OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

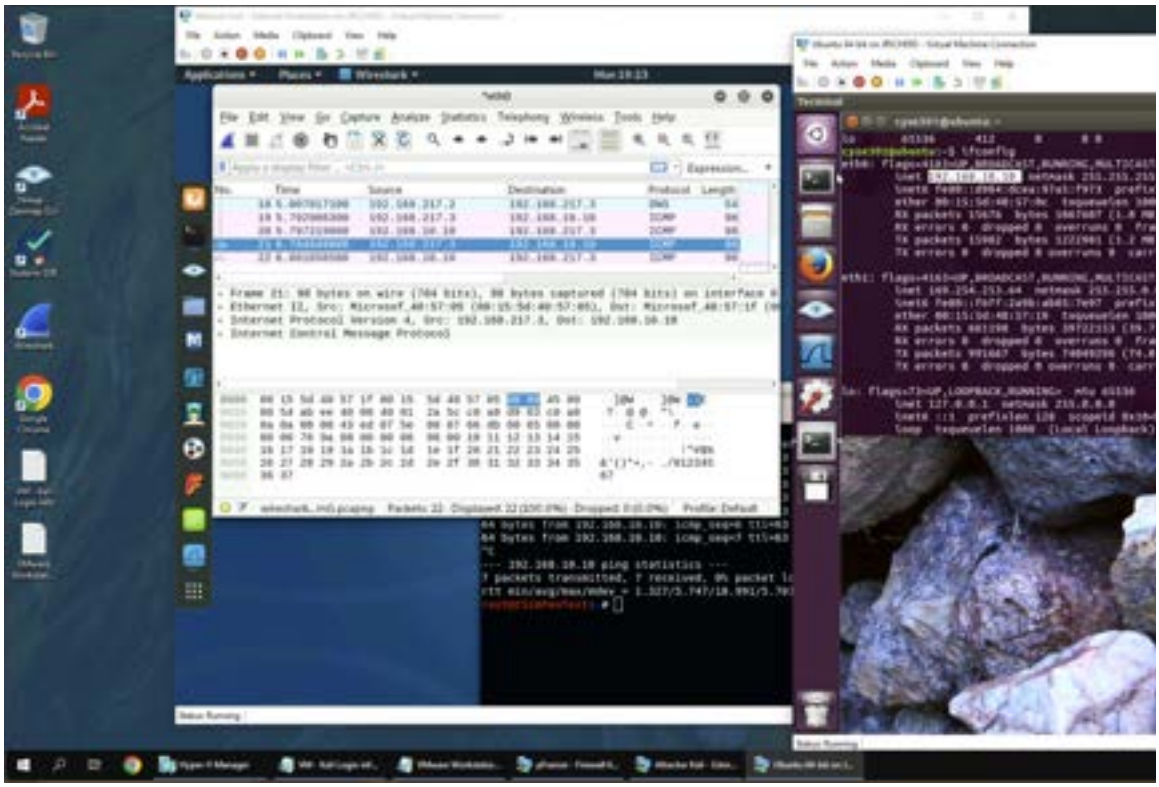
Jadyn Richardson

01221594

Below is the snippet of a sample lab report.

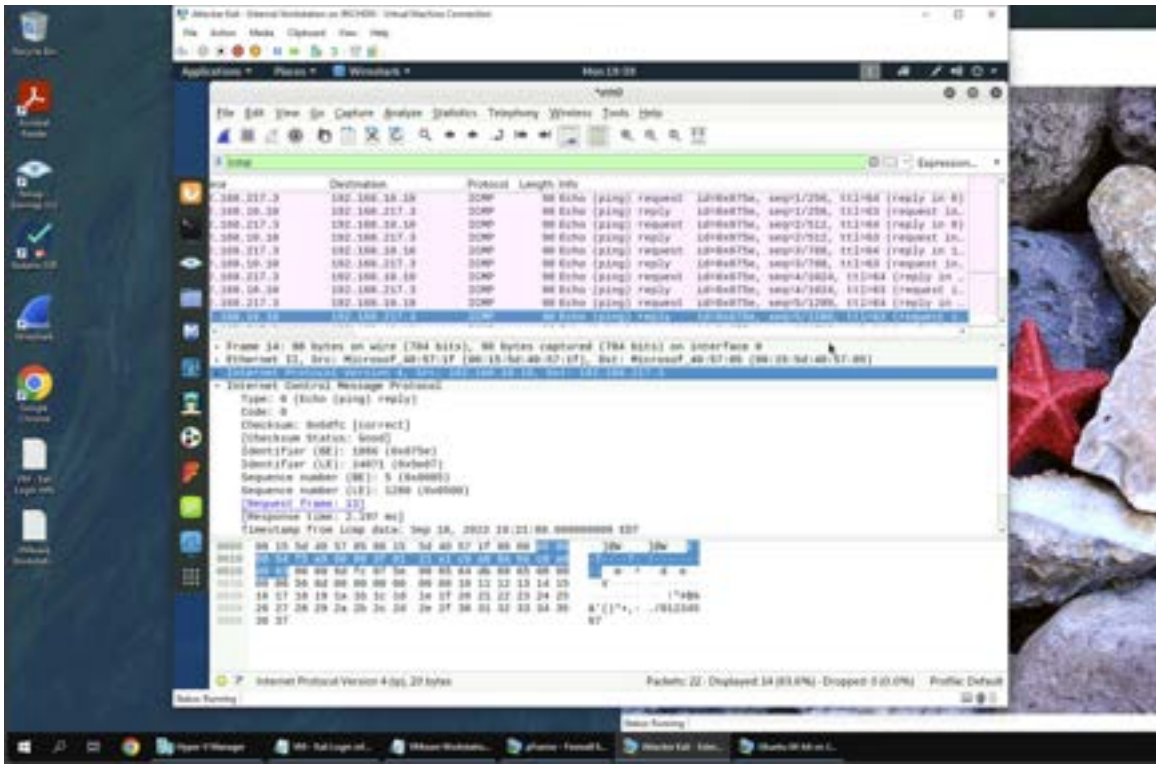
TASK A

Q1



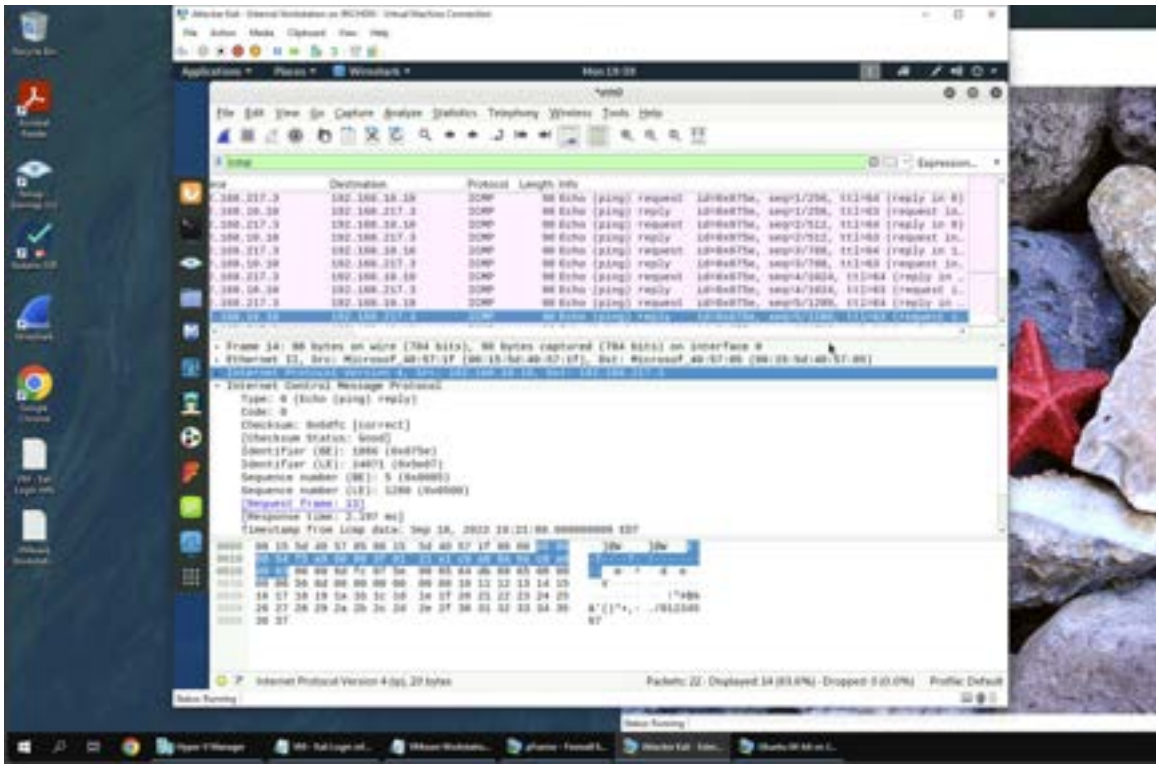
There are 22 packets captured in total. I can tell due to the fact that “Packets: 22 ” is displayed at the bottom of Wireshark. Next to the packets at the bottom of the screen, it says “Displayed: 22”, meaning that 22 packets are shown to the user.

Q2



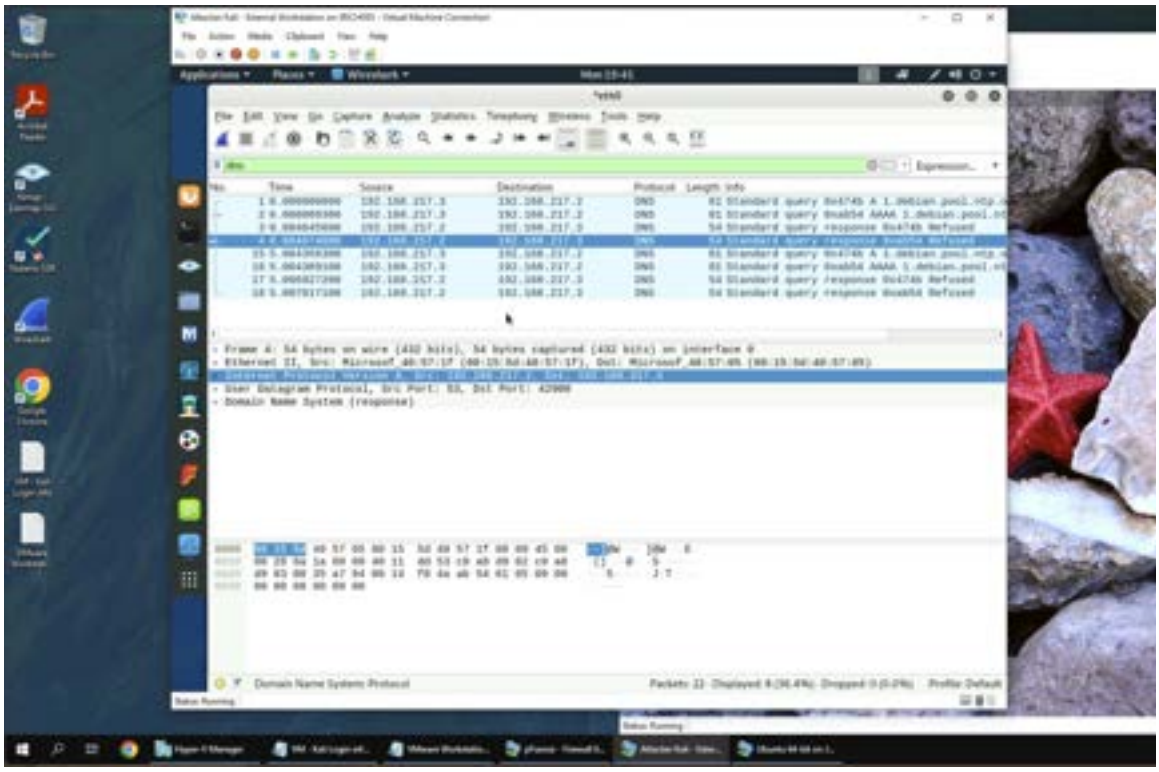
According to the packets and displayed sections at the bottom of wire shark, there are still 22 packets, but only 14 are being displayed after inputting “icmp” into the search filter.

Q3



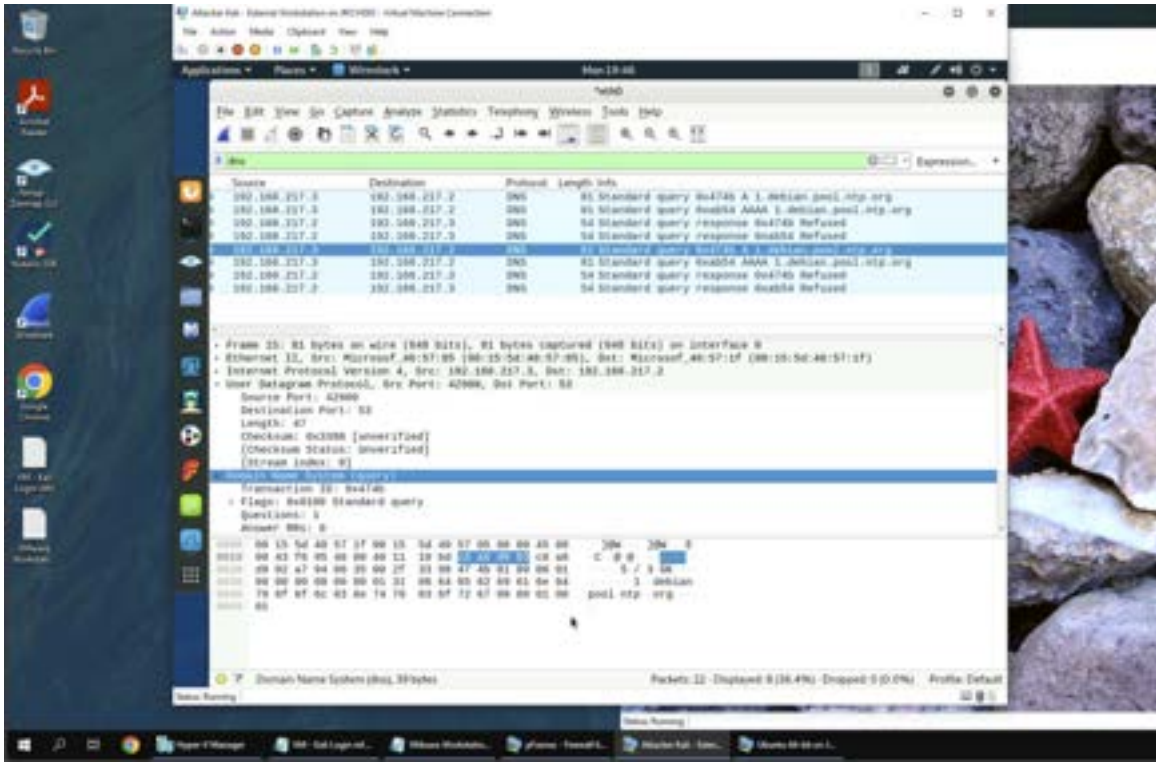
The source and destination IPs of this packet are 192.168.10.10, and 192.168.217.3 respectively. The sequence number is 5/1280 and the size of the packet is 98 bytes. The response time is 2.197 ms

Q4



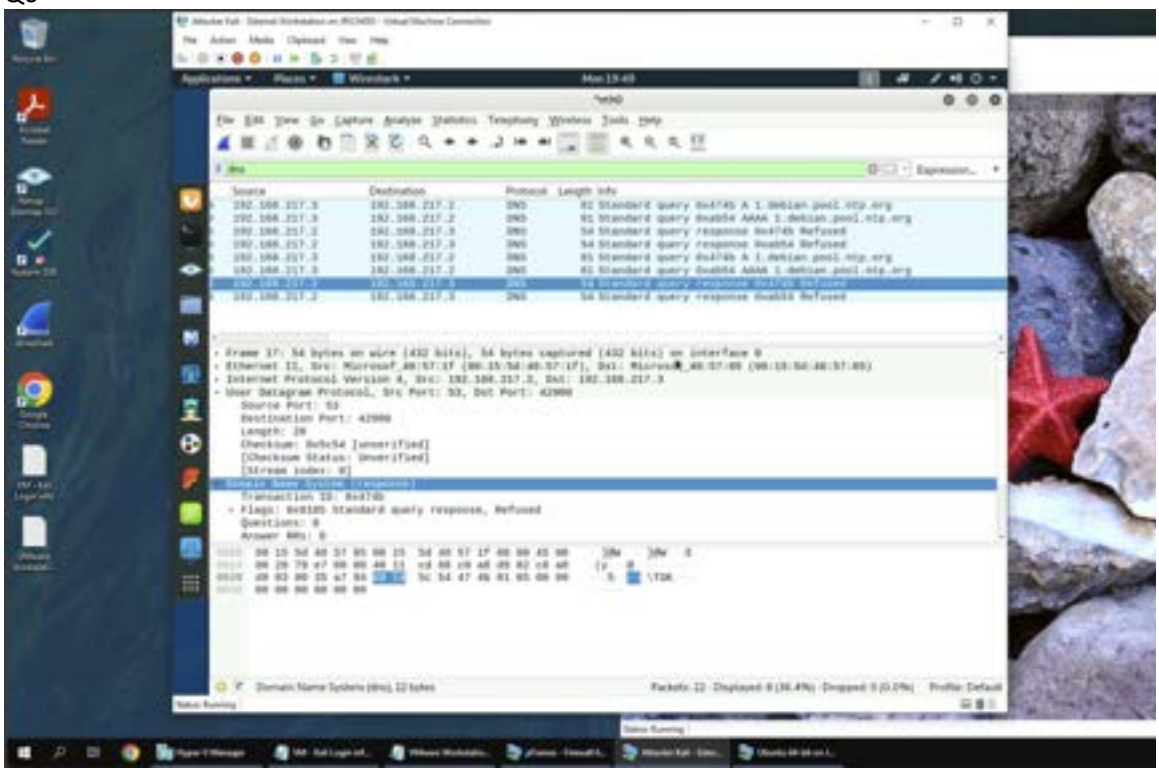
There are only 8 packets displayed with the DNS search filter applied.

Q5

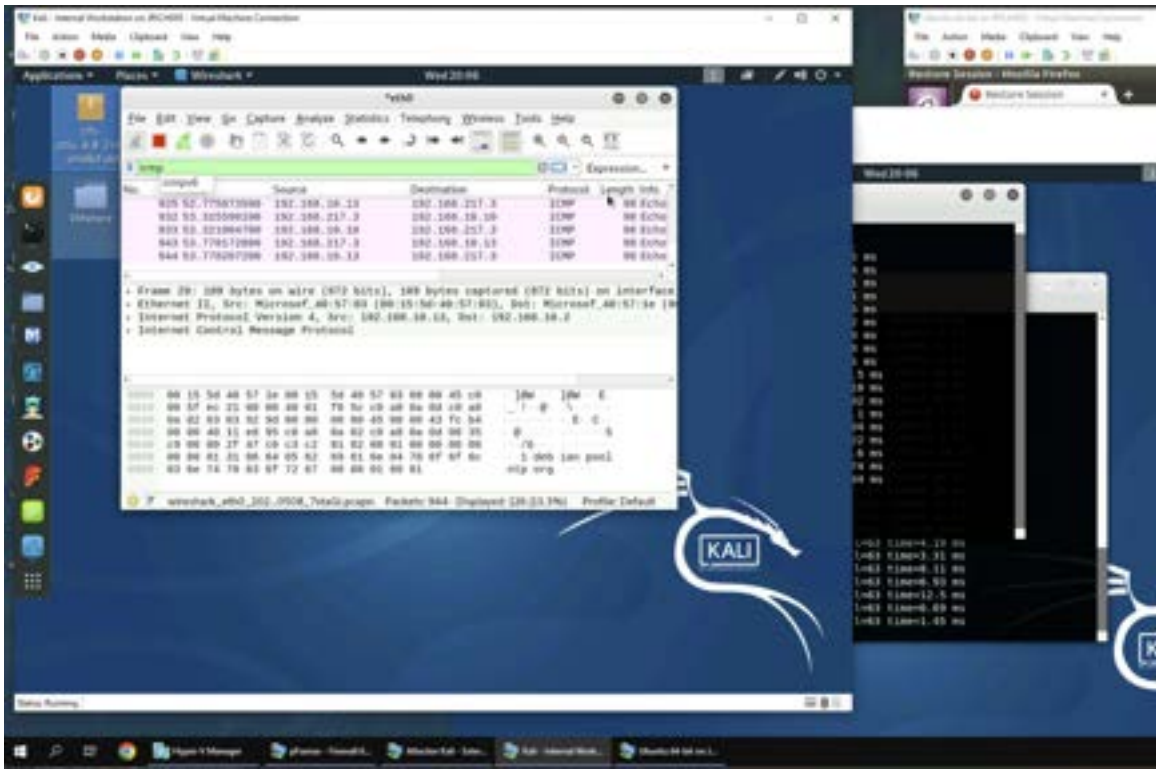


The domain name that is trying to be resolved is 1.debian.pool.ntp.org. The source IP is 192.168.217.3:42900, and the destination IP is 192.168.217.2:53

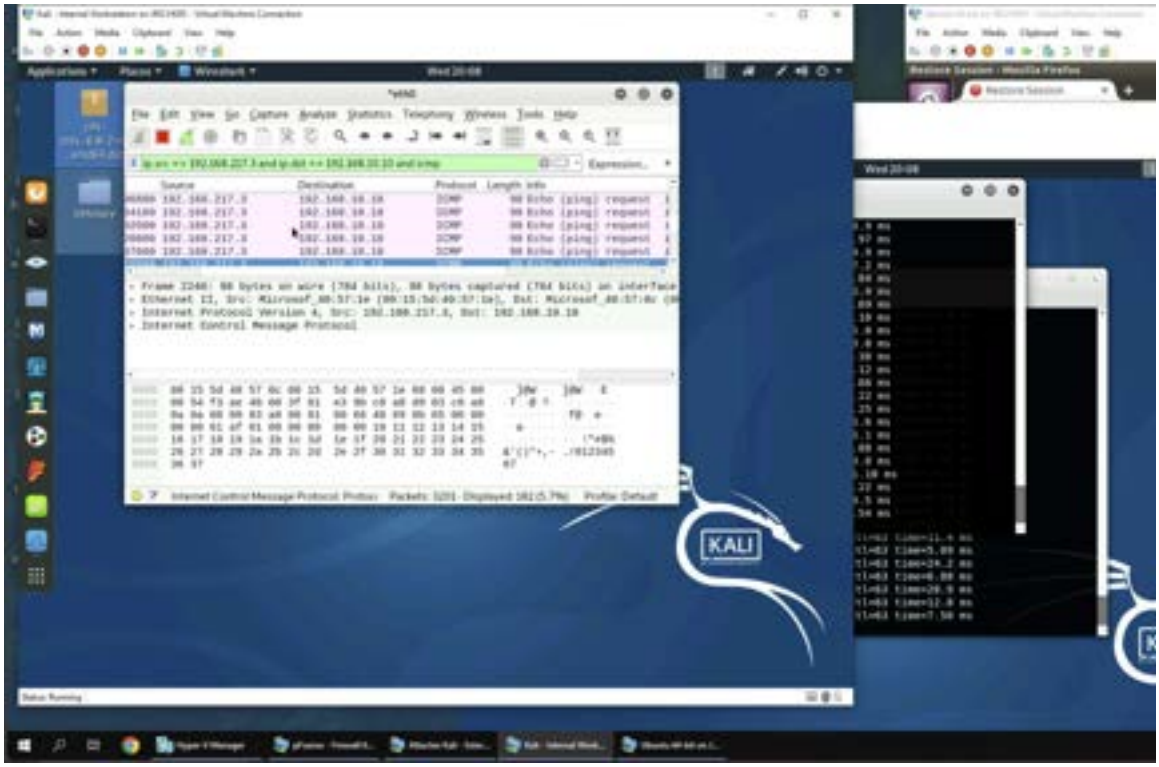
Q6



The source IP and port of the corresponding DNS response is 192.168.217.2:53, and the destination IP and port is 192.168.217.3:42900. The message replied from the DNS server is refused.

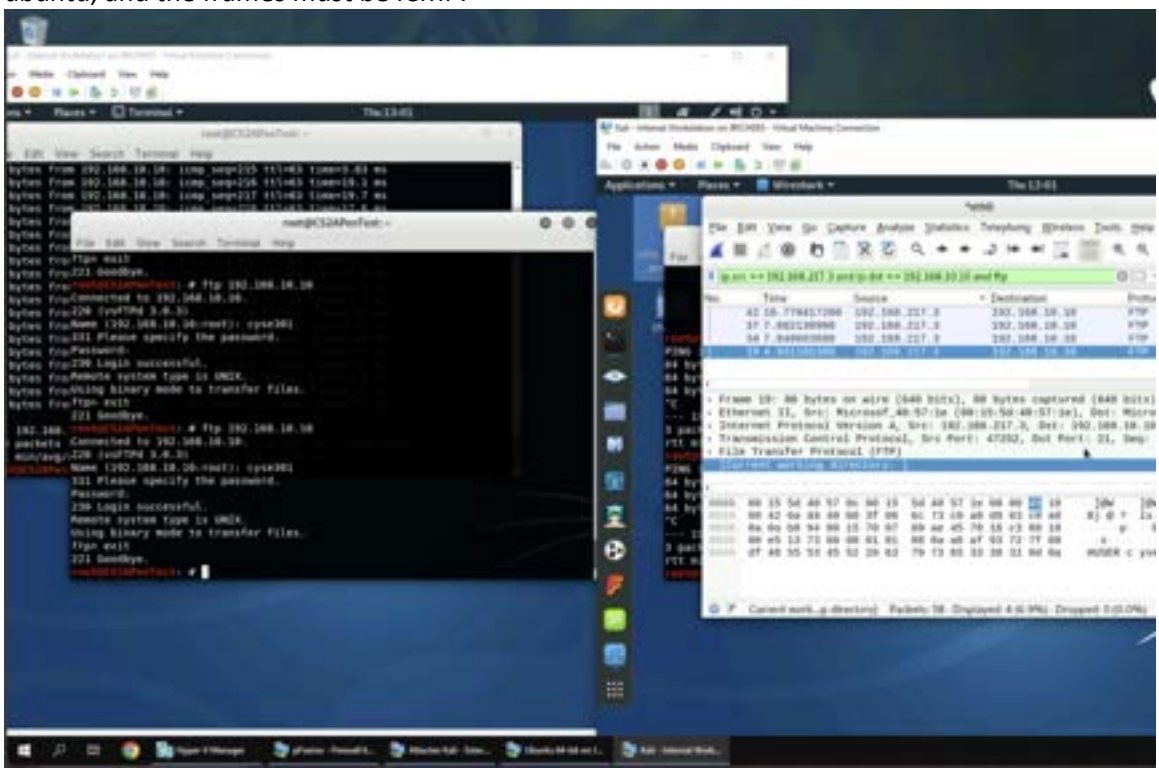


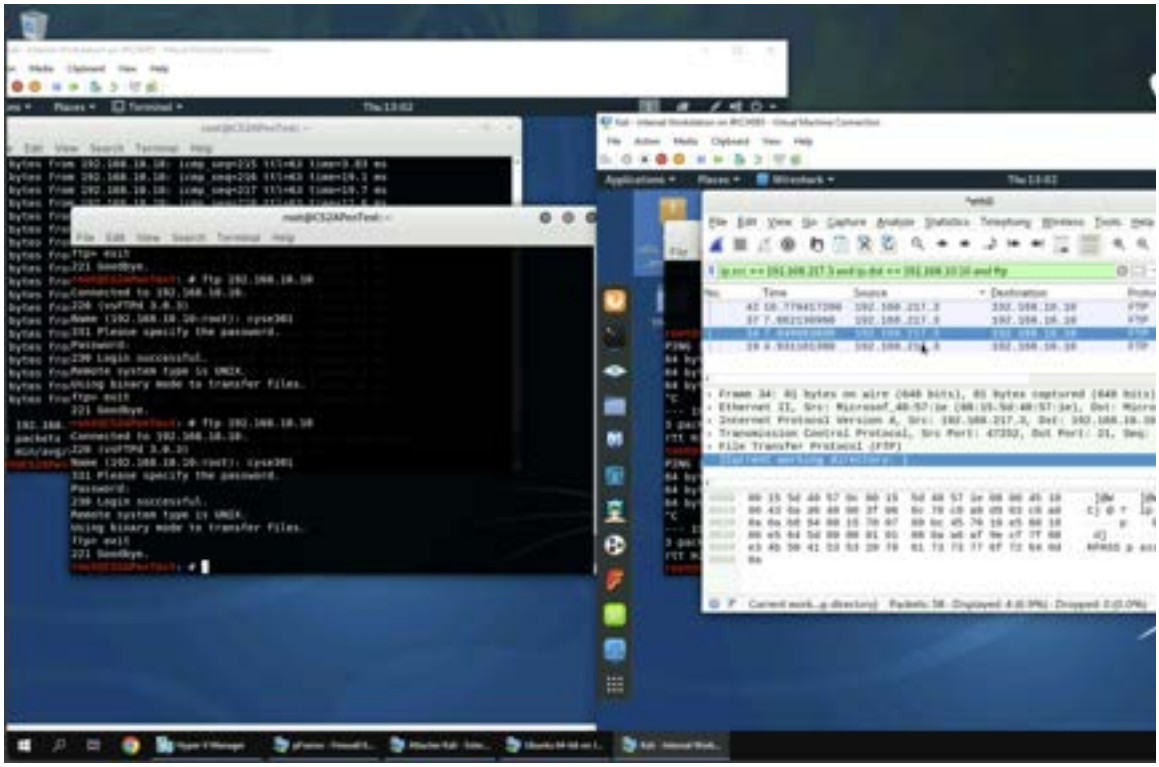
Only ICMP traffic is displayed in the screenshot above due to “icmp” in the display filter.



The only traffic displayed is the traffic from External Kali to Ubuntu due to the display filter that

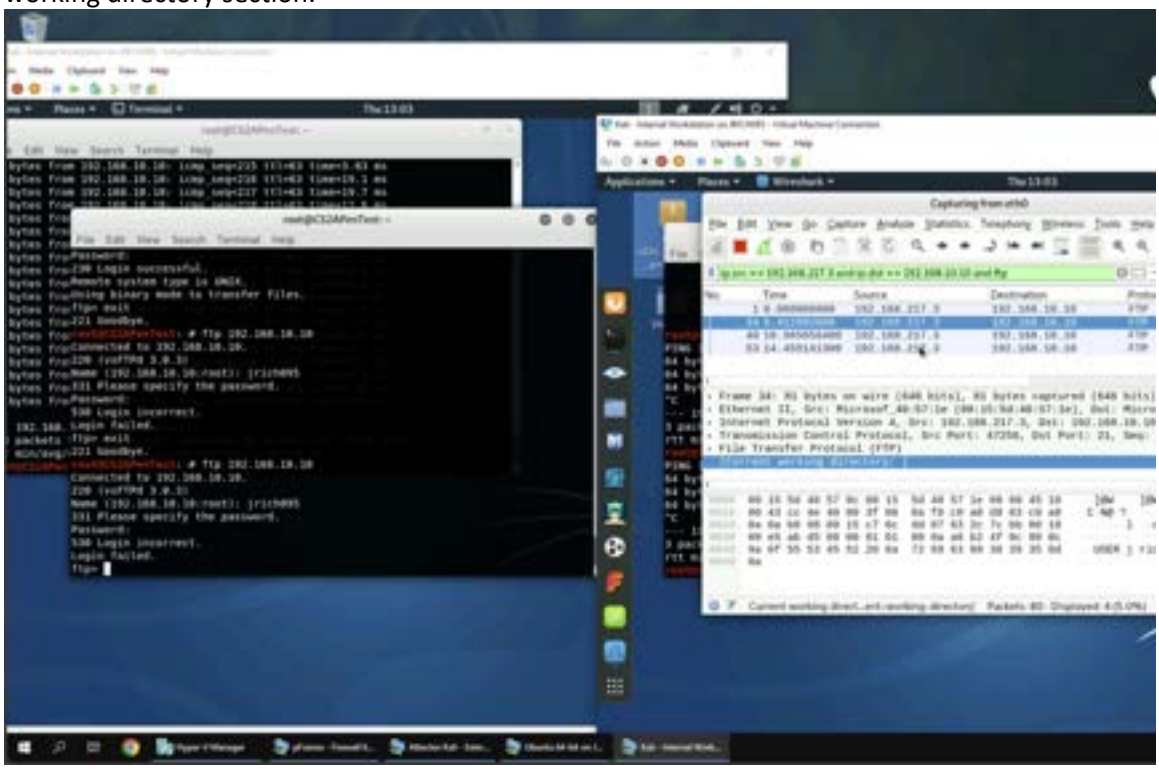
will only show frames with a source IP that matches External Kali, a destination IP that matches ubuntu, and the frames must be ICMP.

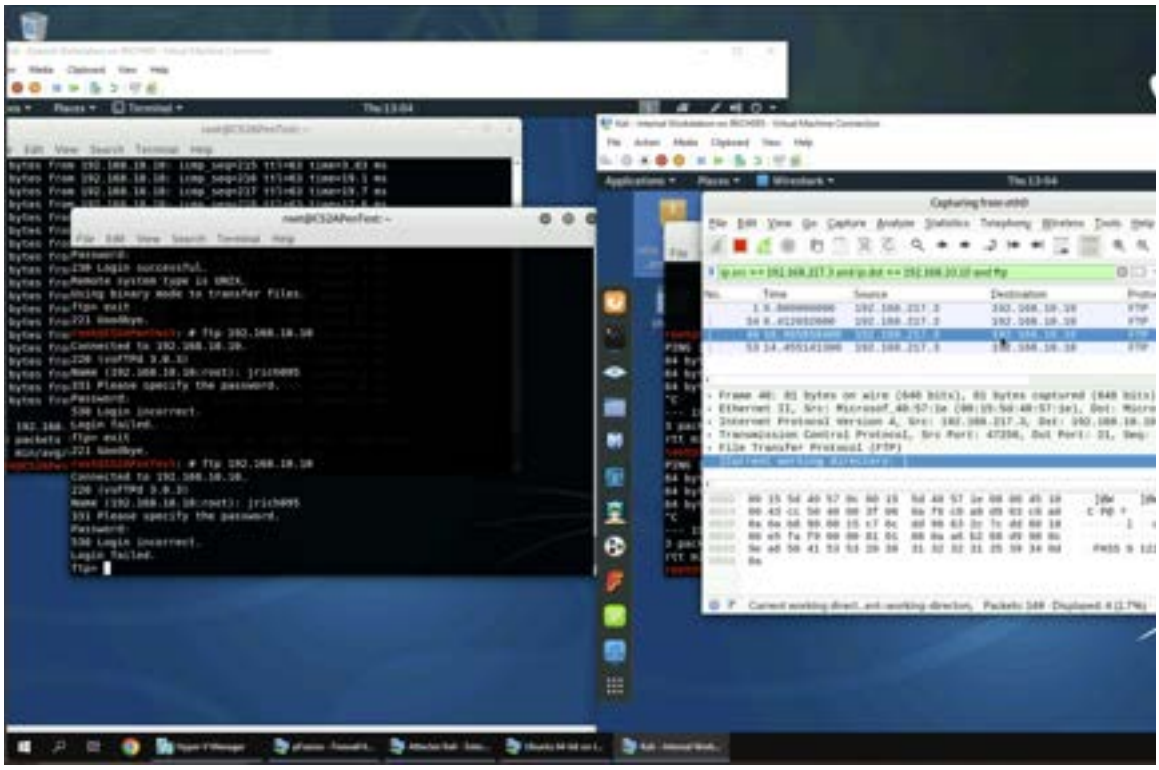




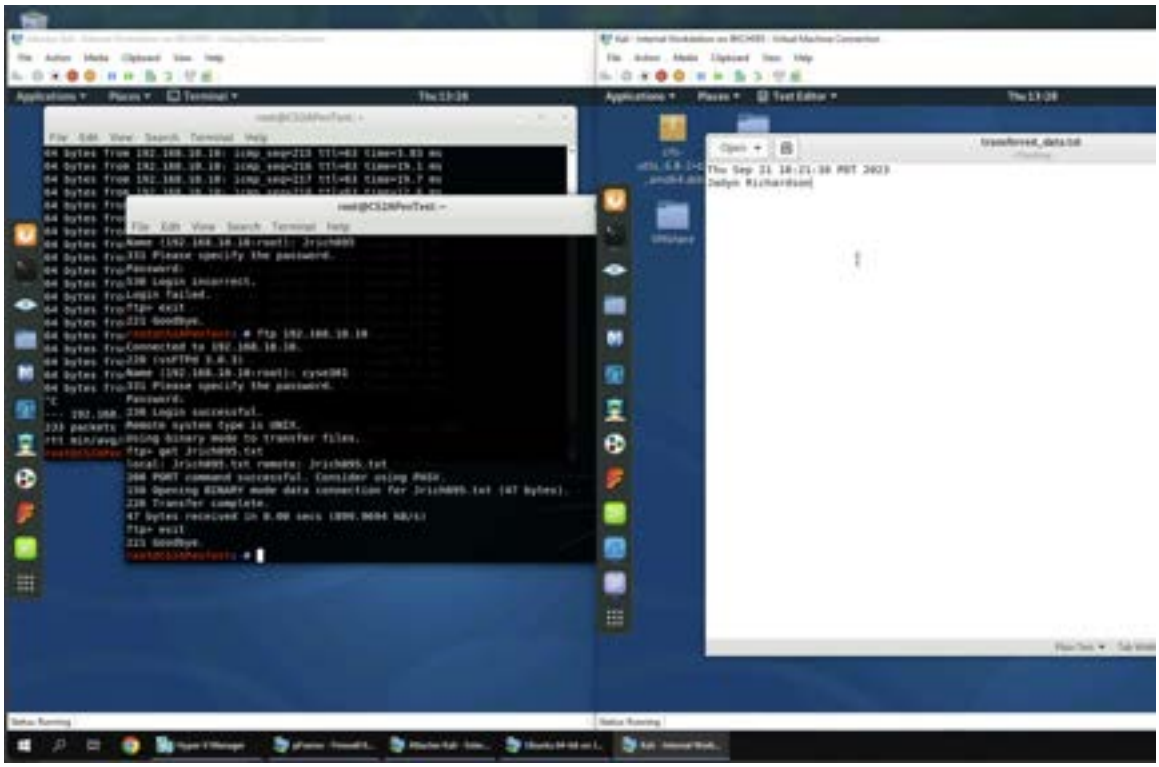
In the two screenshots above, I found the username and password by using a display filter. The display filter was made using the “==” and “and” operators. The “==” operator will only show a

frame if it matches a specified value. The “and” operator will specify a new argument for Wireshark to filter by. I used these operators to find sources from External Kali, and destinations to Ubuntu. I already know that the message will be in FTP, so I also applied the FTP filter. The result is that the only messages that would contain the username or password are shown in two of these four frames. The username and password are found in the current working directory section.





Extra credit



I downloaded the file on external kali by applying the FTP-DATA display filter to find the packet

that contained the text file. Then I right clicked on the packet and clicked follow, then I clicked TCP stream. Then, I clicked save at the bottom of the new window and renamed the file transferred_data.txt.