OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2: Traffic Tracing and Sniffing

RANEEM ALARIAN

UIN: 01199741

Task A

You should keep Wireshark running in the background while performing the following tasks:

1. Open Wireshark on External Kali and listen to the interface “eth0”

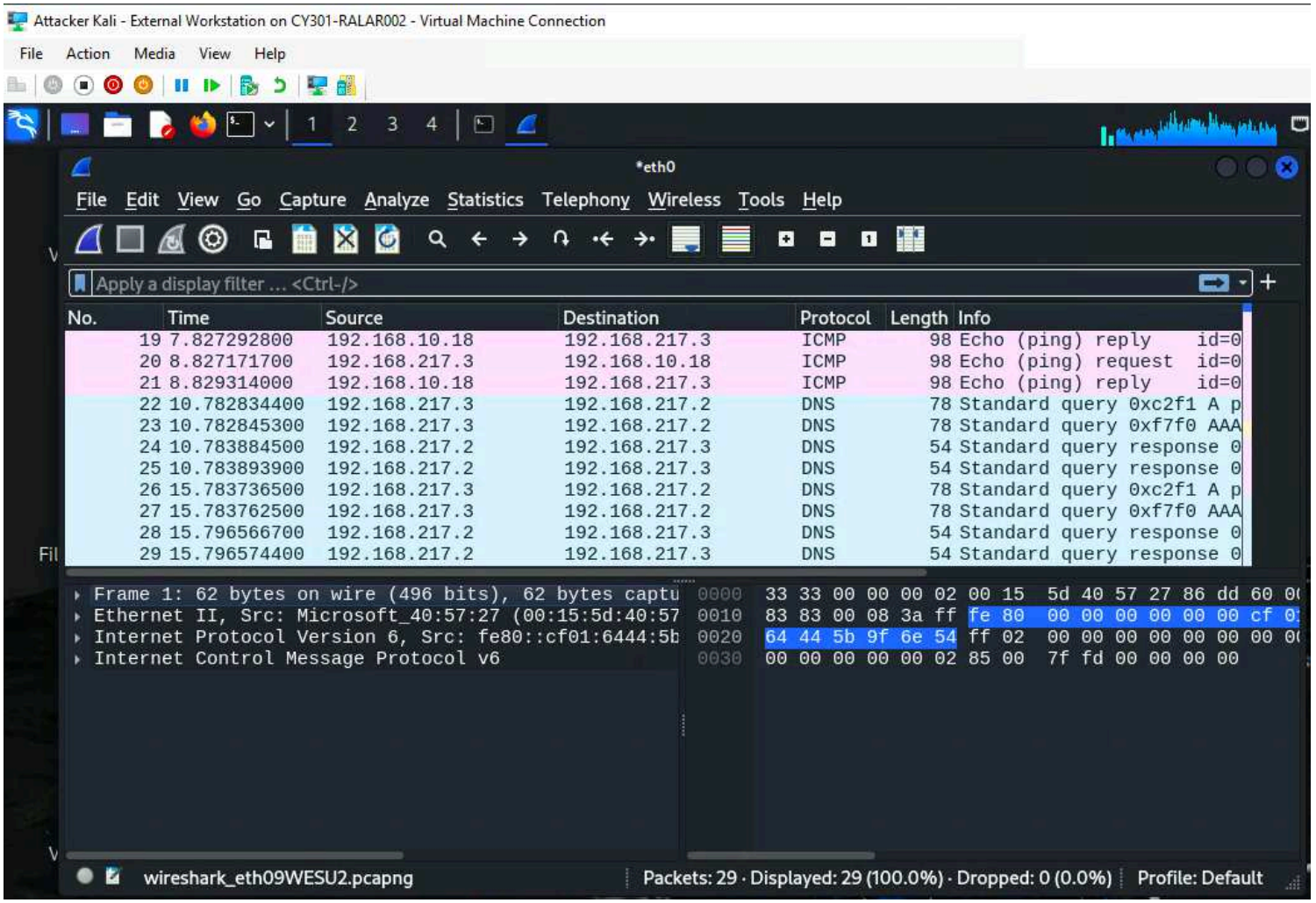
2. Open a new terminal, then ping the Ubuntu VM for 5 – 10 seconds

3. Open a new web browser tab in Kali Linux (even if no webpage will be displayed), and keep it for a couple of seconds

4. **Stop capturing (the red button on the toolbar)**

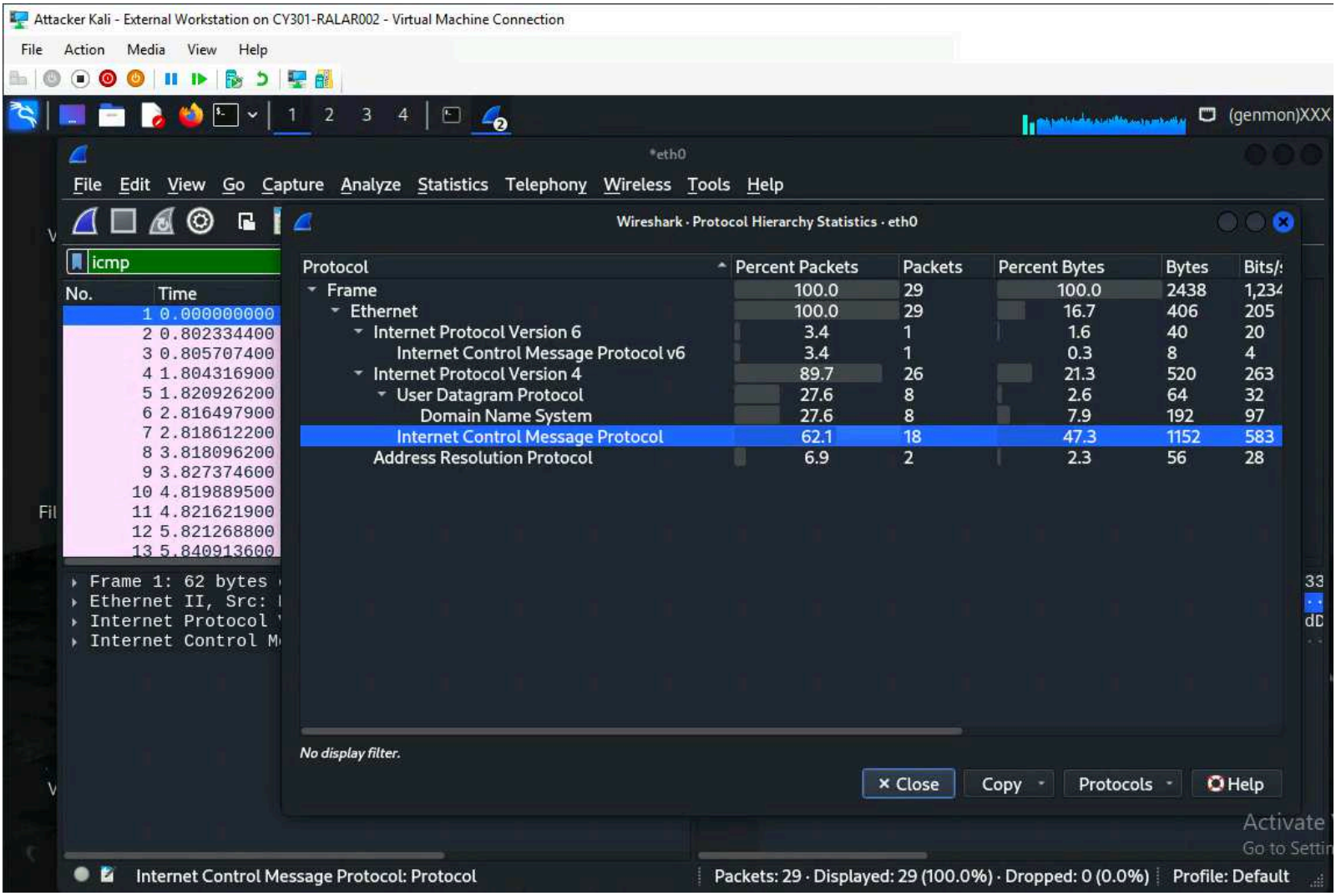
Now, answer the following questions. You need to provide a screenshot that contains the answers to each question

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



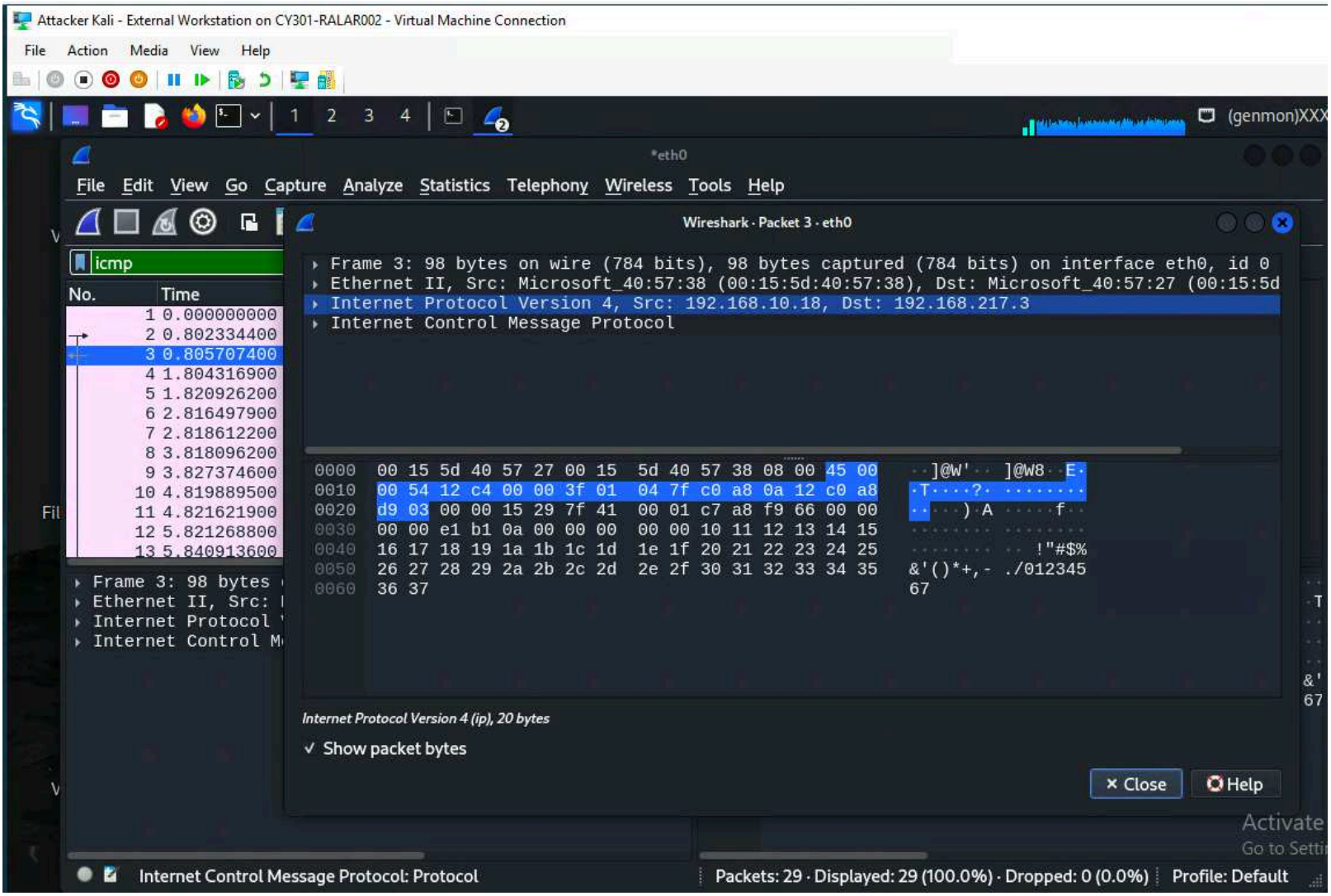
29 packets are captured and **29** packets are displayed, as reflected in the bottom right corner of the Wireshark screen above

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

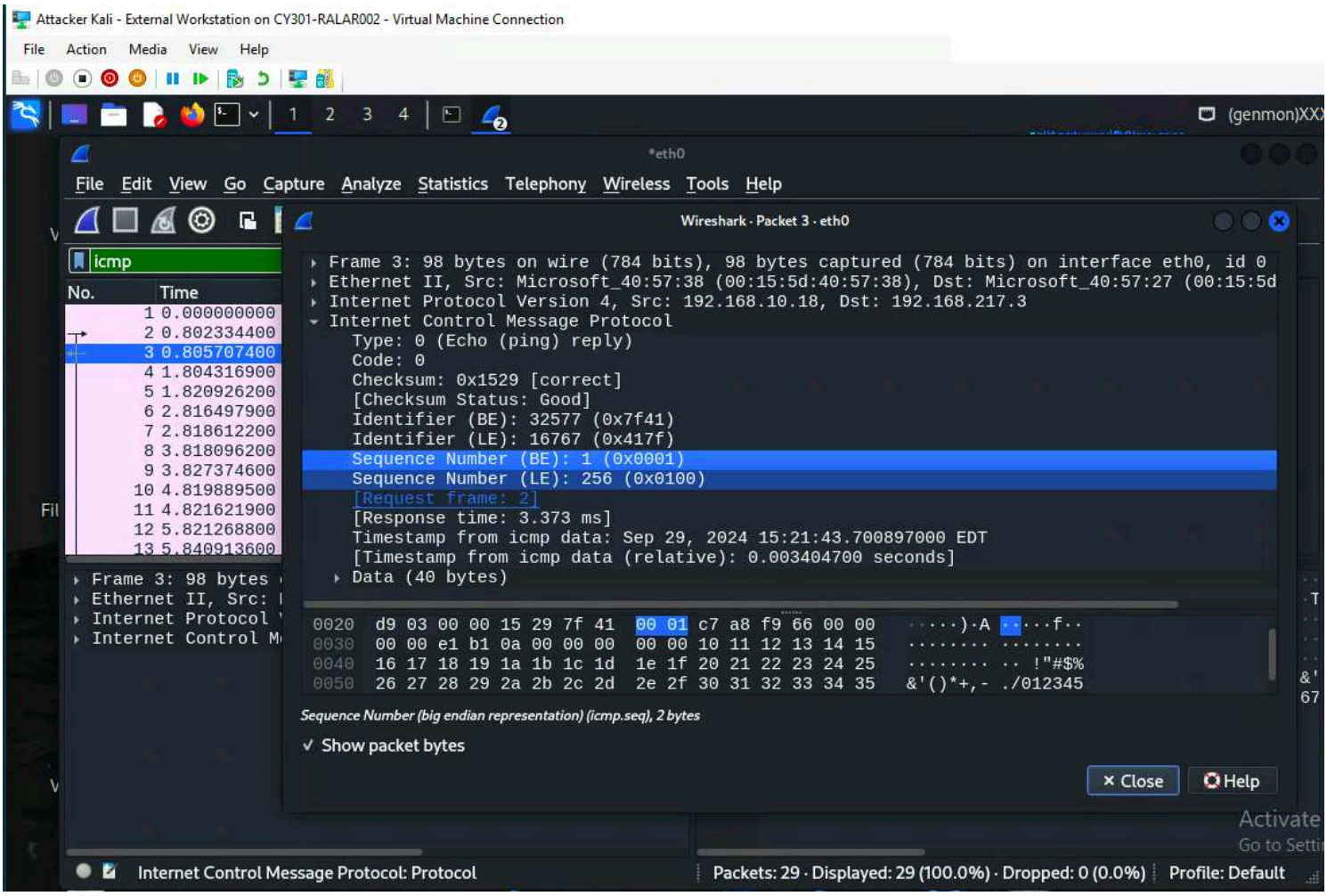


18 ICMP packets are captured

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

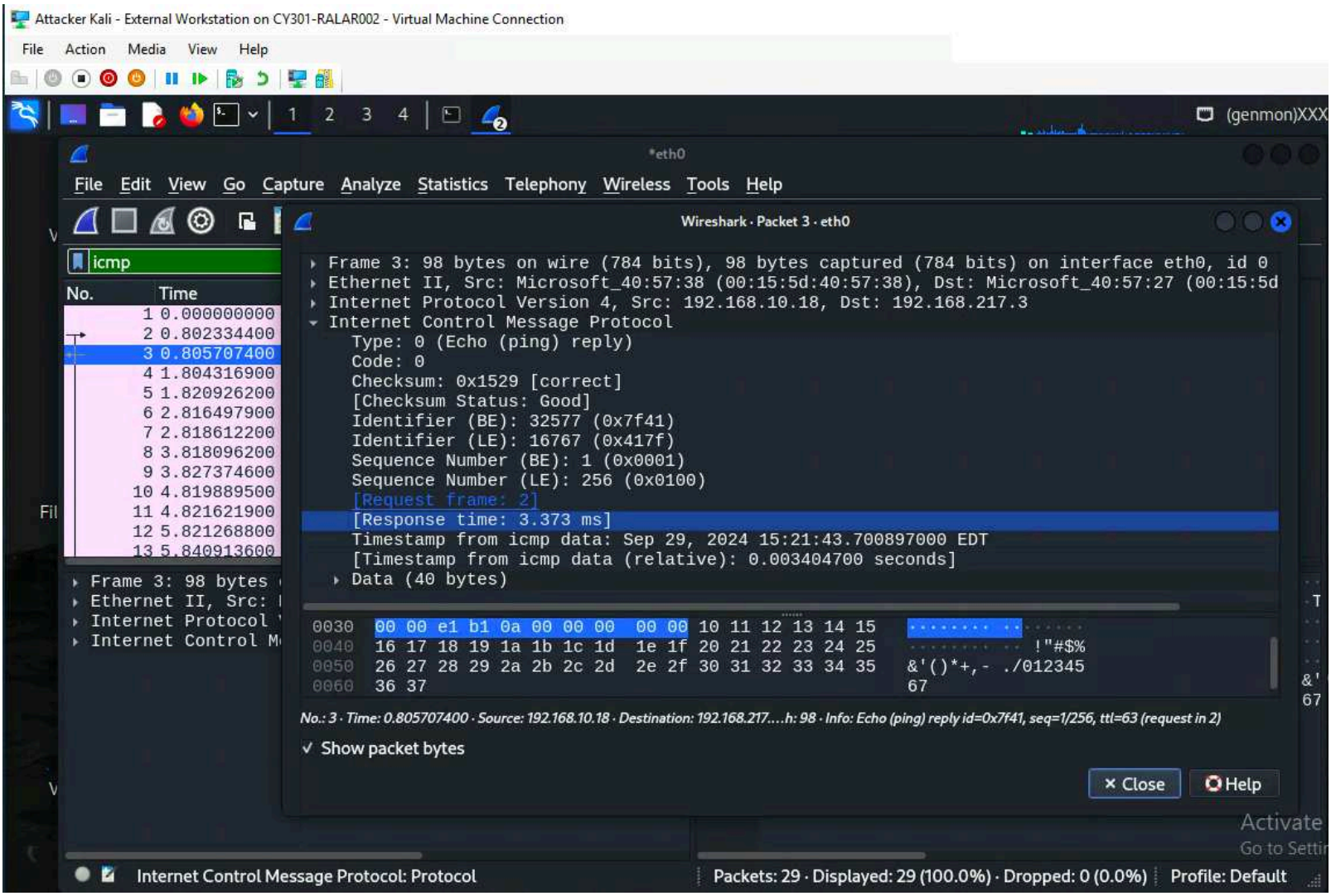


Source IP: 192.168.10.18
Destination IP: 192.168.217.3



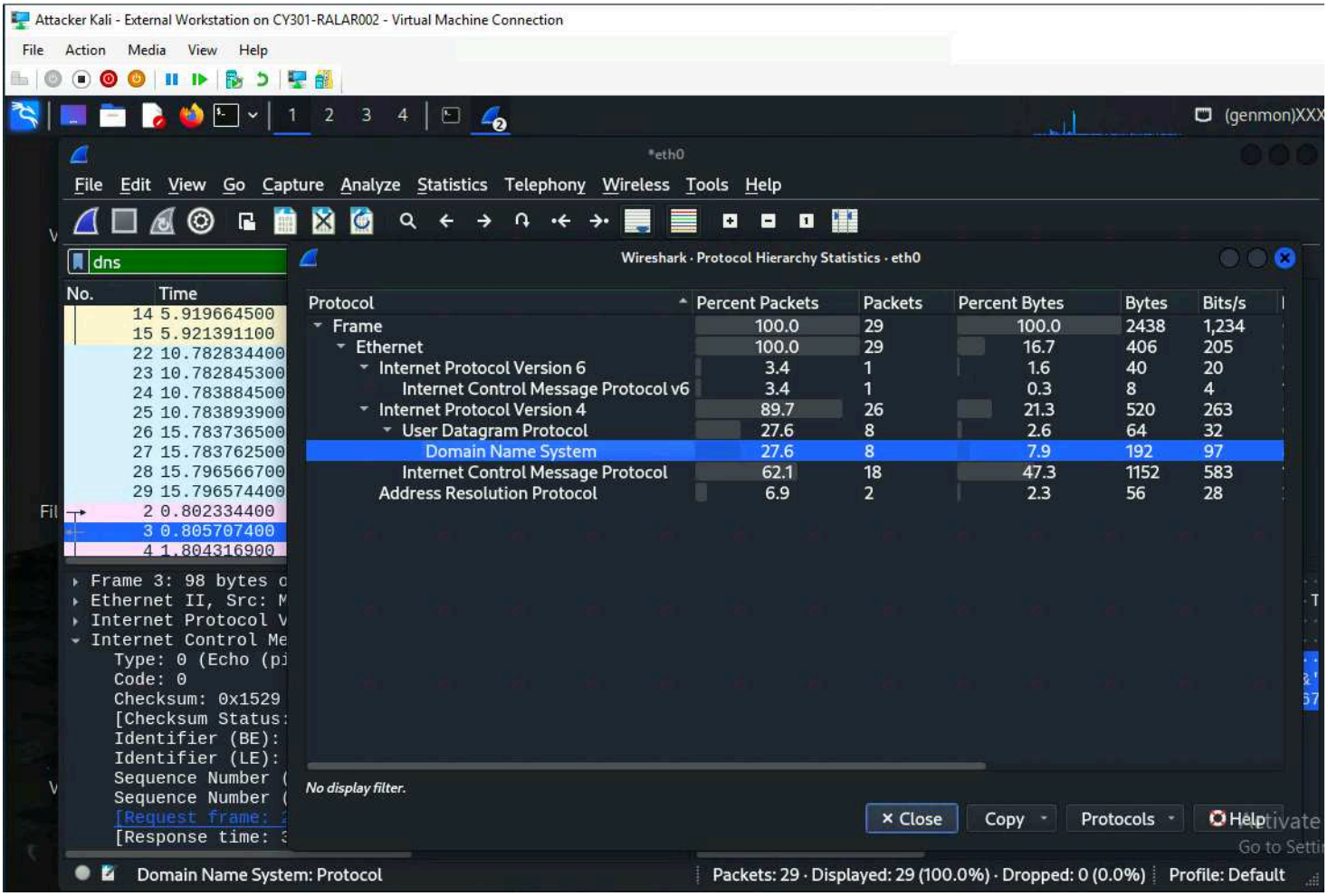
Sequence numbers: 0x0001 and 0x0100

Data size: 40 bytes



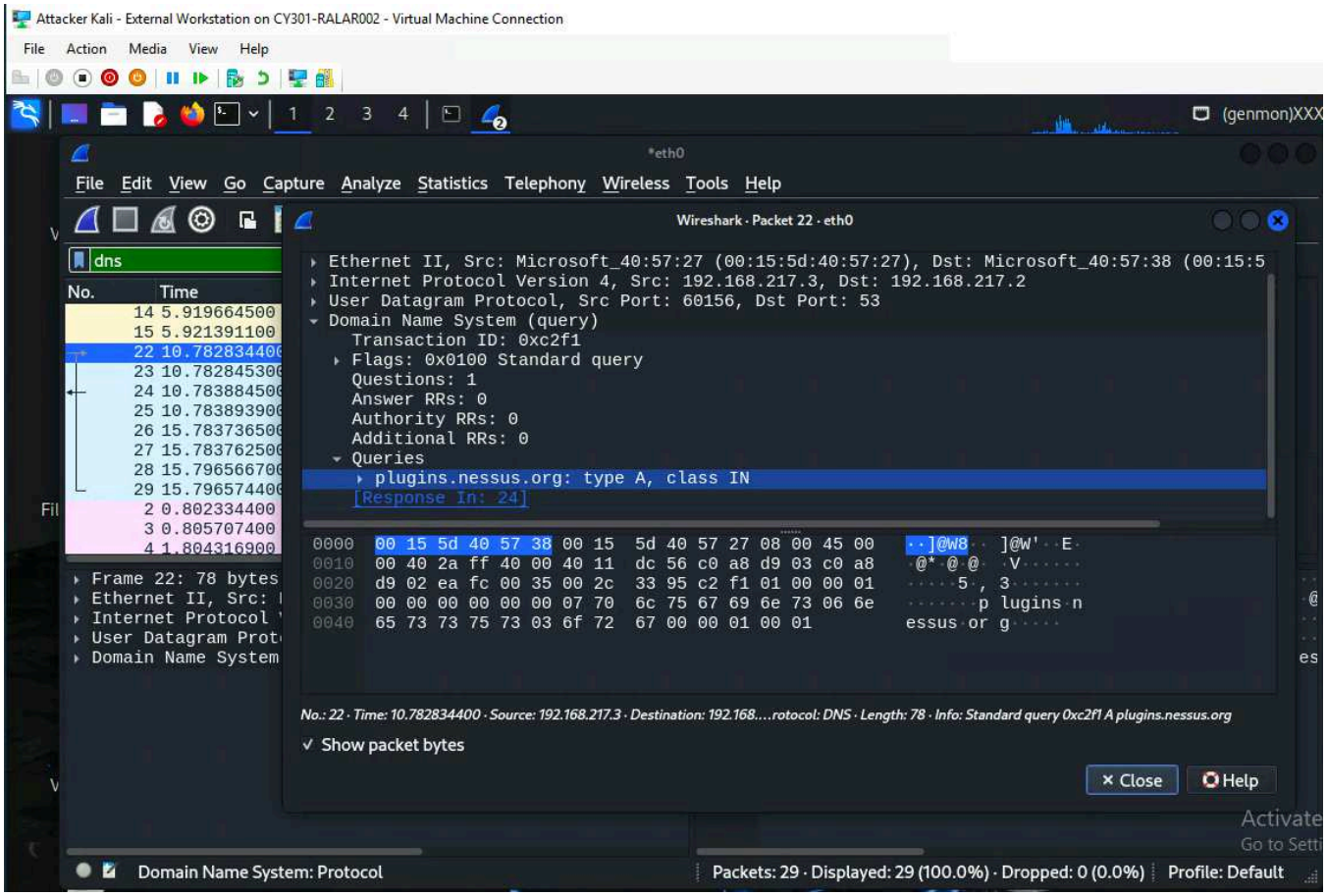
Response time: 3.373 ms

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

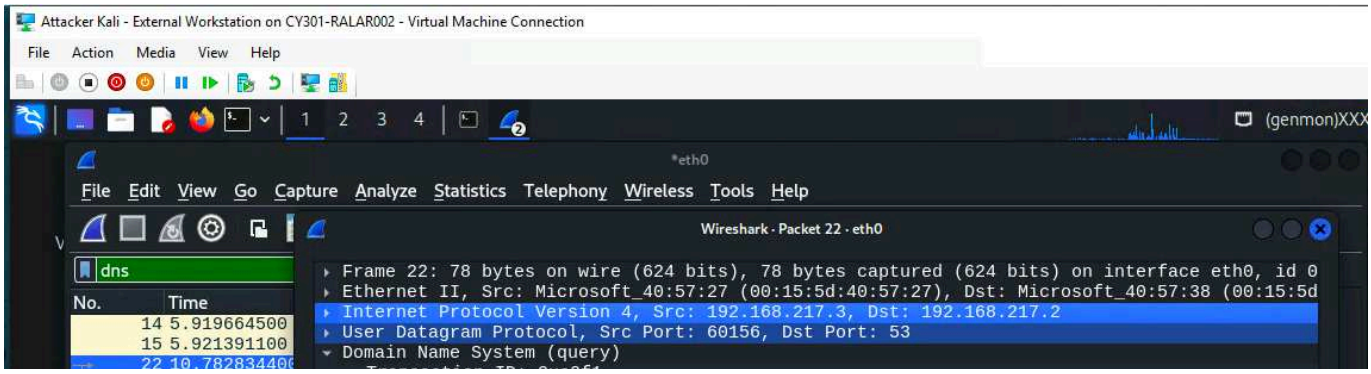


8 packets are displayed

5. 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**

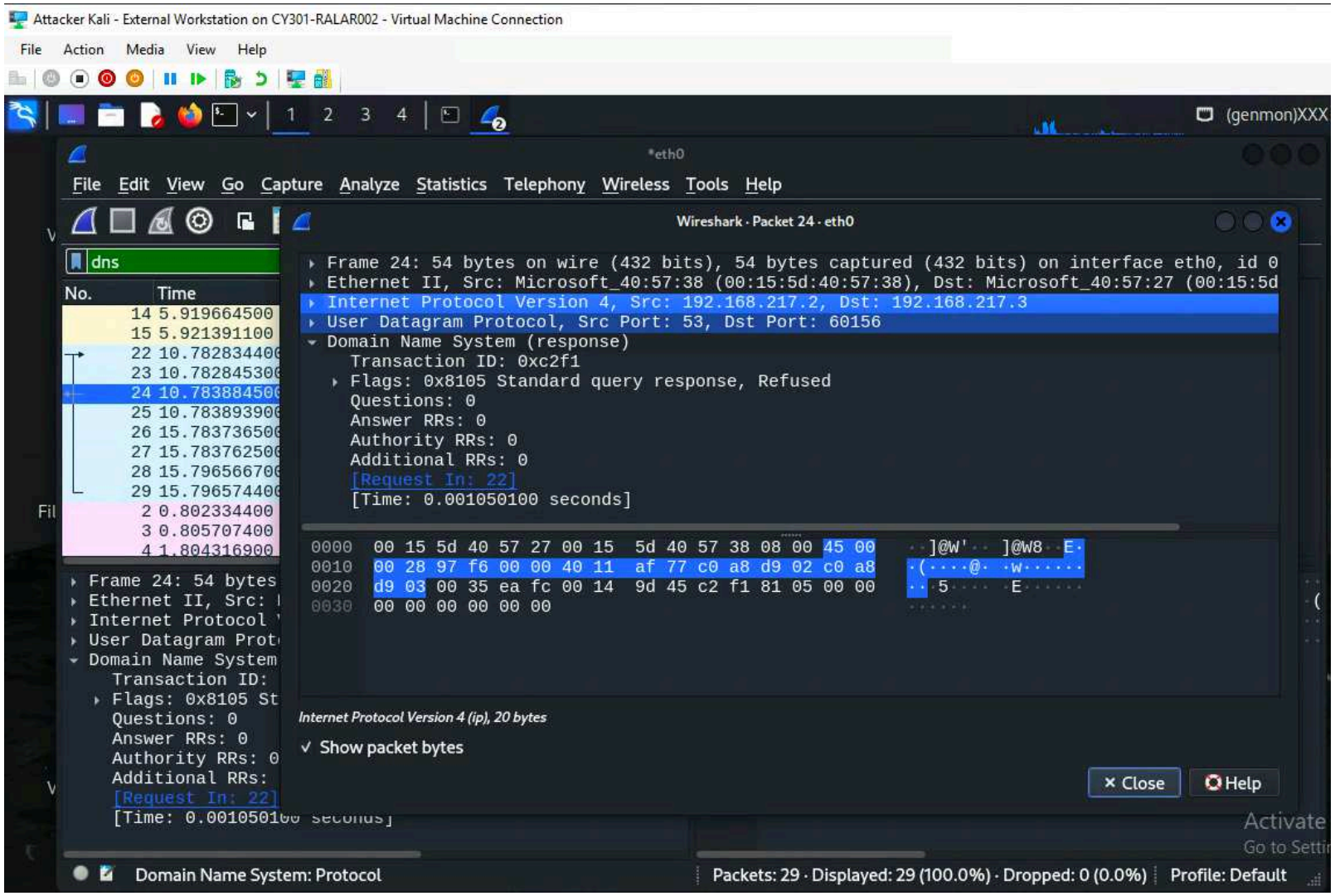


The domain name this host is trying to resolve is **plugins.nessus.org**

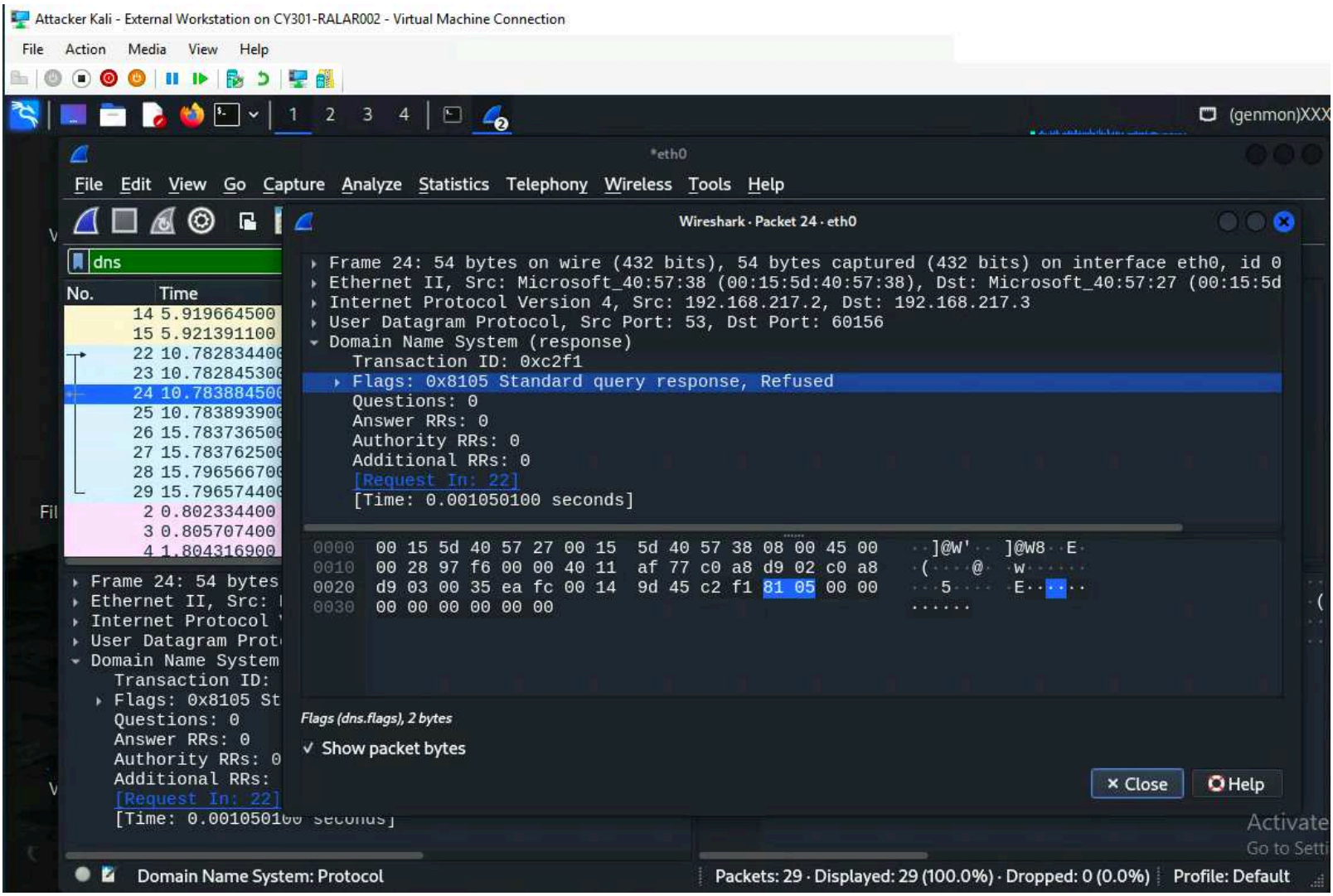


Source IP and port number: 192.168.217.3:60156
Destination IP and port number: 192.168.217.2:53

6. 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 and port number: 192.168.217.2:53
Destination IP and port number: 192.168.217.3:60156



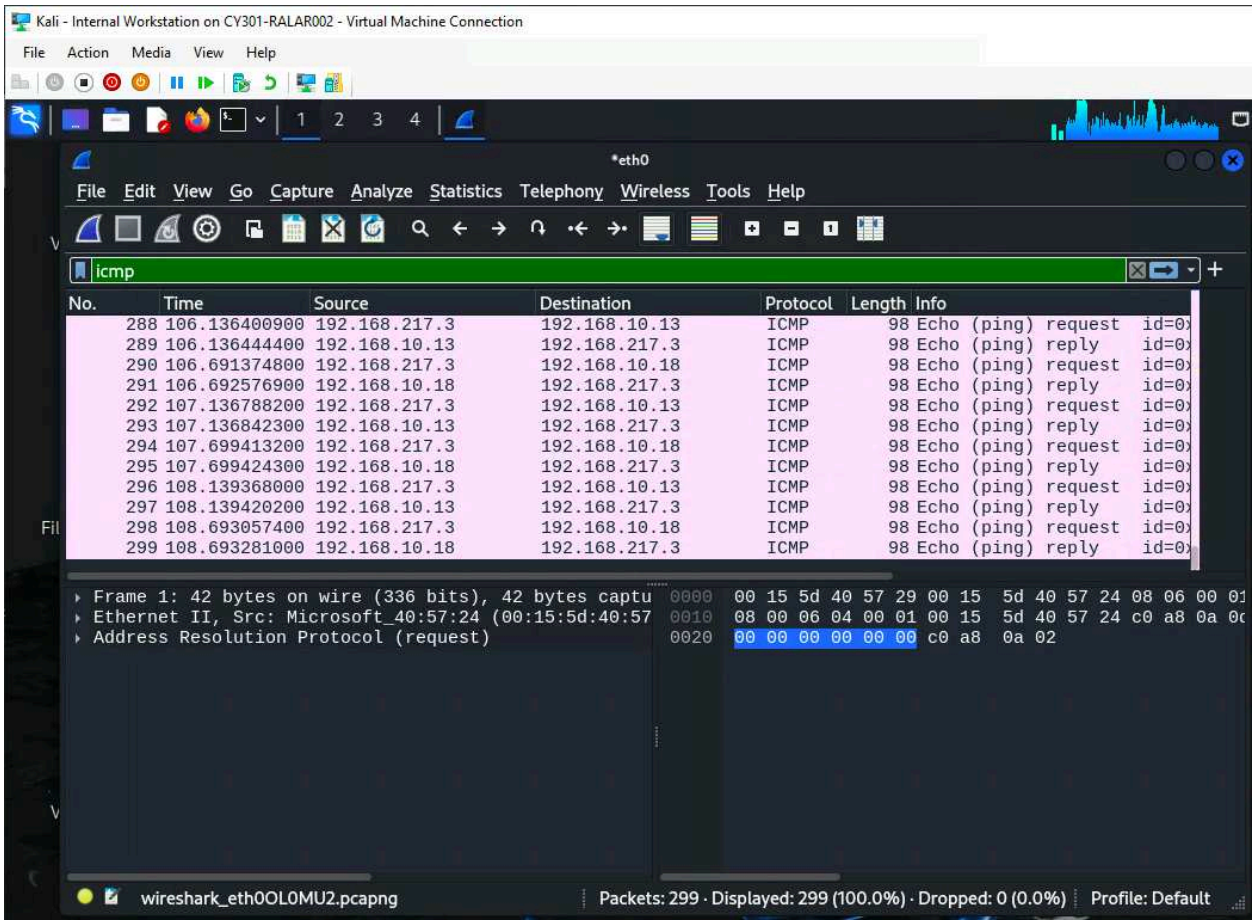
The standard query response was refused by the DNS

Task B

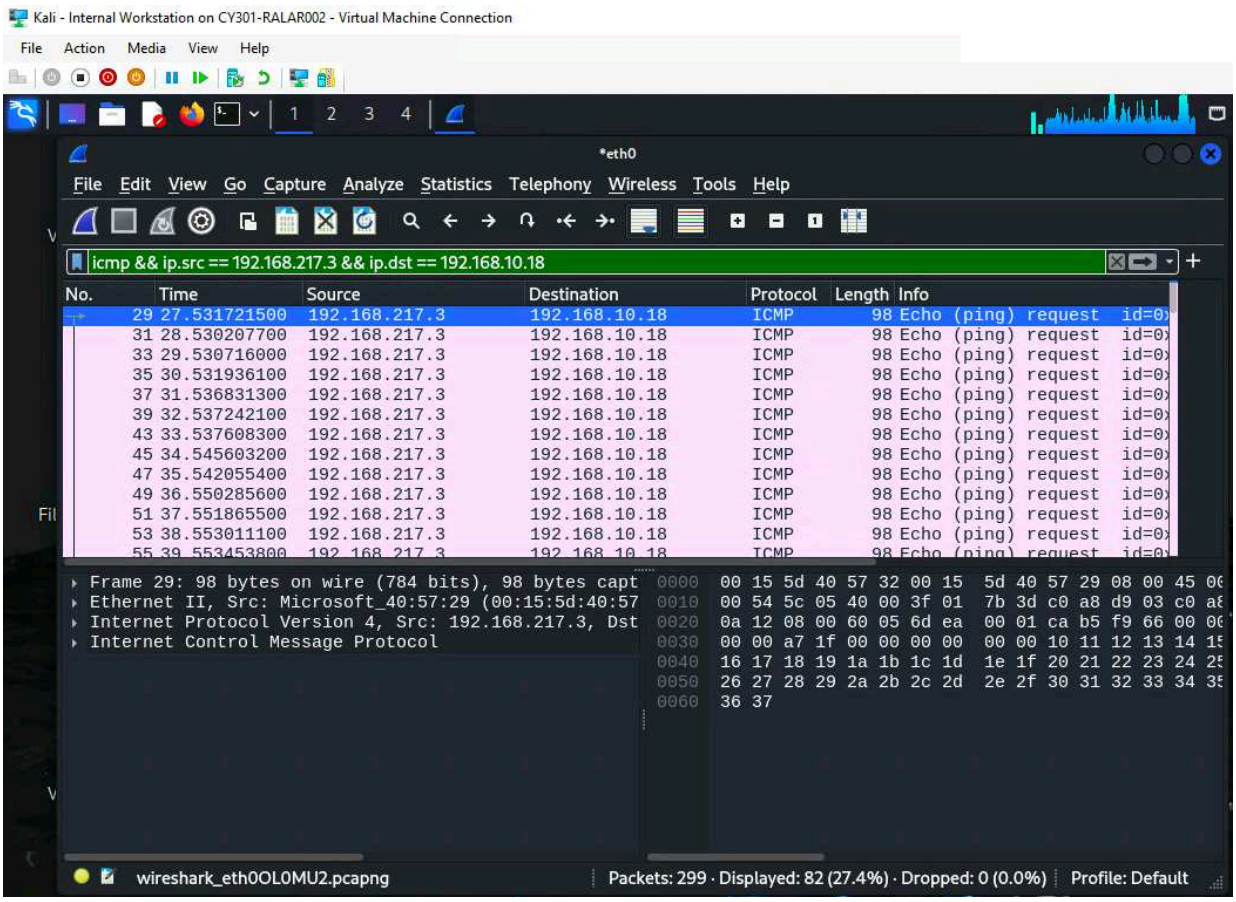
1. **Sniff ICMP traffic:**

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

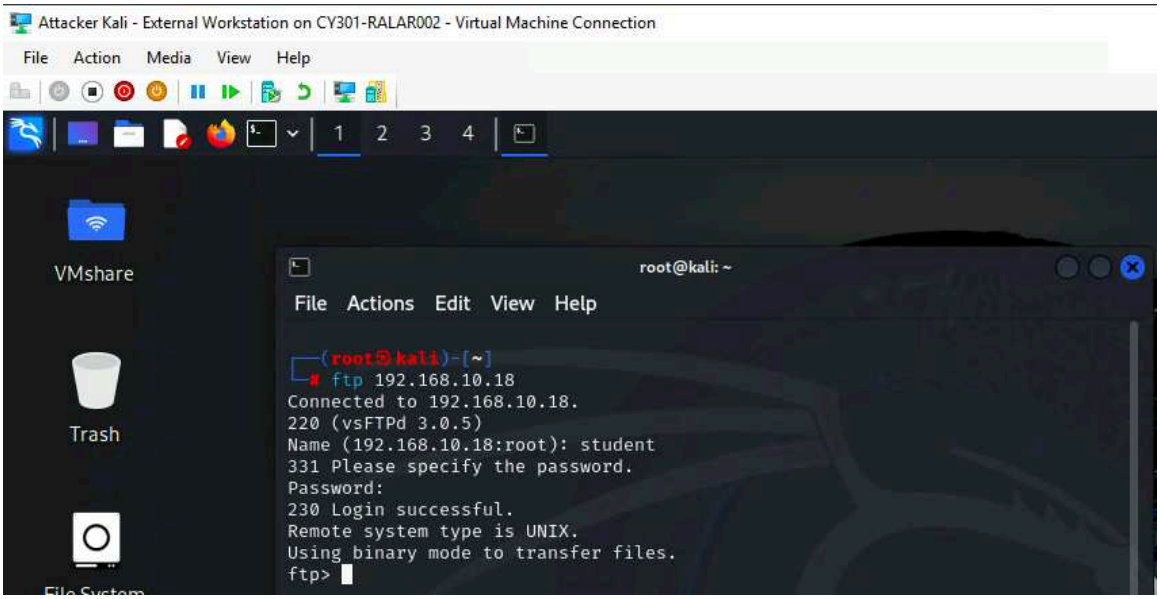
   a. Apply proper display or capture filter on Internal Kali VM to show active ICMP traffic



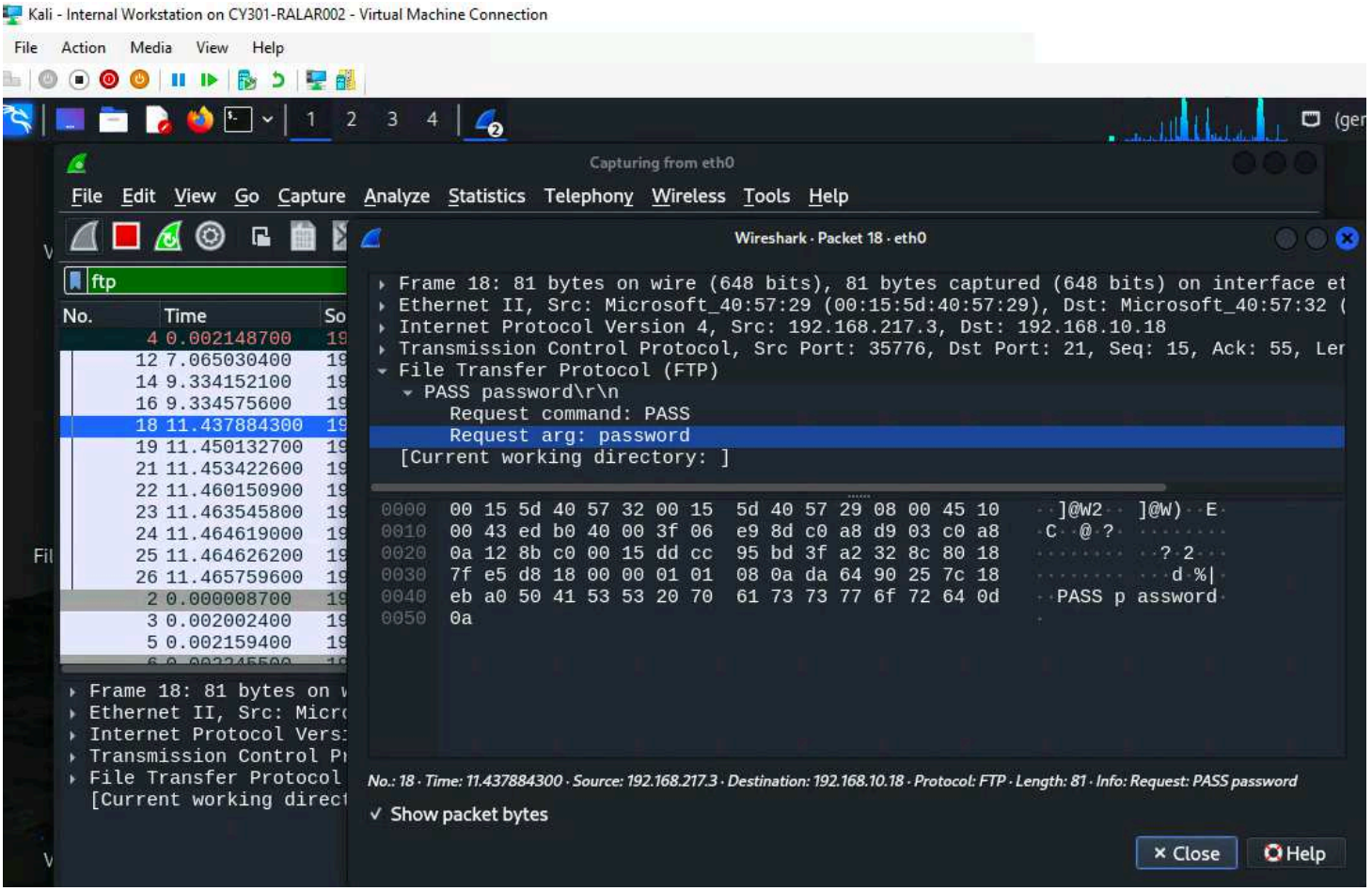
   b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM



2. **Sniff FTP traffic:**
   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

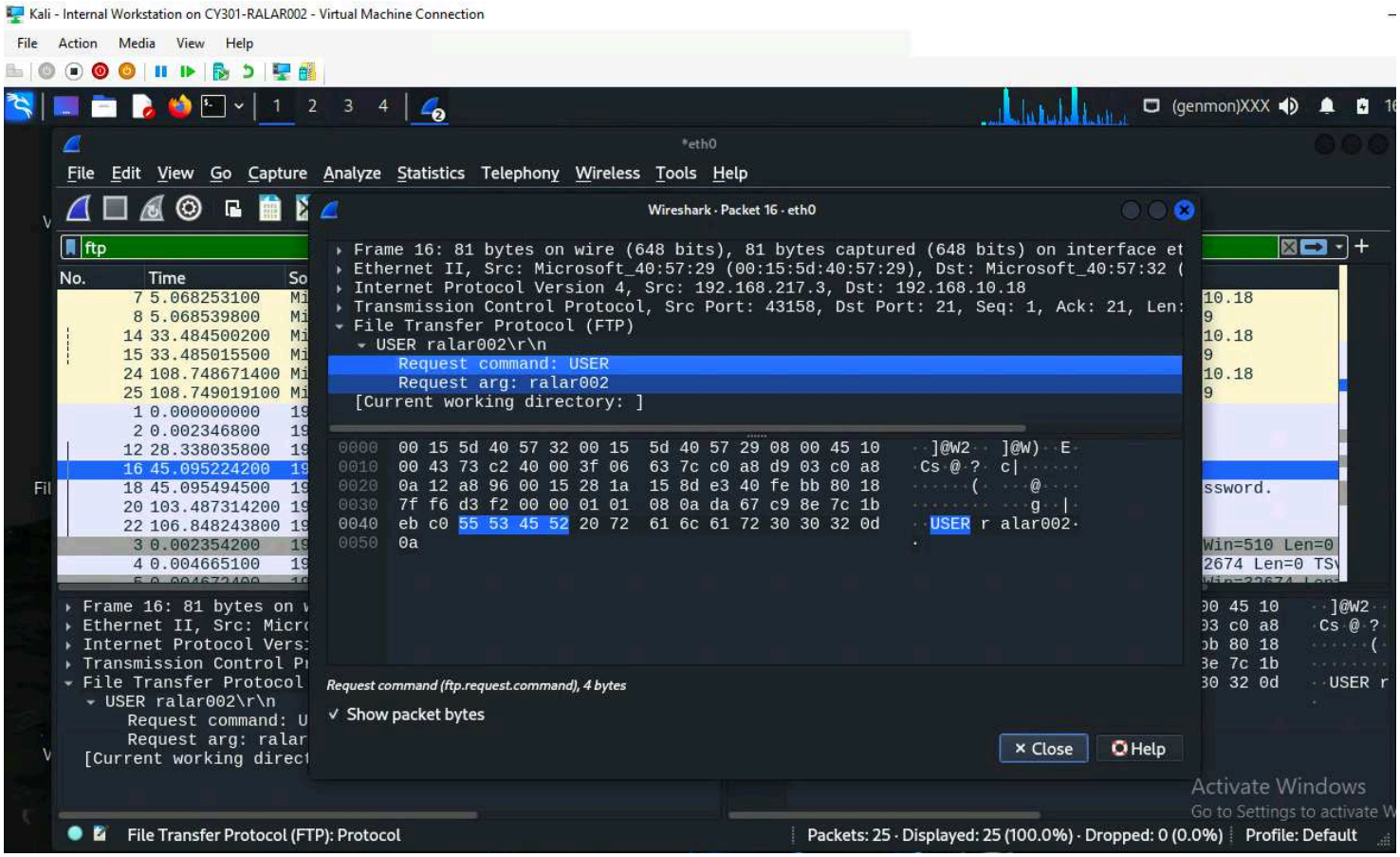


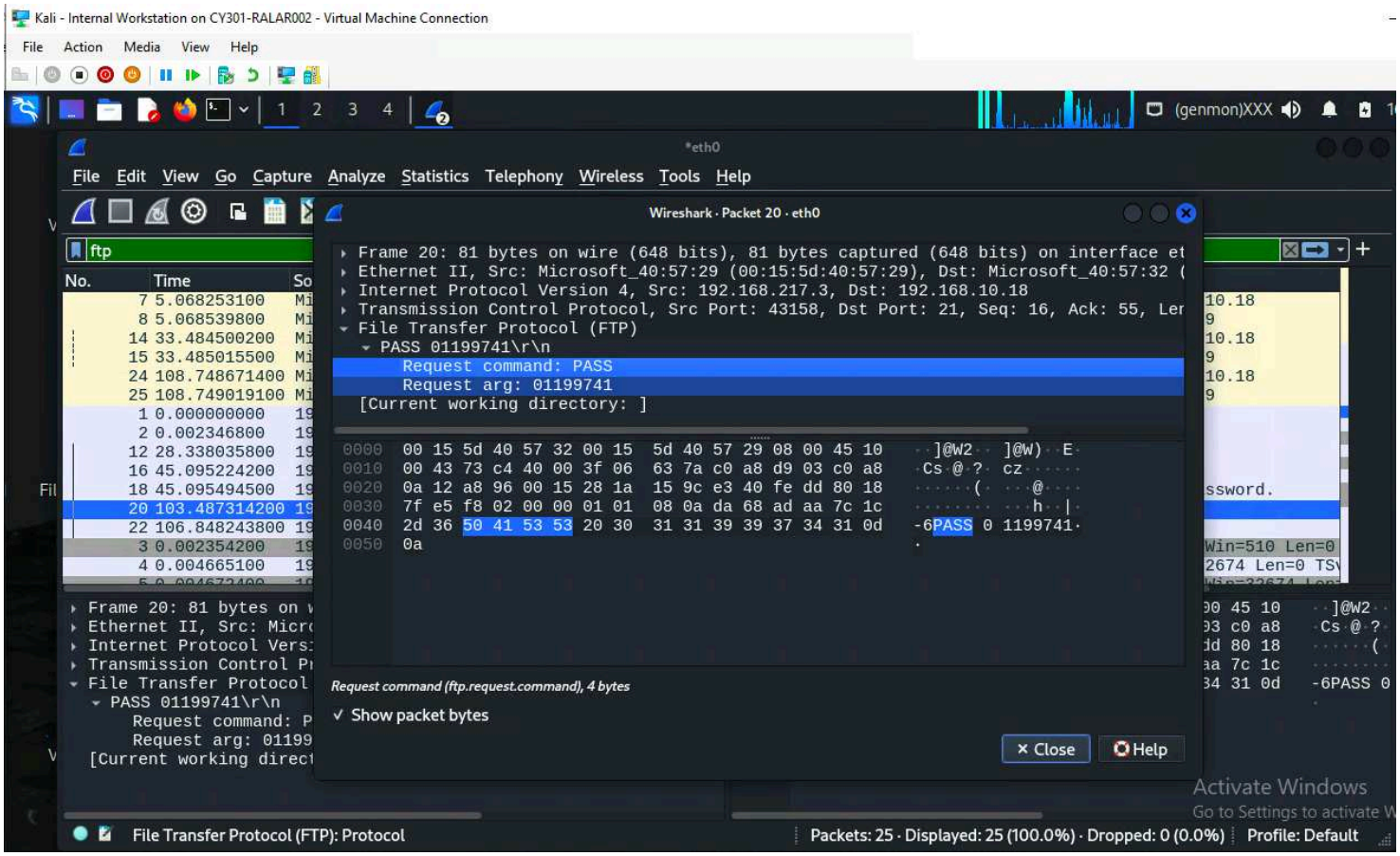
b. Unfortunately, Internal Kali, the attacker, is also sniffing into the communication. Therefore, all of your communication is exposed to the attacker. Now, you need to find out the password used by External Kali to access the FTP server from the intercepted traffic on Internal Kali. You need to take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



I found the password by setting "ftp" as the display filter first, then double clicking on the packet that showcased information about the password request (packet #18). The information about the requested command (password) and the argument (the actual password typed in) is shown under FTP, as shown in the screenshot above

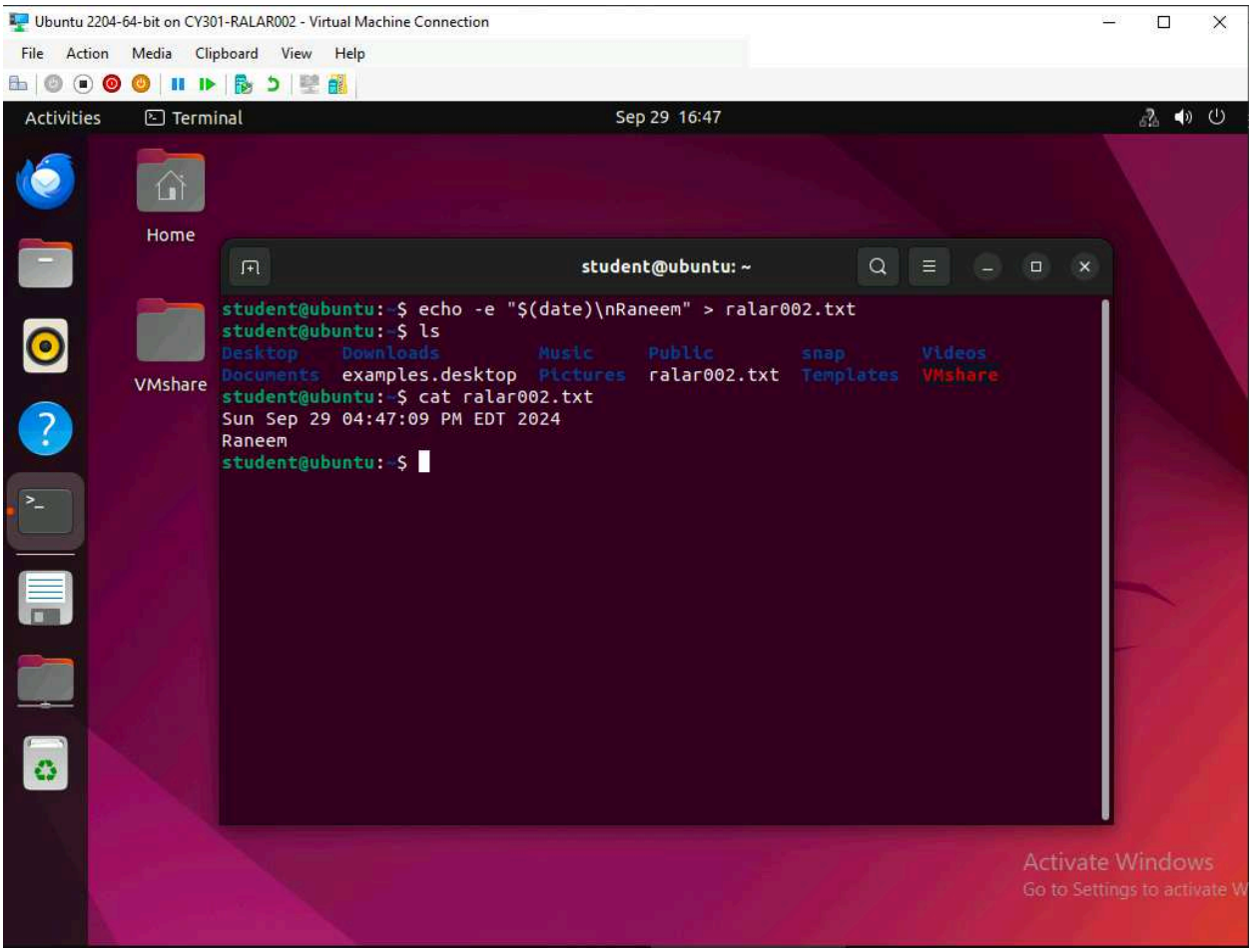
c. After you successfully find the username & password from the FTP traffic, repeat the previous step (2.a), and use your MIDAS ID as the username and UIN as the password to reaccess the FTP server from External Kali. Although External Kali may not access the FTP server, you need to intercept the packets containing these "secrets" from the attacker VM, which is Internal Kali


Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 16 · eth0
Frame 16: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface et
Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft_40:57:32 (
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
Transmission Control Protocol, Src Port: 43158, Dst Port: 21, Seq: 1, Ack: 21, Len:
File Transfer Protocol (FTP)
USER ralar002\r\n
Request command: USER
Request arg: ralar002
[Current working directory:]
0000 00 15 5d 40 57 32 00 15 5d 40 57 29 08 00 45 10
0010 00 43 73 c2 40 00 3f 06 63 7c c0 a8 d9 03 c0 a8
0020 0a 12 a8 96 00 15 28 1a 15 8d e3 40 fe bb 80 18
0030 7f f6 d3 f2 00 00 01 01 08 0a da 67 c9 8e 7c 1b
0040 eb c0 55 53 45 52 20 72 61 6c 61 72 30 30 32 0d
0050 0a
Request command (ftp.request.command), 4 bytes
Show packet bytes
Close
Help
File Transfer Protocol (FTP): Protocol
Packets: 25 · Displayed: 25 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Activate Windows

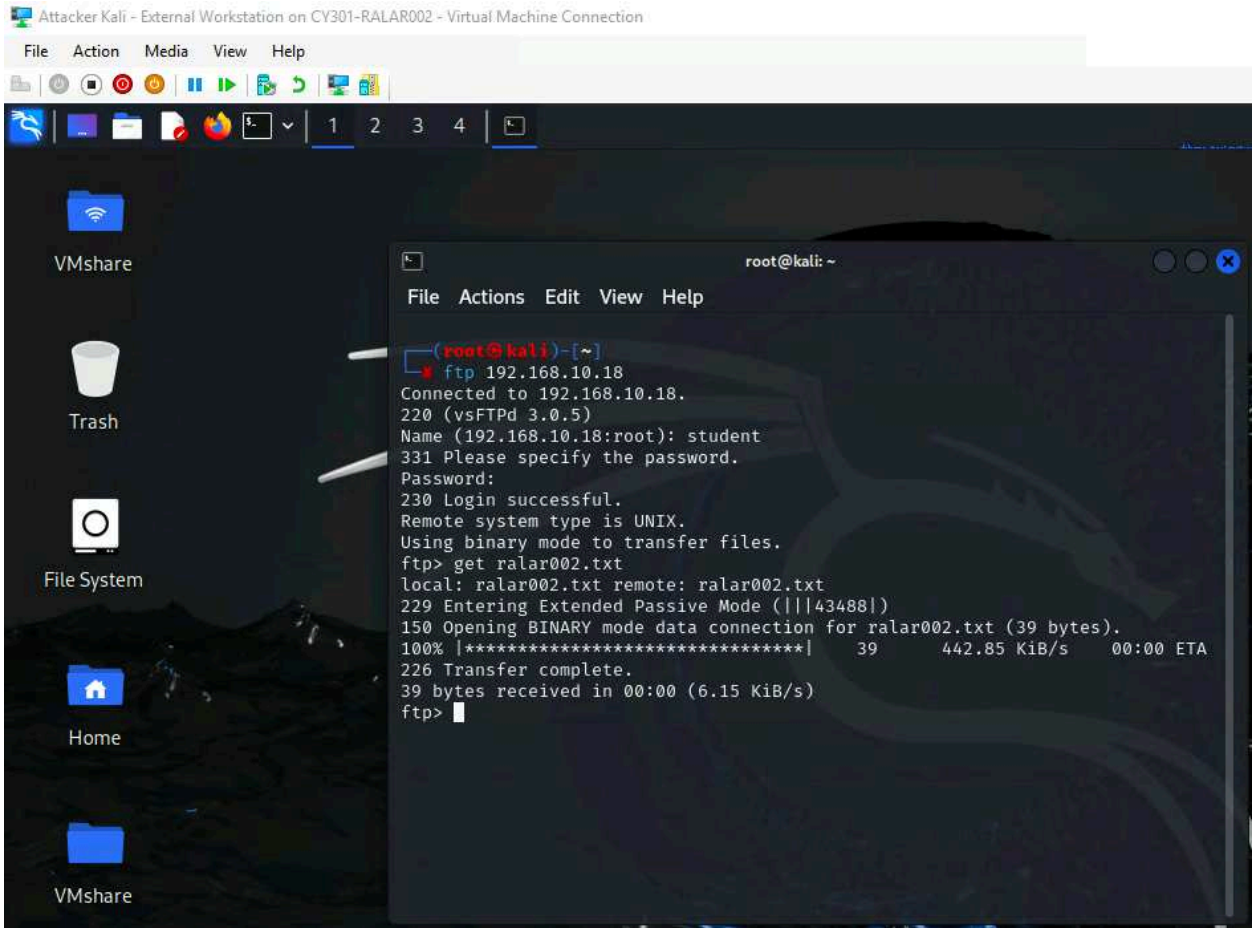

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Packet 20 · eth0
Frame 20: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface et
Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft_40:57:32 (
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
Transmission Control Protocol, Src Port: 43158, Dst Port: 21, Seq: 16, Ack: 55, Ler
File Transfer Protocol (FTP)
PASS 01199741\r\n
Request command: PASS
Request arg: 01199741
[Current working directory:]
0000 00 15 5d 40 57 32 00 15 5d 40 57 29 08 00 45 10
0010 00 43 73 c4 40 00 3f 06 63 7a c0 a8 d9 03 c0 a8
0020 0a 12 a8 96 00 15 28 1a 15 9c e3 40 fe dd 80 18
0030 7f e5 f8 02 00 00 01 01 08 0a da 68 ad aa 7c 1c
0040 2d 36 50 41 53 53 20 30 31 31 39 39 37 34 31 0d
0050 0a
Request command (ftp.request.command), 4 bytes
Show packet bytes
Close
Help
File Transfer Protocol (FTP): Protocol
Packets: 25 · Displayed: 25 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
Activate Windows

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



Once you have the file ready in Ubuntu, switch back to External Kali. Get the file you just created remotely using the FTP protocol



As an attacker, you need to complete the following tasks in Internal Kali:

1. Apply a proper display filter to display the FTP-DATA packets between External Kali and Ubuntu VM
2. Follow the TCP stream of the FTP-DATA packet and view the content of the file just transferred
3. Export (Save) the transferred file as a text file in Internal Kali and view the content