OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2: Traffic Tracing and Analysis

Carl Lochstampfor
Student UIN: 01290201
Date: 02/09/2026

Assignment #2: Traffic Tracing and Analysis

Task A: Get started with Wireshark (30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.

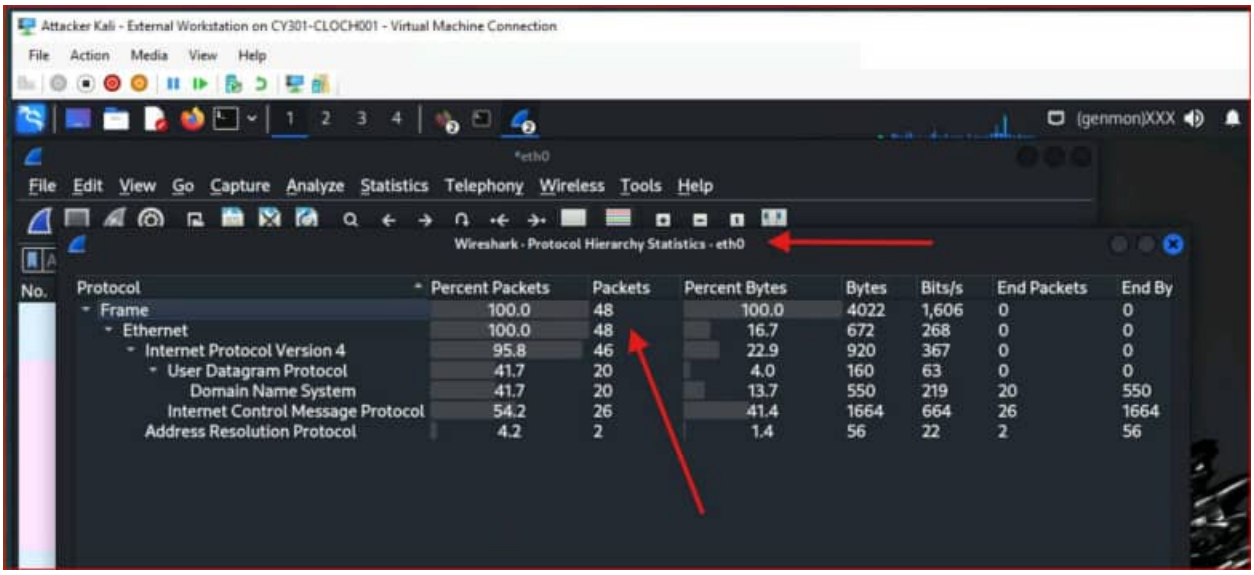
You should keep Wireshark in External / attacker Kali running in the background while performing the following tasks. Connect /Turn on Ubuntu VM (and pfsense VM) as well.

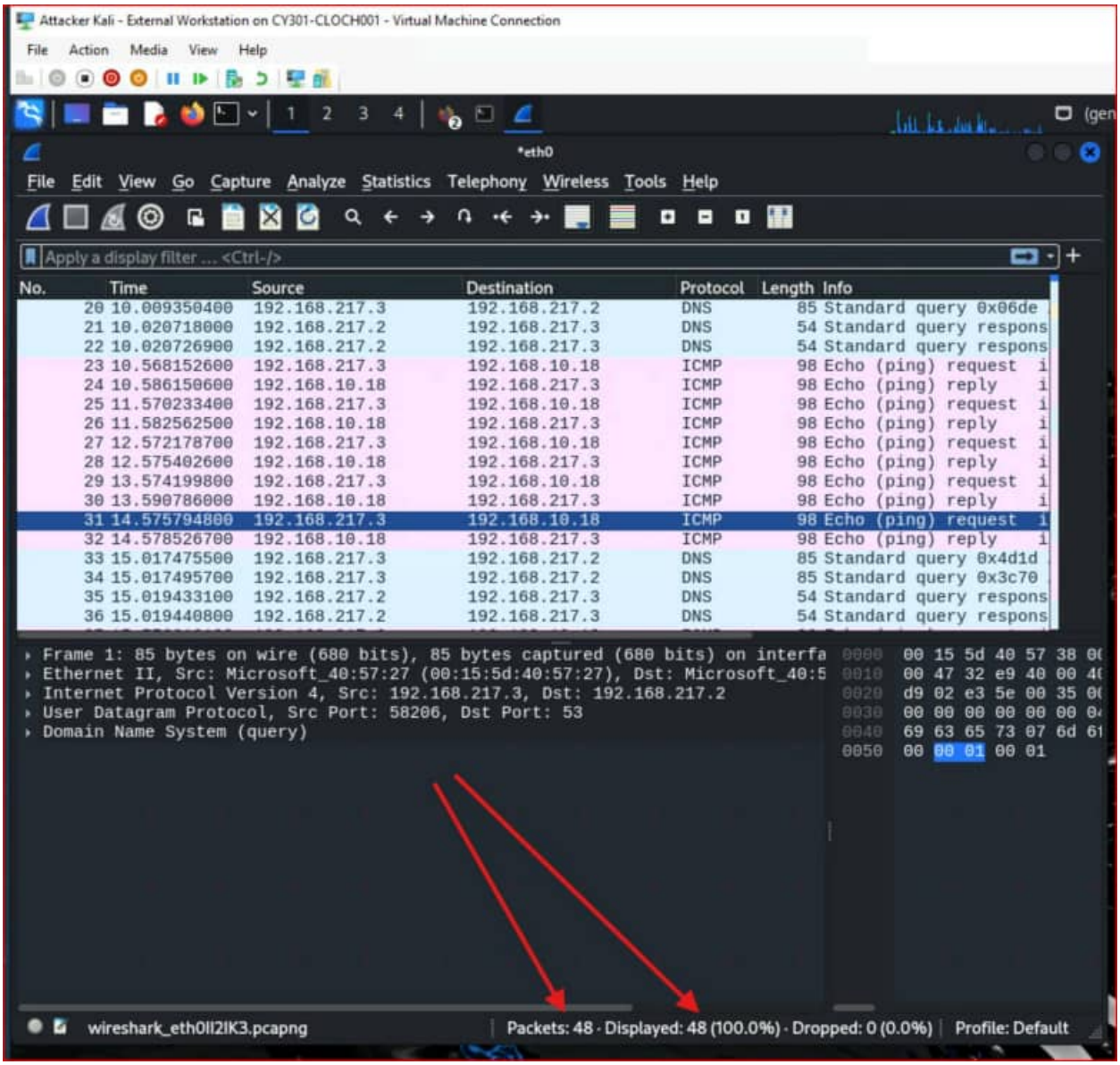
1. Open Wireshark on External / Attacker Kali and listen on interface "eth0".
2. Open a new **terminal** in Attacker Kali, then **ping the Ubuntu VM for 5 – 10 seconds**.
3. Open a **new web browser tab in Attacker Kali** (even if no webpage will be displayed) and **keep it for a couple of seconds**.
4. Stop capturing (by clicking the red button on the tool bar).

Now, answer the following questions. **You need to provide a screenshot for each questions** that proves the answers to each question you write.

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

Answer: **48 packets** captured in total. **48 packets** are displayed.
Screenprint:

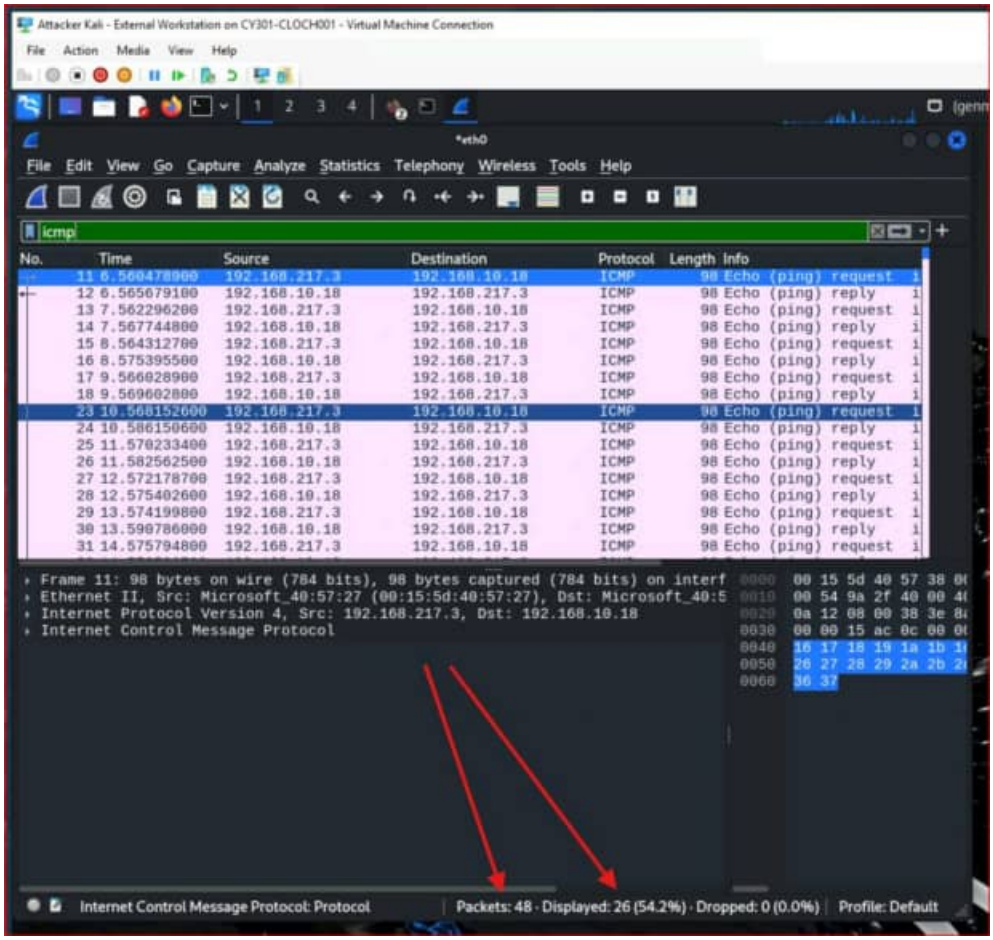


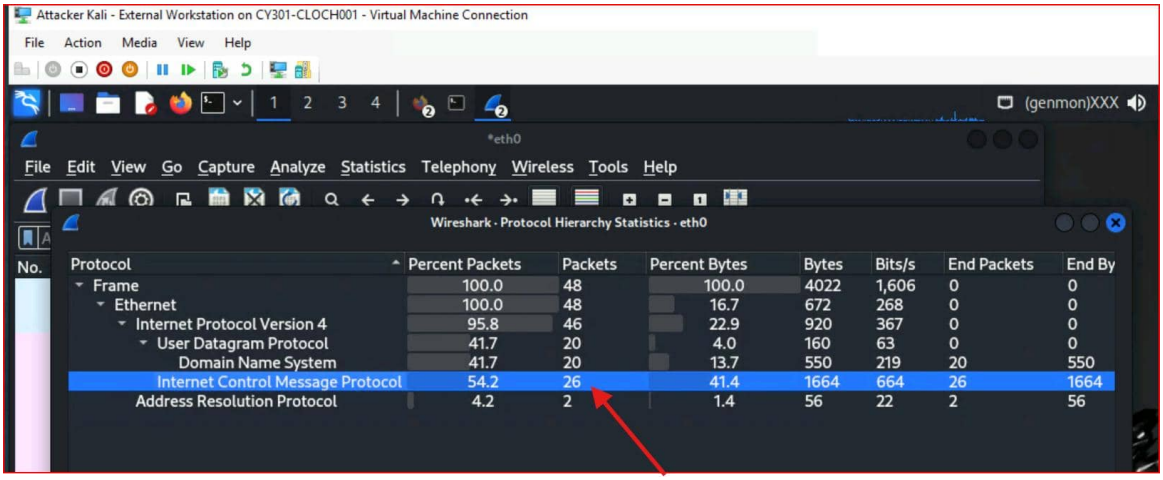

Attacker Kali - External Workstation on CY301-CLOCH001 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
20 10.009350400 192.168.217.3 192.168.217.2 DNS 85 Standard query 0x06de
21 10.020718000 192.168.217.2 192.168.217.3 DNS 54 Standard query respons
22 10.020726900 192.168.217.2 192.168.217.3 DNS 54 Standard query respons
23 10.568152600 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping) request
24 10.586150600 192.168.10.18 192.168.217.3 ICMP 98 Echo (ping) reply
25 11.570233400 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping) request
26 11.582562500 192.168.10.18 192.168.217.3 ICMP 98 Echo (ping) reply
27 12.572178700 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping) request
28 12.575402600 192.168.10.18 192.168.217.3 ICMP 98 Echo (ping) reply
29 13.574199800 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping) request
30 13.590786000 192.168.10.18 192.168.217.3 ICMP 98 Echo (ping) reply
31 14.575794800 192.168.217.3 192.168.10.18 ICMP 98 Echo (ping) request
32 14.578526700 192.168.10.18 192.168.217.3 ICMP 98 Echo (ping) reply
33 15.017475500 192.168.217.3 192.168.217.2 DNS 85 Standard query 0x4d1d
34 15.017495700 192.168.217.3 192.168.217.2 DNS 85 Standard query 0x3c70
35 15.019433100 192.168.217.2 192.168.217.3 DNS 54 Standard query respons
36 15.019440800 192.168.217.2 192.168.217.3 DNS 54 Standard query respons
Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interfa
Ethernet II, Src: Microsoft_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft_40:5
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
User Datagram Protocol, Src Port: 58206, Dst Port: 53
Domain Name System (query)
0000 00 15 5d 40 57 38
0010 00 47 32 e9 40 00
0020 d9 02 e3 5e 00 35
0030 00 00 00 00 00 00
0040 69 63 65 73 07 6d
0050 00 00 01 00 01
wireshark_eth0Il2IK3.pcapng
Packets: 48 · Displayed: 48 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

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

Answer: There are **26 ICMP packets out of a 48 total packets** captured and displayed.

Screenprint:

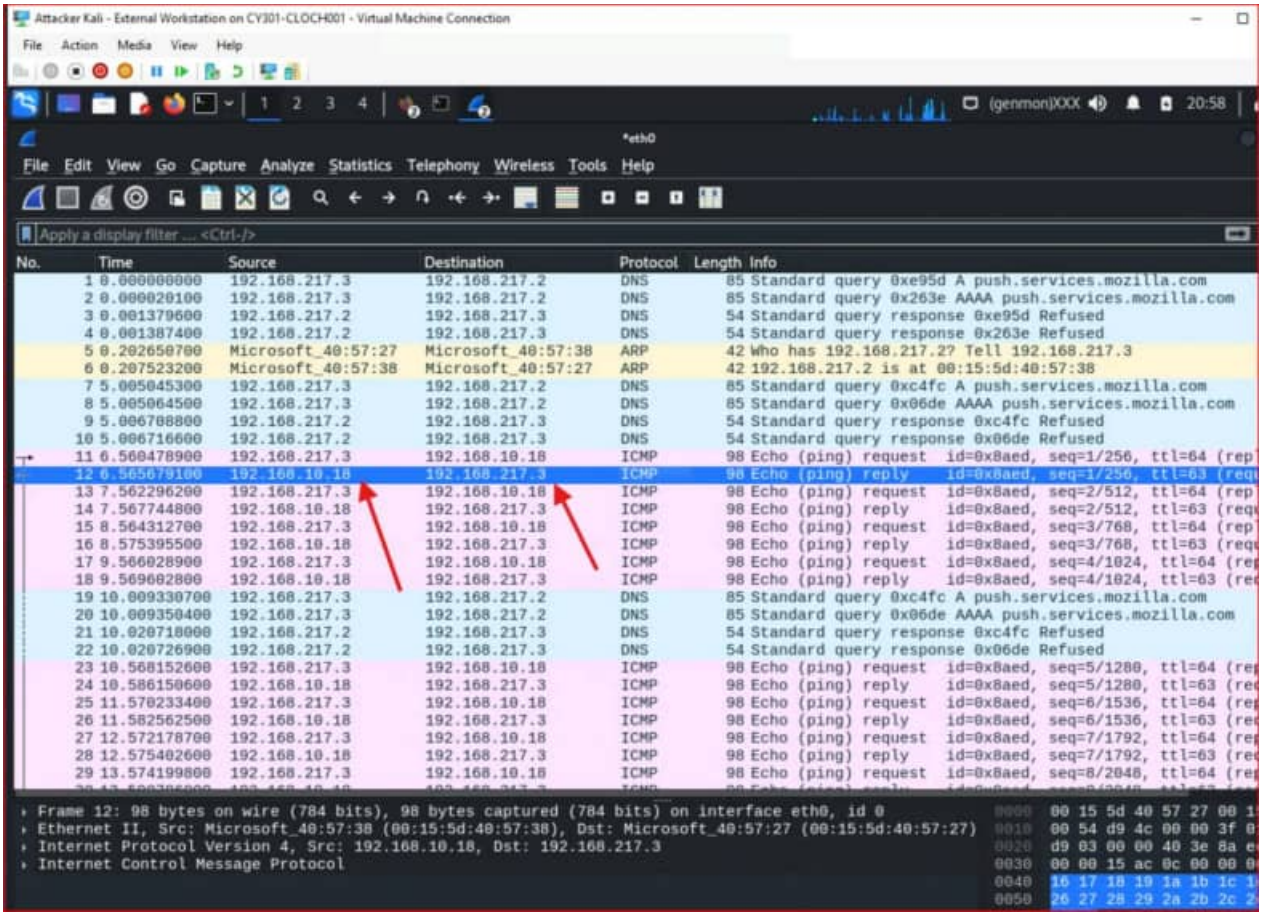




Q3. (5 pts): Select an **Echo (reply)** message from the list. What are the **source** and **destination** IPs of this packet? What are the **sequence** number and the **size** of the **data**? What is the **response** time?

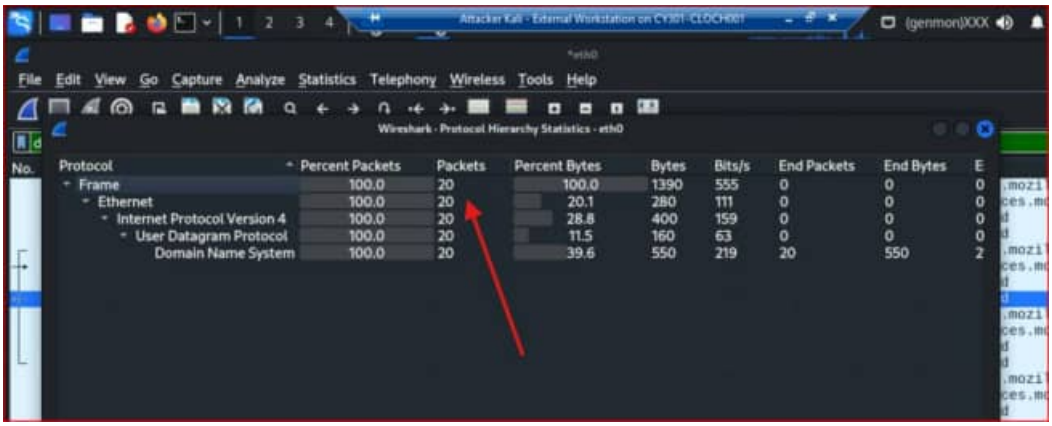
Answer: **Source IP** of the packet: **192.168.217.3**. Destination IP of the packet: **192.168.10.18**. The **sequence number** is **1 (0x0001**) and the size of the **data is 40 bytes**. The **response time** is **5.200 ms.**

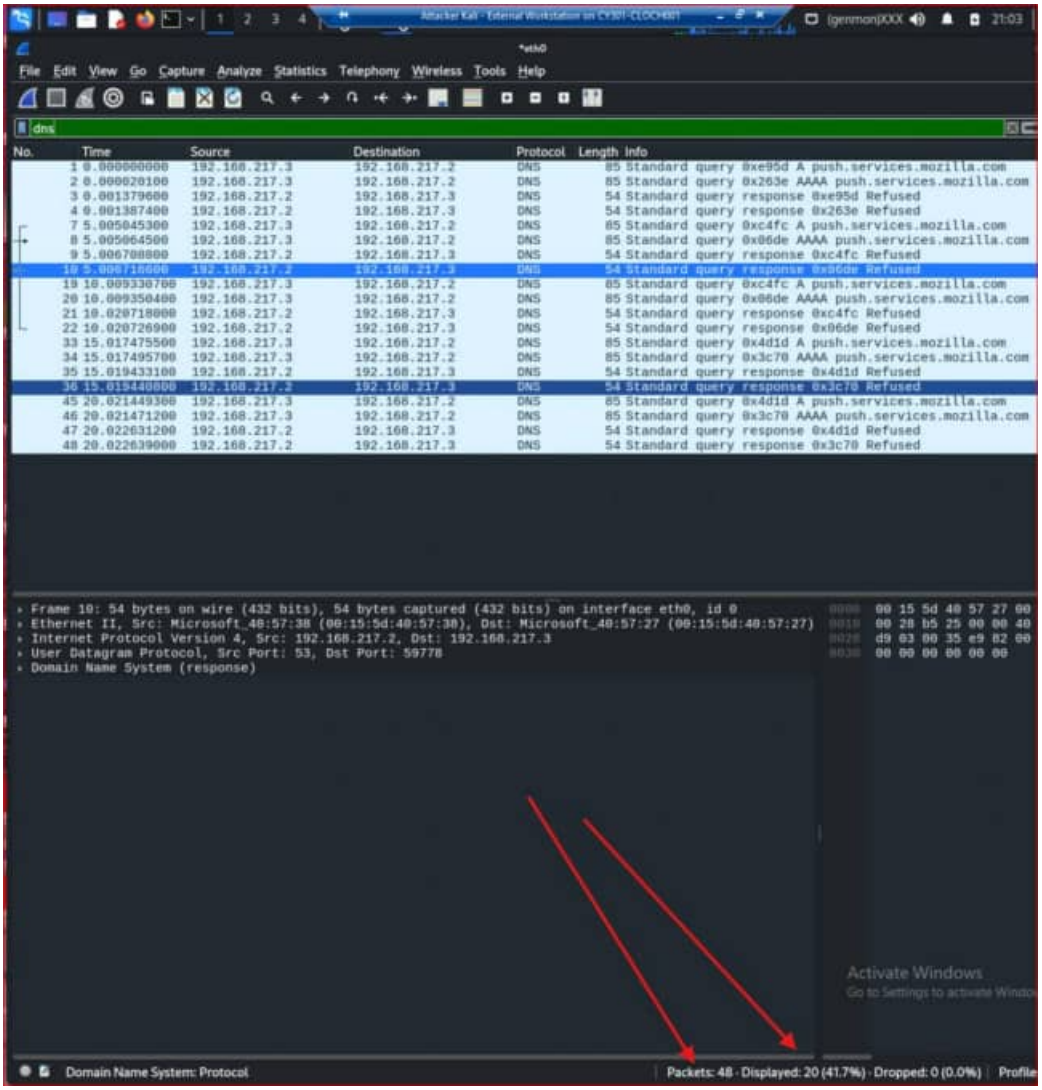
Screenprint:



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

Answer: There are **20 packets displayed** out of 48 total packets.
Screenprint:

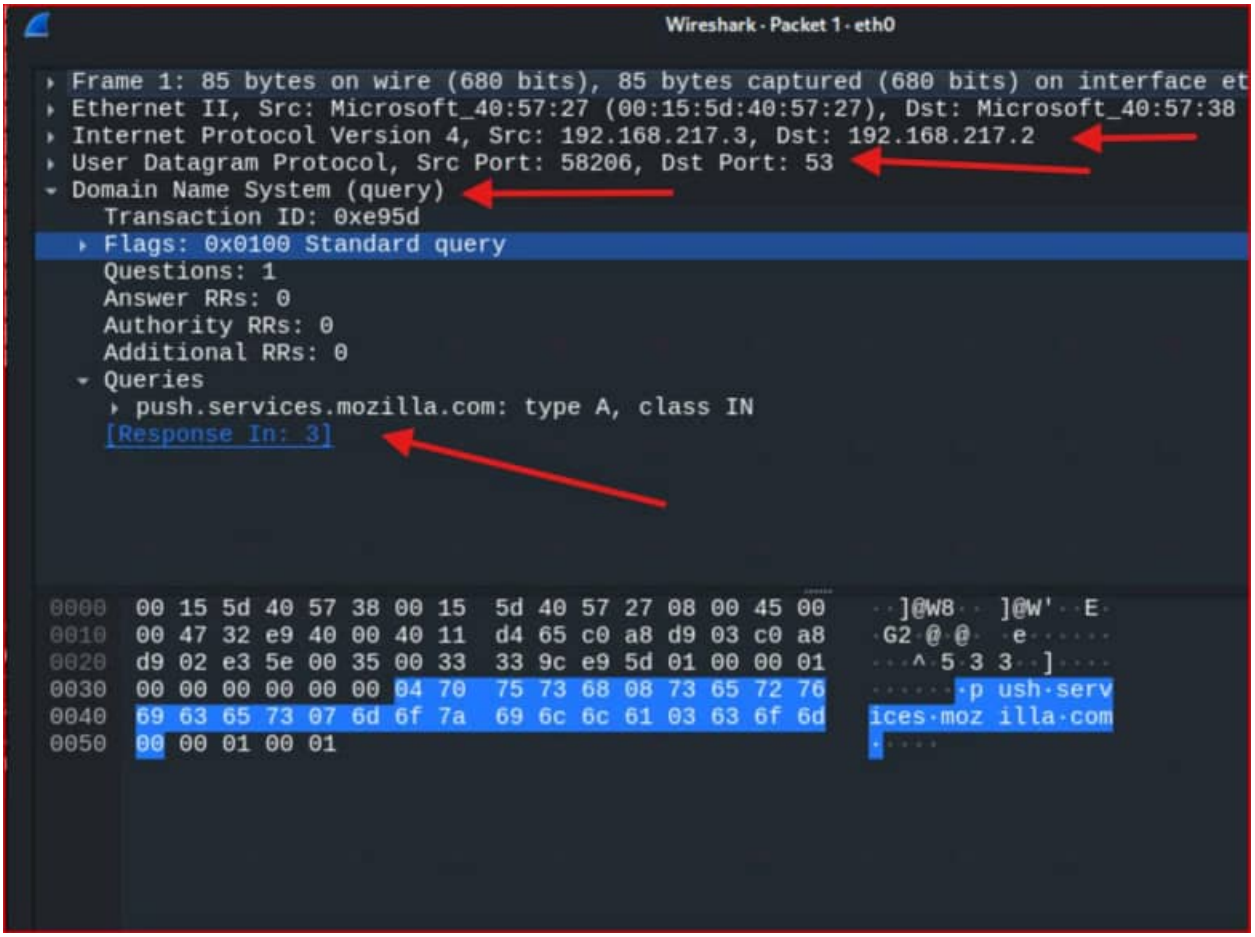




Q5. (5 pts): Find a **DNS** query packet. What is the **domain name** this host is trying to resolve? What is the **source IP** and **port number, destination IP** and **port number**?

Answer: **Domain name** the host is trying to resolve is **push.services.mozilla.com**. The **source IP** is **192.168.217.3** and the **source port number** is **58206**. The **destination IP** is **192.168.217.2** and the **destination port number** is **53**.

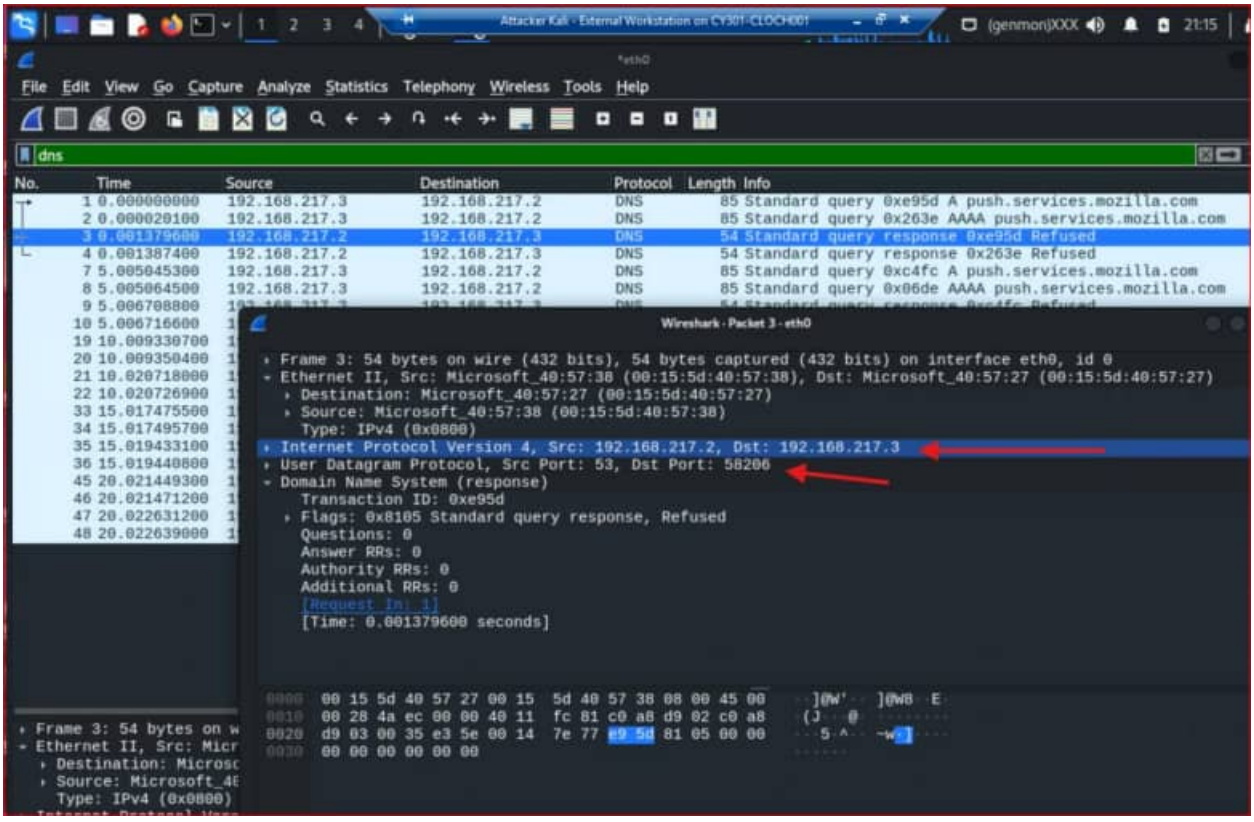
Screenprint:

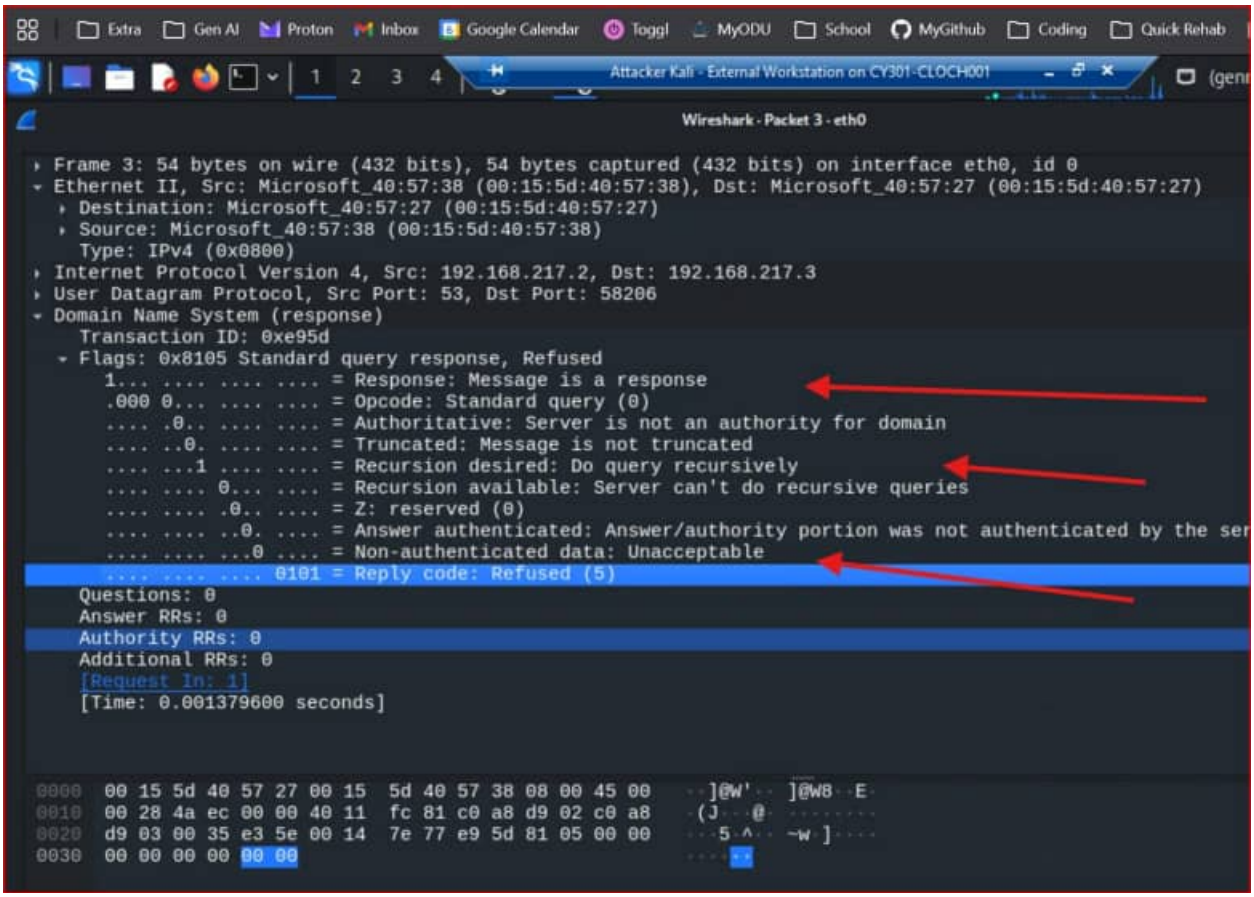


Q6. (5 pts): Find the corresponding (i.e., click **Response In: #)** DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

Answer: The **source IP** is **192.168.217.2** and the **source port number** is **53**. The **destination IP** is **192.168.217.3** and the **destination port number** is **58206**. Lastly, the DNS server replied with "**Reply code: Refused** (5)". The server refused to process the DNS query for push.services.mozilla.com. The response indicates that while the server received the query, it declined to provide an answer. There are **no answer records (Answer RRs: 0)** in the response because the **query was refused rather than resolved**.

Screenprint:




Extra
Gen AI
Proton
Inbox
Google Calendar
Toggl
MyODU
School
MyGithub
Coding
Quick Rehab
Attacker Kali - External Workstation on CY301-CLOCH001
Wireshark · Packet 3 · eth0
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: Microsoft_40:57:38 (00:15:5d:40:57:38), Dst: Microsoft_40:57:27 (00:15:5d:40:57:27)
Destination: Microsoft_40:57:27 (00:15:5d:40:57:27)
Source: Microsoft_40:57:38 (00:15:5d:40:57:38)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
User Datagram Protocol, Src Port: 53, Dst Port: 58206
Domain Name System (response)
Transaction ID: 0xe95d
Flags: 0x8105 Standard query response, Refused
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 0... .... = Recursion available: Server can't do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the ser
....0 .... = Non-authenticated data: Unacceptable
.... 0101 = Reply code: Refused (5)
Questions: 0
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
[Request In: 1]
[Time: 0.001379600 seconds]
0000 00 15 5d 40 57 27 00 15 5d 40 57 38 08 00 45 00
0010 00 28 4a ec 00 00 40 11 fc 81 c0 a8 d9 02 c0 a8
0020 d9 03 00 35 e3 5e 00 14 7e 77 e9 5d 81 05 00 00
0030 00 00 00 00 00 00

Task B: Sniff LAN traffic (70 Points)

In this task, you will be acting as an **ATTACKER** who sniffs the regular communications between peers (External Attacker Kali and Ubuntu) by using Wireshark on **Internal Attacker Kali VM.**

I would recommend you keep the Wireshark running on Internal Kali all the time.

IMPORTANT NOTES!

* Because the current Hyper-V setting in CCIA does not "broadcast" the communication between hosts in the same network, we need to enable port mirroring to allow Internal Kali to "see" communications between External Kali and Ubuntu.

To be specific, you need to put the sniffer (Internal Kali) as the ***mirroring Destination***, and the target VMs are ***mirroring Source*** (See the above Figure 1 under Task-B).

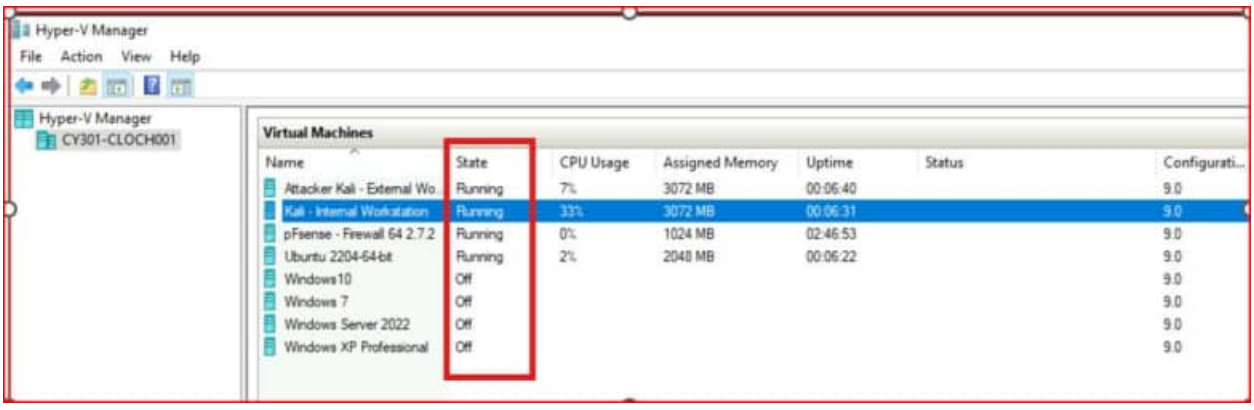
Each VM has two network adapters, one for regular connection and the other for sharing with the CCIA server. We need to configure port mirroring on the first adapter. To be specific,

- Internal Kali: Set Mirroring mode to "**Destination**" in the "**Port Mirroring**"
- Ubuntu Kali: Set Mirroring mode to "**Source**" in the "**Port Mirroring**"
- External Kali: Set Mirroring mode to "**Source**" in the "**Port Mirroring**"

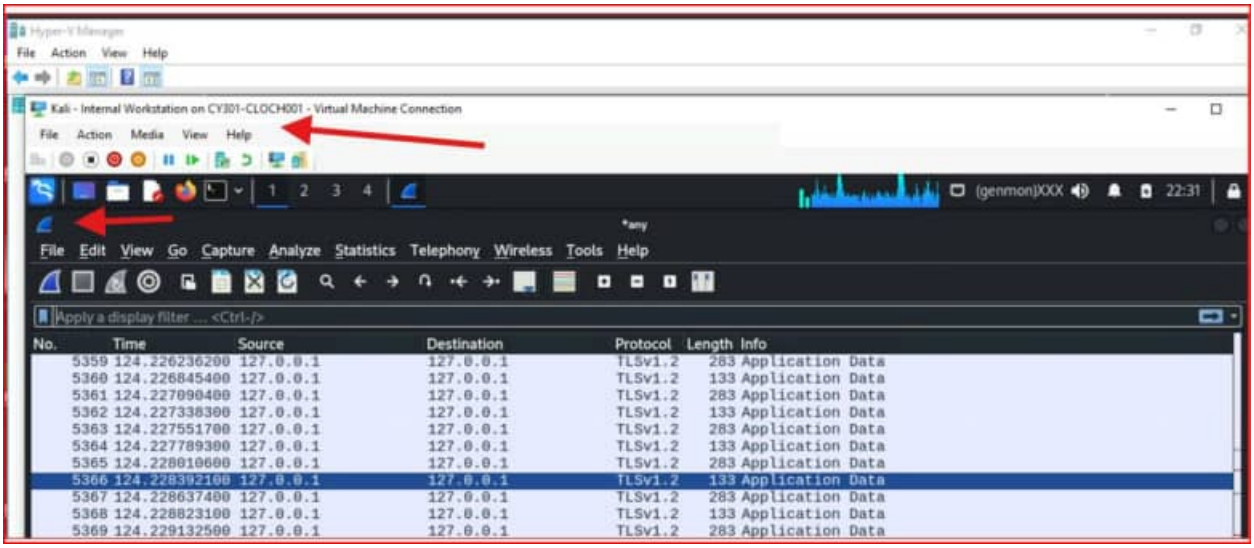
Here is the screenshot showing how to enable Port Mirroring to "source" in External Kali, for your reference. You need to set for Ubuntu and Internal Kali as asked in the instructions above and complete the steps.

1. **Sniff ICMP traffic (5 + 5 + 5 + 15 = 30 points)**
    a. Please turn on **Attacker/External Kali, internal kali, pfsense,** and **Ubuntu**.

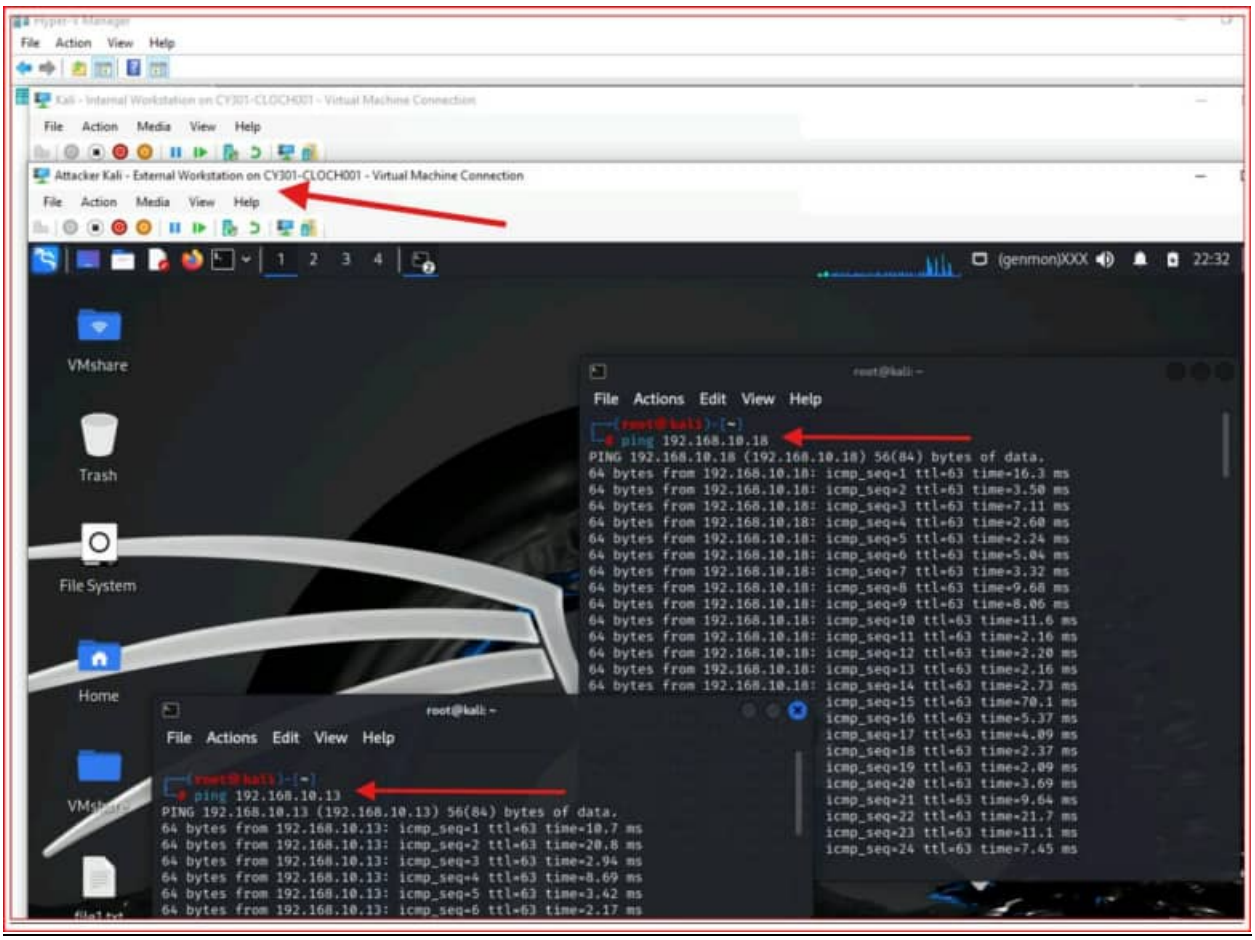
Answer: All four necessary VMs are running.



b. Launch and run Wireshark in Internal Kali (eth0).

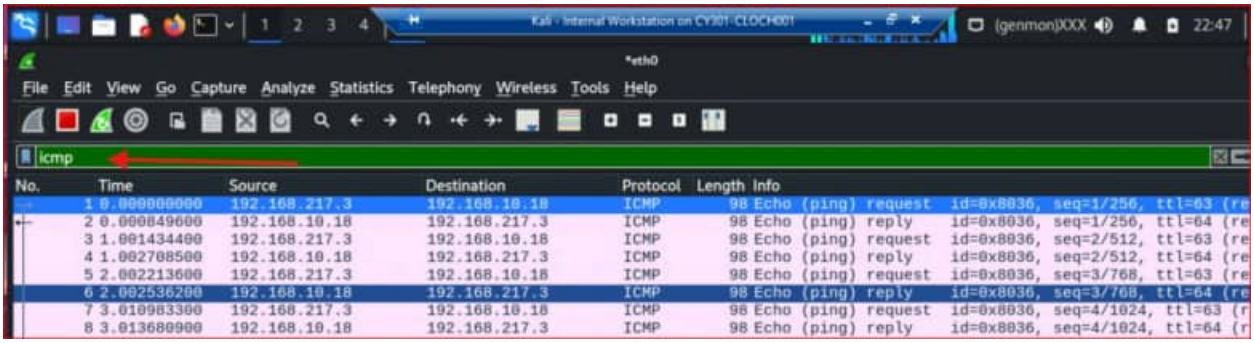


c. Open two terminals on External Kali VM. Use one to ping **Ubuntu VM (192.168.10.18)** and use the other to ping **Internal Kali (192.168.10.13)**.



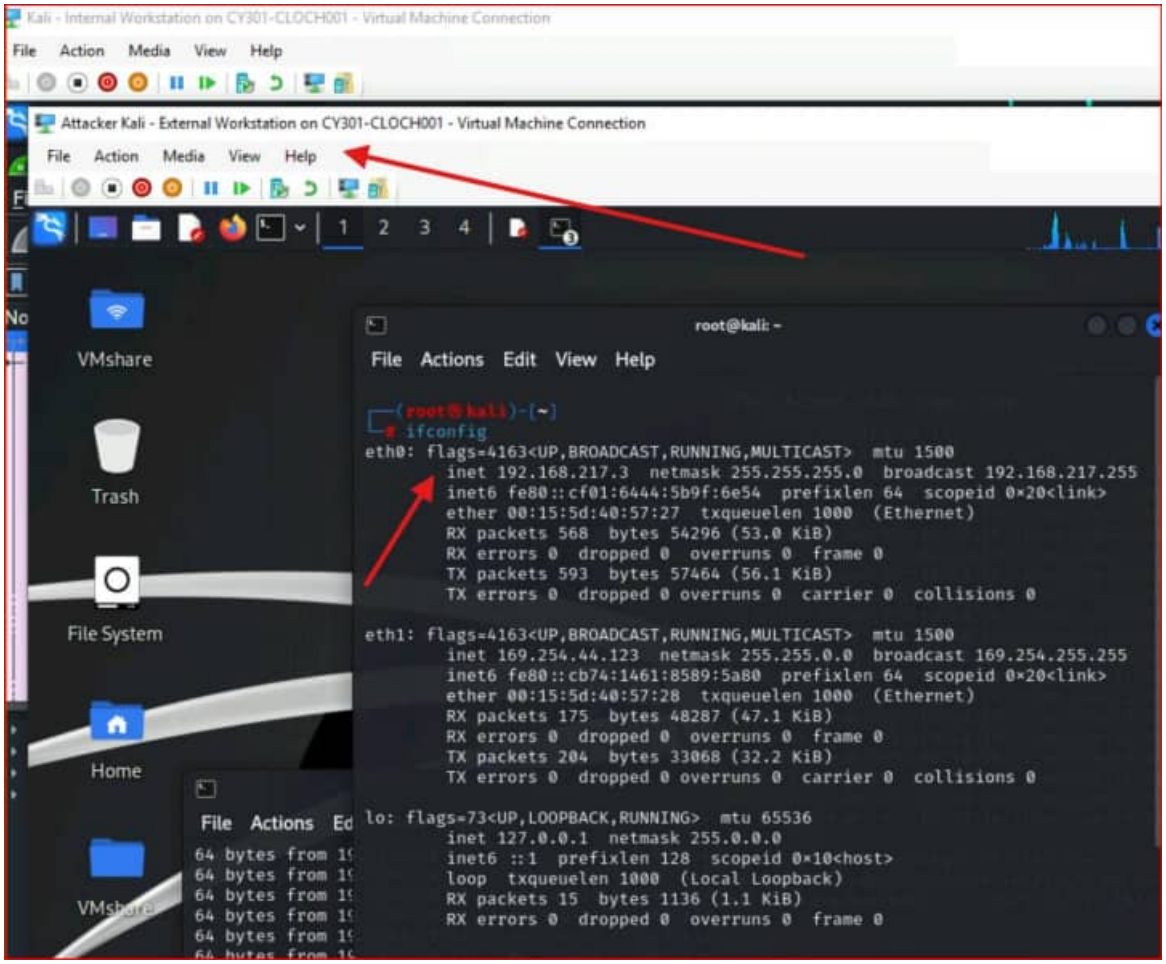
d. Apply proper display or capture filter in Wireshark on **Internal Kali VM** to show active ICMP traffic.

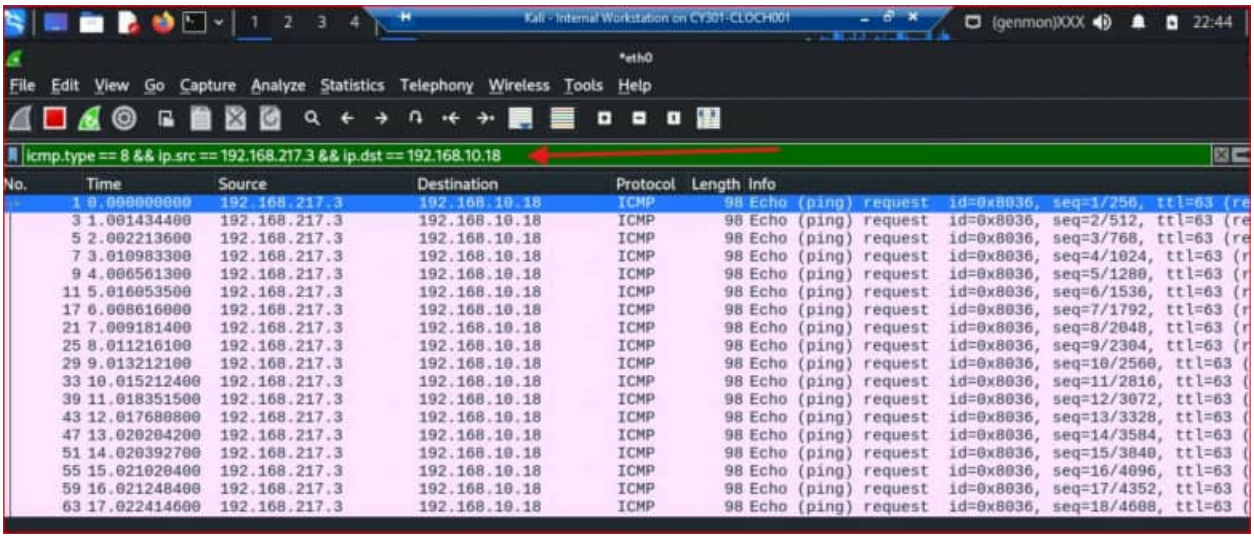
Answer: Filter: icmp



e. 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.

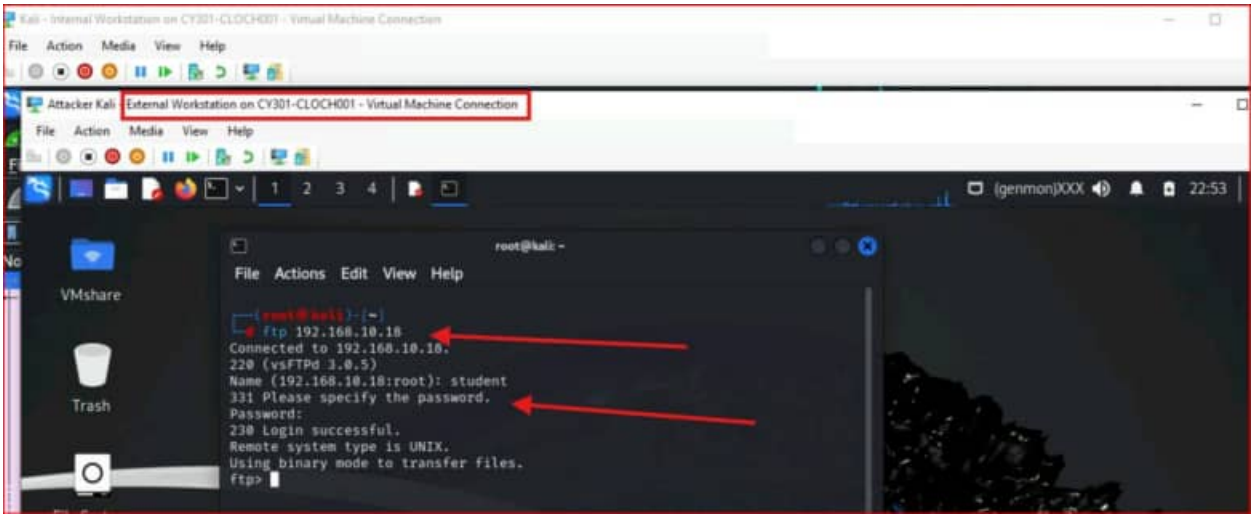
Answer: ***Filter:*** icmp.type == 8 && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18





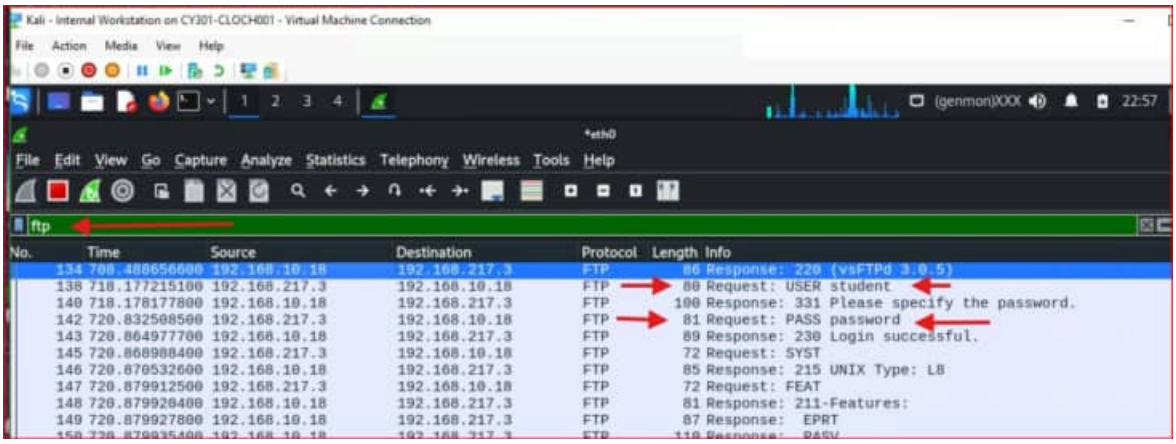
2. **Sniff FTP traffic (10 + 15 + 15 = 40 pts points)**
   a. **Ubuntu VM** is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command**: ftp** [ip_addr of ubuntu VM]. The username for the FTP server is **student**, and the password is **password**.

Answer: ftp 192.168.10.18. I connected to the FTP server running on Ubuntu VM using the command **'ftp 192.168.10.18'** from External Kali. I logged in with **username 'student'** and **password 'password'**, which returned a '230 Login successful' message.



   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.

Answer: As an attacker on Internal Kali VM, I intercepted the FTP traffic using Wireshark with the **'ftp'** display filter. I found the **username** in a packet containing **'USER student'** and the **password** in a packet containing **'PASS password'**. This demonstrates that FTP transmits credentials in **plaintext**, making them easily accessible to anyone monitoring network traffic. Again, the username is 'student' and the password is 'password;' the login was successful.



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.**

Answer: The username is '**cloch001'**, the UIN is **01290201**. Login unsuccessful.