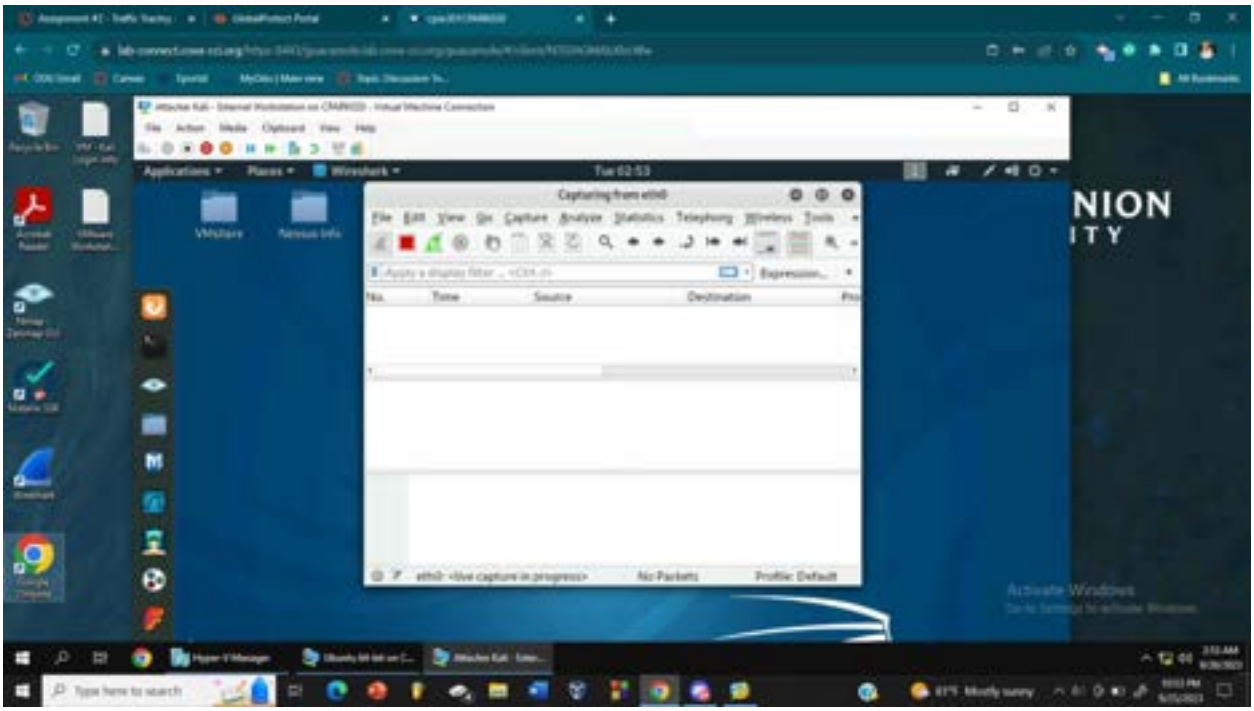
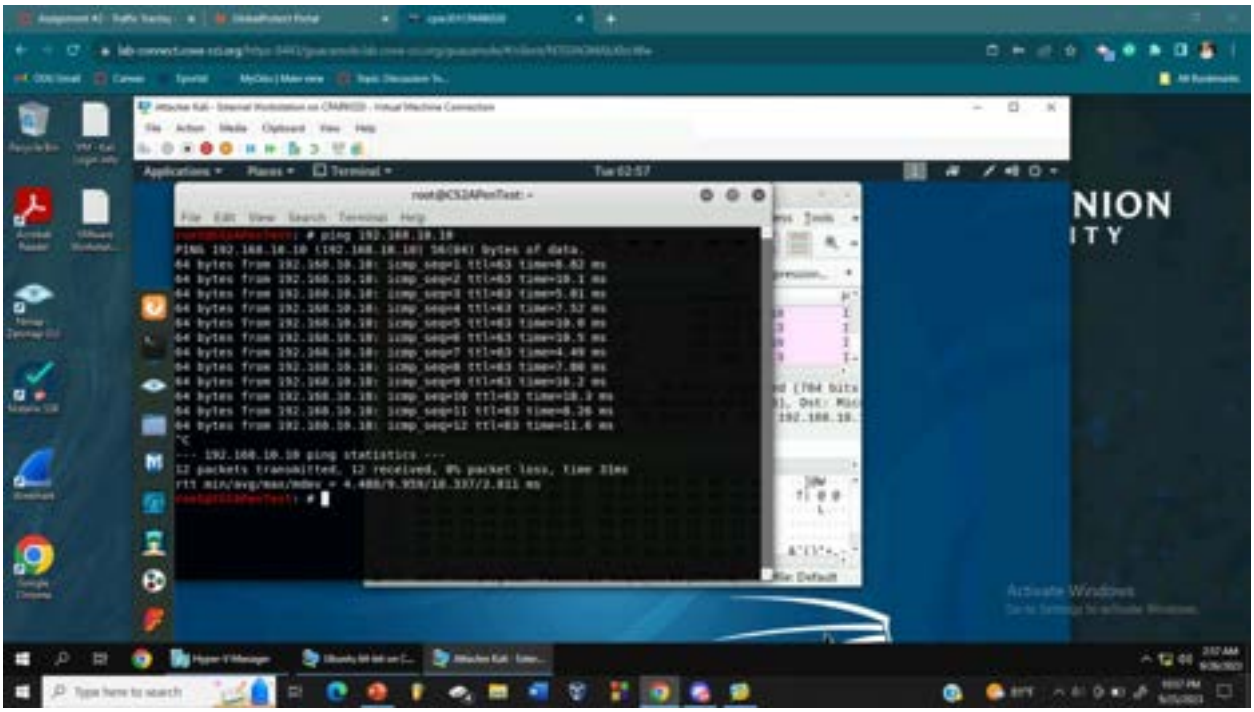
OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

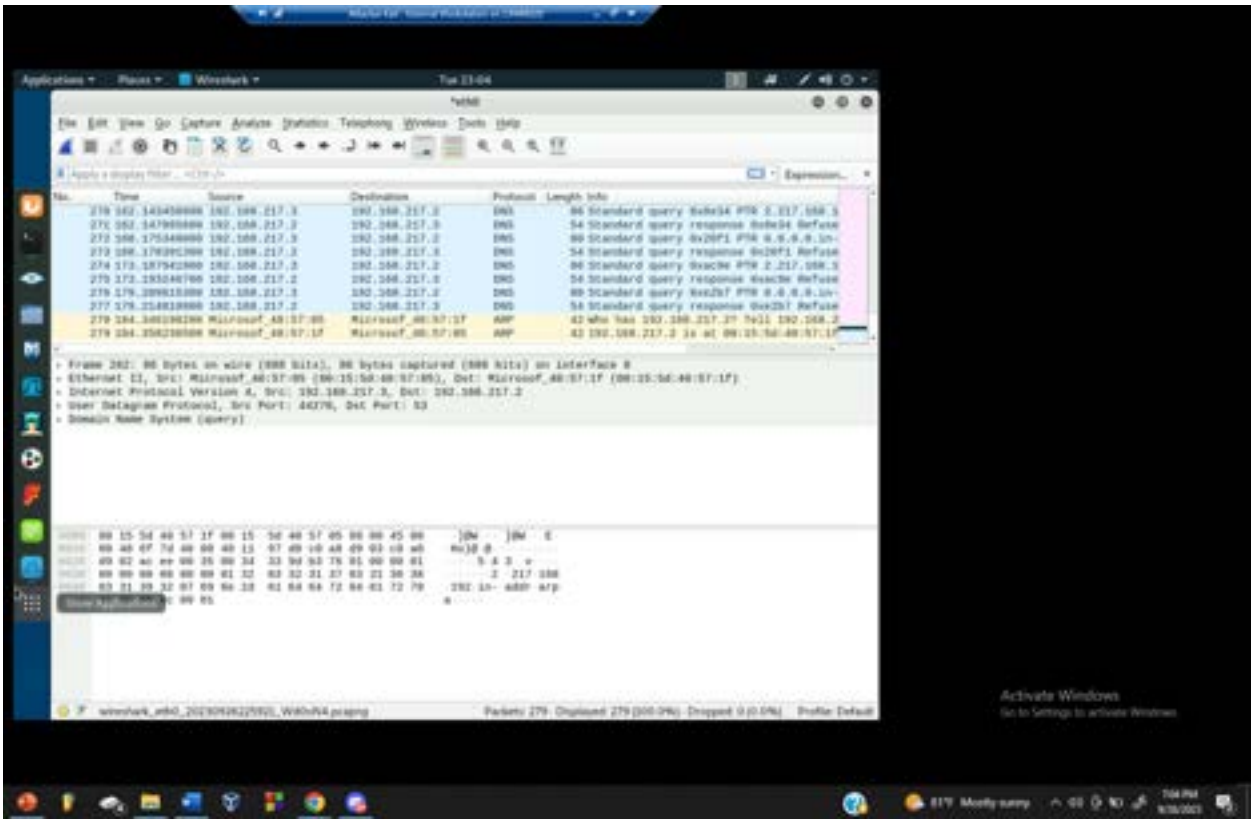
Traffic Tracing and Sniffing Packets with Wireshark

Corey Parker

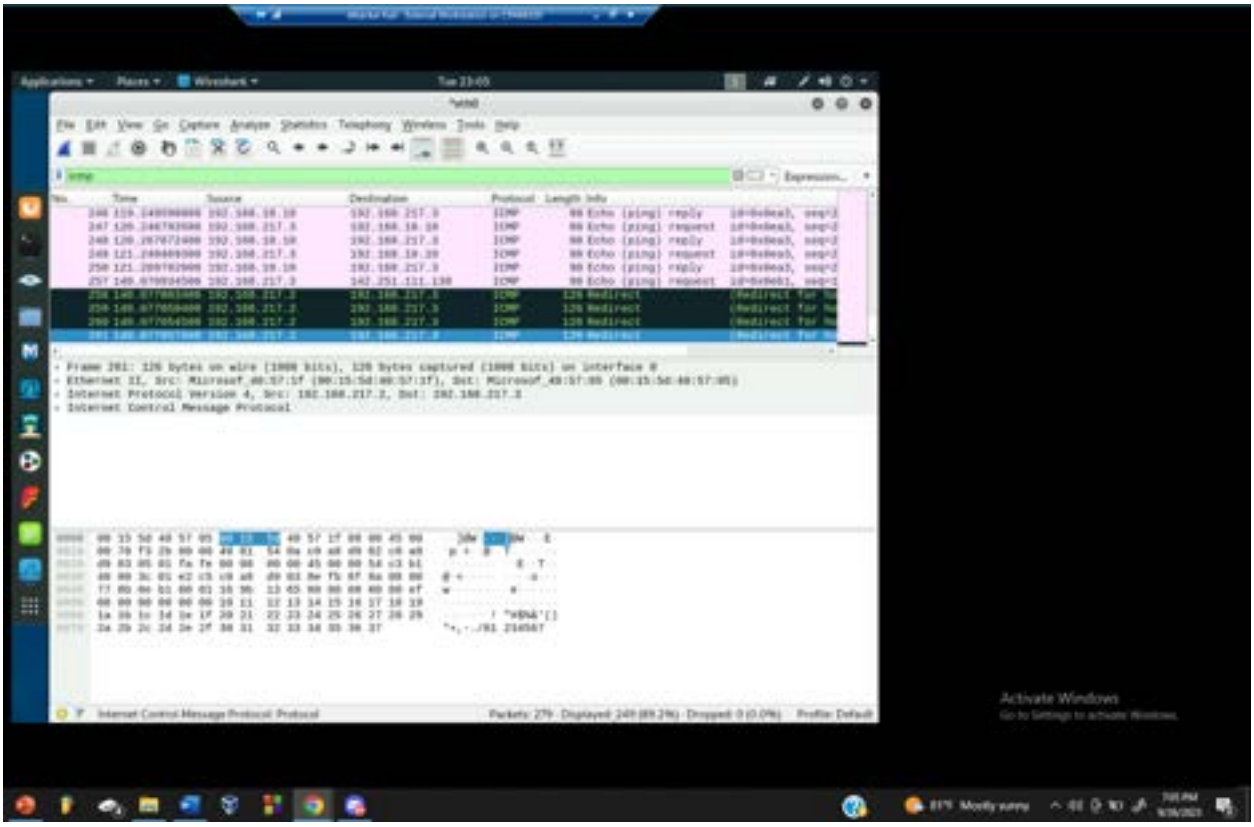




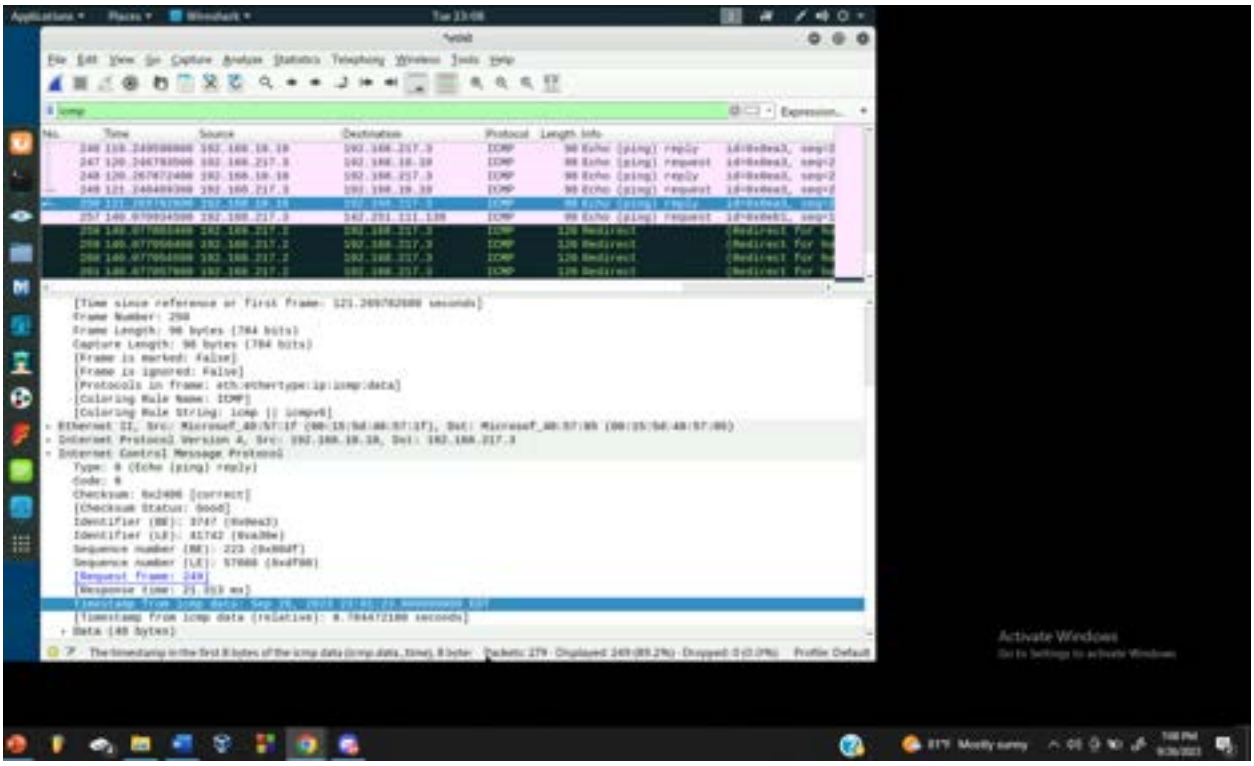
Wireshark was opened on external Kali in the first screenshot. Once Wireshark was monitoring packets on the “eth0” interface, the Ubuntu 64 bit VM was pinged as shown in the second screenshot.



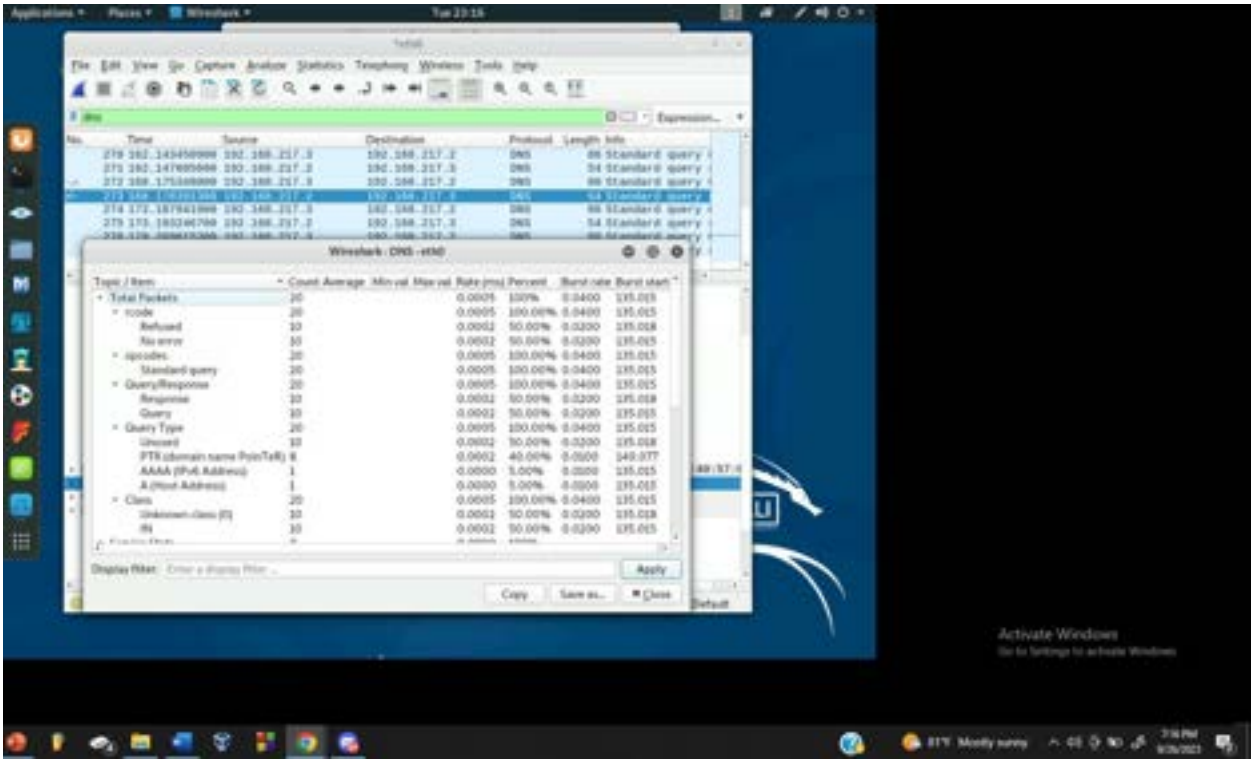
Once the traffic monitoring was stopped with the red square button, we are shown all of the packets that were sniffed. As shown in the bottom righthand corner where it says, “Packets 279,” 279 packets were displayed and 279 packets were displayed.



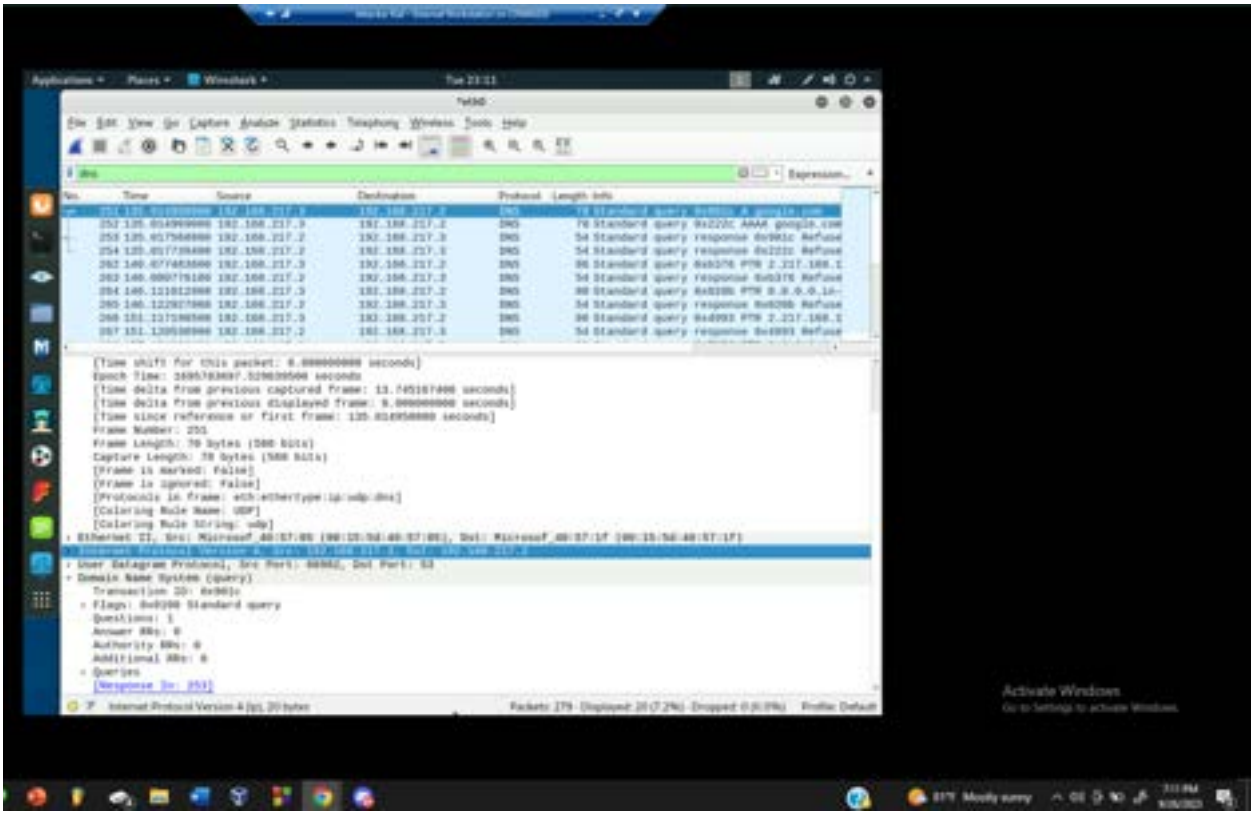
Once the ICMP display filter was applied, 249 packets were displayed, as shown in the bottom right corner where it say, “displayed 249.”



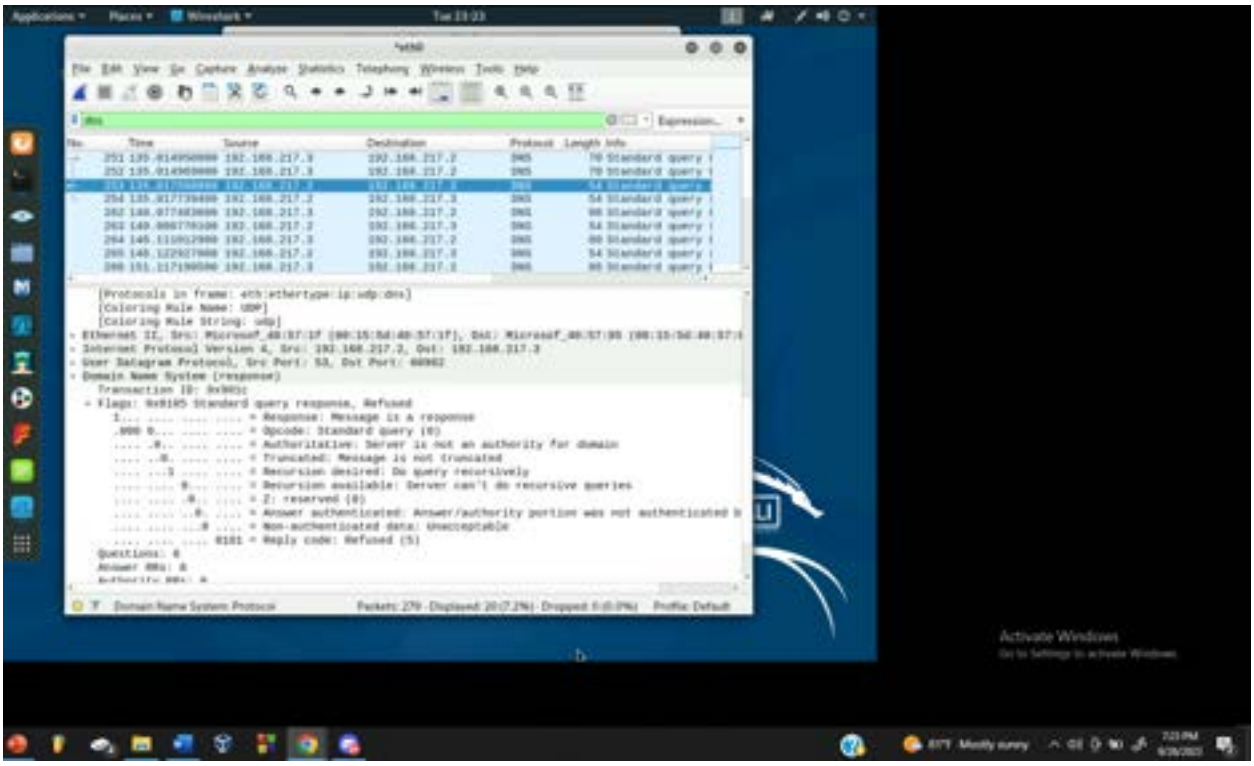
After choosing the Echo (reply) message, packet 250, we can see that the source IP is 192.168.10.10 and the destination IP is 192.168.217.3. In the screenshot we can also see that the sequence number (BE) is 223 (0x00df) and the sequence number (LE) is 57888 (0xdf00) with a data size of 48 bytes. There is a response time of 21.313 ms.



With the DNS display filter applied, we can see that there are a total of 20 DNS packets captured and displayed.

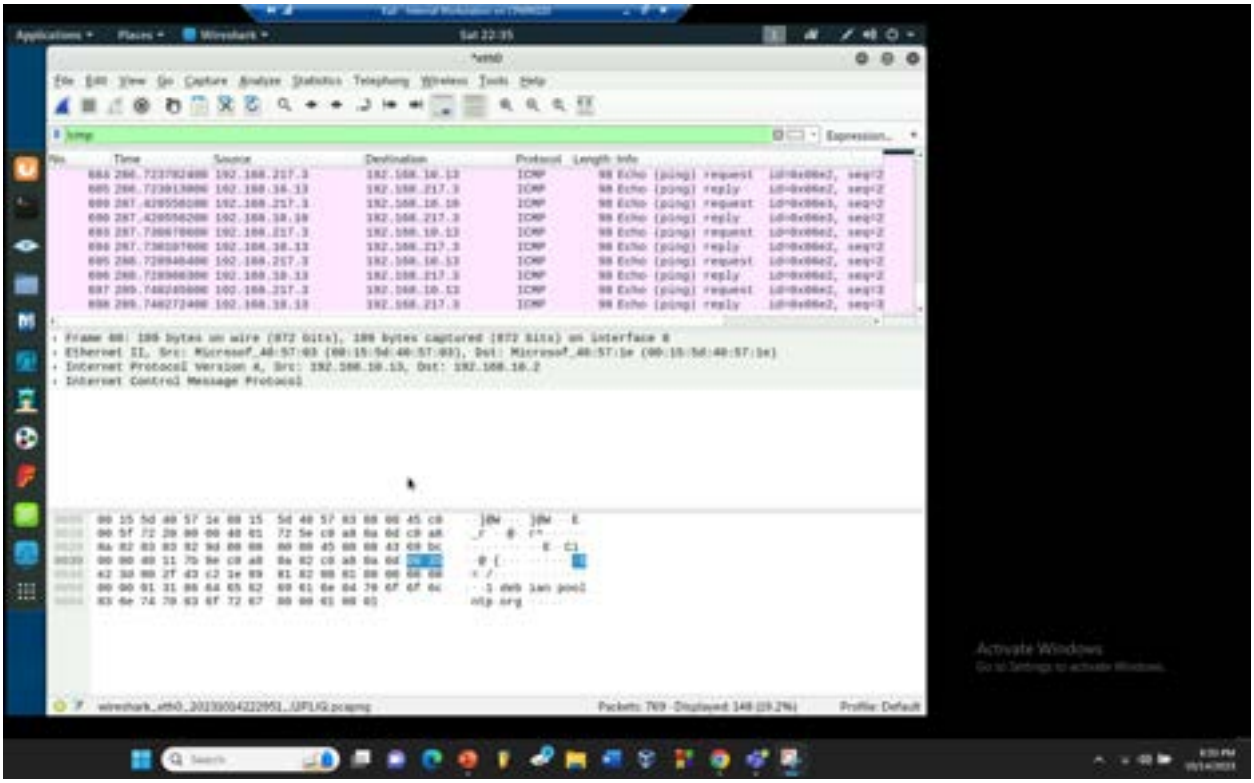


After displaying the information of packet 251, the DNS query packet, we can see that the domain name that the host attempting to resolve is google.com. We can see that the source IP and port number is 192.168.217.3: 60982. The destination IP and port number is 192.168.217.2: 53.

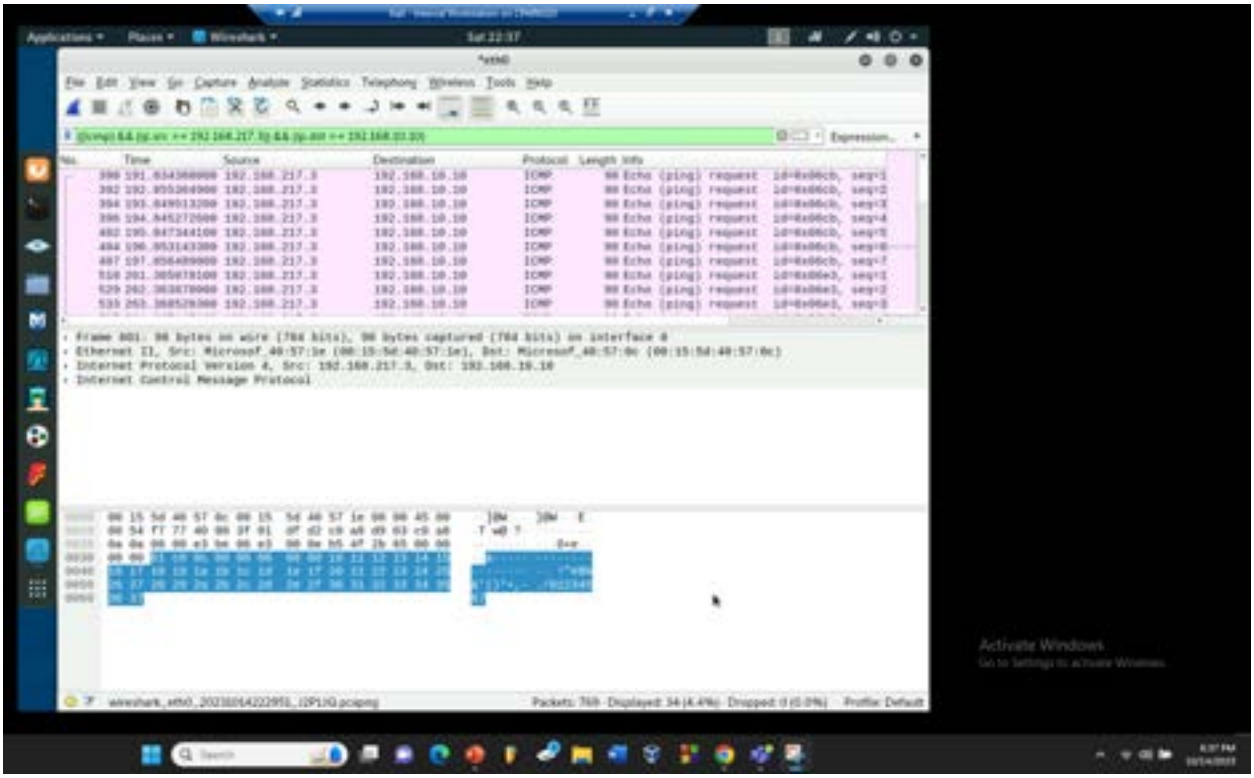


The DNS response was found with the matching transaction ID: 0x901c. We can see that the source IP and port number is 192.168.217.2: 53 and the destination IP and port number is 192.168.217.3: 60982. We can see that the response from the DNS server is “refused” as our virtual environment is not connected to the internet to reach google.com and receive the IP address from the domain name server.

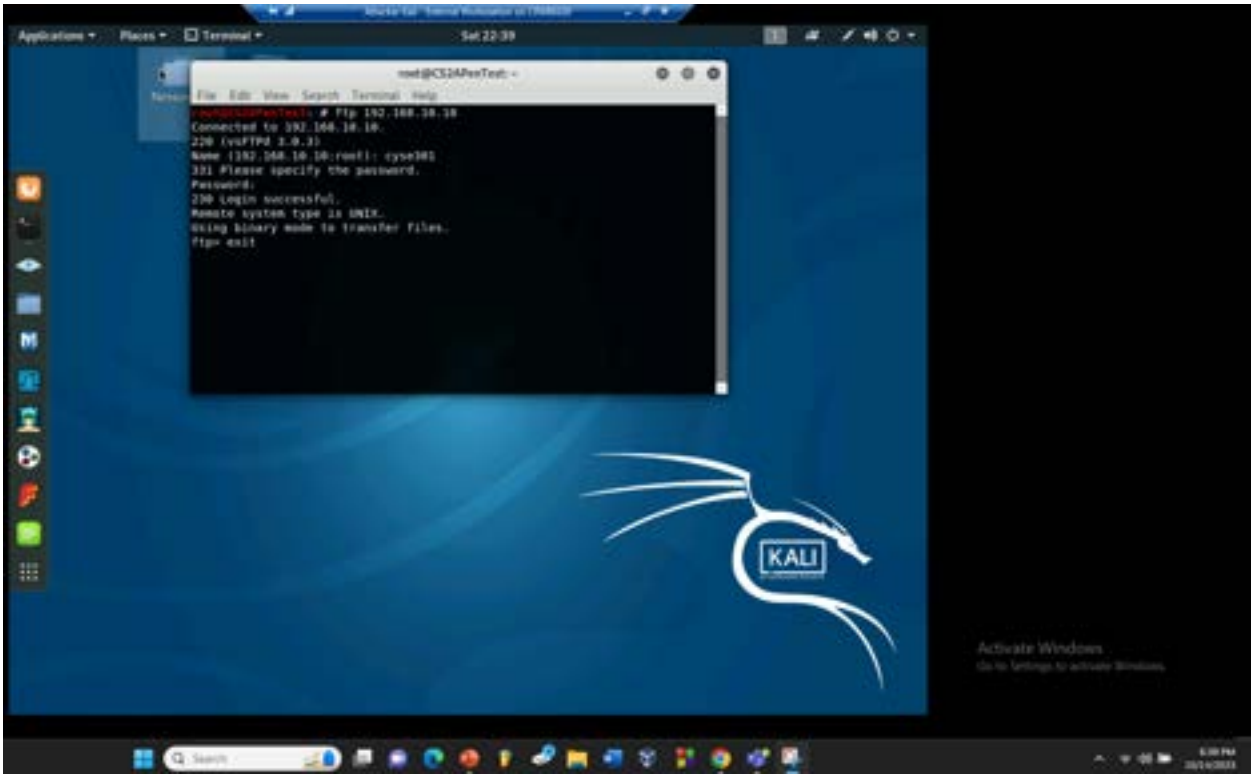
Two terminals are open from external Kali. The top terminal is pinging Ubuntu VM (192.168.10.10) and the bottom terminal is pinging internal Kali (192.168.10.13)



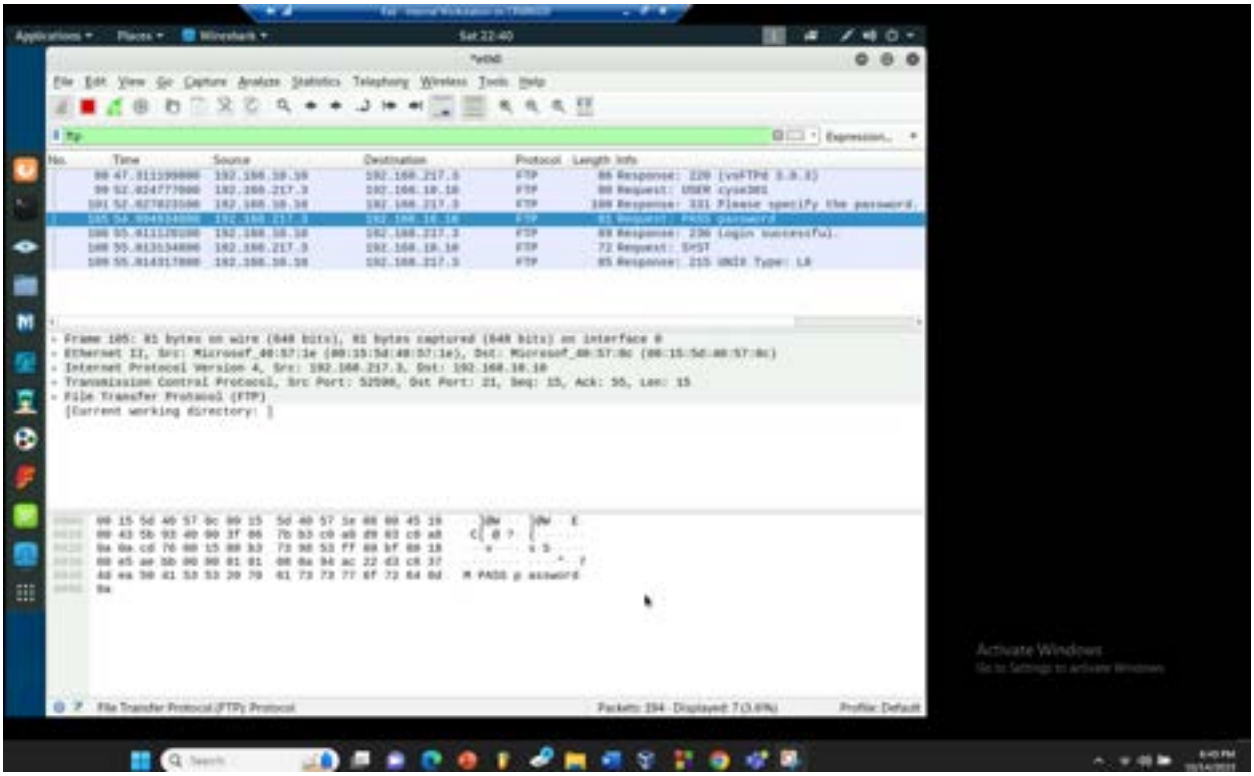
The ICMP display filter is applied in the green search bar.



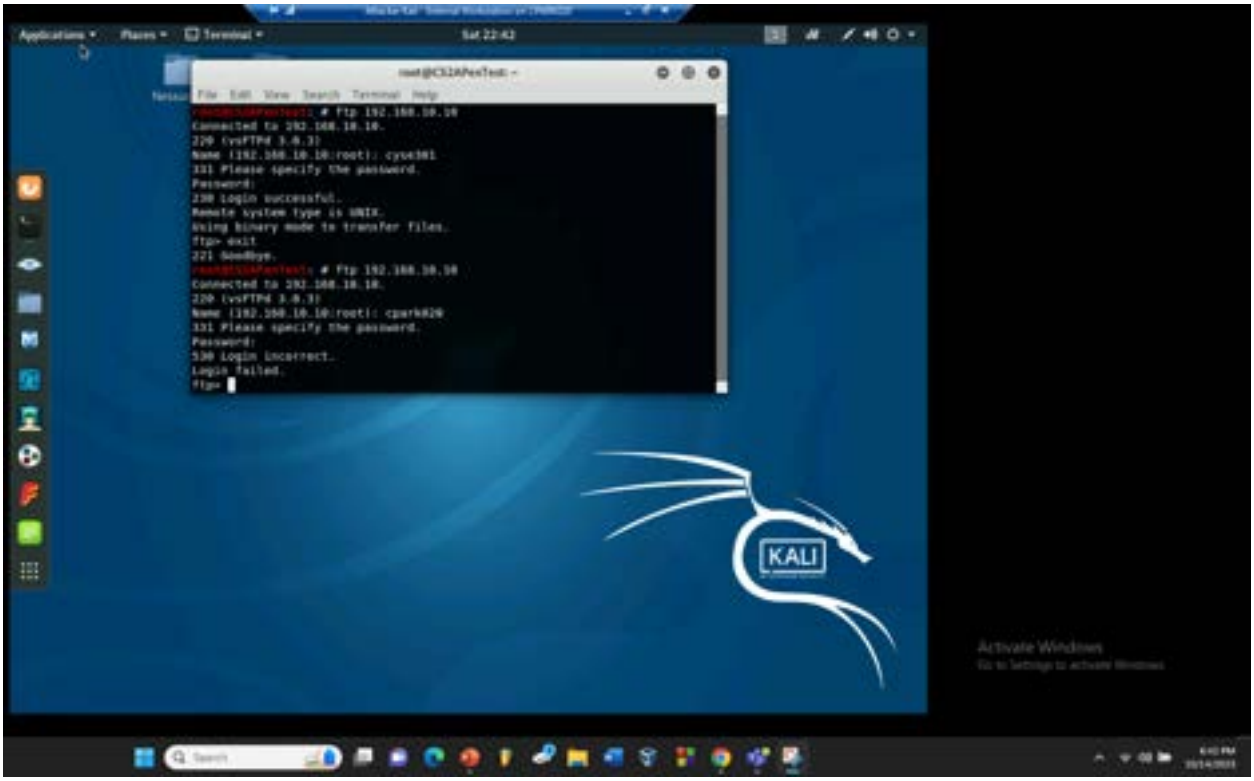
The filters to limit the display of ICMP request from External Kali VM, going to Ubuntu 64-bit VM are shown in the green display filter bar in the screenshot above. The ICMP filter displays only the ICMP packets, the ip.src == 192.168.217.2 filter displays only packets with a source IP from external Kali, and the ip.src == 192.168.10.10 filer displays only packets with a destination IP from the Ubuntu VM.

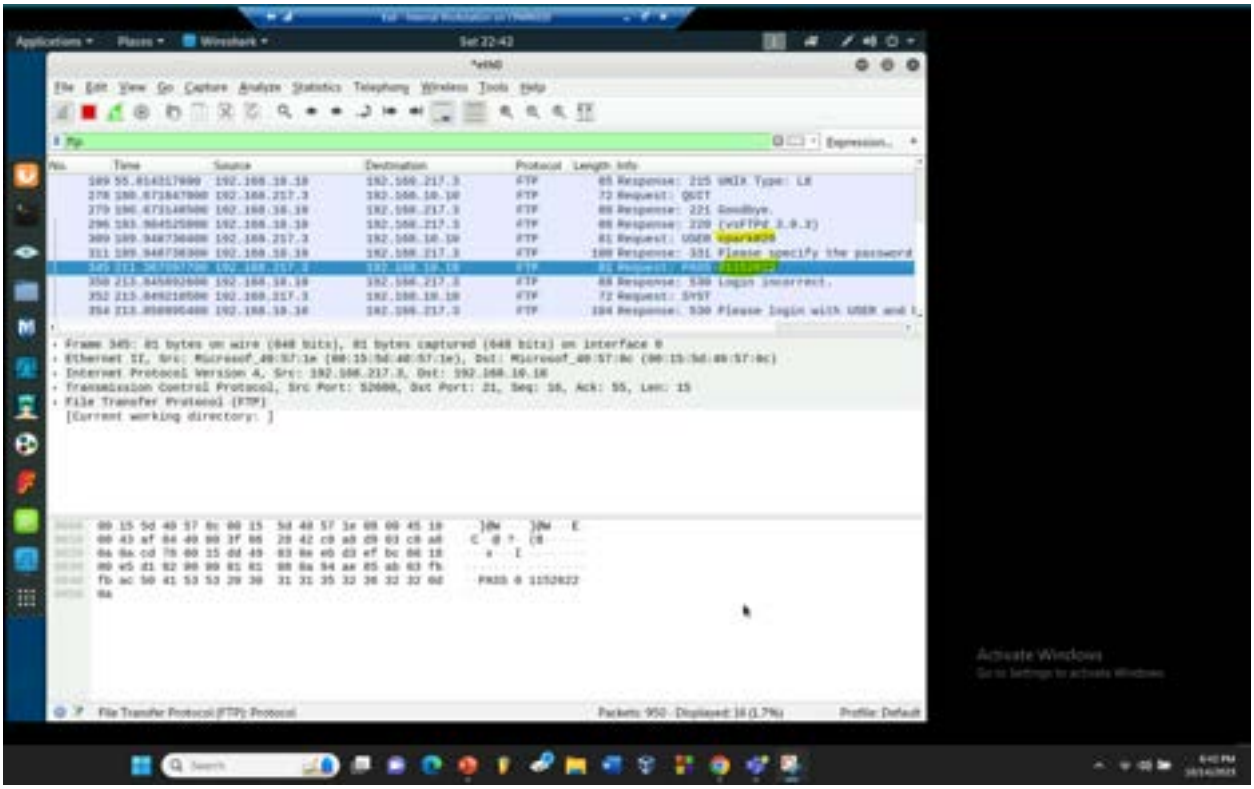


The screenshot above shows the external Kali accessing and exiting the FTP server on Ubuntu VM.

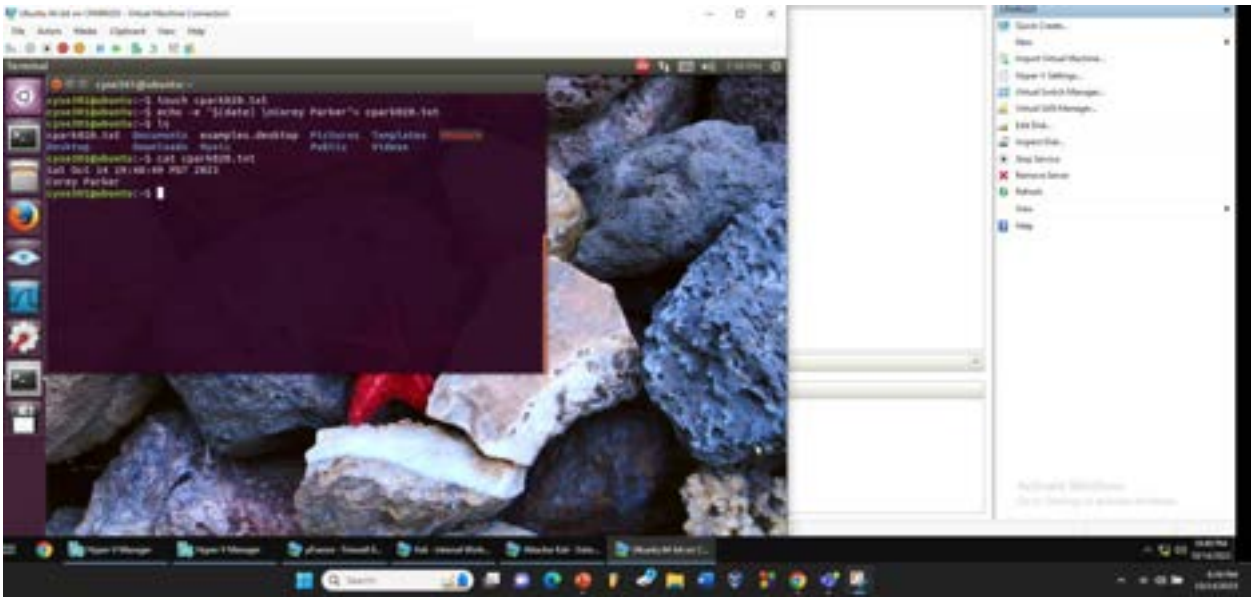


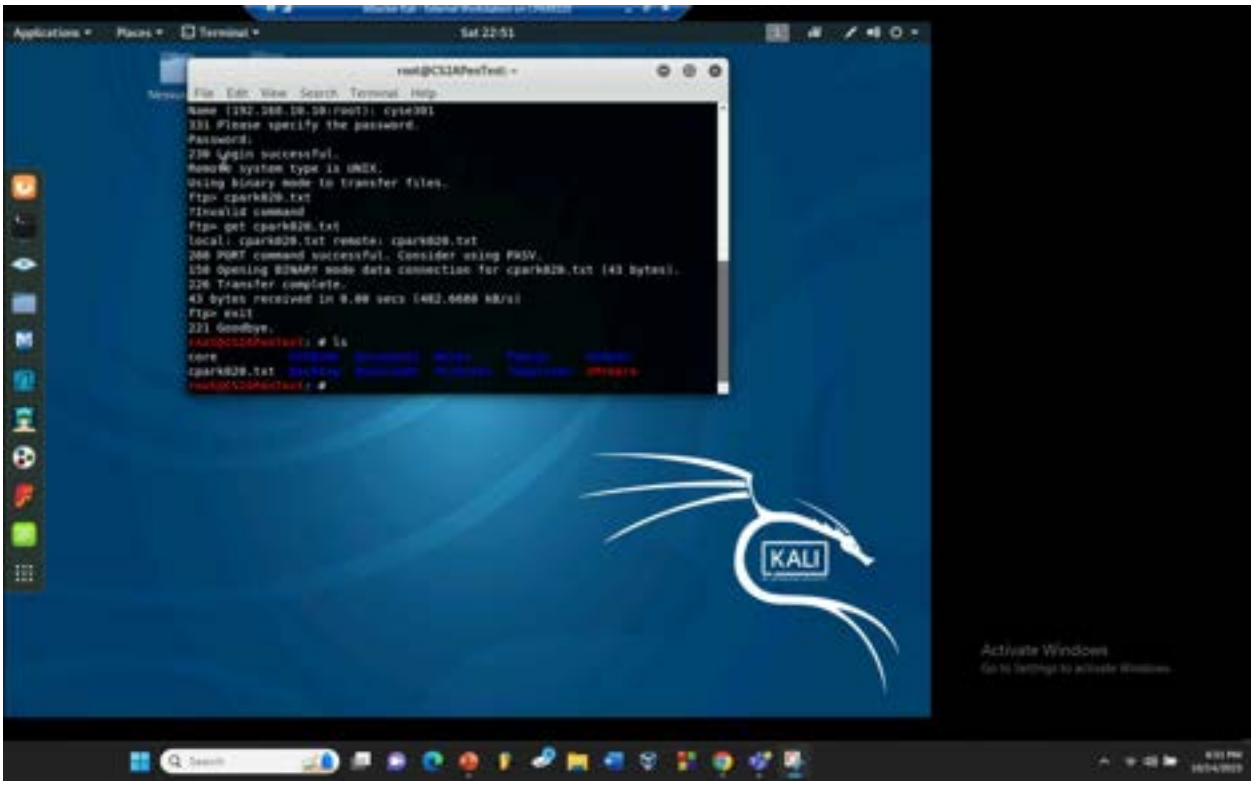
While sniffing packets with internal kali, we can view the username used to access Ubuntu's FTP server under "USER" and the password used under "PASS." I used a FTP display filter to limit the packets displayed to only FTP packets.



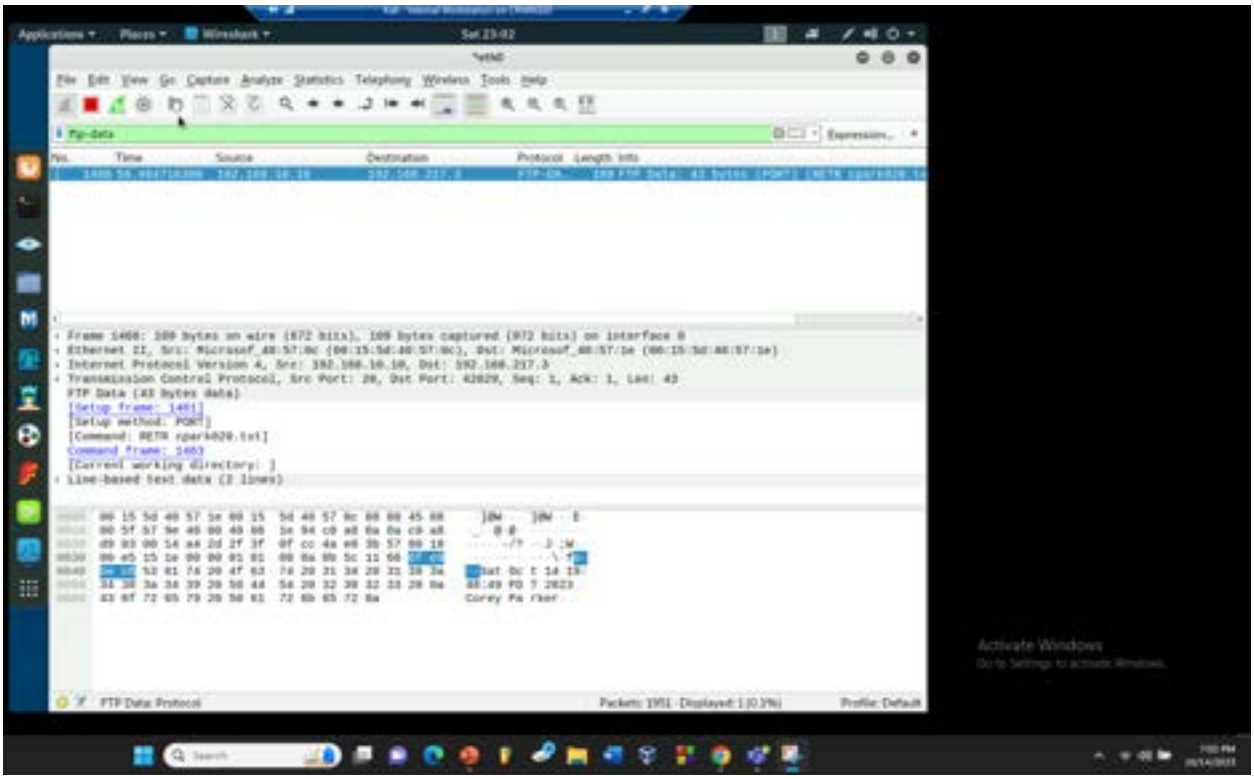


While sniffing packets using Wireshark on internal Kali again, we can see the other username and password used. The username and password are highlighted in the screenshot above.

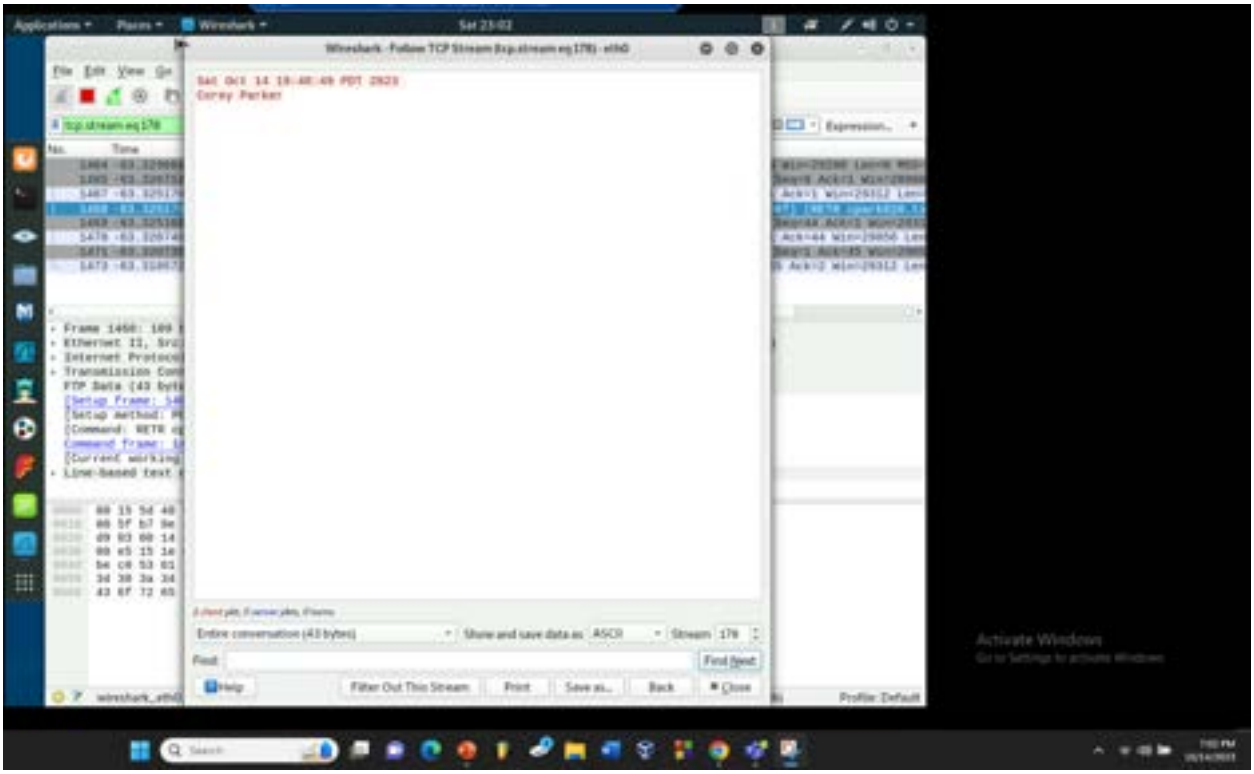




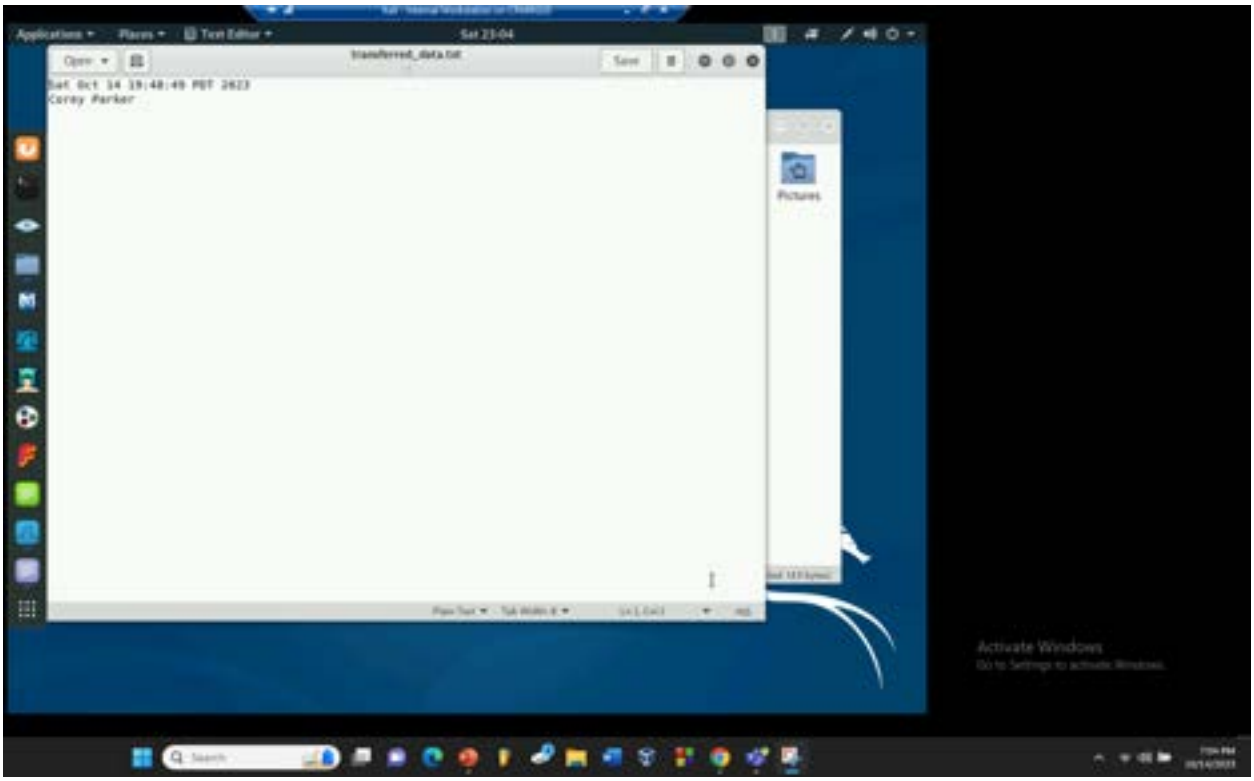
The screenshot above shows me using FTP to transfer the file created on the Ubuntu VM to External Kali.



The Wireshark filter on internal Kali was set to ftp-data.



After choosing the “follow TCP stream” option in Wireshark, I saved the raw data as a text file.



The screenshot above shows the raw data of the TCP stream that was saved as a .txt file and opened.