CYSE 301: Cybersecurity Technique and Operations

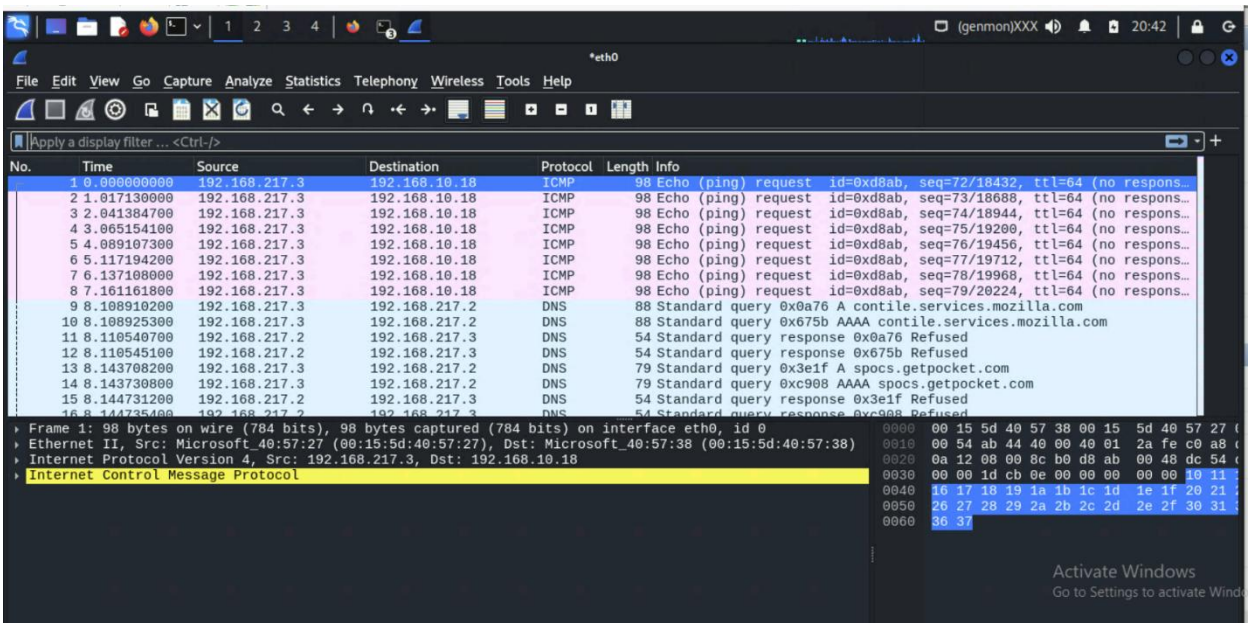
Assignment 2: Traffic Tracing and Sniffing

Owin Ifill

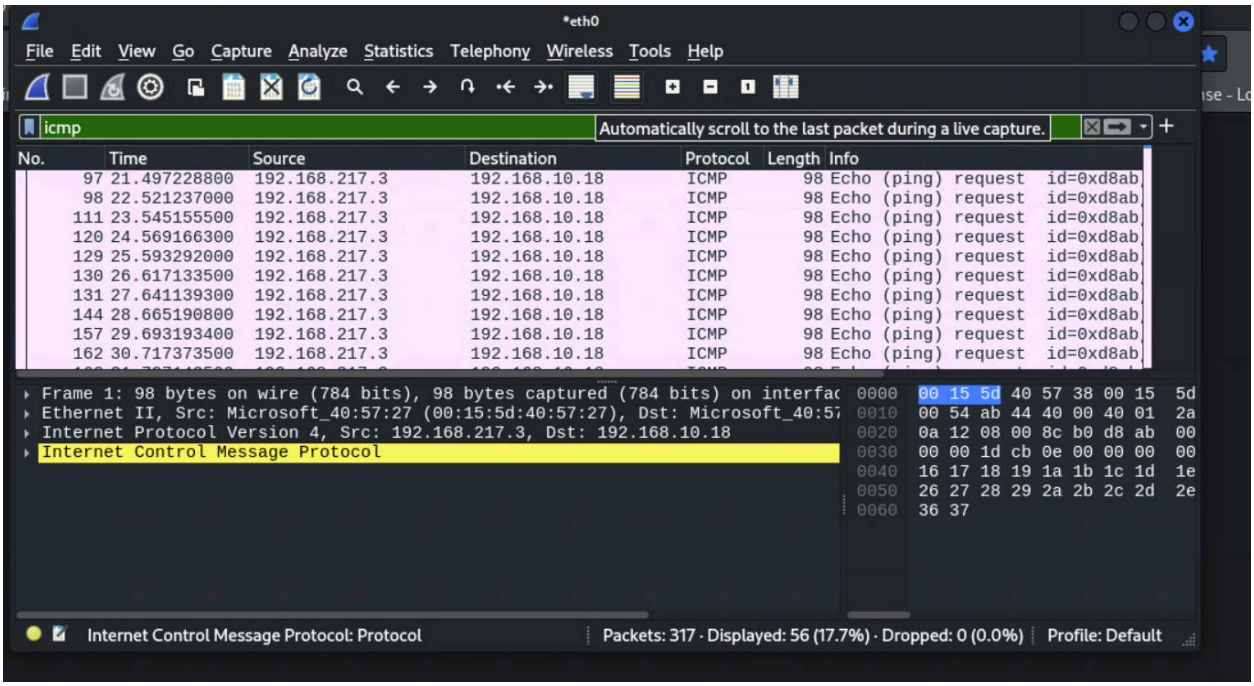
01230552

Task A:

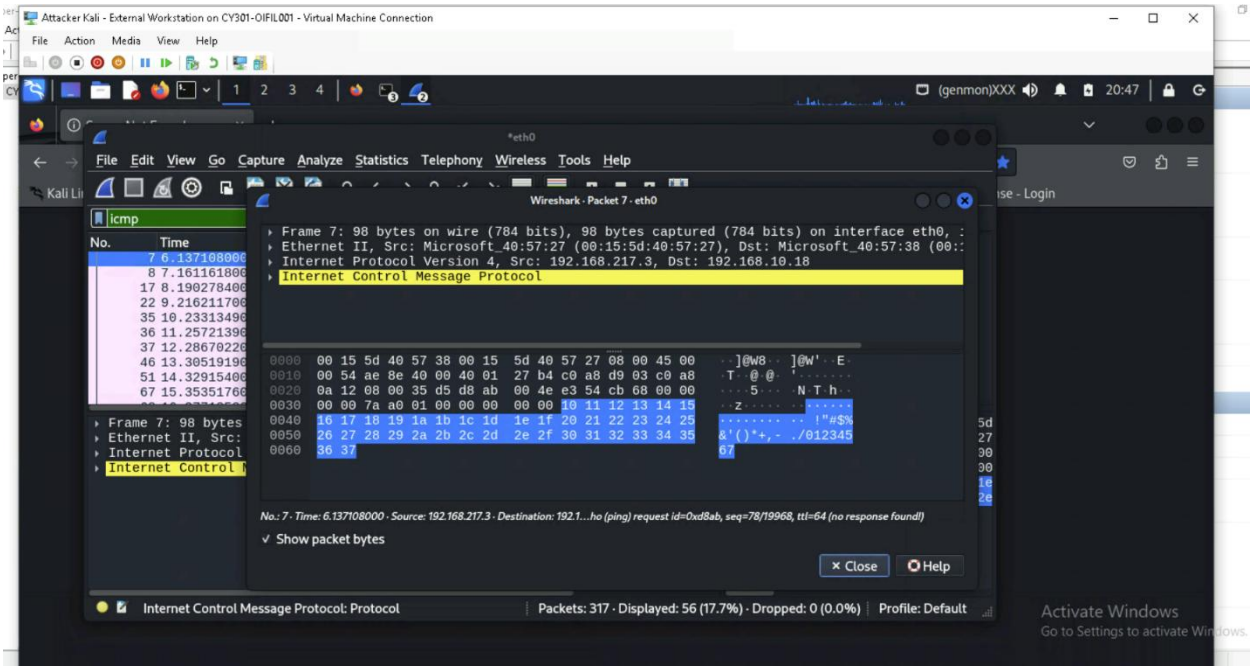
Q1. How many packets are captured in total? How many packets are displayed?
317 packets were captured.

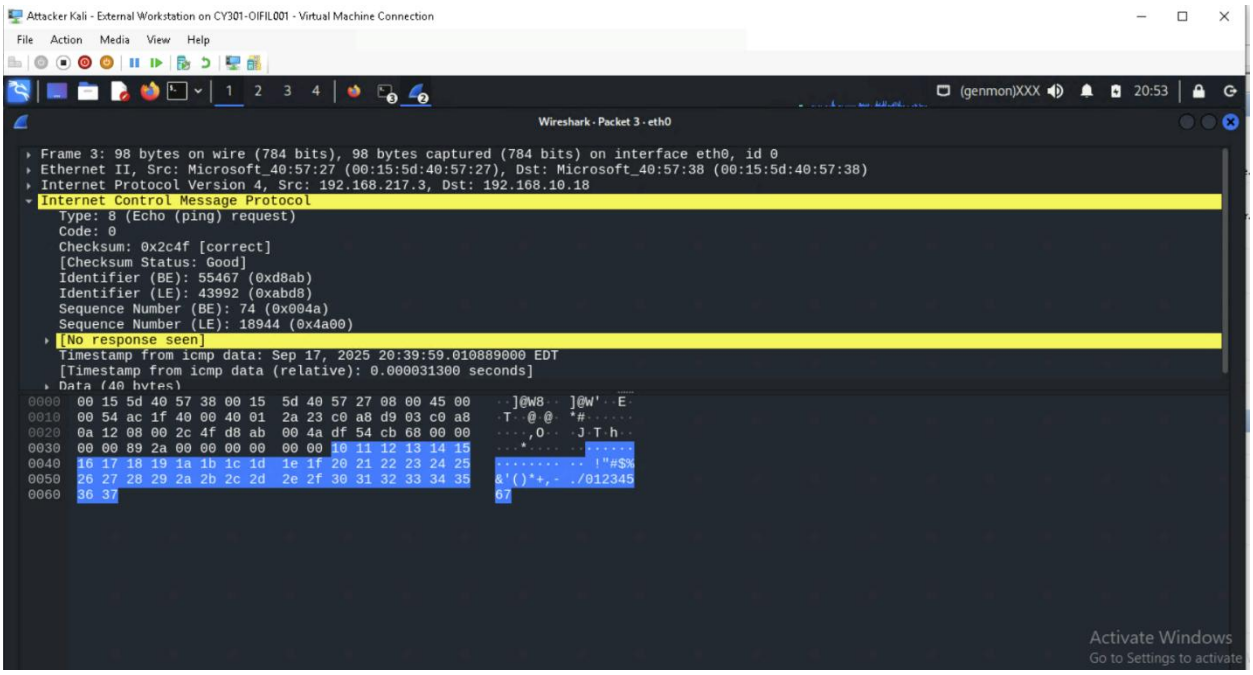


Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1). **56 packets were found.**



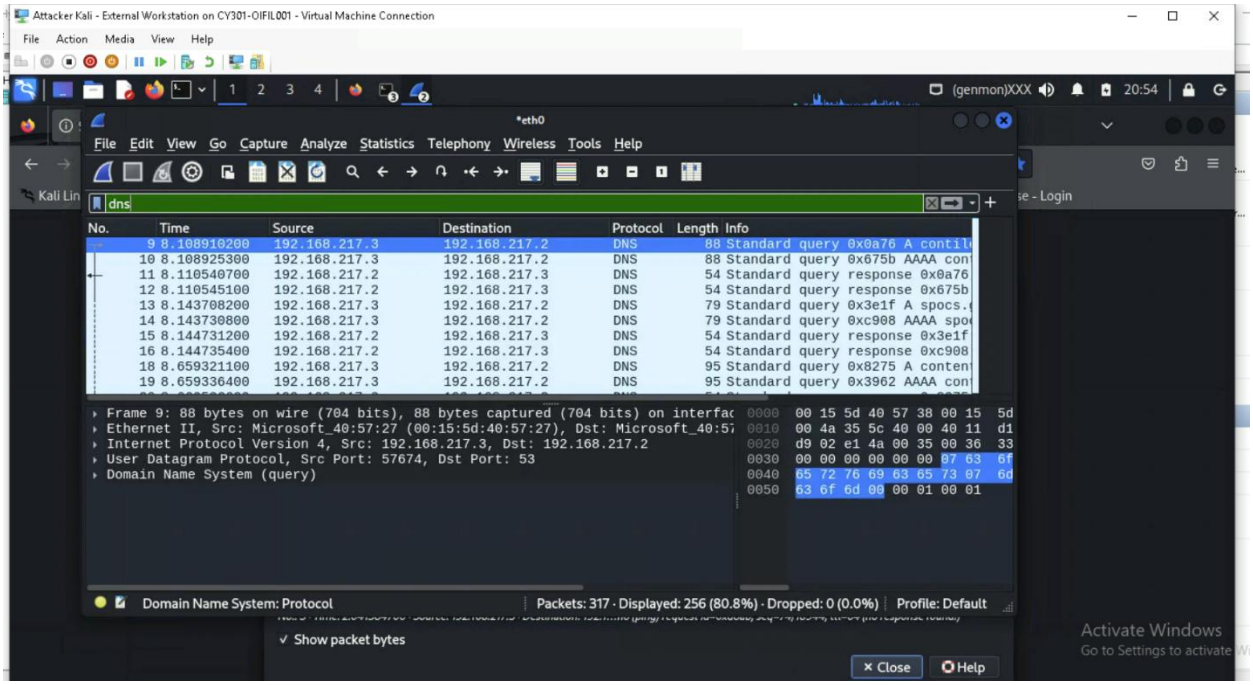
Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



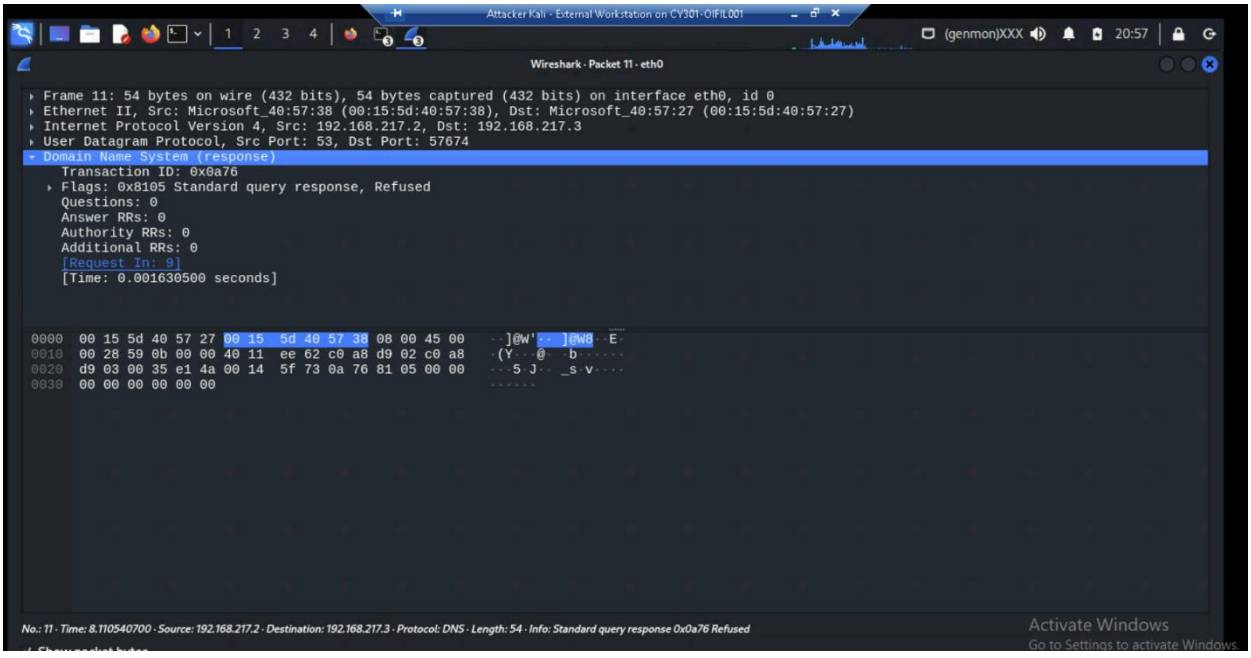


Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

256 packets were displayed.

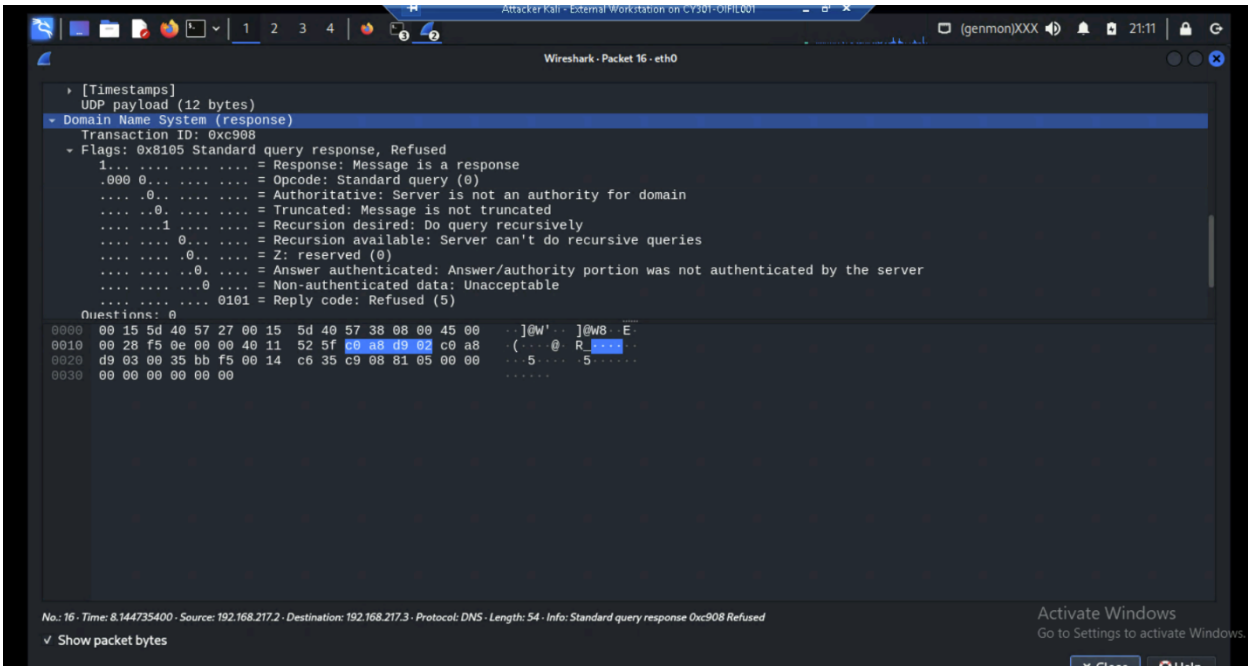


Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port. **The source is 192.168.217, the destination is 192.168.217.3**



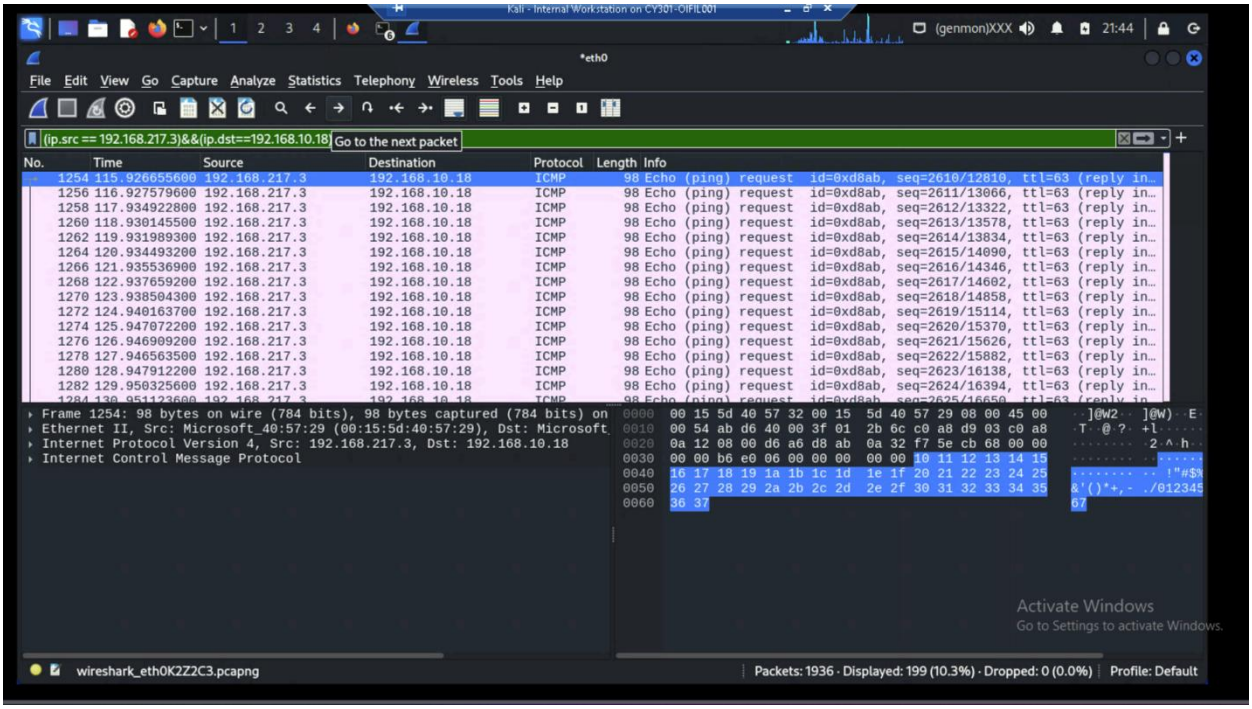
Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port

number? What is the message replied from the DNS server? External Attacker Kali Ubuntu 64 bit VM pFsense Firewall LAN: 192.168.10.2 WAN: 192.168.217.2

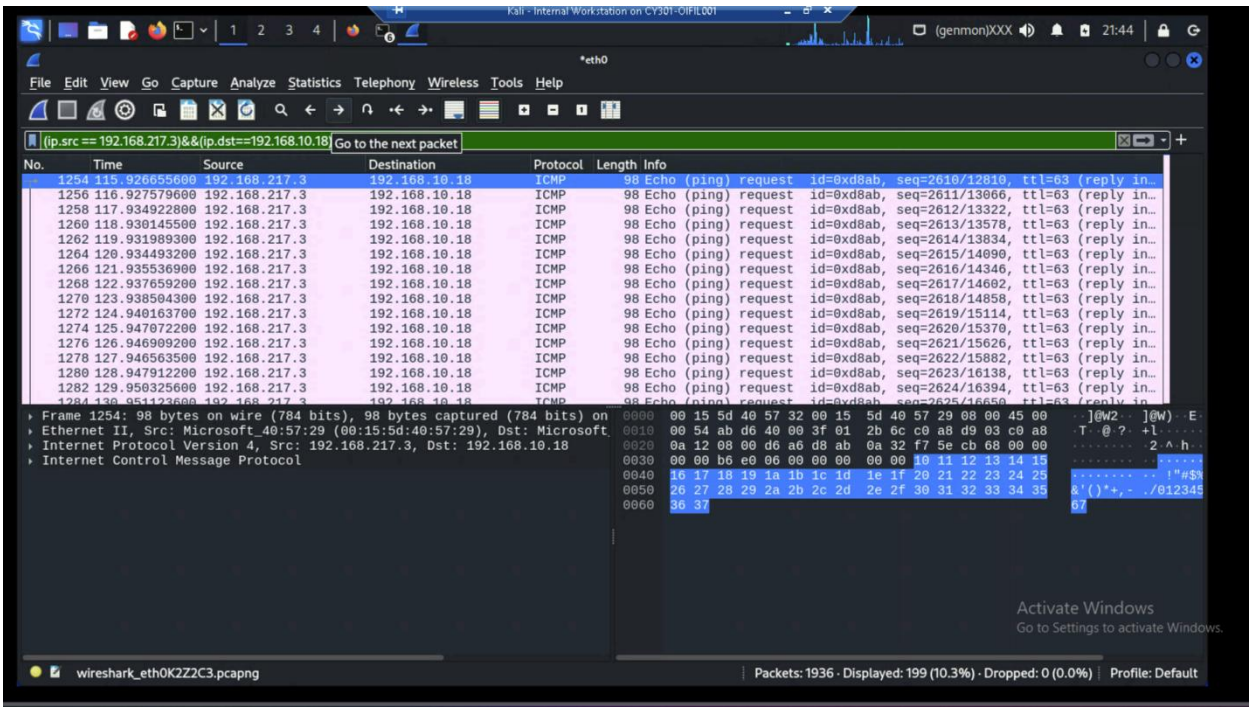


Task B:

1. Sniff ICMP traffic (10 + 10 = 20 points)
   Please turn on Attacker/External Kali, internal kali, pfsense, and Ubuntu
   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 in Wireshark on Internal Kali VM to show active ICMP traffic.



b. 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.

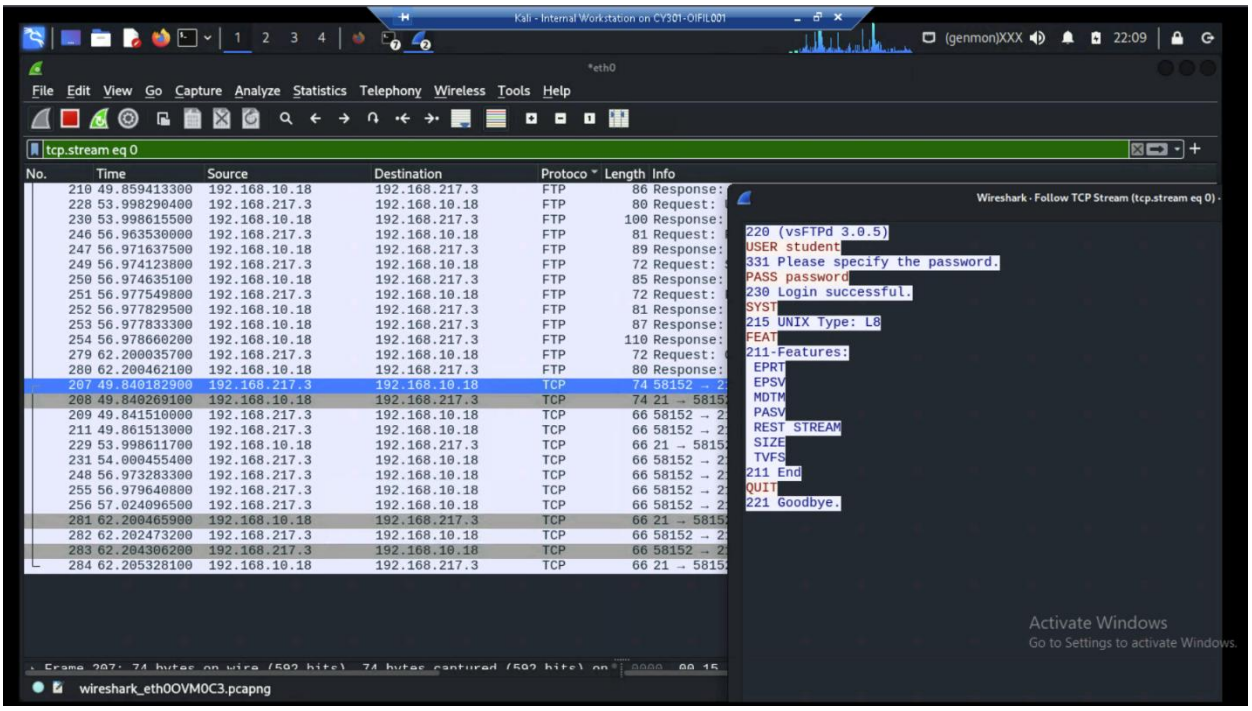


2. Sniff FTP traffic (10 + 15 + 15 = 40 pts points)

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.



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.