OLD DOMINION UNIVERSITY

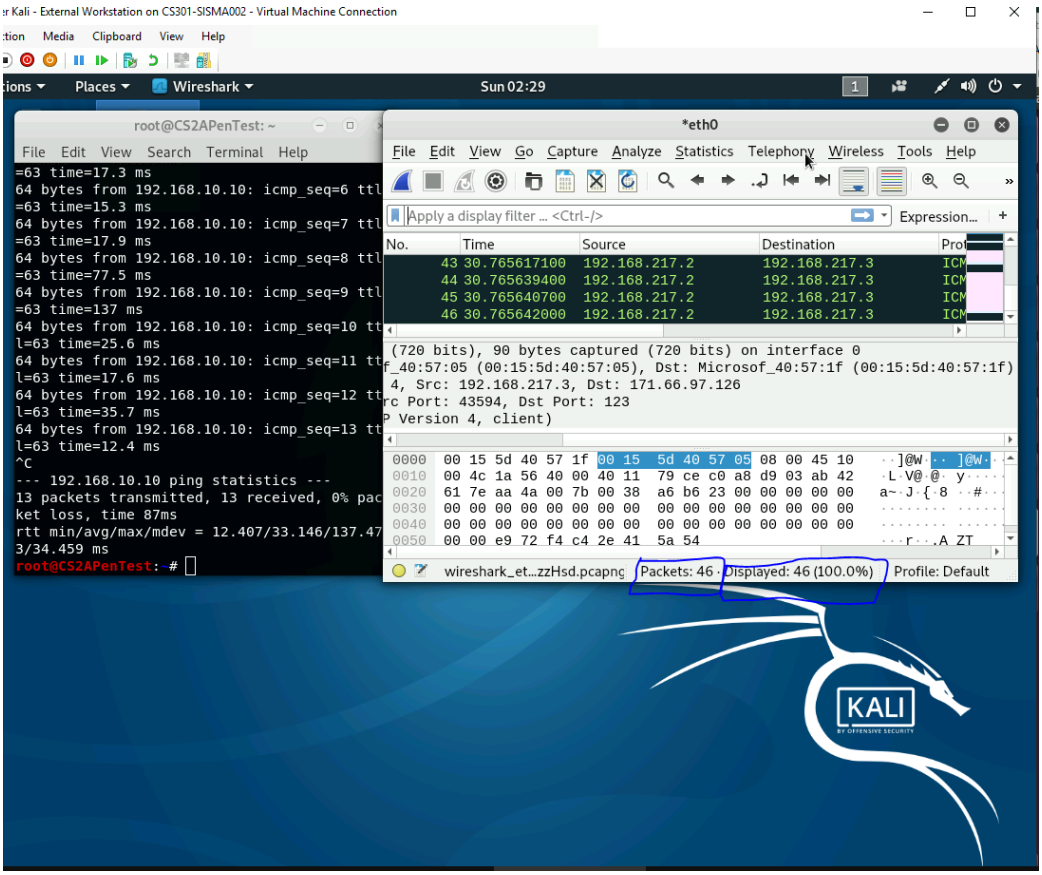
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Sahmer Ismael

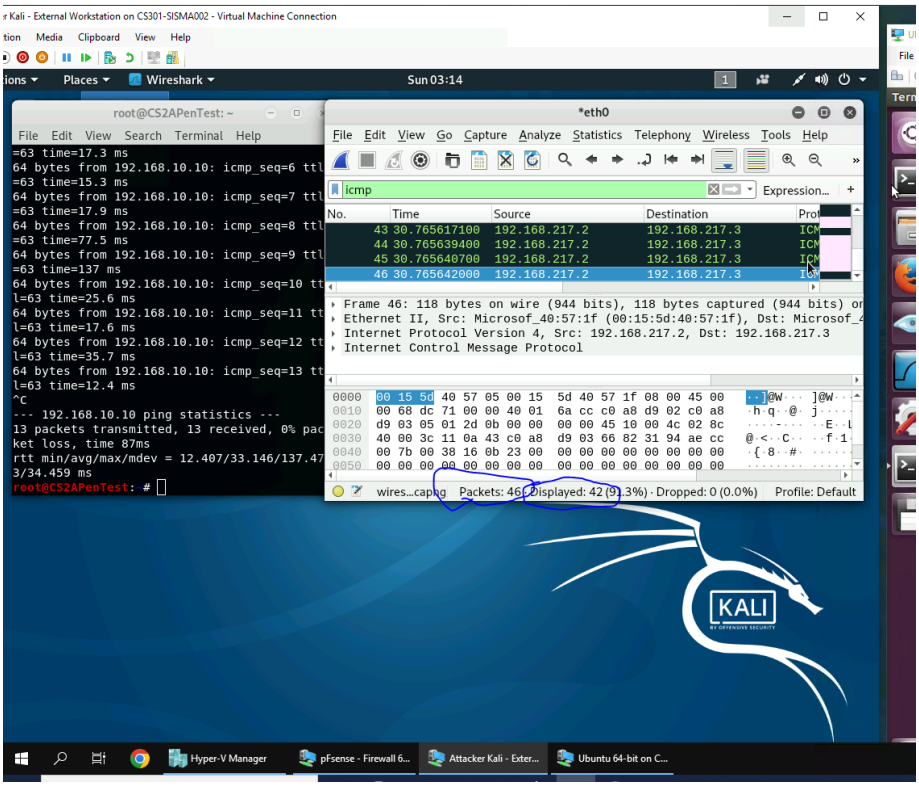
01219271

Q1. How many packets are captured in total? How many packets are displayed?



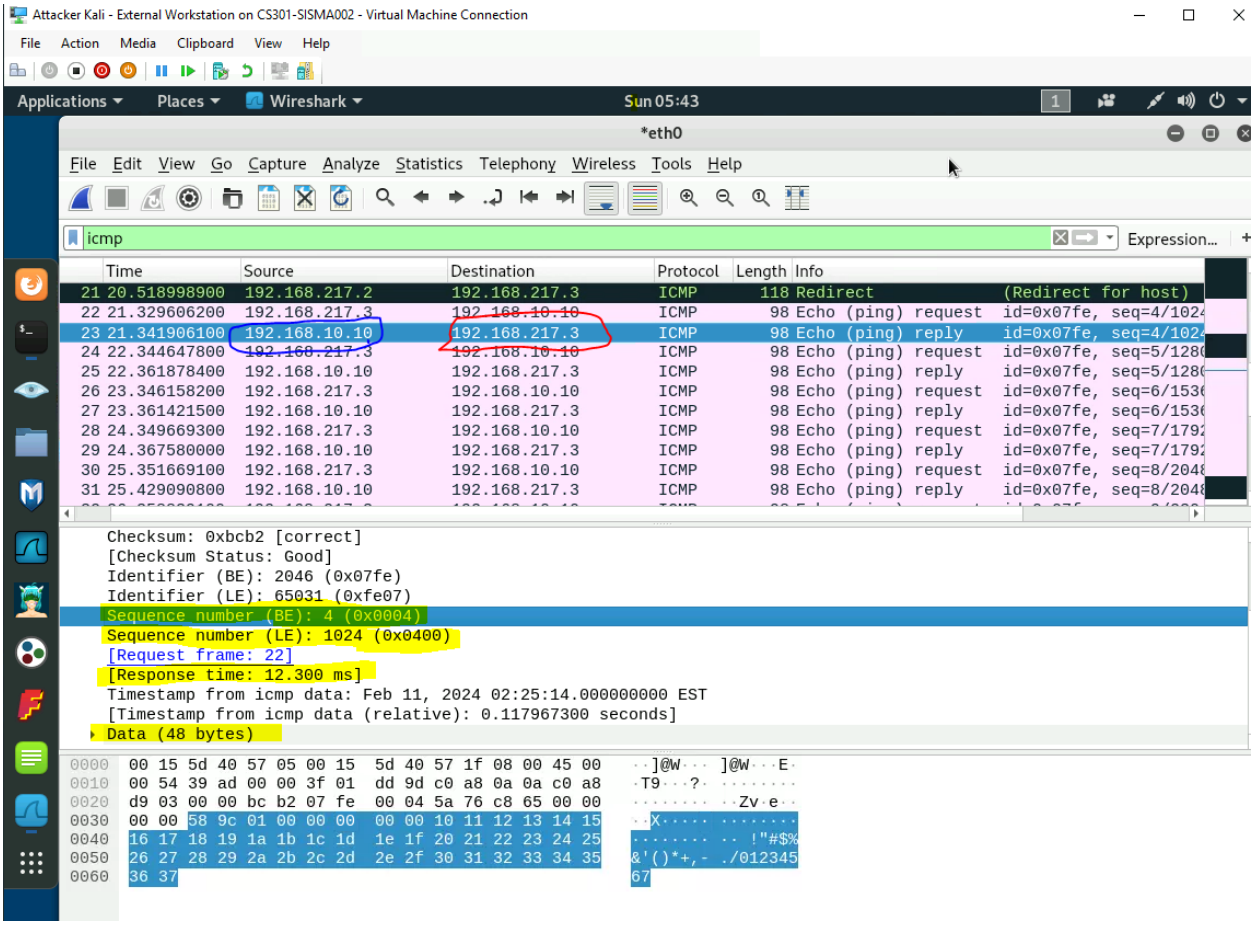
Description- The total number of packets that have been captured are 46, and the total number of packets displayed are 46.

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).



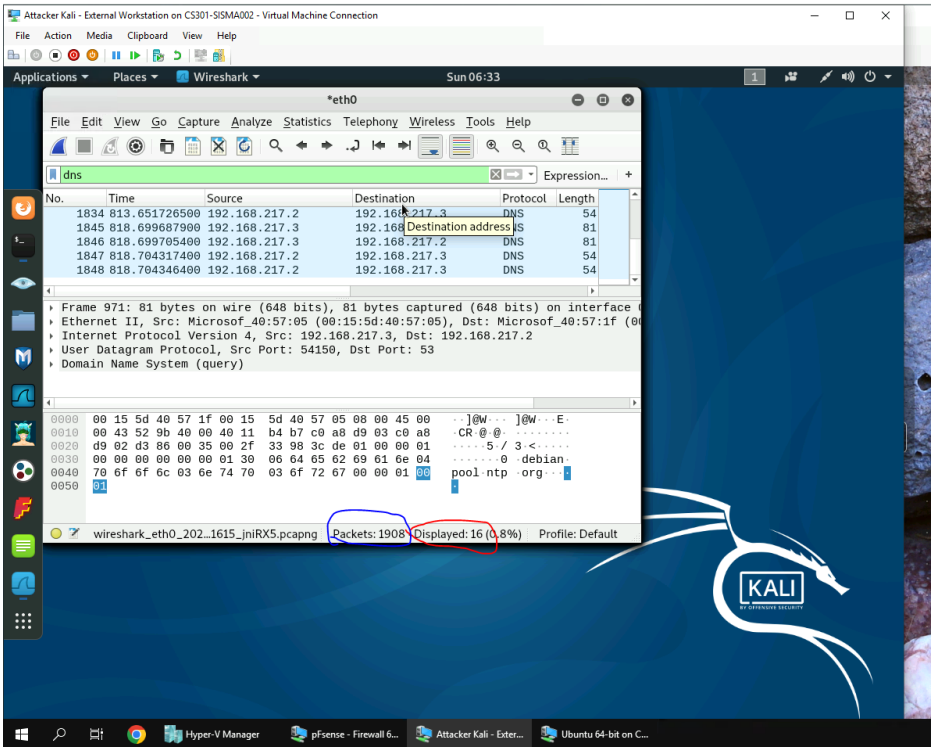
Description: After applying the ICMP filter, in Wireshark the amount of the packets captured stayed the same. However, the amount of the packets that where displayed have changed.

Q3. 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?



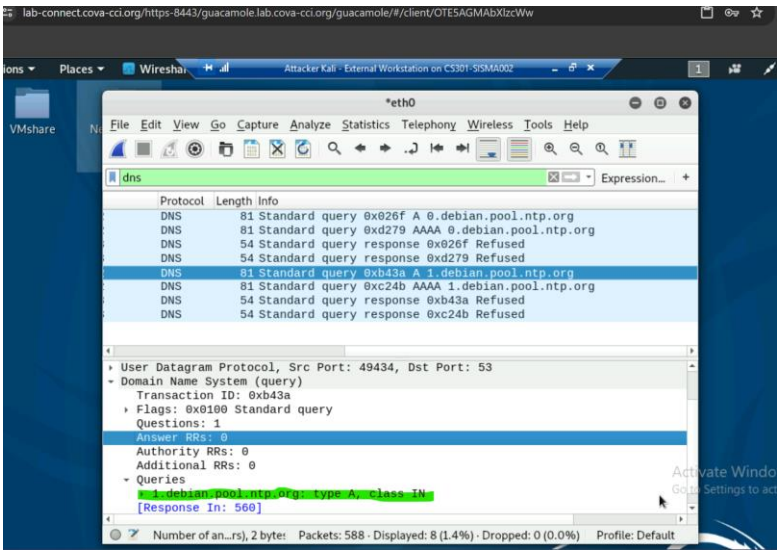
Description: The source IP, for this reply packet is 192.168.10.10, which I circled in blue. The destination IP for this certain packet, is 192.168.217.3, which I circled with red above, in the photo. The sequence number is 4 (0x0004) for big Endian (BE), which I highlighted. And the sequence number for Little Endian (LE) is 1024 (0x0400), which I highlighted. The size of the data is currently (48 bytes), and the response time is, 12.300 ms , which I highlighted both in the above diagram.

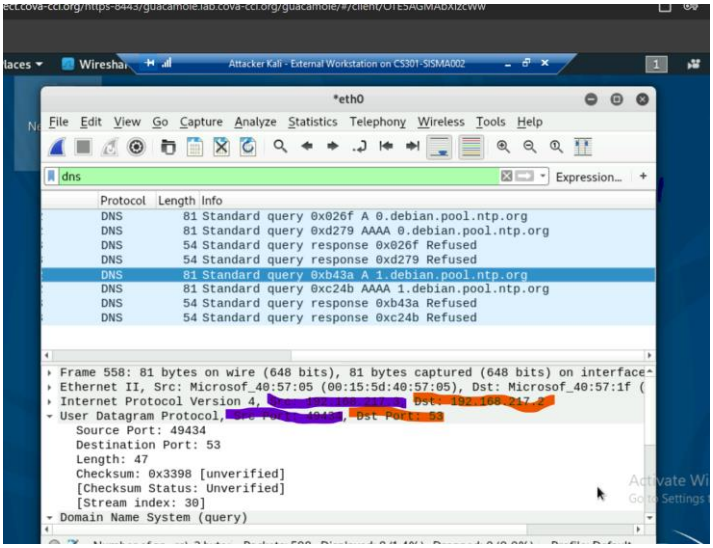
Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?



Description: There a total of 16 DNS packets, that are displayed currently.

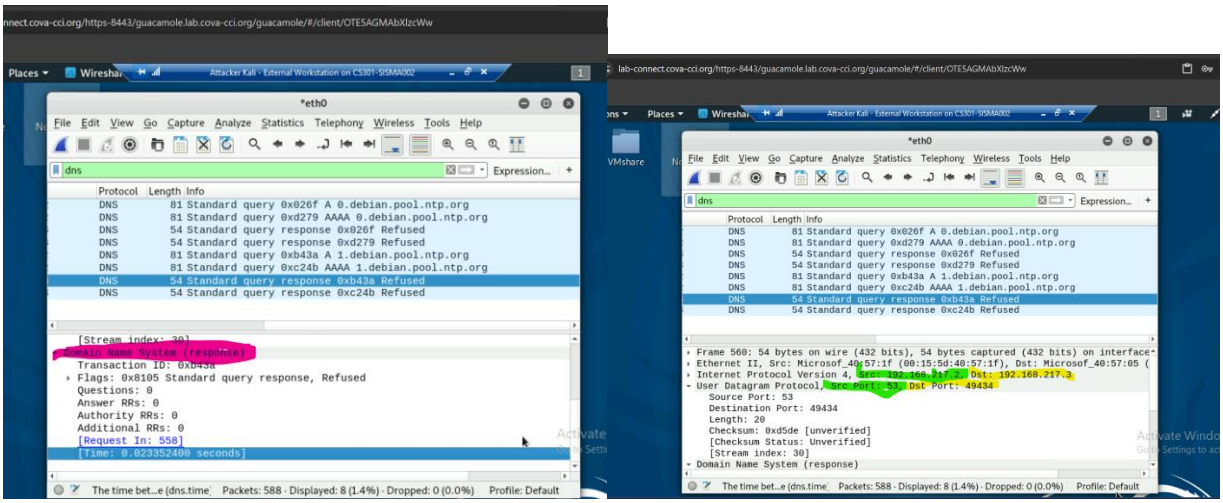
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.





Description: The domain name, this is host is trying to resolve, 1.debian.pool.ntp.org: Type A, class IN, which is displayed in green. The source IP and Port number is highlighted in purple, 192.168.217.3:49434. The destination Ip and Port number is highlighted in orange, 192.168.217.2:53.

Q6. 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?



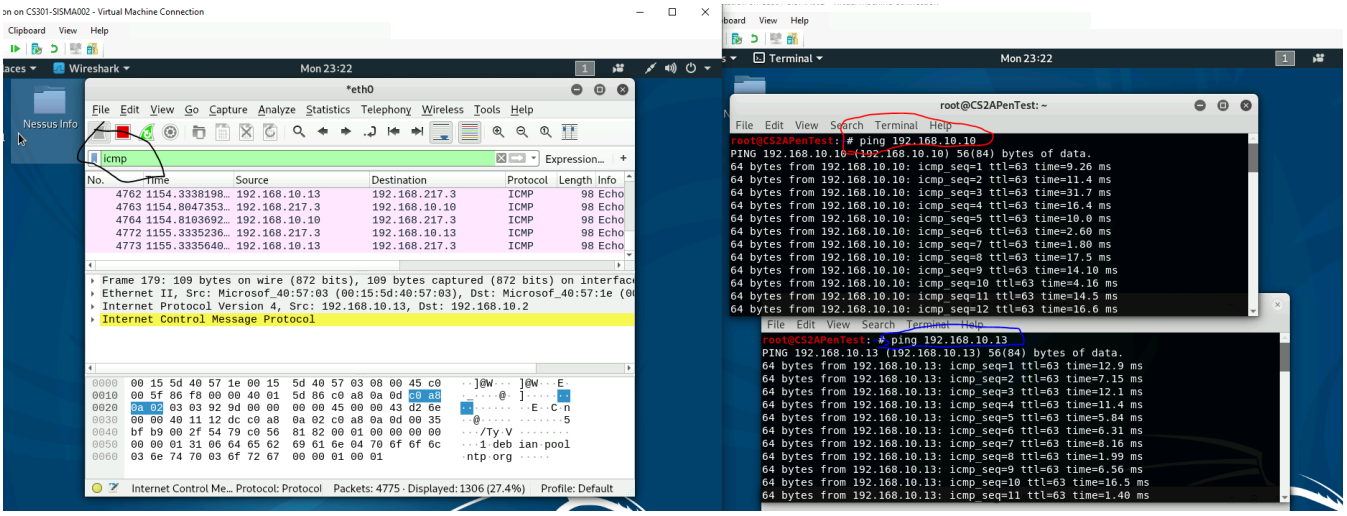
Description: the source IP and port number, is 192.168.217.2:53, displayed green. The destination IP and port number is 192.168.217.3:49434 and it is displayed in yellow.

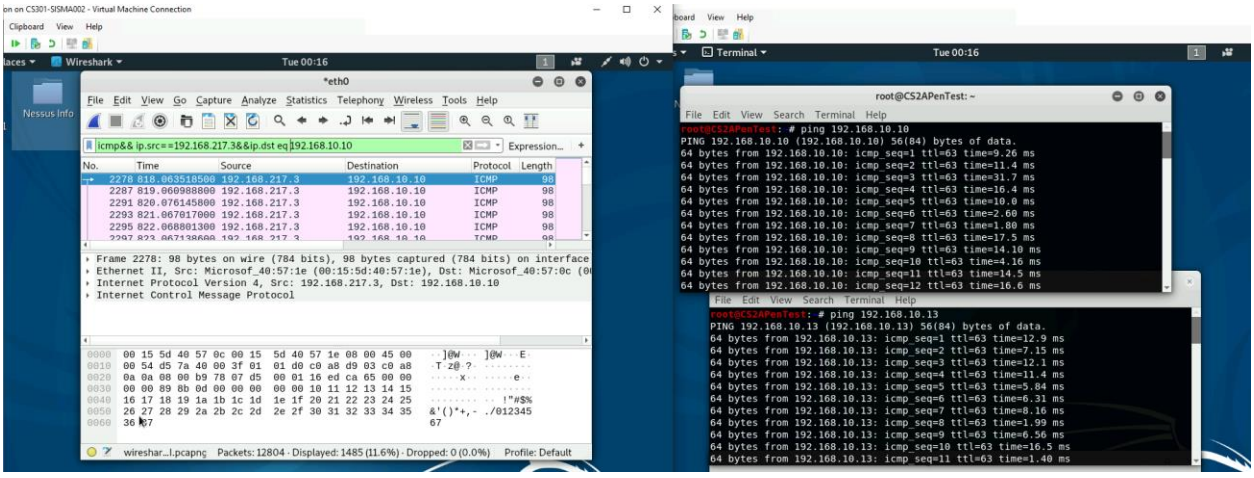
Task B: Sniff LAN traffic

1. Sniff ICMP traffic (10 + 10 = 20 points)

Open two terminals on External Kali VM. Use one ping Ubuntu VM and use the other ping Internal Kali.

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

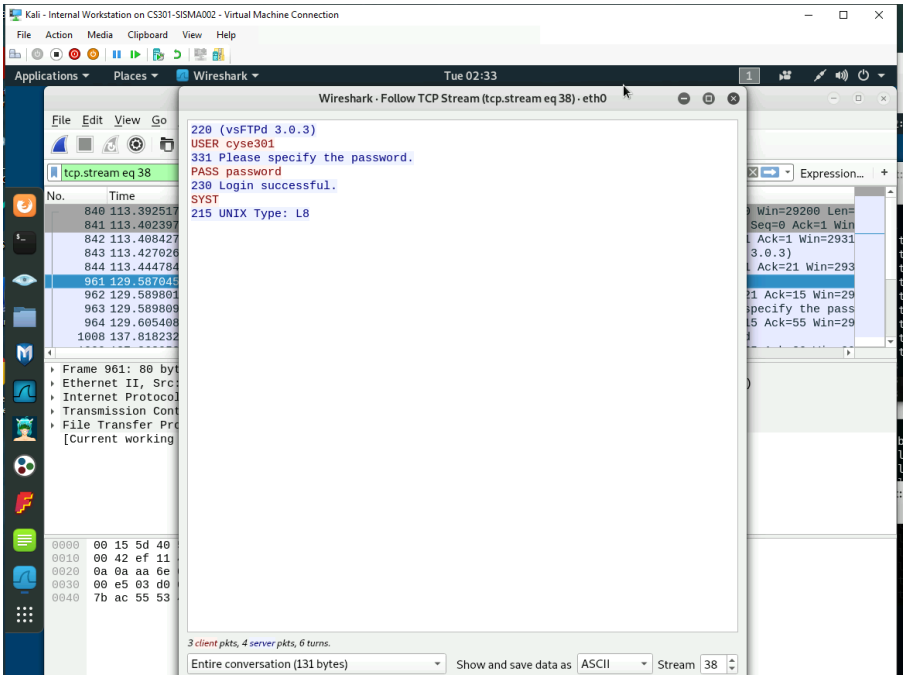




Description: The screenshot displays, that I pinged, the ubuntu vm, and the second is external kali vm. Then after I used the icmp filter, to show the proper packets, that where being displayed.

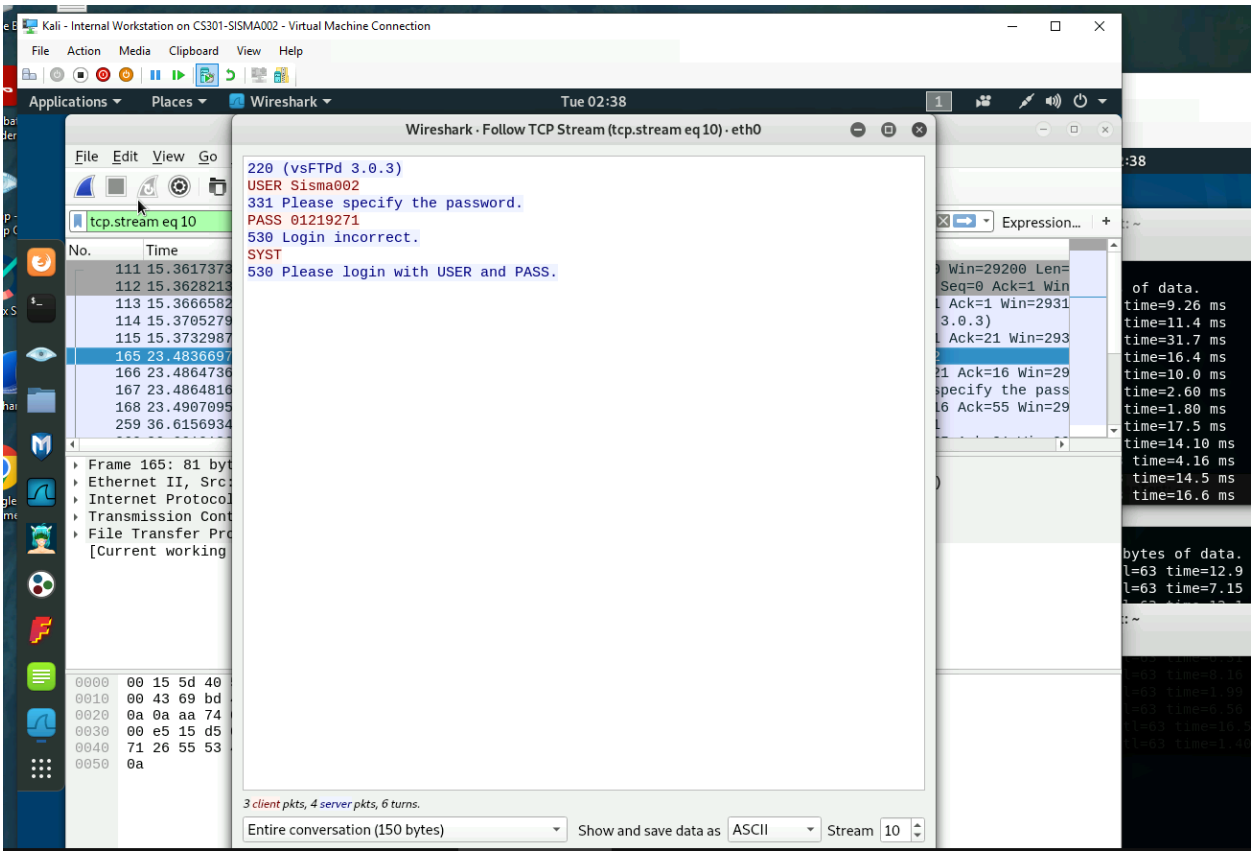
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)
a. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntuVM]. The username for the FTP server is cyse301, and the password is password. You can follow the steps below to access the FTP server

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



Description: The way, that I was able to find the password, was by using the FTP, filter and then following the TCP stream.

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 reassess 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.



Description: I was able to locate my Midas Id and password, by using the FTP filter, and then after locating the packet, and following TCP stream.