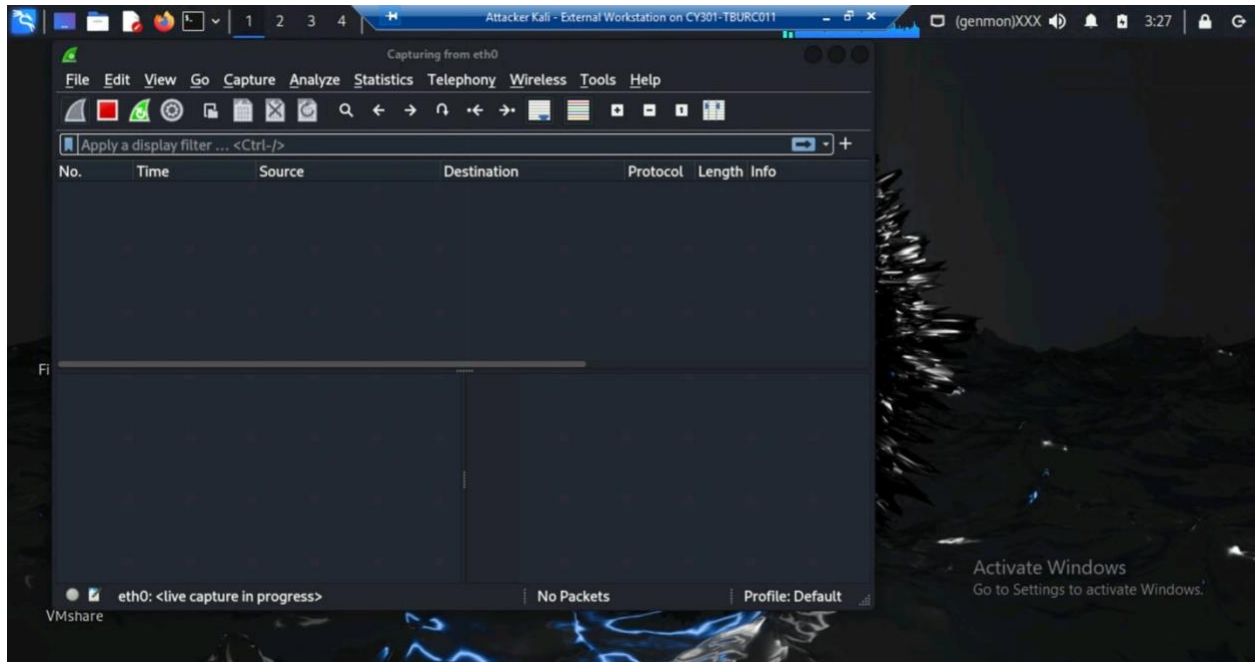
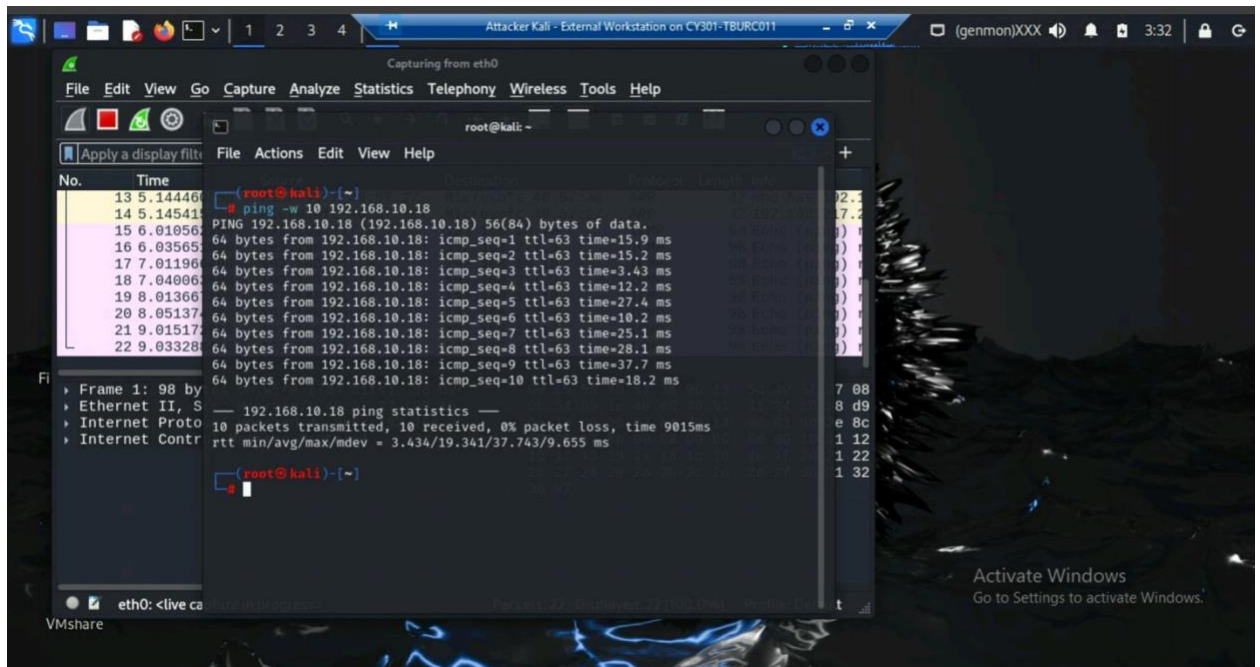


Task A

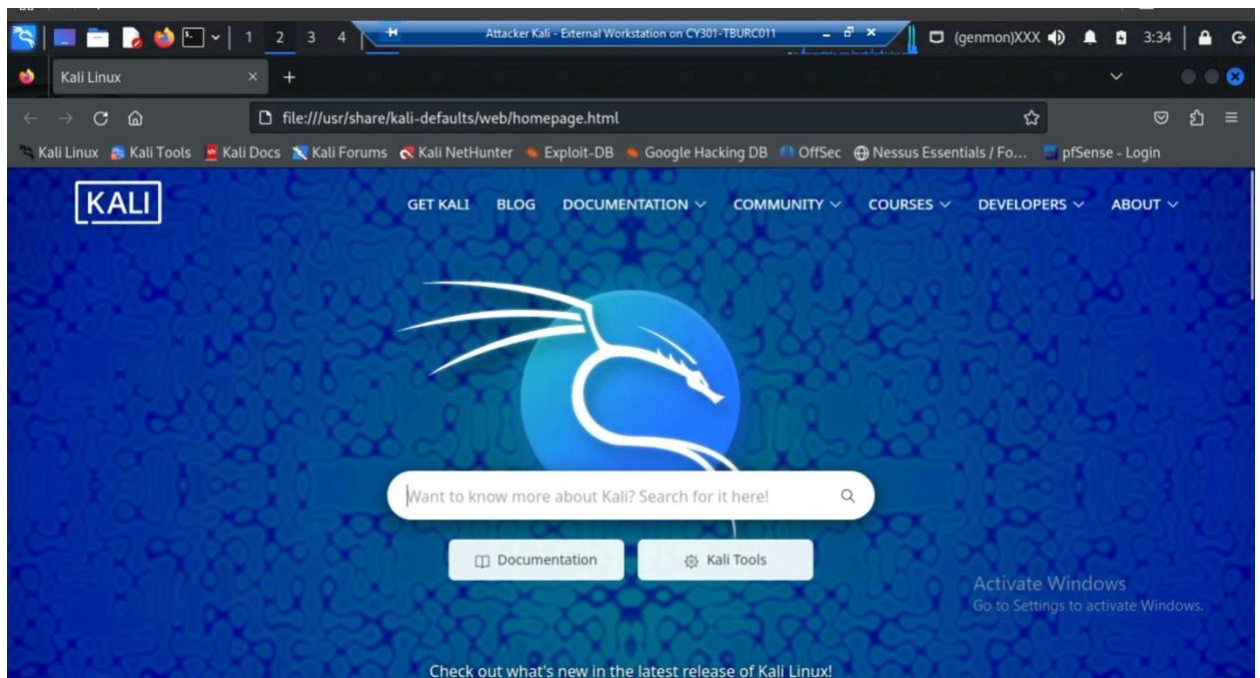
1. Open Wireshark on External / Attacker Kali and listen on interface “eth0”.



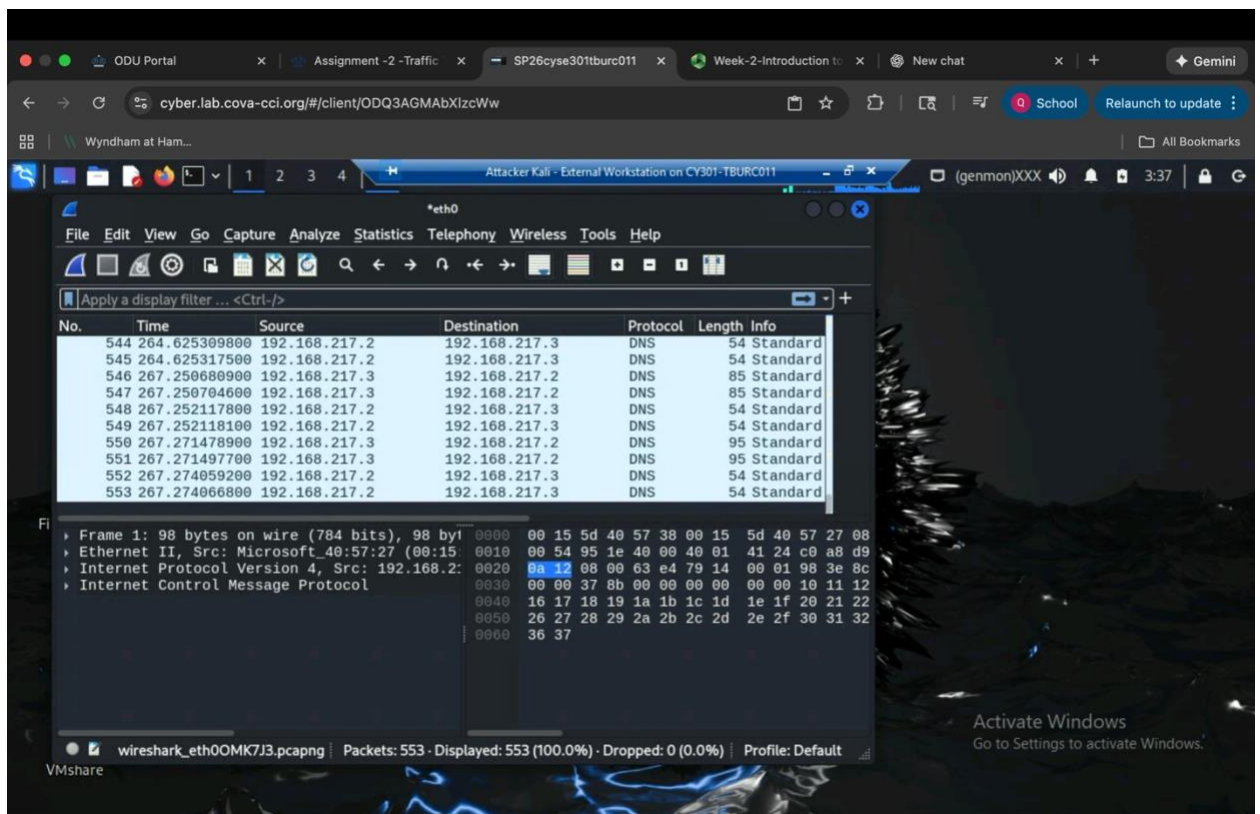
2. Open a new terminal in Attacker Kali, then ping the Ubuntu VM for 5 – 10 seconds.



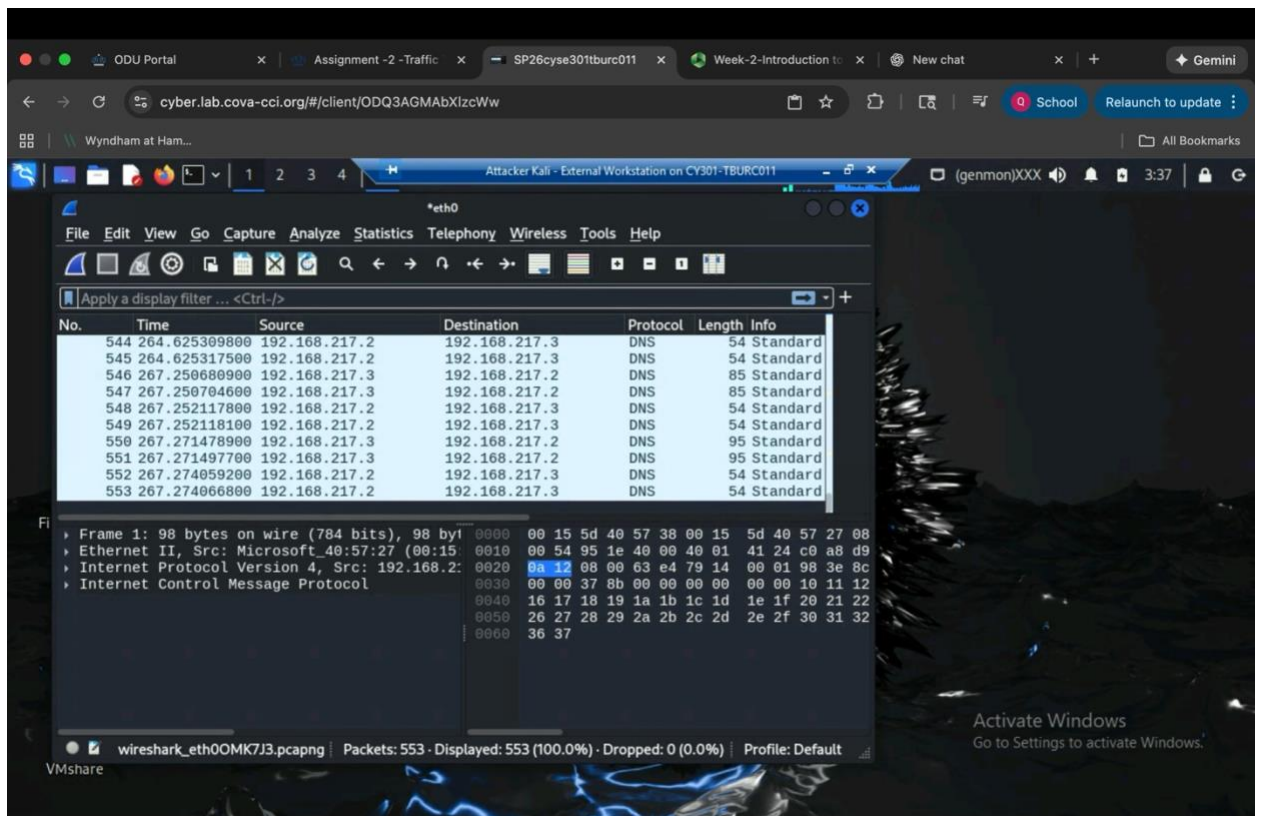
3. Open a new web browser tab in Attacker Kali (even if no webpage will be displayed)



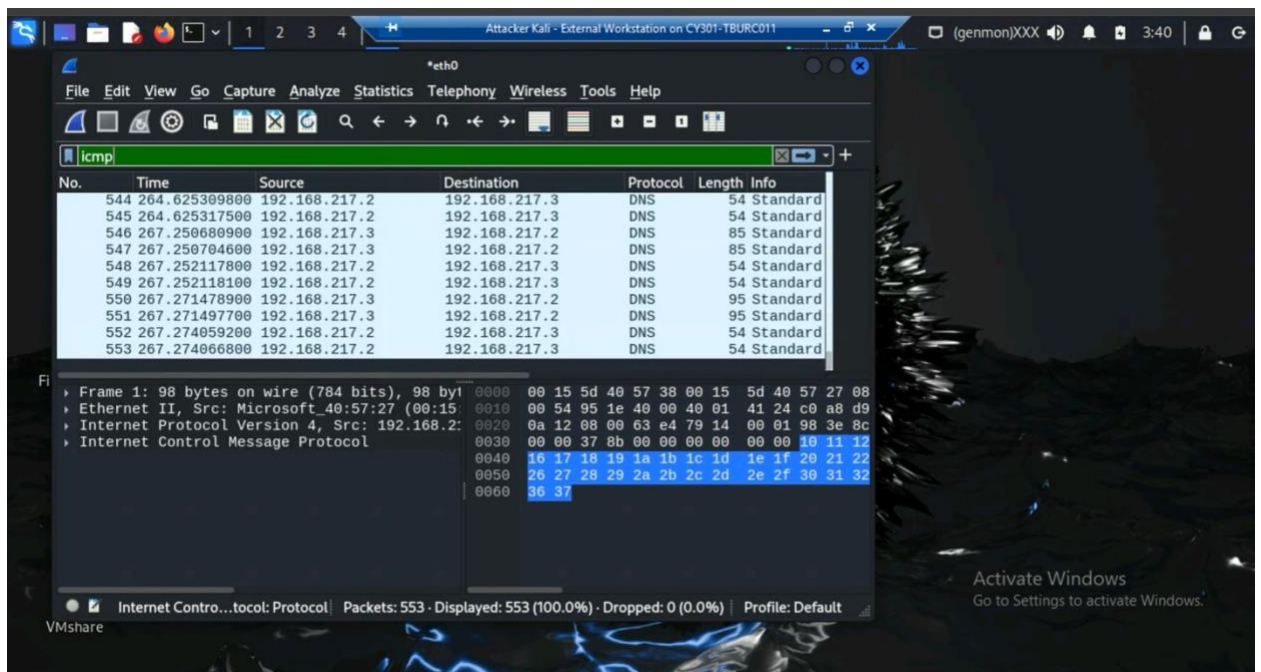
4. Stop capturing (by clicking the red button on the tool bar)



Q1. How many packets are captured in total? How many packets are displayed? 553 captured and 553 displayed.

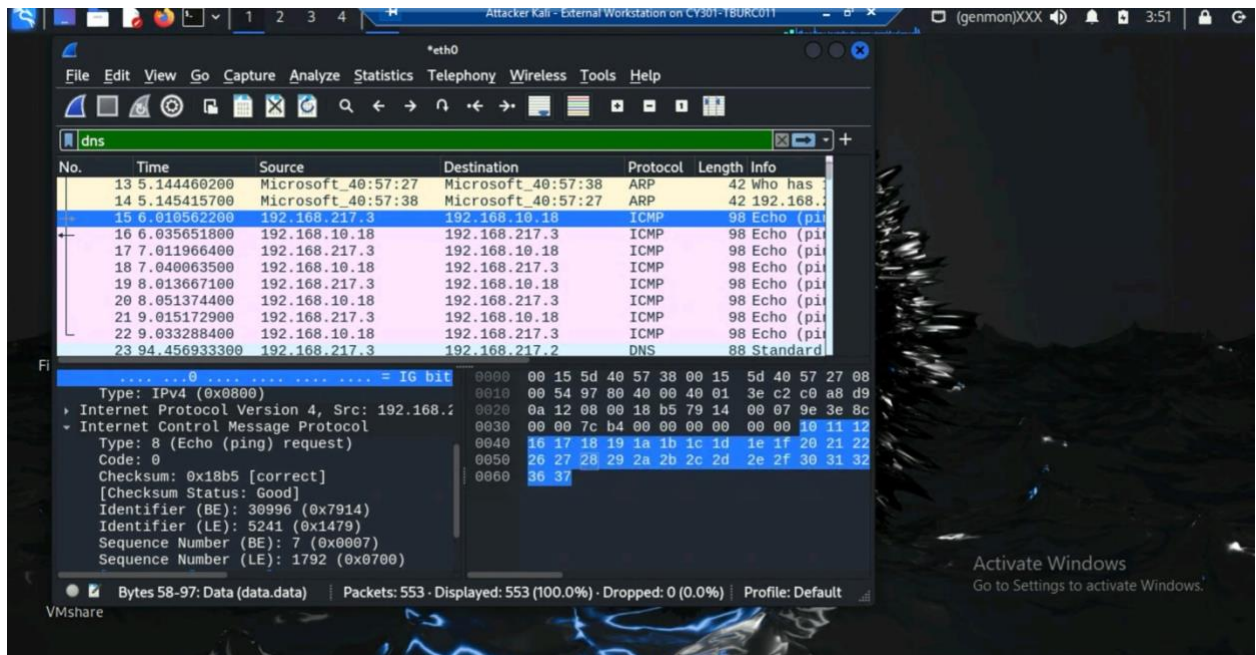


Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1). 533 captured and 553 displayed.

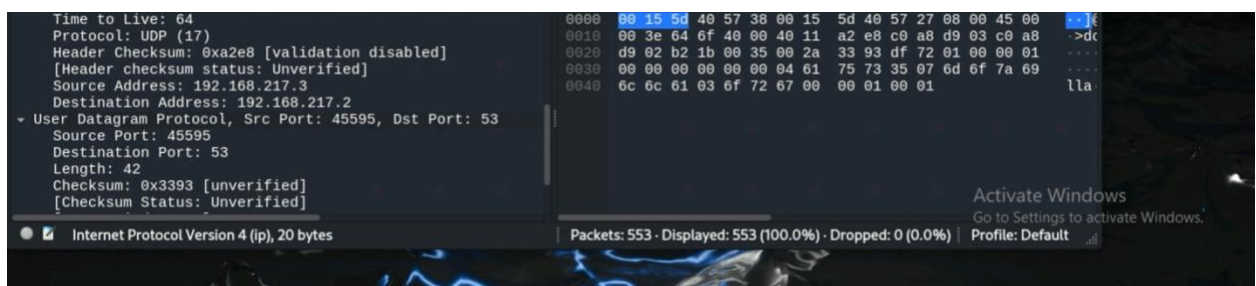


Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time? Ip is 192.168.217.3, destination ip is 192.168.10.18, sequence is 1/256, size is 40, and response time is 0.000019600

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed? 553 being displayed.



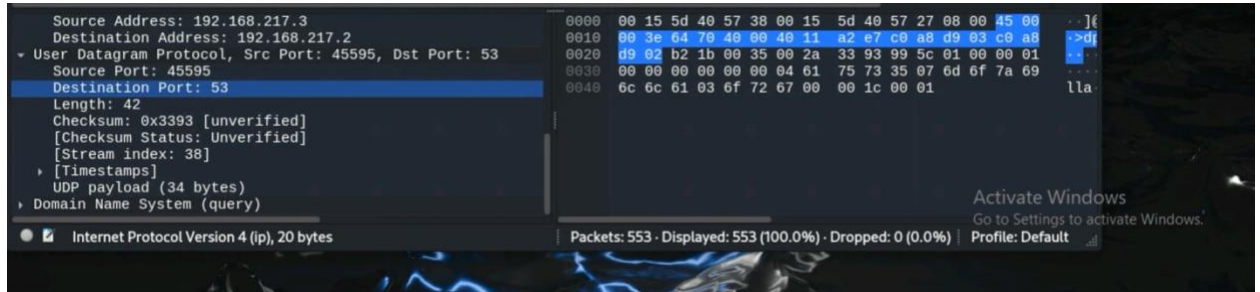
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Source ip is 192.168.217.3, port number is 45595, the destination ip is 192.168.217.2 port number is 53.



Q6. Find the corresponding DNS response to the query you selected at the previous step, and

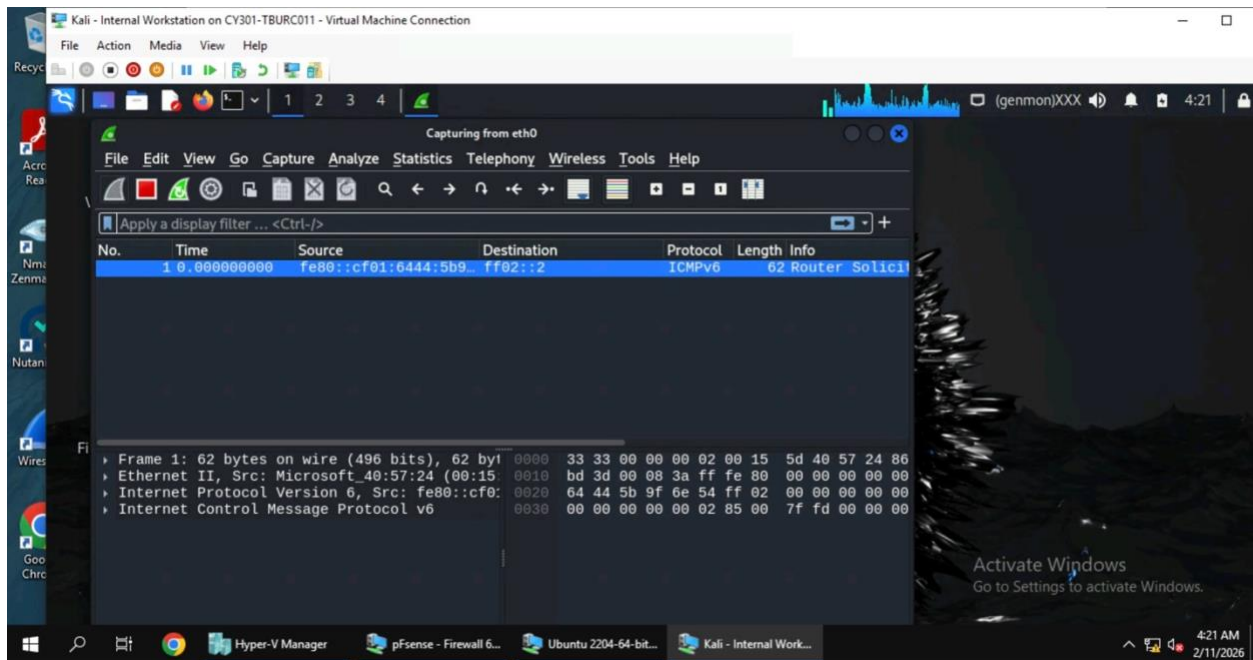
what is the source IP and port number, destination IP and port number? What is the message replied

from the DNS server? Source ip is 192.168.217.3, port number is 45595, destination ip is 192.168.217.3 port number is 53

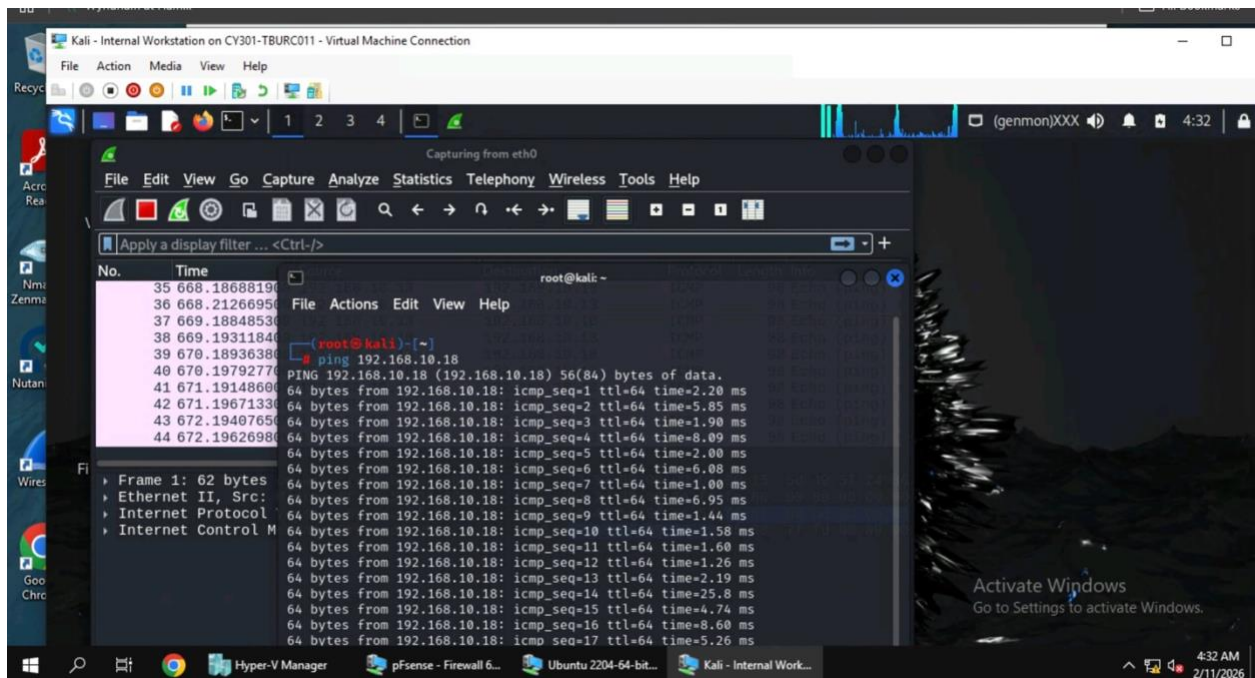
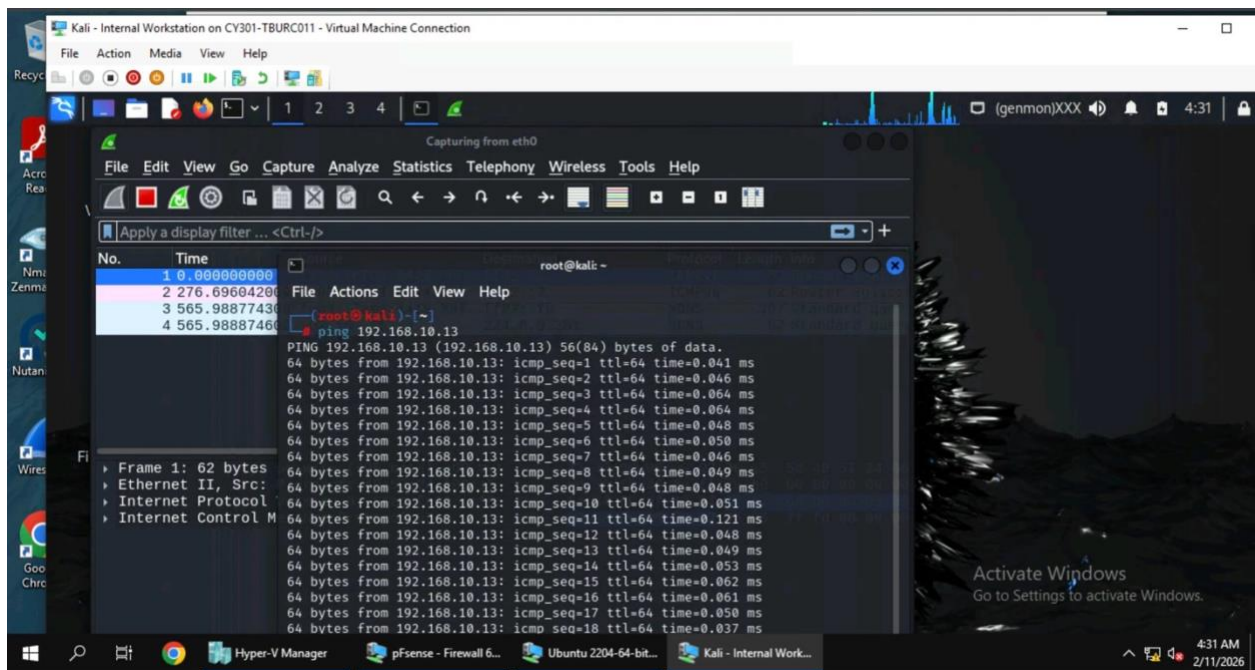


Task B1

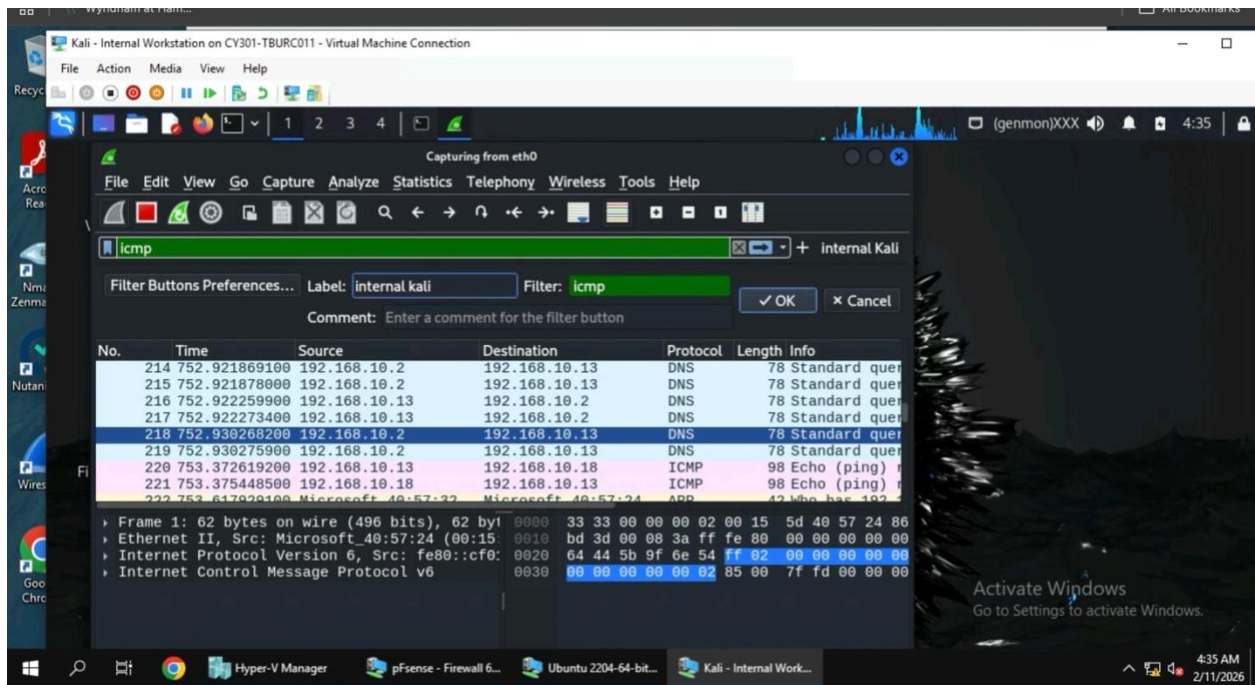
A. Launch and run Wireshark in Internal Kali



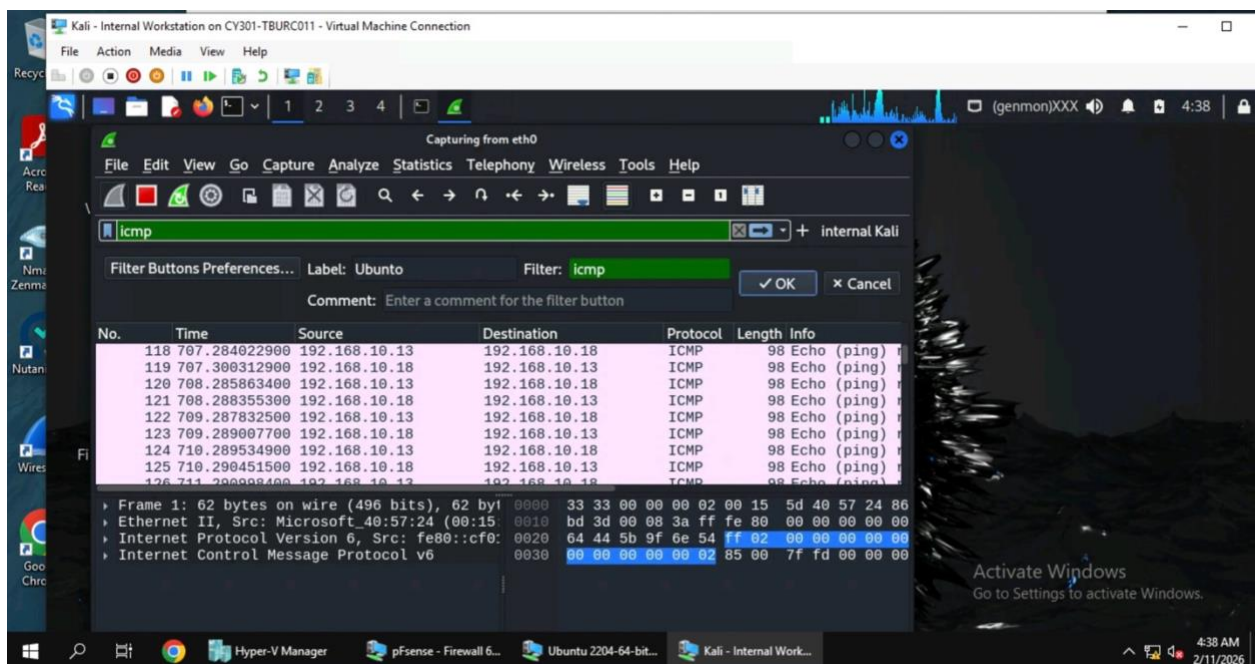
B. Open two terminals on External Kali VM. Use one to ping Ubuntu VM, and use the other to ping Internal Kali.



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

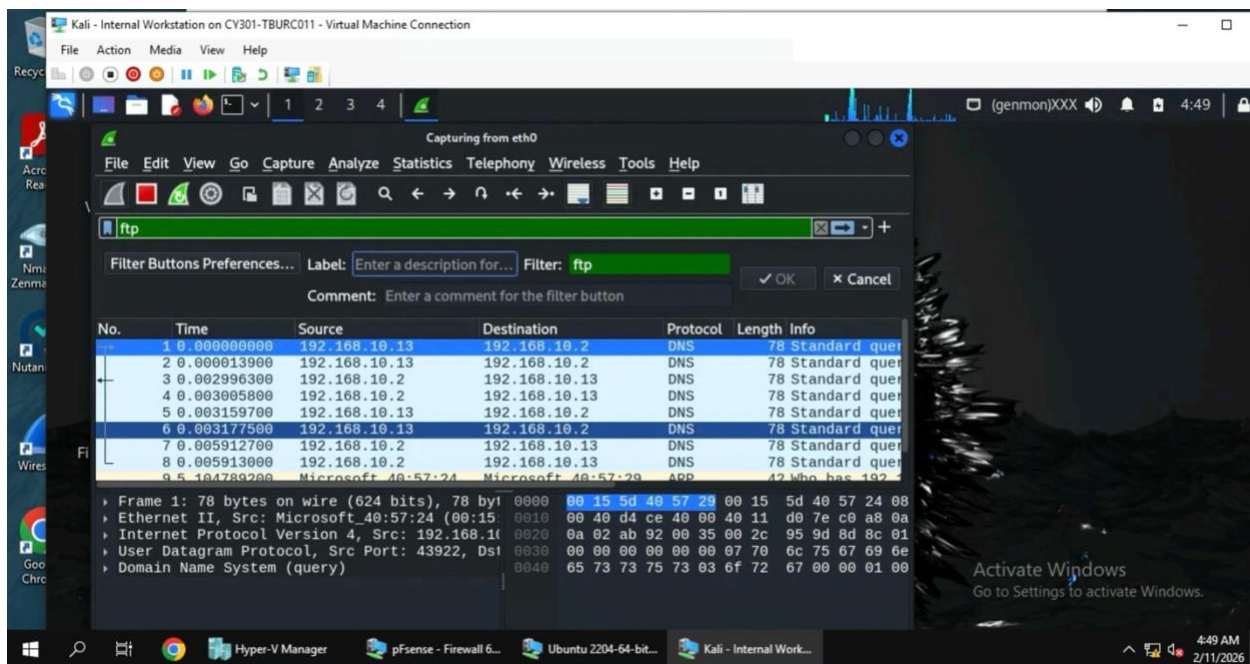


- D. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu64-bit VM.

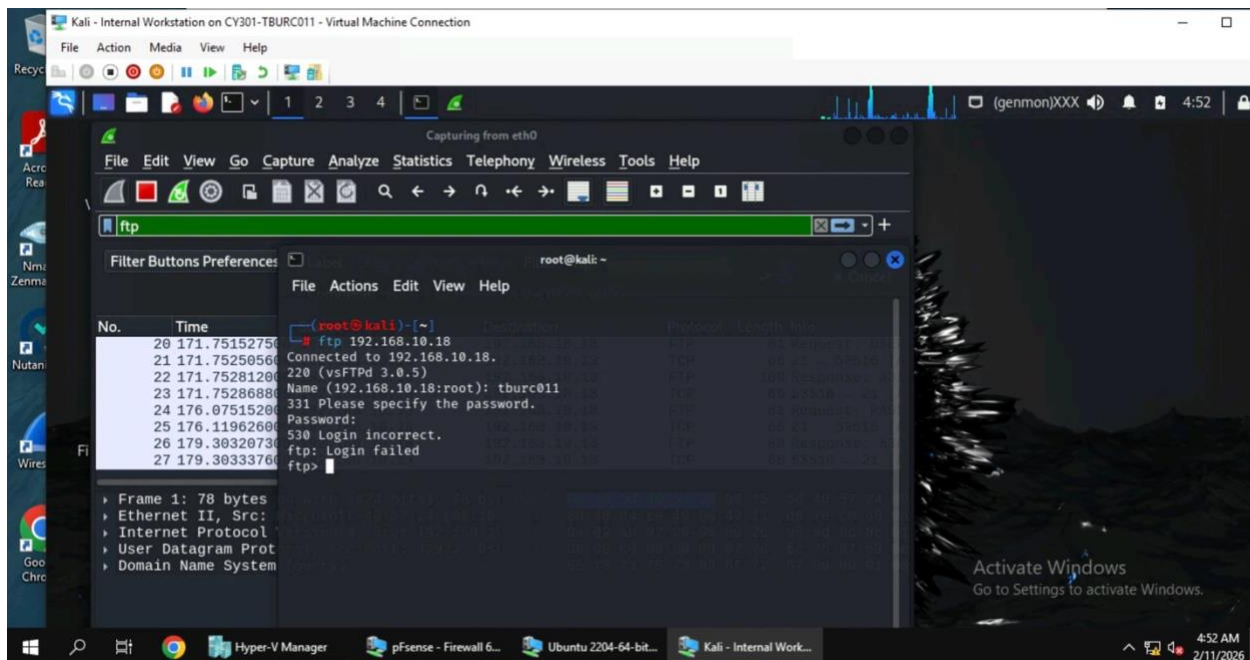


A. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: `ftp [ip_addr of ubuntu VM]`. The username for the FTP server is `student`, and the password is `password`. You can follow the steps below to access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



Kali - Internal Workstation on CY301-TBURC011 (genmon)XXX 4:55

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

No.	Time	Source	Destination	Protocol	Length	Info
11	27.678409400	192.168.10.18	192.168.10.13	FTP	86	Response: 220 (vsFTPd 3.0.5)
12	27.678496500	192.168.10.13	192.168.10.18	TCP	66	56680 → 21 [ACK] Seq=1 Ack=21 Win=65516 Len=0 TSval=
13	32.765259800	192.168.10.13	192.168.10.18	FTP	81	Request: USER tburc011
14	32.766782500	192.168.10.18	192.168.10.13	TCP	66	21 → 56680 [ACK] Seq=21 Ack=16 Win=65280 Len=0 TSval=
15	32.766790300	192.168.10.18	192.168.10.13	FTP	100	Response: 331 Please specify the password.
16	32.766910400	192.168.10.13	192.168.10.18	TCP	66	56680 → 21 [ACK] Seq=16 Ack=55 Win=65482 Len=0 TSval=
17	35.475499200	192.168.10.13	192.168.10.18	FTP	81	Request: PASS 01226537
18	35.518145600	192.168.10.18	192.168.10.13	TCP	66	21 → 56680 [ACK] Seq=55 Ack=31 Win=65280 Len=0 TSval=
19	38.495345200	192.168.10.18	192.168.10.13	FTP	88	Response: 530 Login incorrect.
20	38.495412500	192.168.10.13	192.168.10.18	TCP	66	56680 → 21 [ACK] Seq=31 Ack=77 Win=65460 Len=0 TSval=

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bi 0000 00 15 5d 40 57 32 00 15 5d 40 57 24 08 00 45 10 ...]@W2...

Ethernet II, Src: Microsoft_40:57:24 (00:15:5d:40:57:24), Dst: 0010 00 34 d5 de 40 00 40 06 cf 65 c0 a8 0a 0d c0 a8 ...4...@...

Internet Protocol Version 4, Src: 192.168.10.13, Dst: 192.168.1 0020 0a 12 d1 0c 00 15 48 d1 3e 80 61 b4 97 92 80 11 ...H...

Transmission Control Protocol, Src Port: 53516, Dst Port: 21, S 0030 7f da 95 96 00 00 01 01 08 0a ca ec 09 47 49 de ...@...

0040 f5 40

File Transfer Protocol (FTP): Protocol Packets: 20 - Displayed: 20 (100.0%) Profile: Default