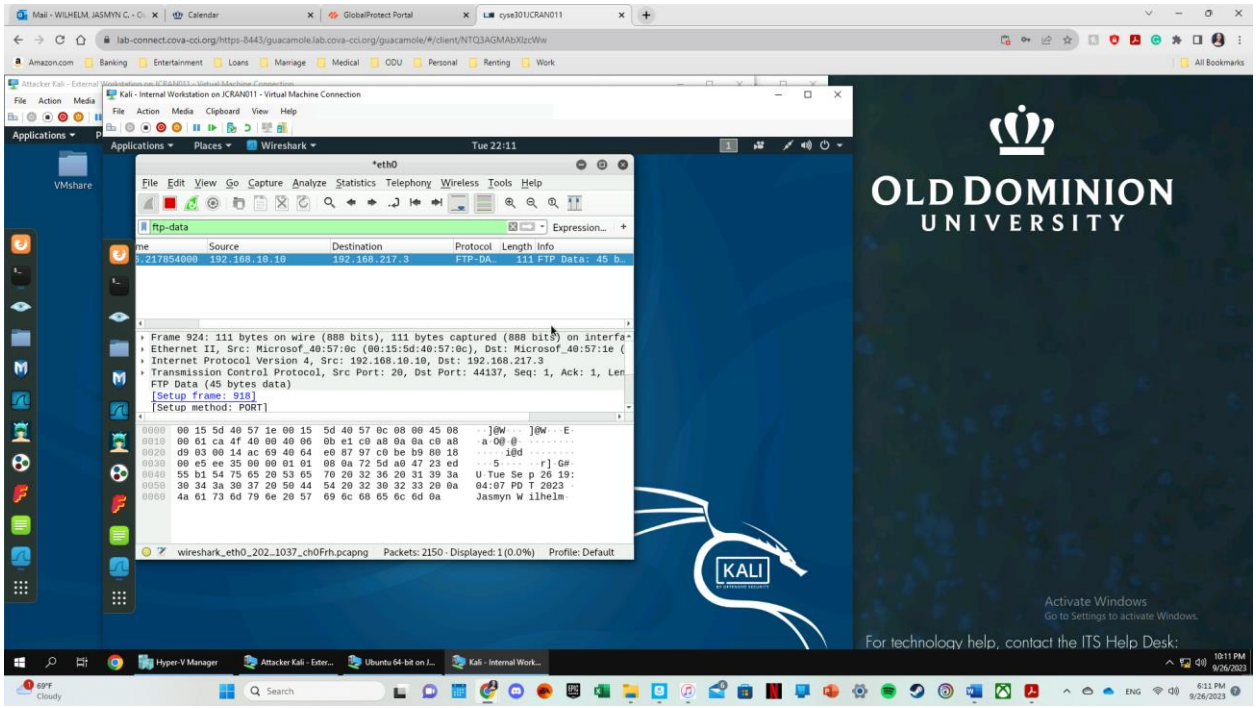
To complete the next task of using the MIDAS ID and UIN, but not being able to access the server you follow the same steps.



Task C: Extra Credit: Steal files with Wireshark

Question 1:

To display an FTP-Data filter you type into the filter search box “ftp-data” (all lowercase) and it will display the packet that was transferred from Ubuntu to External Kali that was picked up by Internal Kali.



Question 2 and 3:

To follow the TCP stream, I clicked “analyze” and selected follow “TCP steam”. I was then able to save the file as my own and labeled it jcran011. This screenshot shows both.