OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment 2 -Traffic Tracing and Analysis

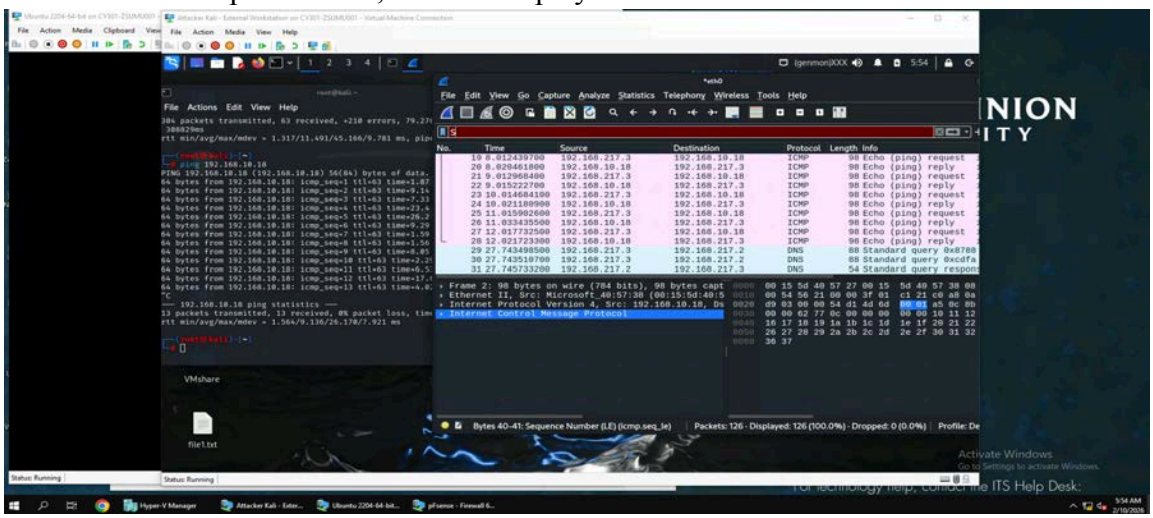
Zyron James M. Sumulong

01058957

Task A: Get started with Wireshark (30 points)

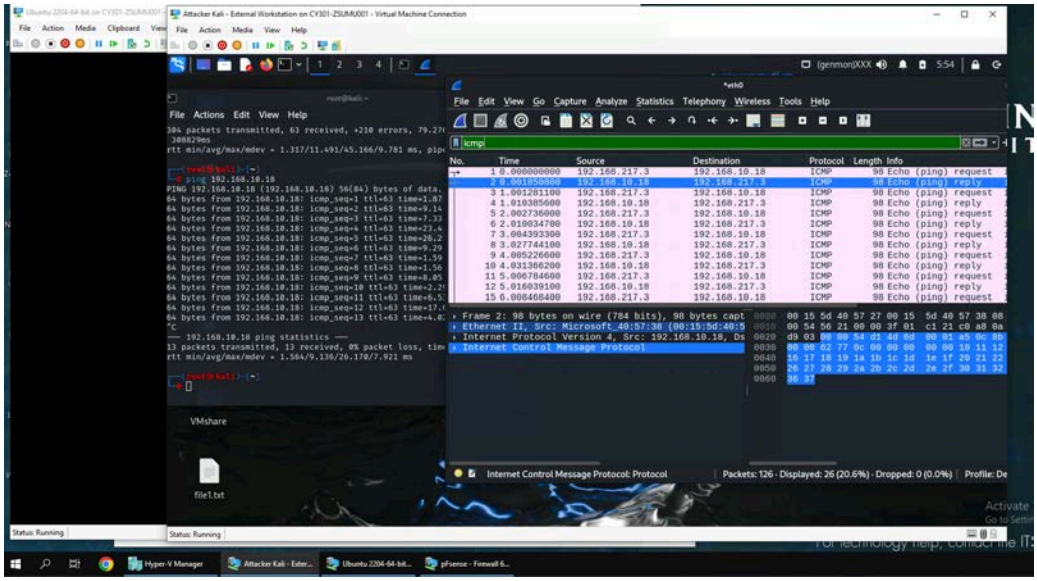
Q1(5pts) How many packets are captured in total? How many packets are displayed?

Packets captured: 126, Packets displayed: 126



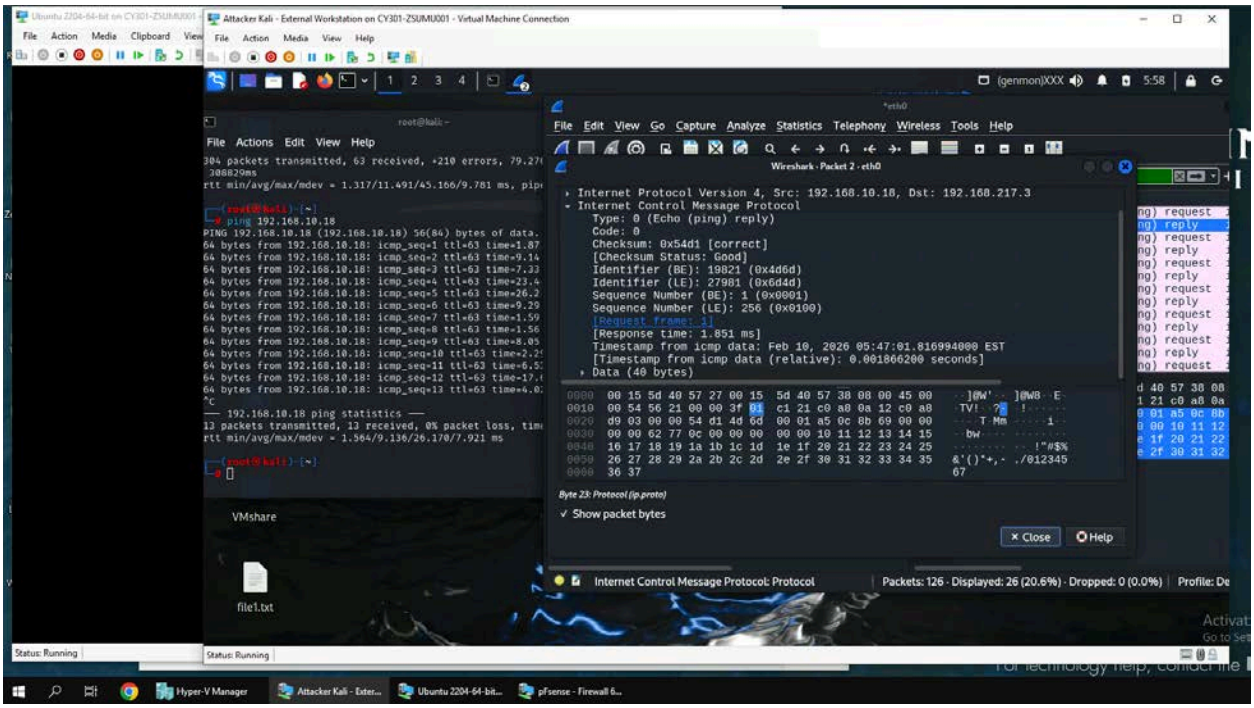
Q2(5pts) Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

Packets captured: 126, Packets displayed: 26



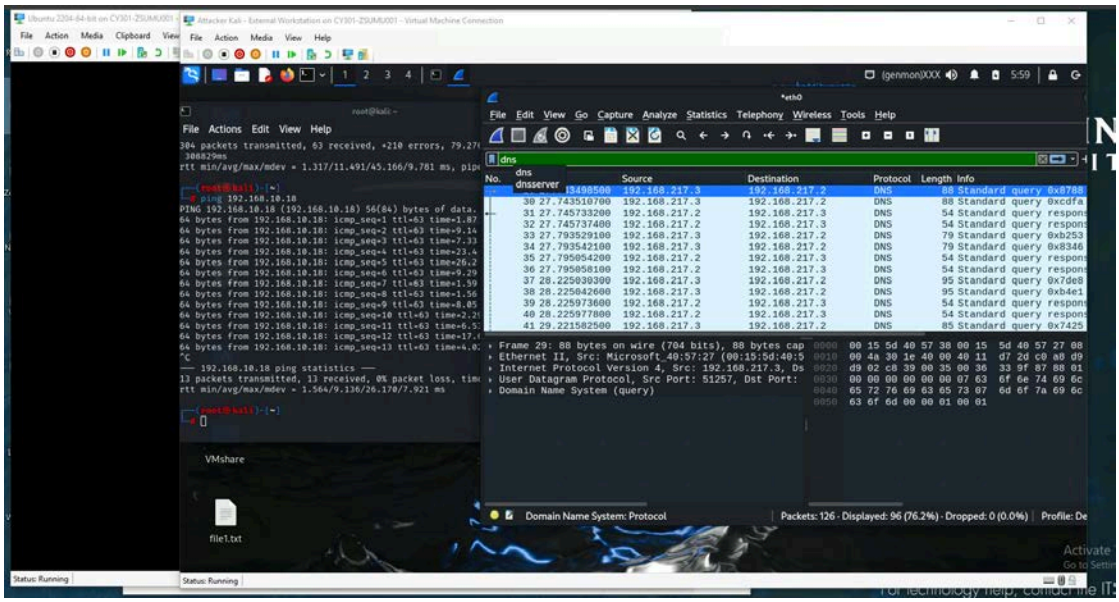
Q3. (5pts) Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

Source IP: 192.168.10.18 Destination IP: 192.168.217.3
Sequence Number: 1/256 Size of Data: 40 bytes
Response Time: 1.851 ms

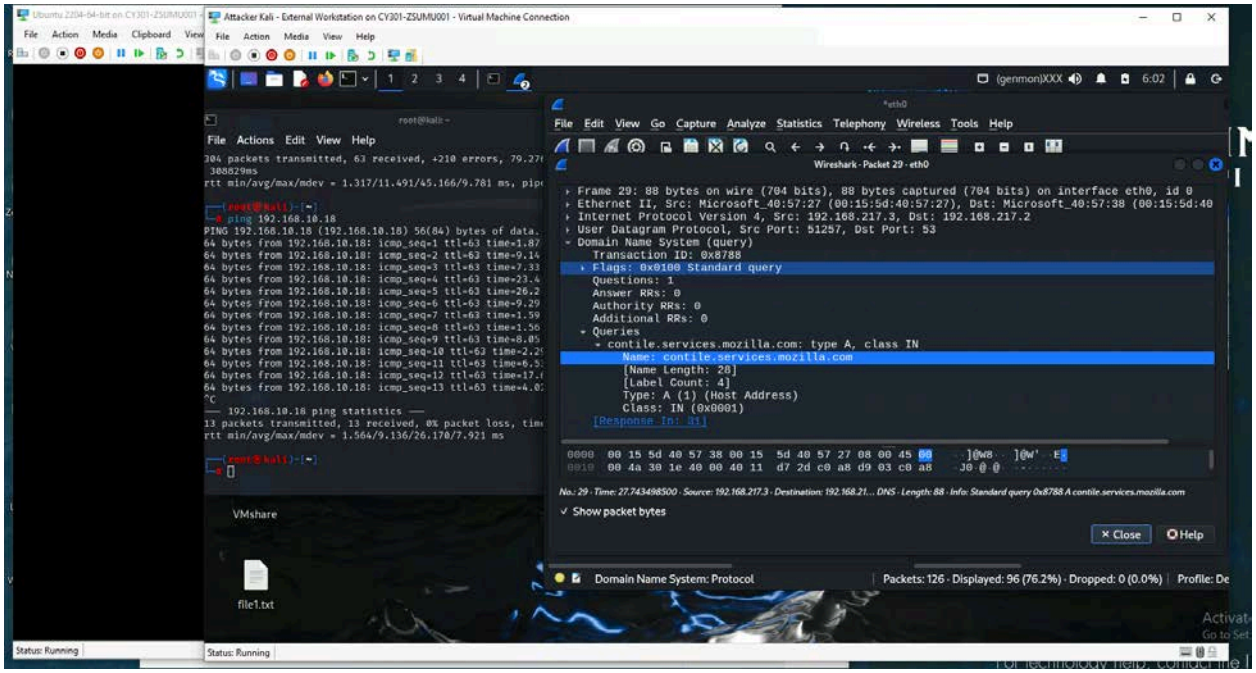


Q4. (5 pts) Apply "DNS" as a display filter in Wireshark. How many packets are displayed?

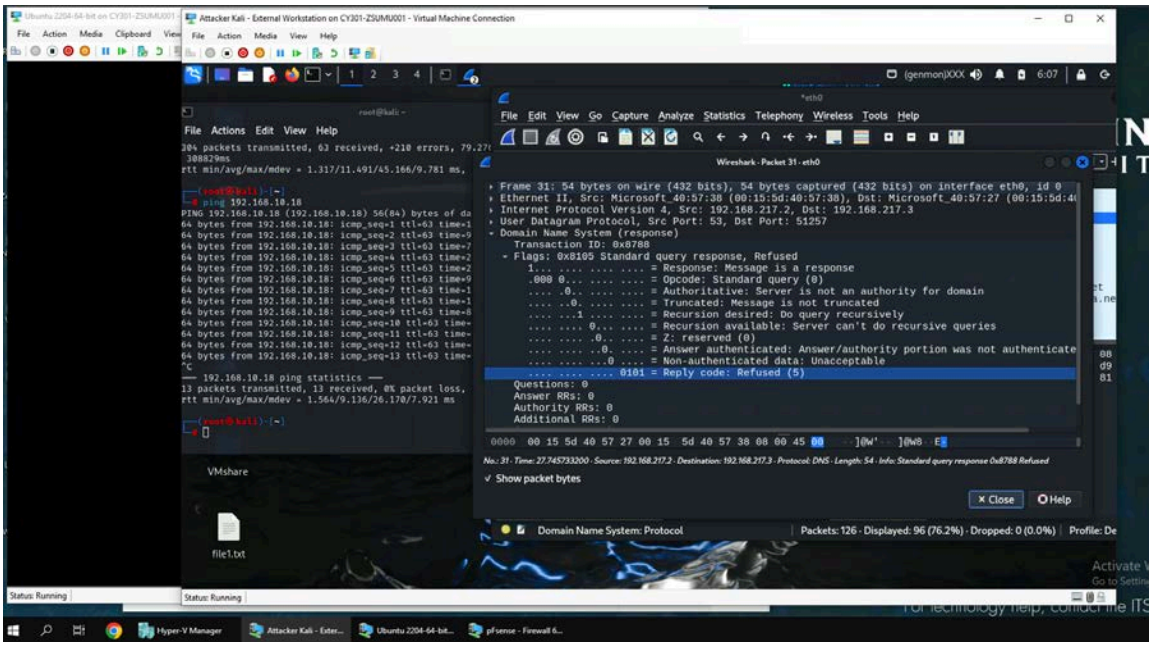
Packets displayed: 96



Q5. (5 pts) 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?
Domain Name: contile.services.mozilla.com
Source IP: 192.168.217.3 Port Number: 51257
Destination IP: 192.168.217.2 Port Number: 53



Q6. (5 pts) 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?
Source IP: 192.168.217.2 Port Number: 53
Destination IP: 192.168.217.3 Port Number: 51257
Reply code: Refused (5)

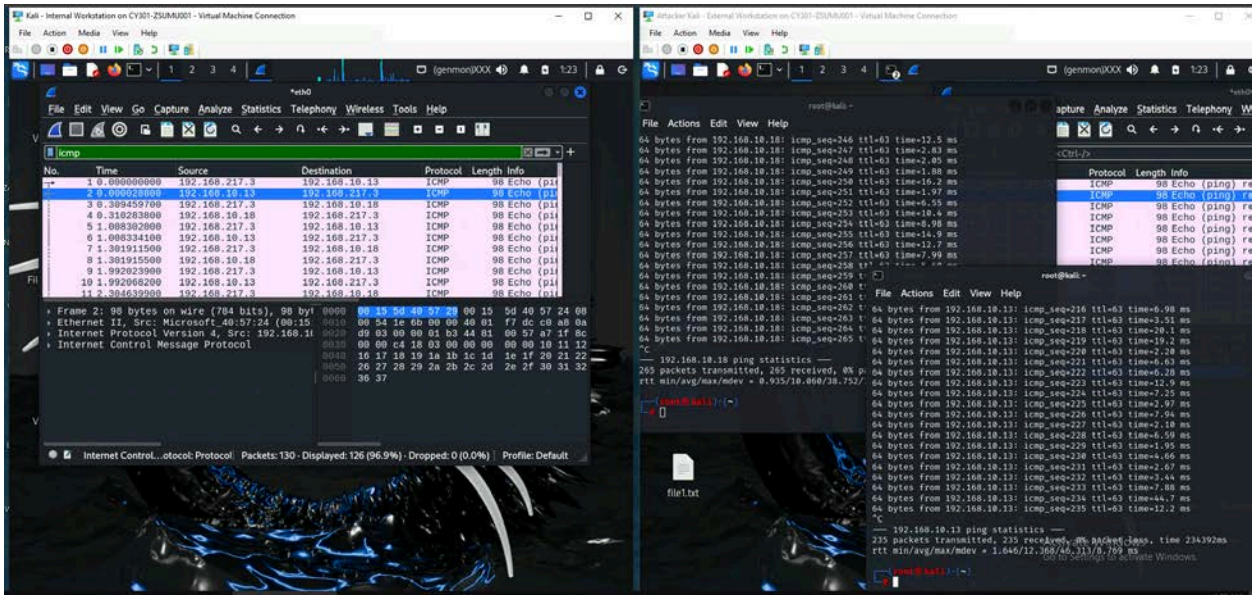


Task B: Sniff LAN traffic (70 Points)

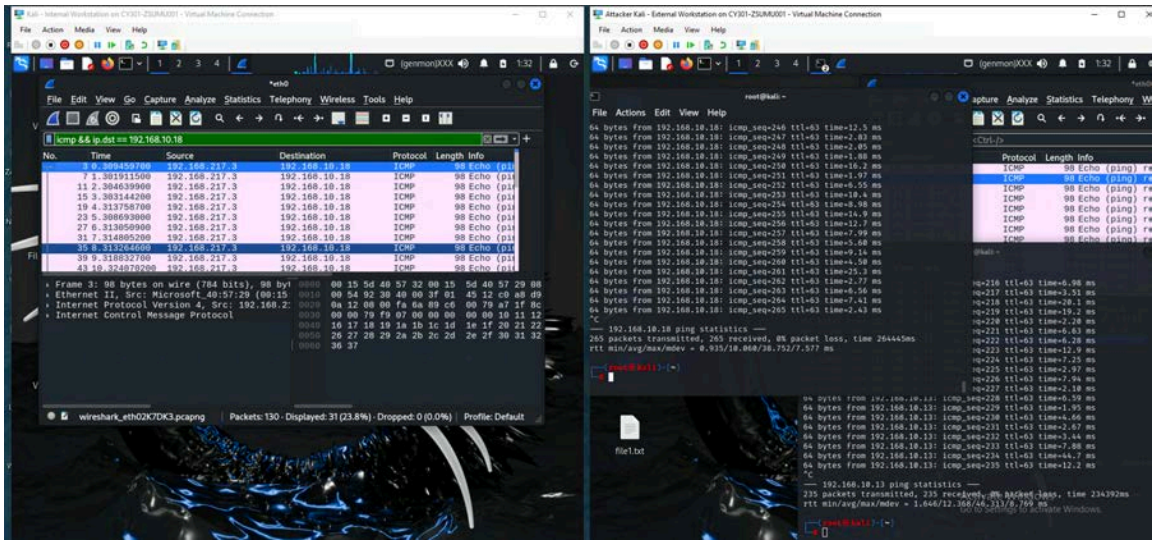
1. Sniff ICMP traffic (5 + 5 + 5 + 15 = 30 points)

Please turn on Attacker/External Kali, internal kali, pfsense, and Ubuntu.

a. Launch and run Wireshark in Internal Kali.
b. Open two terminals on External Kali VM. Use one to ping Ubuntu VM, and use the other to ping Internal Kali.
c. Apply proper display or capture filter in Wireshark on **Internal Kali VM** to show active ICMP traffic.

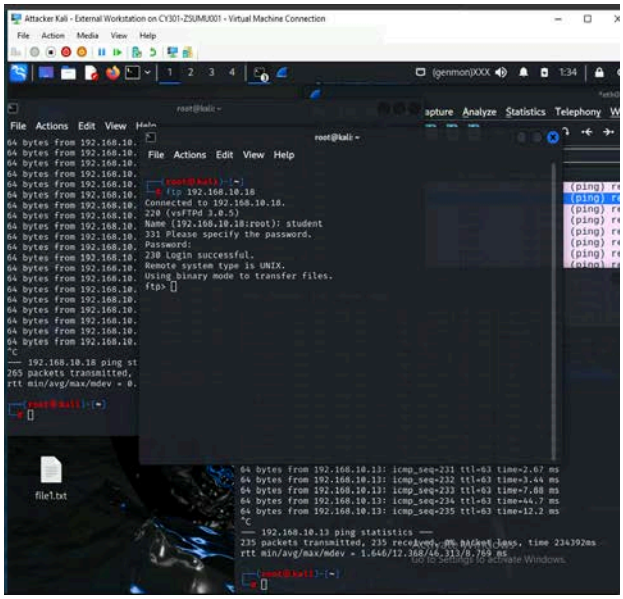


d. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.
Filtered by using : icmp && ip.dst == 192.168.10.18 (Ubuntu VM)



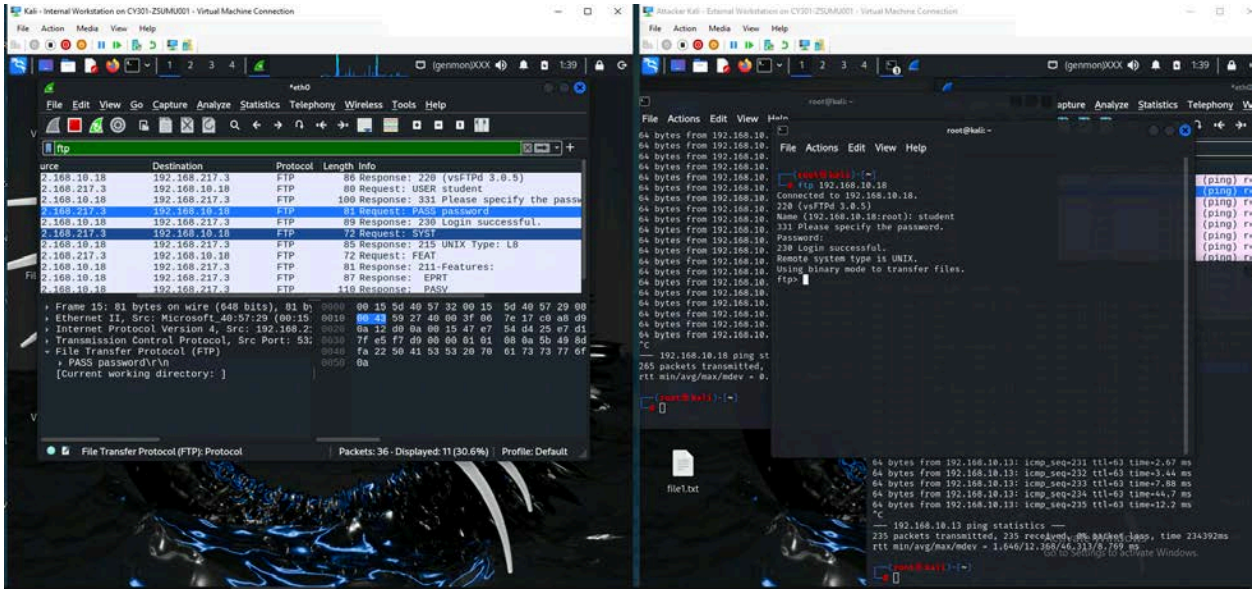
2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

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 ubuntu VM]*. The username for the FTP server is **student** , 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 into the communication. Therefore, all of 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 take a screenshot and explain how you found the password.

Went into Internal Kali Wireshook and filtered by ftp. Looked at the Request: USER and Request: PASS in which the corresponding username and password was displayed.



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 re-access 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**.

Utilized the same strategy in 2.b, even though the login failed, we were still able to intercept the packets that contained what username (MIDAS ID) and password (UIN) was utilized.