OLD DOMINION UNIVERSITY

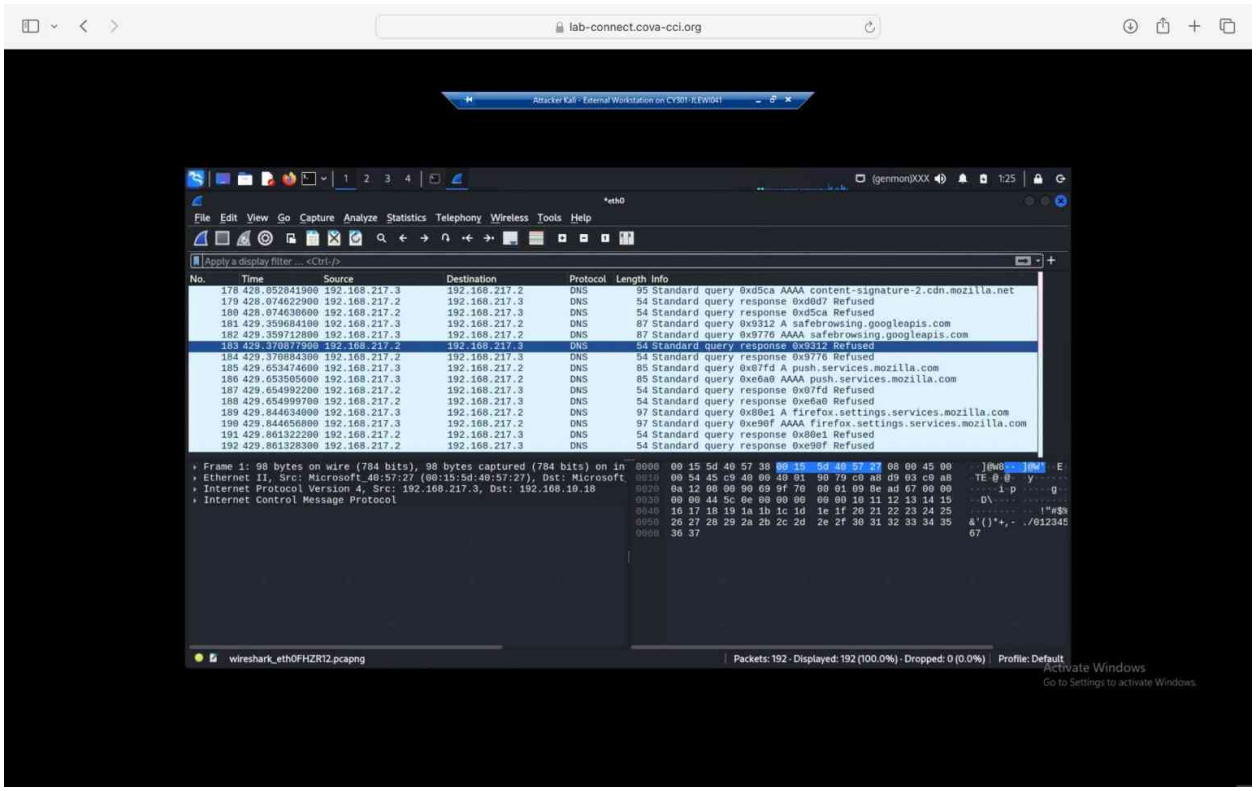
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

JaQwah Lewis

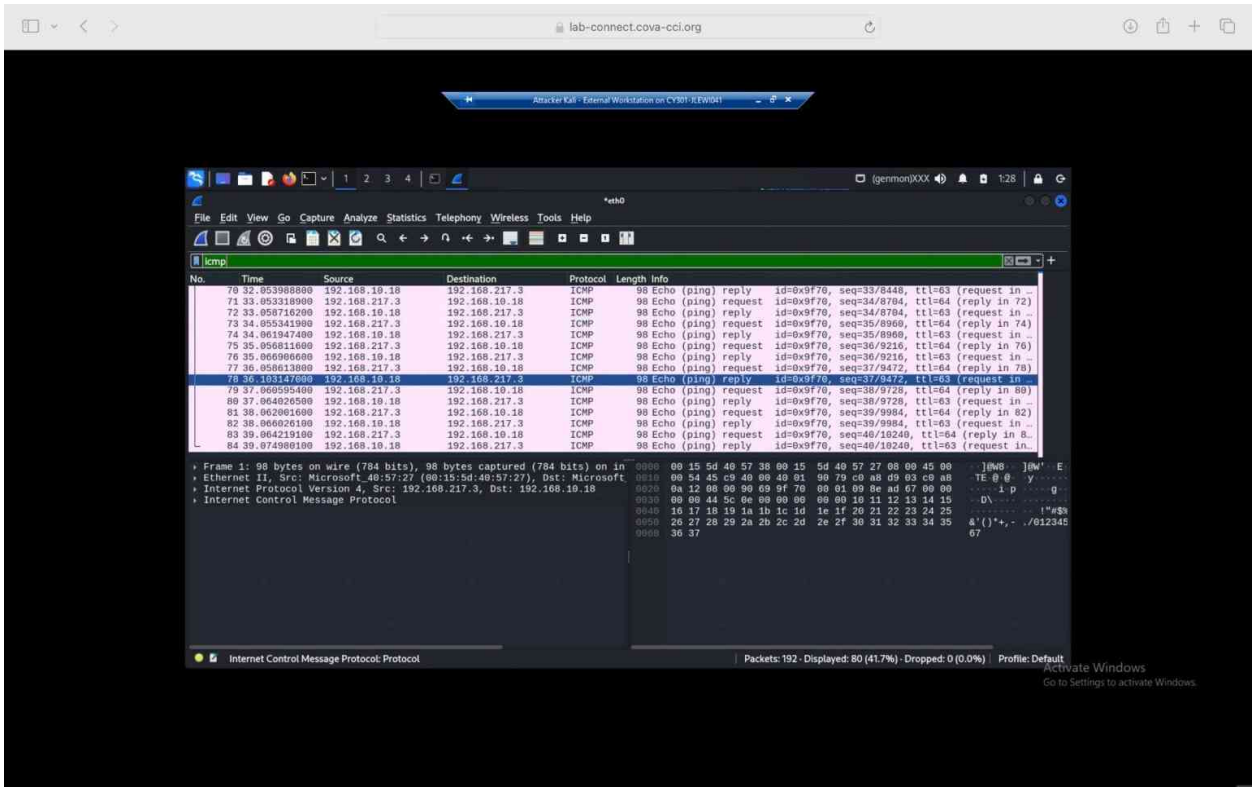
Q1. How many packets are captured in total? How many packets are displayed?

In total, there are 192 packets captured. Next to where it shows how many packets are there in total it also shows how many packets are displayed in. In total, there are 192 packets displayed.



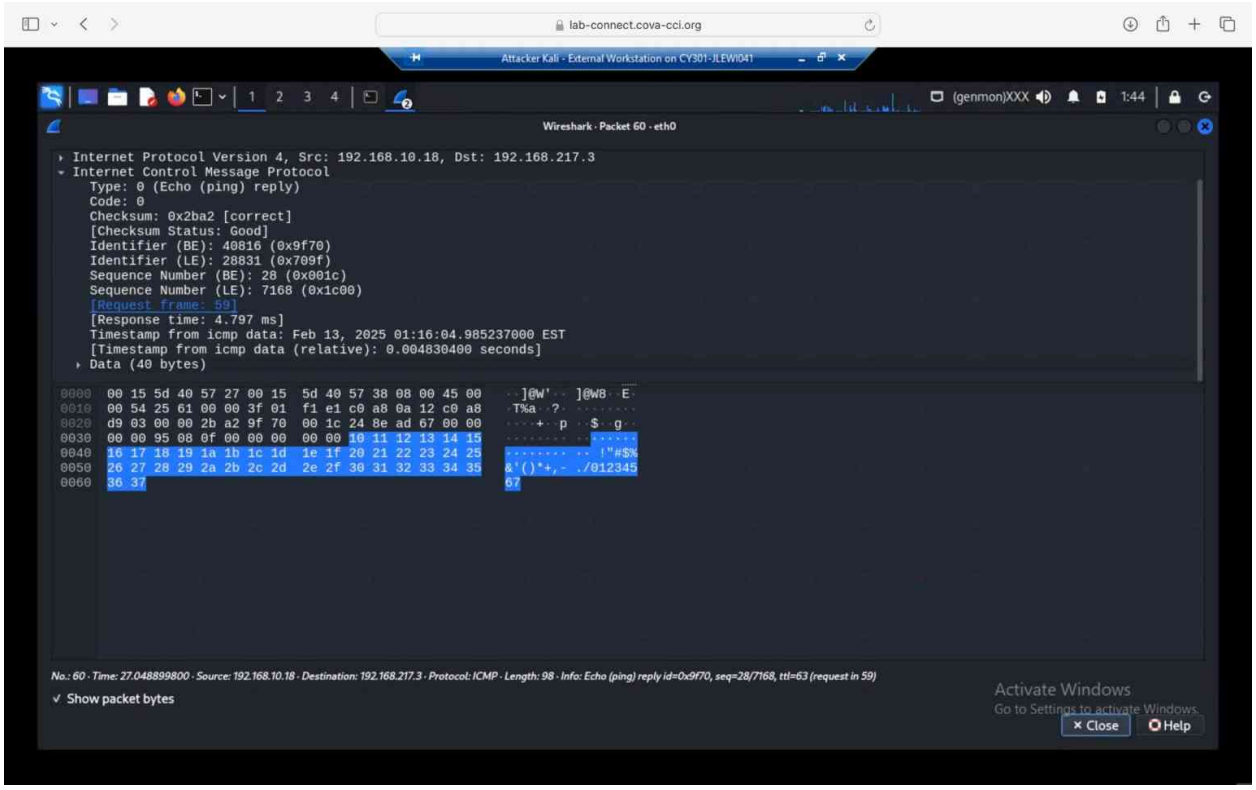
Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).

When applying the protocol ICMP filter in Wireshark I have a total of 80 that are displayed out of the 192 packets.



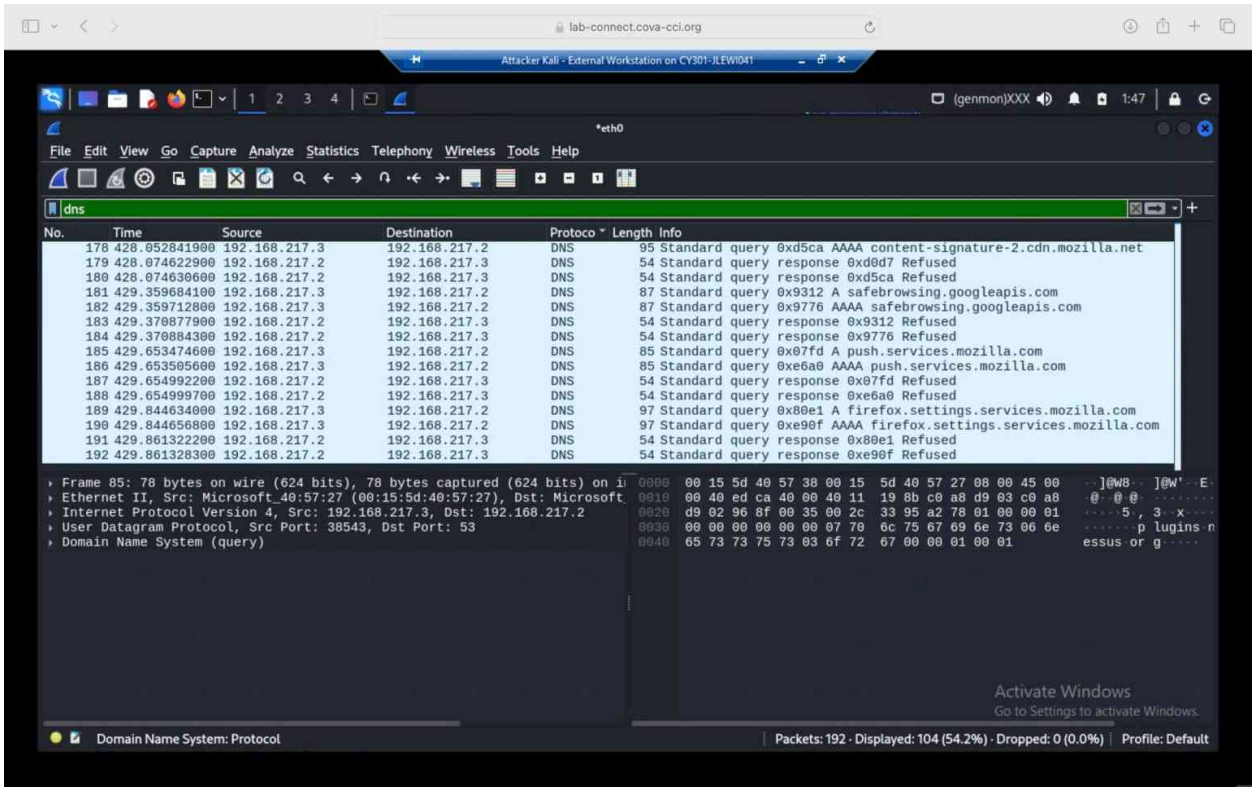
Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

When analyzing this packet, the source IP address is 192.168.10.18 and destination IP address is 192.168.217.3. Following that, the sequence number is 28 and the data size for 40 bytes. Finally, the response time for this packet is 4.797 ms.



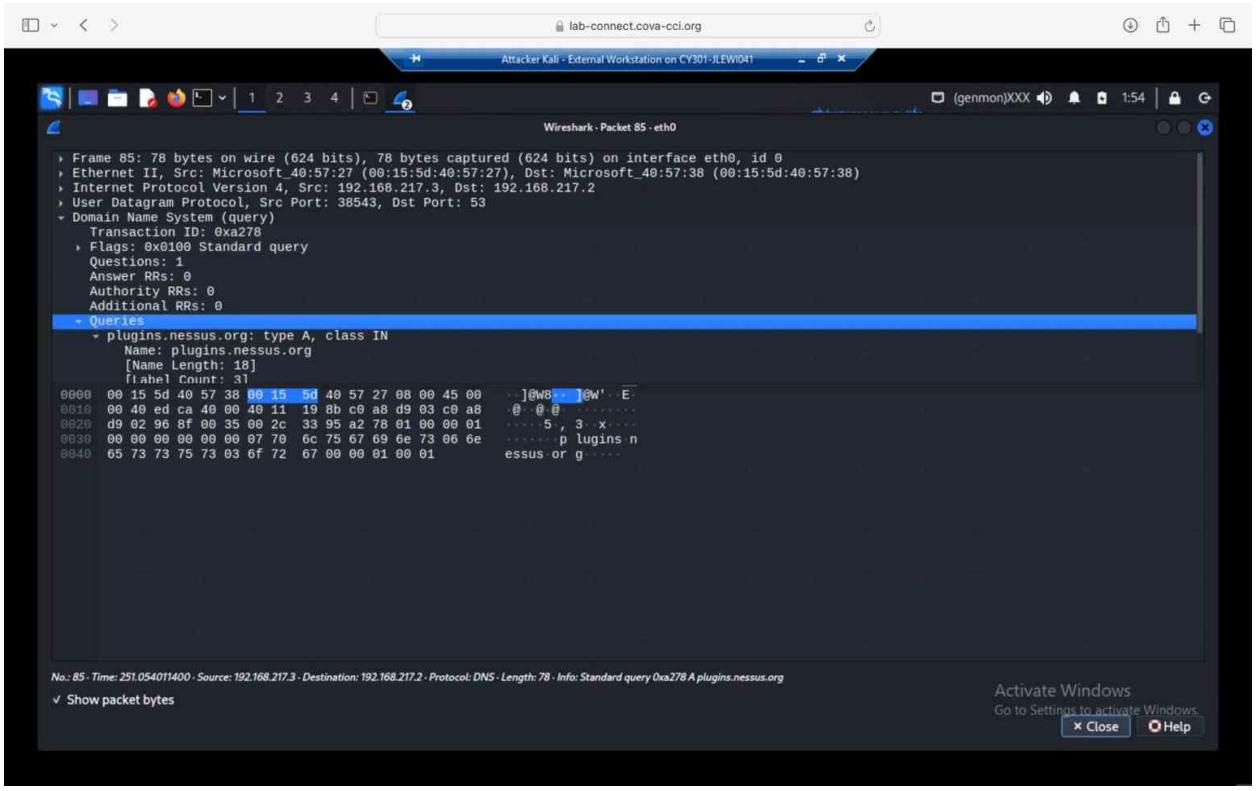
Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

The amount of packets displayed when applying DNS as a display filter is 104 packets.



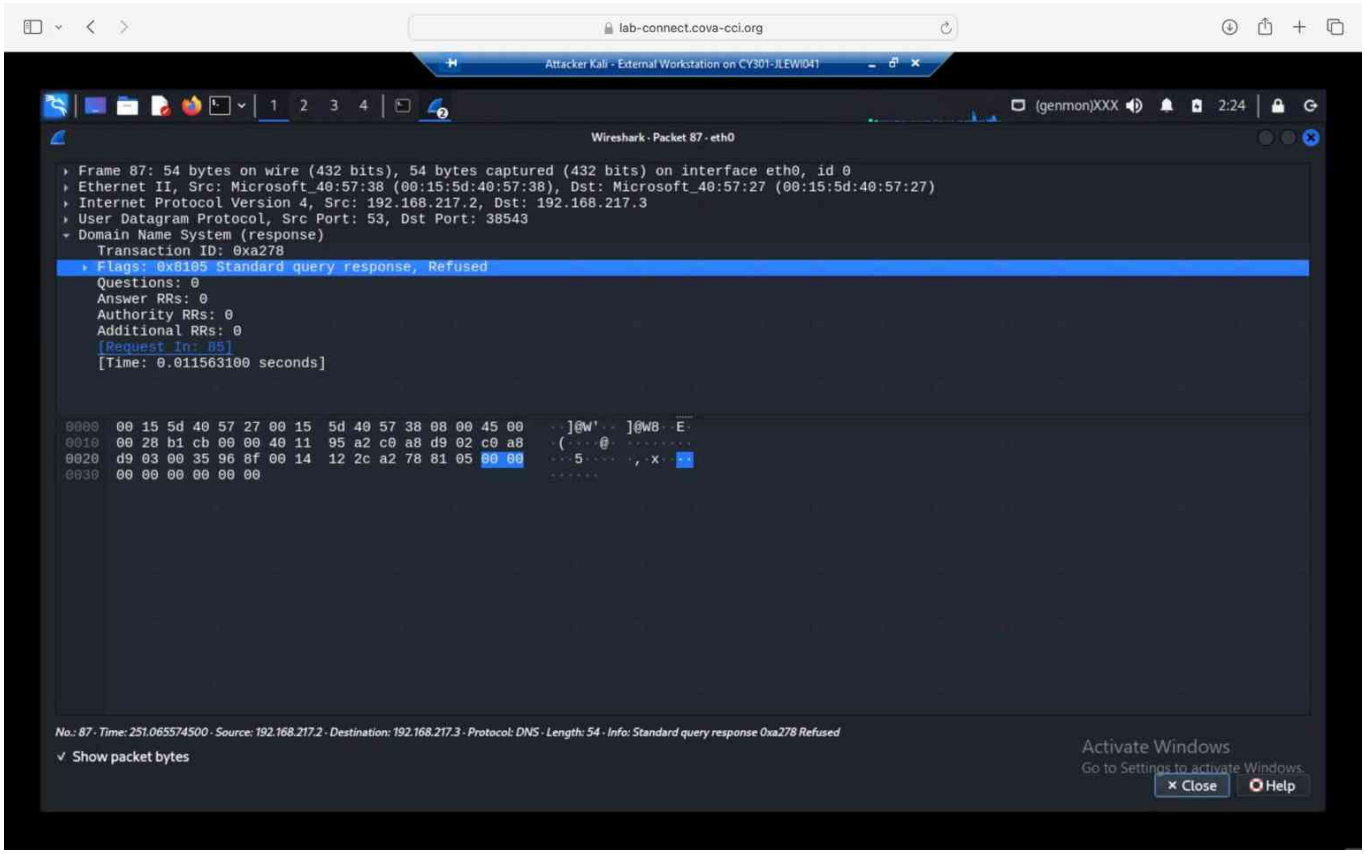
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format:IP:port.

Domain Name: plugins.nessus.org
Source IP & Port: 192.168.217.3 : 38543
Destination IP & Port: 192.162.217.2 : 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?

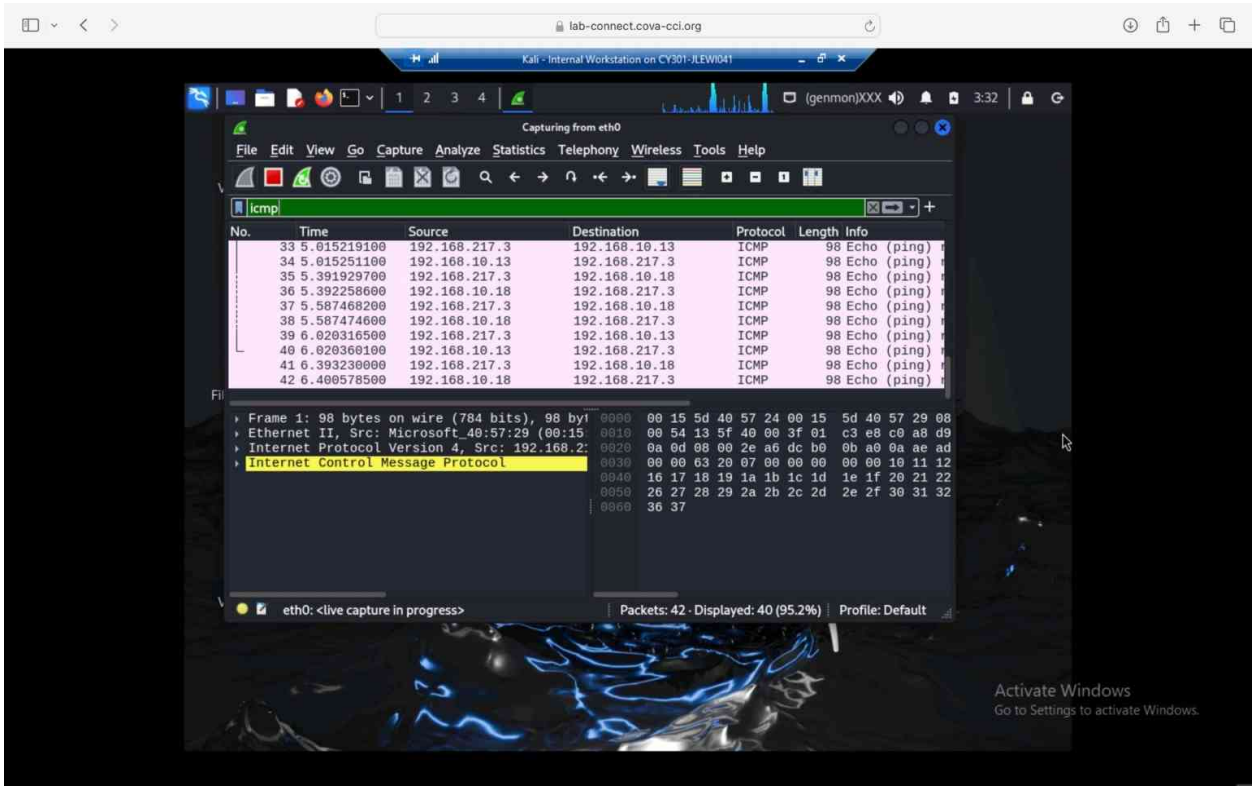
Source IP & Port: 192.168.217.2 : 53
Destination IP & Port: 192.168.21.3 : 38543
Message replied from the DNS server: Refused



Task B:

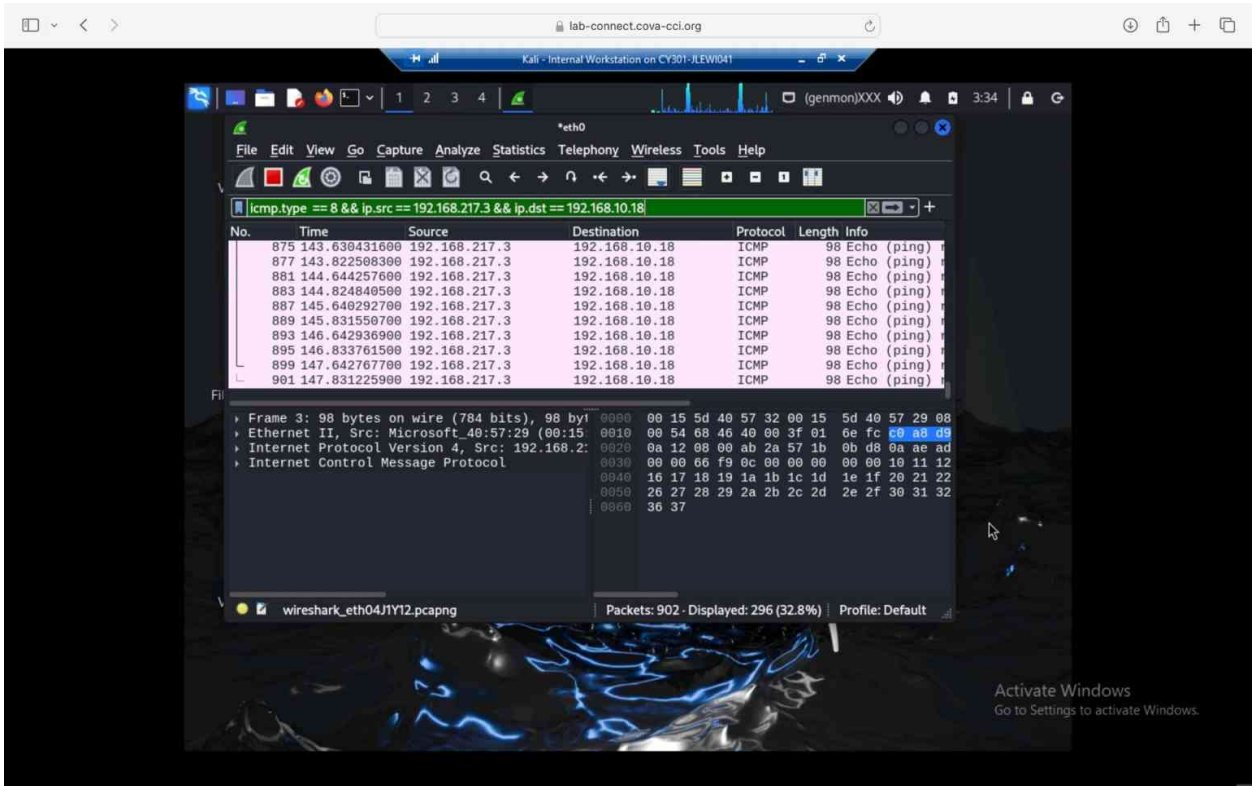
Q1: Apply proper display or capture filter in Wireshark on Internal Kali VM to show active ICMP traffic.

What I did here is the protocol ICMP in the Wireshark filter to show the ICM.



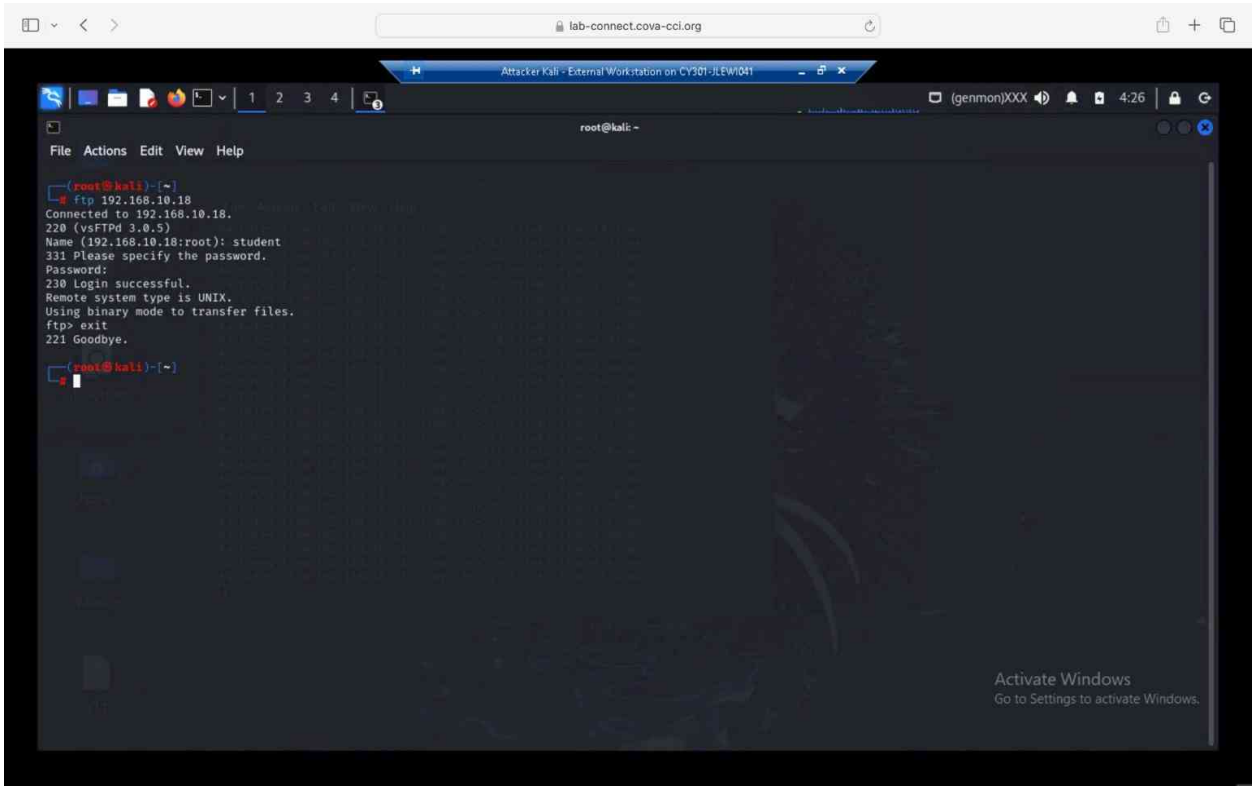
Q2: Apply proper display or capture filter in Wireshark on the Internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM.

The protocol I used to filter in Wireshark is ICMP.type==&& ip.src==192.168.217.3&& ip.dst ==192.168.10.18. This protocol uses the IP address from the external Kali VM and the Ubuntu 64-bit VM to achieve ICMP request that originated from the external Kali VM that goes to the Ubuntu 64-bit VM. While I also used ICMP.type to only find ICMP Echo requests.



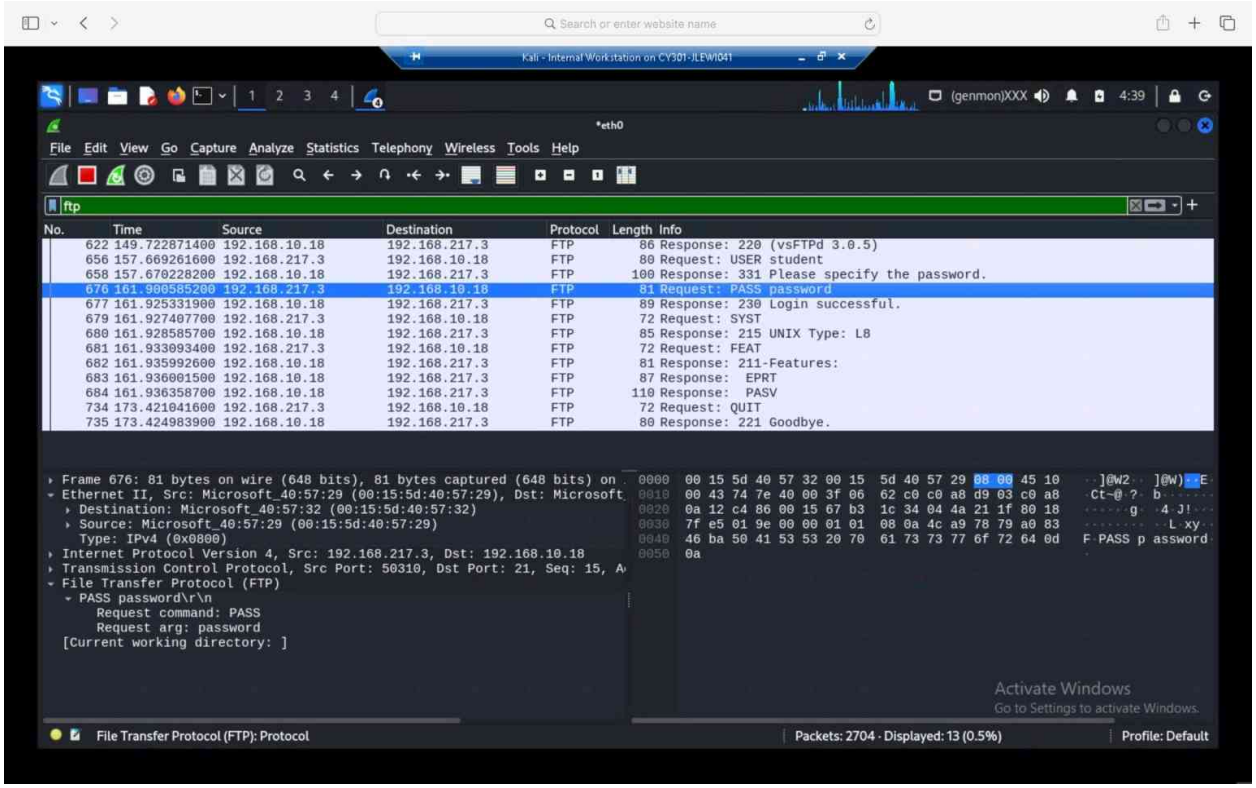
A. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: ftp [ip_addr of ubuntu VM]. The username for the FTP server is student, and the password is password. You can follow the steps below to access the FTP server.

To execute this task I simply followed the instructions above. As I accessed the External Kali and typed FTP followed by the IP address to Ubuntu. I gained the IP address from Ubuntu from the previous steps. After that I typed in the username and password for Ubuntu when prompted. Which was overall successful.



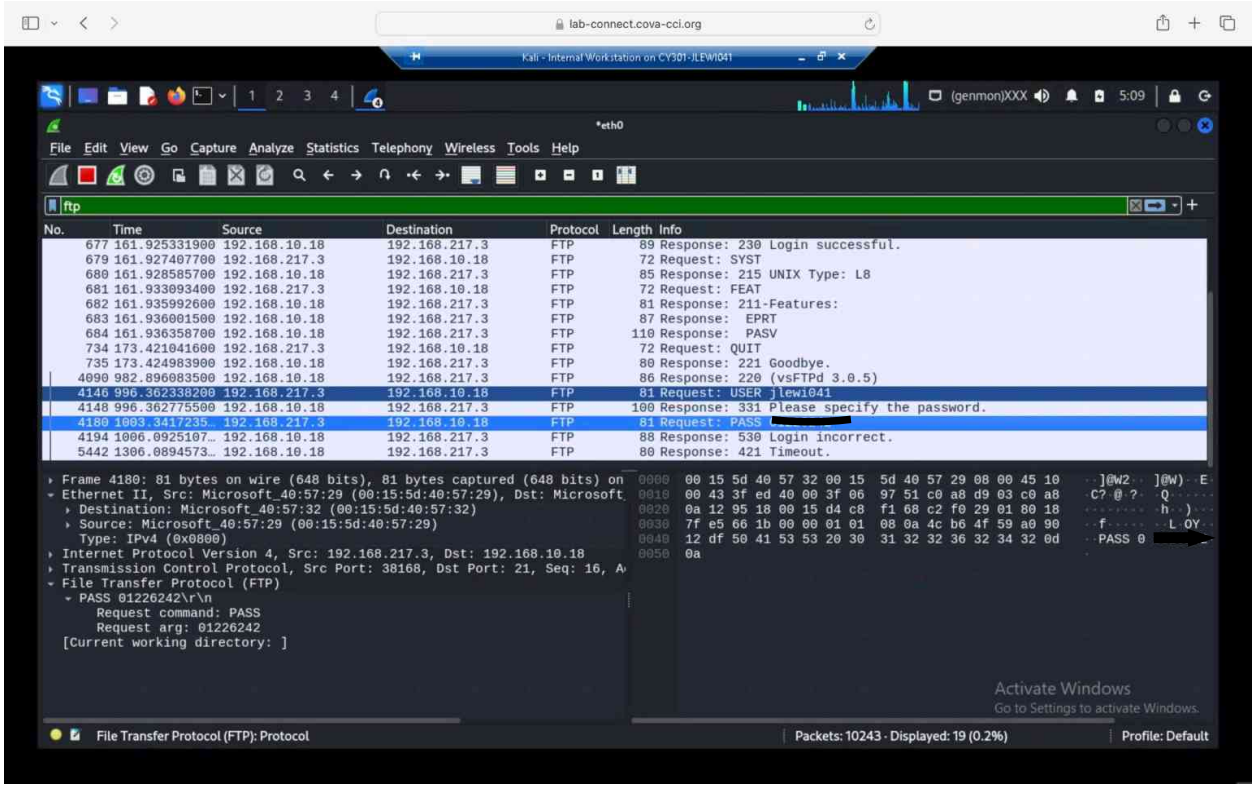
B. Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to take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

To sniff out the password I used in the External Kali for the FTP to Ubuntu I used the knowledge I gained from the previous task using wireshark. As I know now when accessing wireshark I have the ability to analyze all of the packets and data being transmitted in the system. Having said that, I thought to myself I could possibly go to wireshark and try typing in the ftp in the wireshark filter and see if it works. Doing that it showed all of the FTP packets. Following that, I saw two packets that had USER username and PASS password in their info column in wireshark. So I clicked on the packet that said password and then clicked on the tab that said PASS password\r\n. Which in return showed me the password I typed in when accessing the FTP on the External Kali.



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.

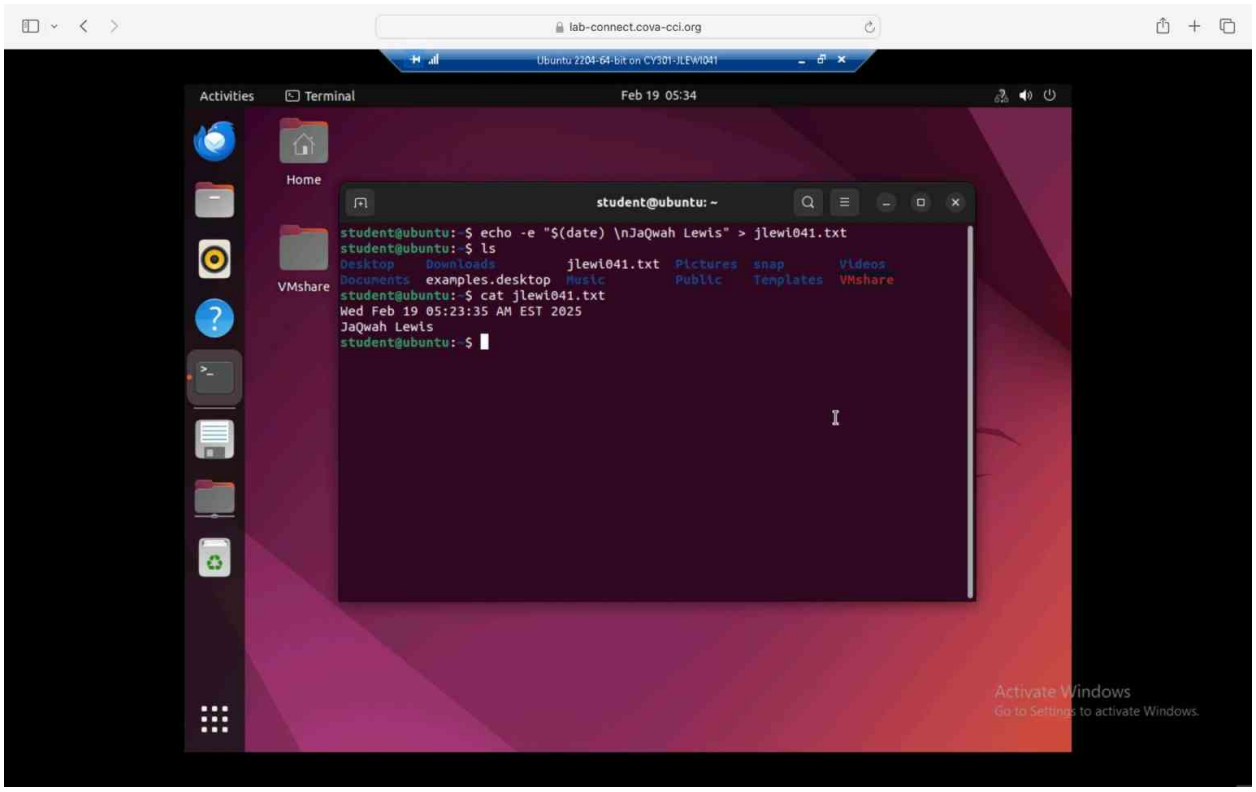
To complete this task I did the same commands as the previous task. As I went on to the External Kali and tried to FTP the Ubuntu server. Instead of using the correct login to Ubuntu I used my ODU credentials. As when for the username I used my MIDAS ID and for the password I used my UIN. Following that, I went to the Internal Kali and on to wireshark and used the FTP in the filter again and searched for the packet that was named USER and PASS. While also primarily looking for the one with my ODU credentials.



Task C Extra Credit:

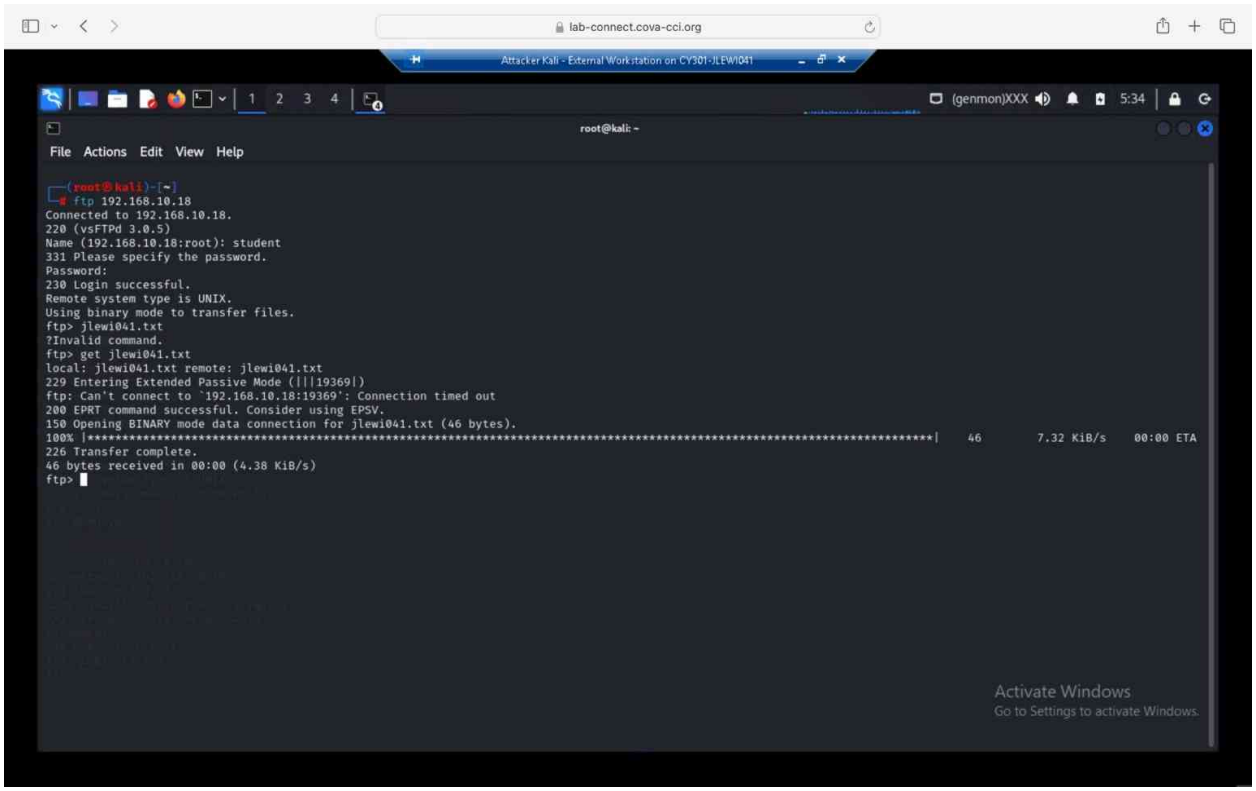
Login to Ubuntu VM, and create a file in your home directory named “YOUR_MIDAS.txt”. Put the current timestamp and your name in the file. You can use the following command in the example below to do the job. Once you have the file ready in Ubuntu, switch back to External Kali. Get the file you just created remotely using the FTP protocol. Below is an example. As an attacker, you need to complete the following tasks in Internal Kali:

For this task I followed the instructions in the photo which allowed me to make a text file. Following that, I displayed all of the files in the directory. Lastly, I used the command to display the text file I created. Which also showed the time and date.



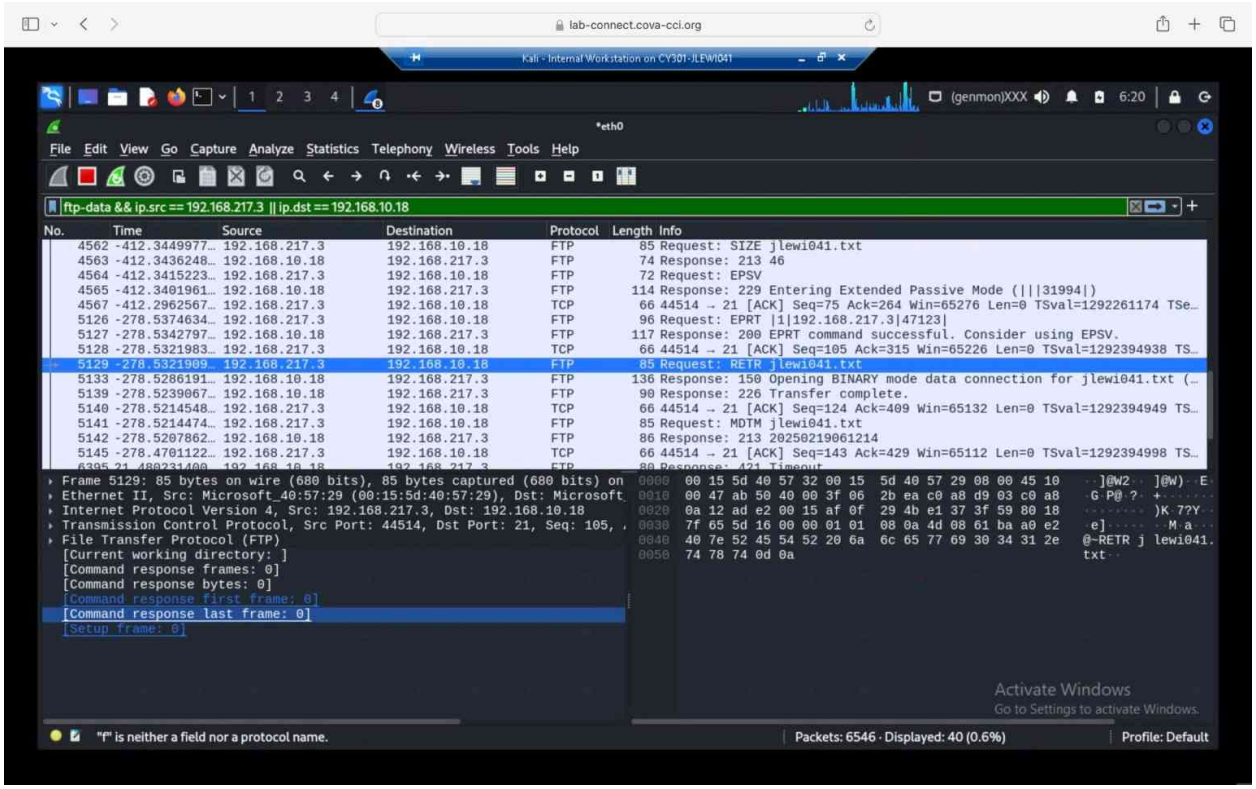
Once you have the file ready in Ubuntu, switch back to External Kali. Get the file you just created remotely using the FTP protocol. Below is an example. As an attacker, you need to complete the following tasks in Internal Kali:

I followed the step shown in the example and was able to execute it. As I did have to redo it a few times because of mistakes I made.



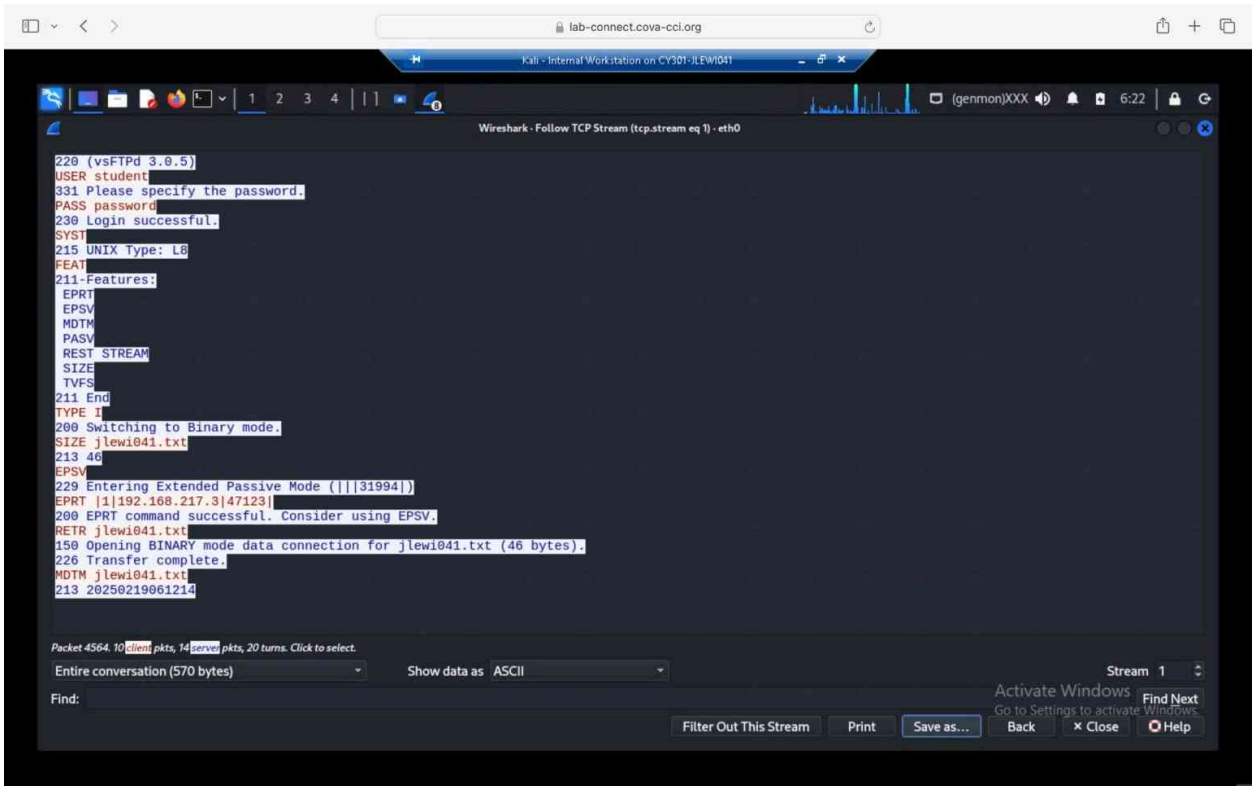
1. Apply a proper display filter to display the FTP-DATA packets between External Kali and Ubuntu VM.
2. Follow the TCP steam of the FTP-DATA packet and view the content of the file just transferred.

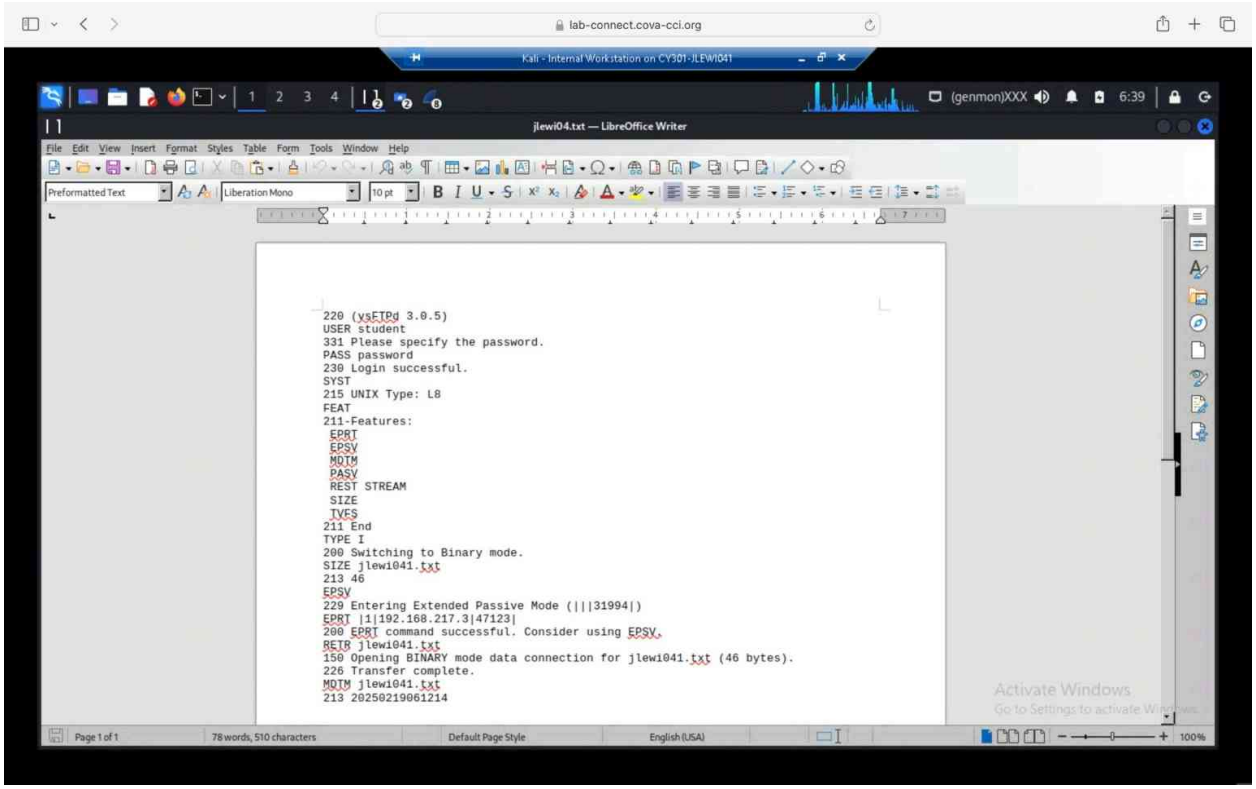
To filter through wireshark to find the FTP-DATA packets between the External Kali and Ubuntu VM I used the same method from the previous task as when looking for the source and destination when using the ICMP. Doing this I was able to find the packets between the External Kali and Ubuntu VM. When following the TCP steam I right clicked on the packet and hit follow and TCP. Following that I was given the answer to #3.



3. Export (Save) the transferred file as a text file in Internal Kali and view the content. Below is an example.

After completing the previous step, I expand the window and export the transferred file as a text file. Then saving the packet to the VM itself and an example of the text file below


lab-connect.cova-cci.org
Kali - Internal Workstation on CY301-JLEWI041
(genmon)XXX
6:22
Wireshark · Follow TCP Stream (tcp.stream eq 1) · eth0
220 (vsFTPd 3.0.5)
USER student
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End
TYPE I
200 Switching to Binary mode.
SIZE jlewi041.txt
213 46
EPSV
229 Entering Extended Passive Mode (|||31994|)
EPRT |1|192.168.217.3|47123|
200 EPRT command successful. Consider using EPSV.
RETR jlewi041.txt
150 Opening BINARY mode data connection for jlewi041.txt (46 bytes).
226 Transfer complete.
MDTM jlewi041.txt
213 20250219061214
Packet 4564. 10 client pkts, 14 server pkts, 20 turns. Click to select.
Entire conversation (570 bytes)
Show data as ASCII
Stream 1
Find:
Find Next
Activate Windows
Go to Settings to activate Windows.
Filter Out This Stream
Print
Save as...
Back
Close
Help


lab-connect.cova-cci.org
Kali - Internal Workstation on CY301-JLEWI041
(genmon)XXX
6:39
jlewi04.txt — LibreOffice Writer
File Edit View Insert Format Styles Table Form Tools Window Help
Preformatted Text
Liberation Mono
10 pt
220 (vsFTPd 3.0.5)
USER student
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
EPRT
EPSV
MDTM
PASV
REST STREAM
SIZE
TVFS
211 End
TYPE I
200 Switching to Binary mode.
SIZE jlewi041.txt
213 46
EPSV
229 Entering Extended Passive Mode (|||31994|)
EPRT |1|192.168.217.3|47123|
200 EPRT command successful. Consider using EPSV.
RETR jlewi041.txt
150 Opening BINARY mode data connection for jlewi041.txt (46 bytes).
226 Transfer complete.
MDTM jlewi041.txt
213 20250219061214
Activate Windows
Go to Settings to activate Windows.
Page 1 of 1
78 words, 510 characters
Default Page Style
English (USA)
100%