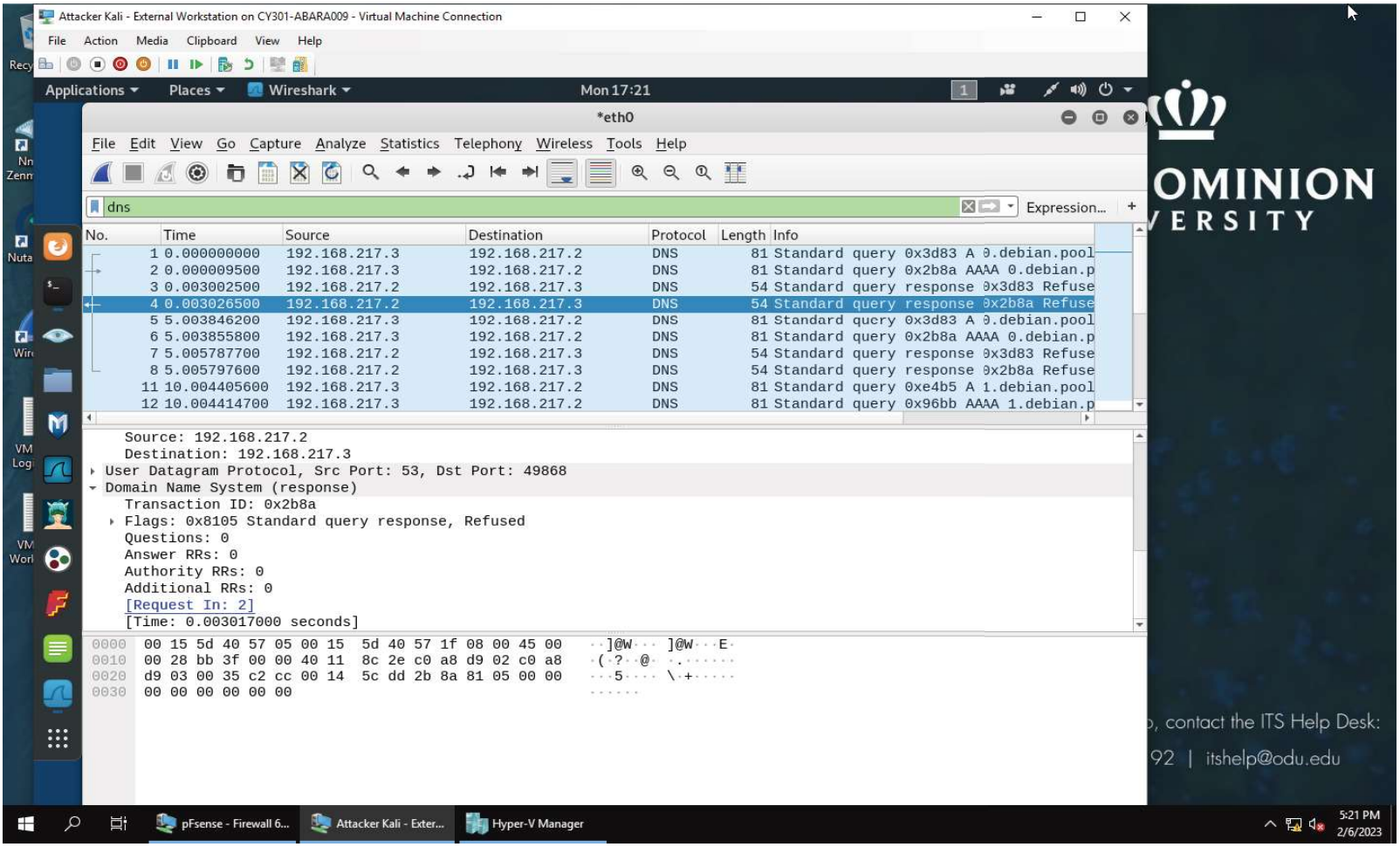
TASK A (CONTINUED)

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?

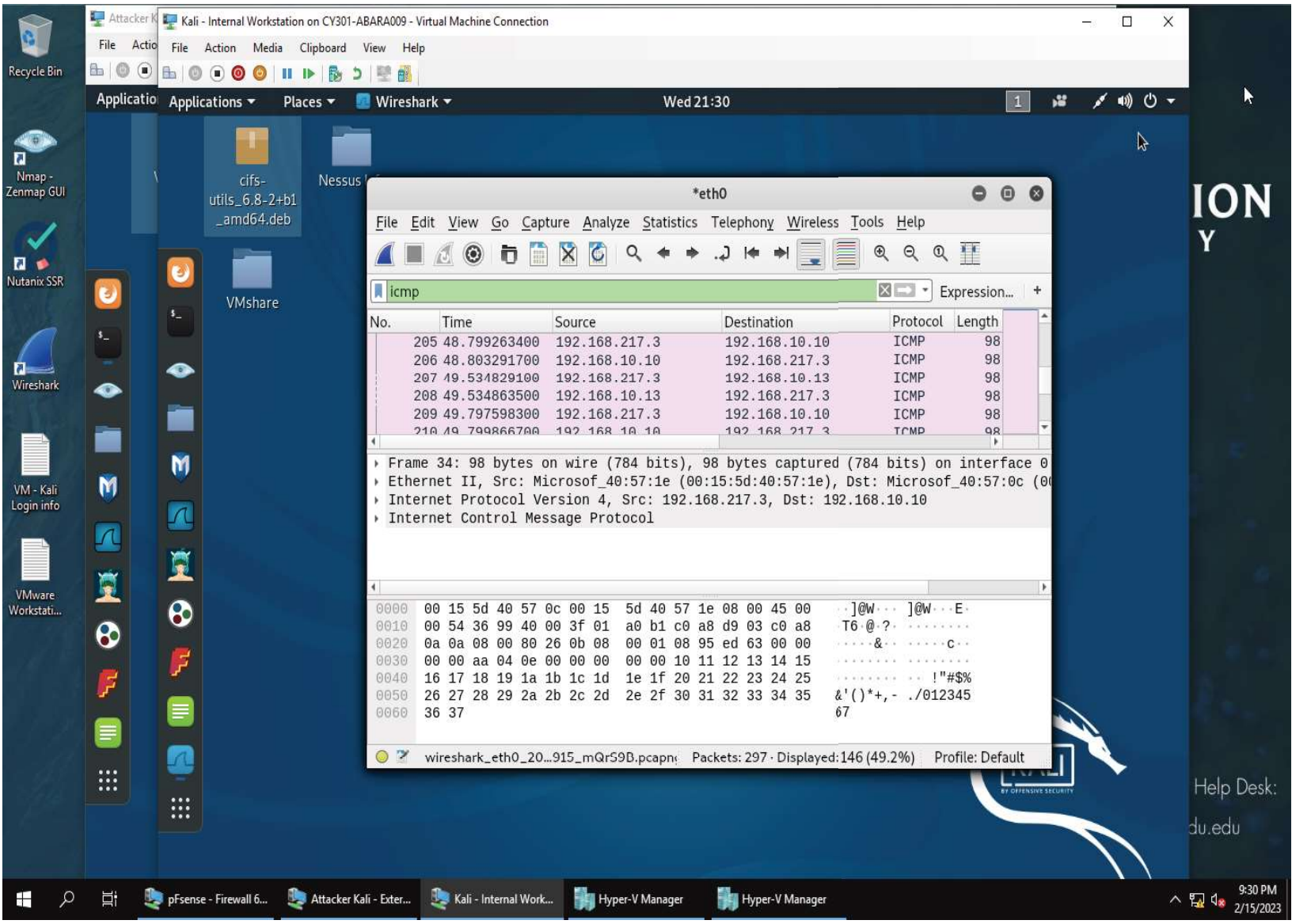


Here, I found the DNS query response for 0x2b8a. The source IP and source port is 192.168.217.2 : 53. The destination IP and source is 192.168.217.3 : 49868. The message is refused.

TASK B

1) Sniff ICMP Traffic

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

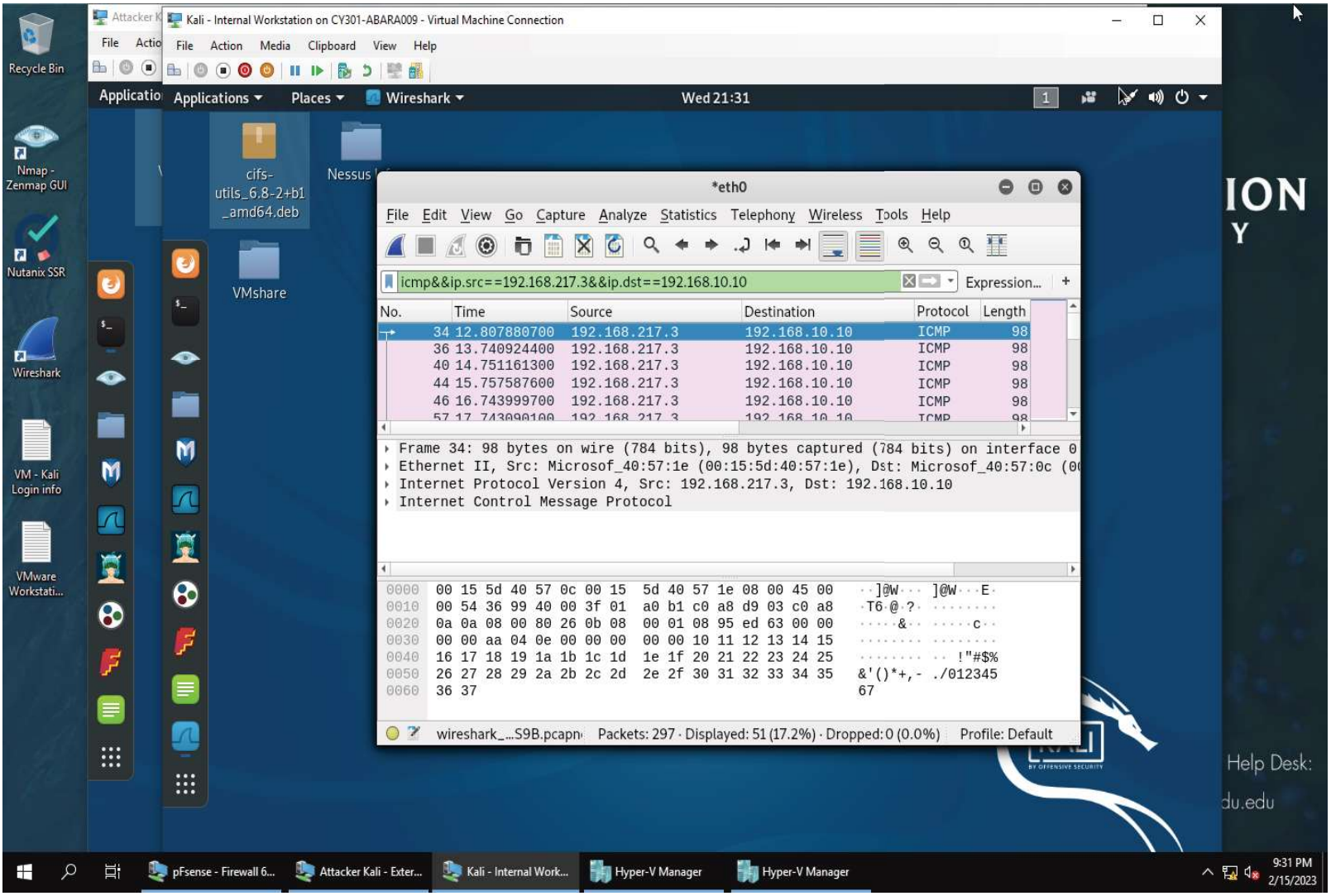


Here, on Wireshark, I applied “icmp” in the filter bar in Wireshark. Here, you can see ICMP packets from Ubuntu 192.168.10.10 and External Kali 192.168.217.3.

TASK B (CONTINUED)

1) Sniff ICMP Traffic

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.

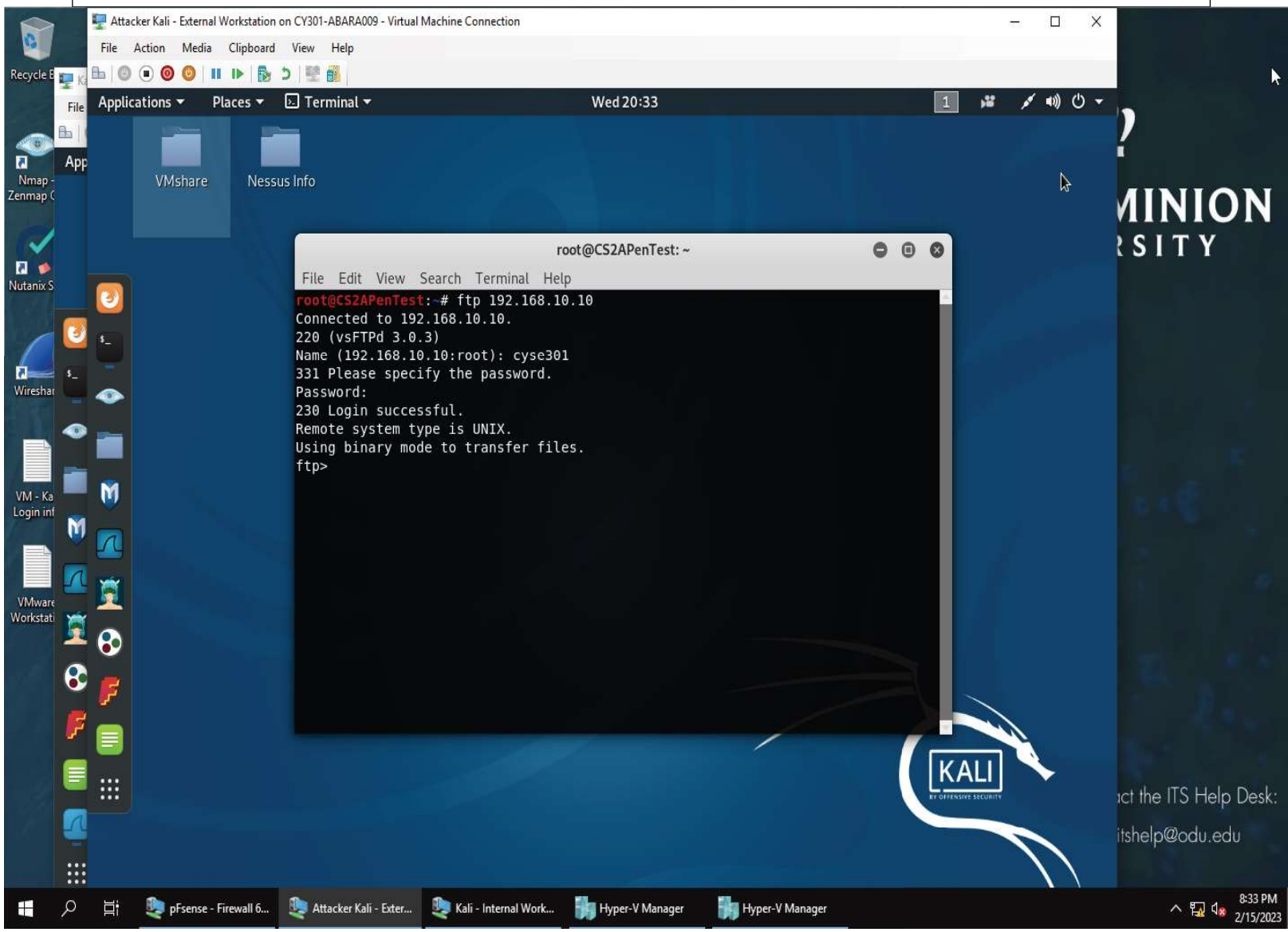


Here, I applied "icmp&&ip.src==192.168.217.3&&ip.dst==192.168.10.10" to capture the filter that displays requests originating from External Kali VM and going to Ubuntu-64 bit VM. The first part of the filter, "icmp" filters to display only icmp packets. The "&&" connects all parts of the filter in the search bar. Then the next part "ip.src==192.168.217.3" filters out specifically the packets originating from External Kali's VM, using its IP address. The last part, "ip.dst==192.168.10.10", I am filtering the ICMP packets that are sent to the Ubuntu VM using its IP address.

TASK B (CONTINUED)

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.

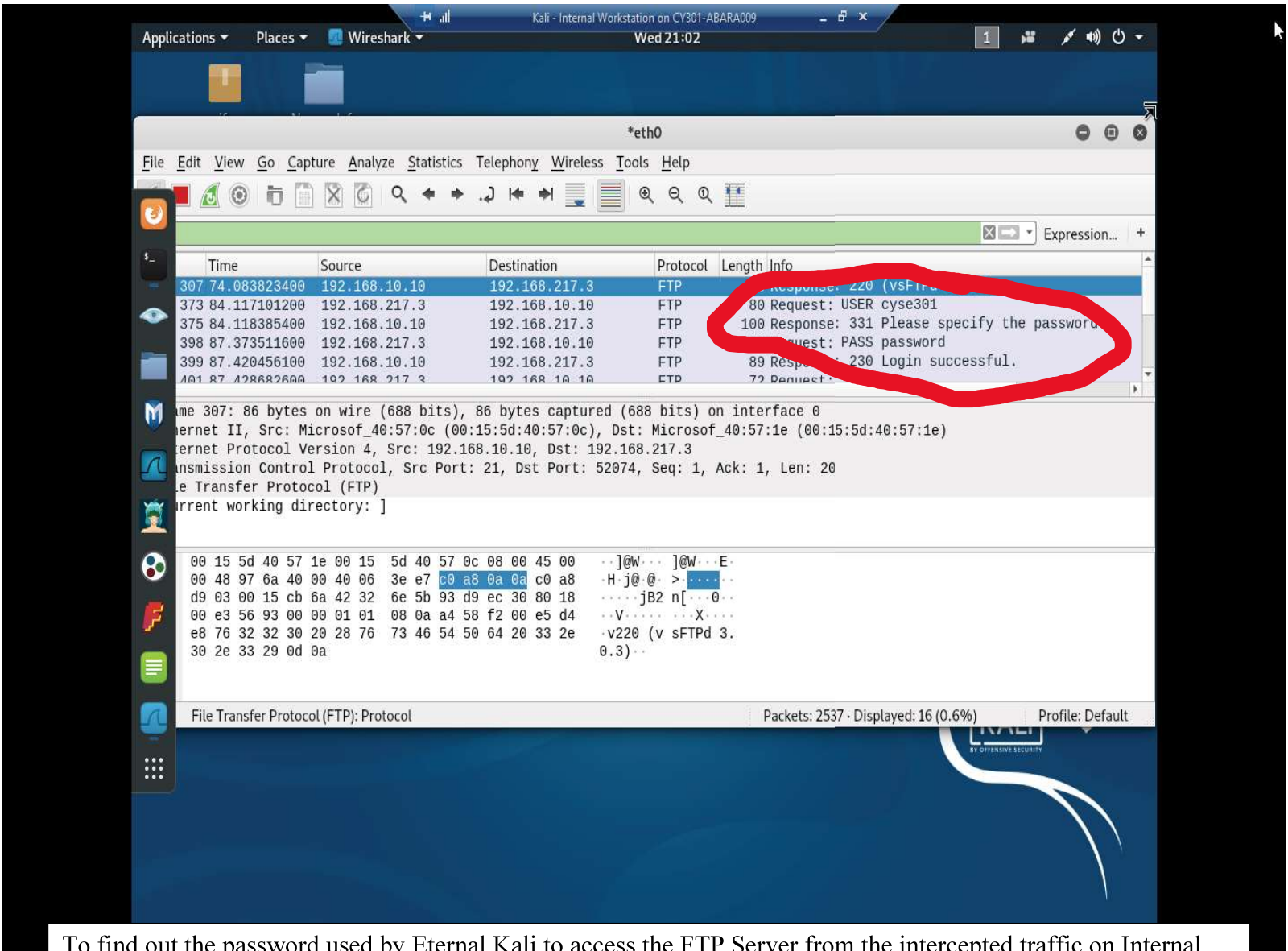


Here, I accessed Ubuntu's FTP server on External Kali using" ftp 192.168.10.10. " This is using the command "ftp" with Ubuntu's VM IP address. I logged in using the credentials that are stated in the directions in 2a.

TASK B (CONTINUED)

2) Sniff FTP Traffic

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

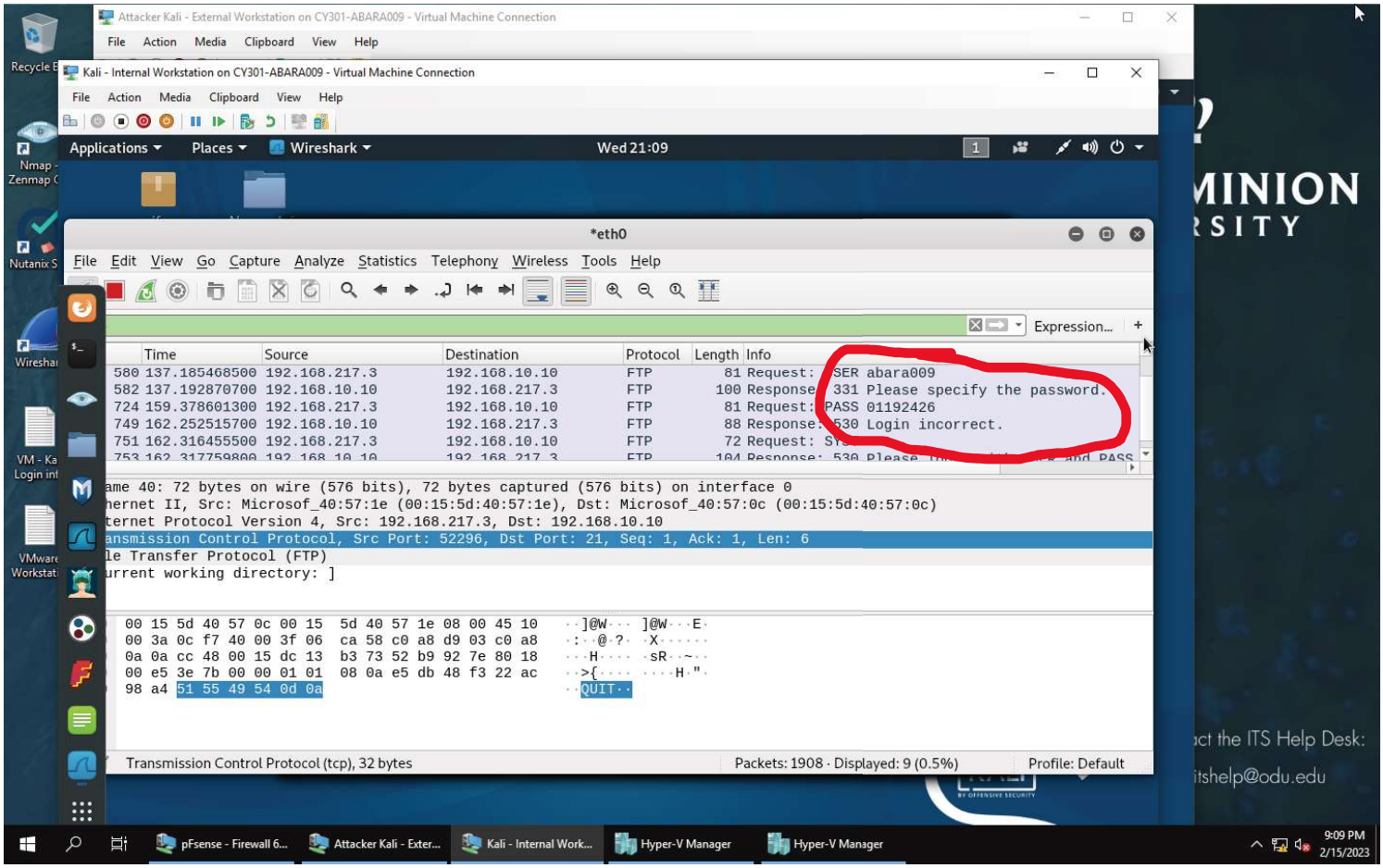


To find out the password used by Eternal Kali to access the FTP Server from the intercepted traffic on Internal Kali, I first executed “Wireshark” via the command line on External Kali. Then, I used External Kali to ping Internal Kali VM using its IP address of 192.168.10.13. Then, I opened up a second terminal in External Kali and pinged the Ubuntu VM using it’s IP address of 192.168.10.10. Then, I opened Internal Kali and started the capture on Wireshark. Then, I went back to External Kali used ftp 192.168.10.10 using Ubuntu VM IP address to access the intercepted traffic. After logging in as CYSE301 and inputting “password” as the password in the FTP login, I was able to see in Internal Kali wireshark through the FTP packets that the username was cyse301 and the password was password that Eternal Kali used to access the FTP server from intercepted traffic on Internal Kali.

TASK B (CONTINUED)

2) Sniff FTP Traffic

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.



For this step, I completed the exact same process as question 2. However, once I accessed the FTP server using ftp 192.168.10.10, I used my login “abara009” and password “01192426”. Once I went to the Internal Kali Wireshark, I saw the “secrets” from the attacker VM that my login was incorrect. This gives me the hint to try a different login combination.