

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 – Traffic Tracing and Sniffing

My Nguyen

01277464

February 19, 2025

Task A: Get started with Wireshark (5 point each x 6 questions = 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.

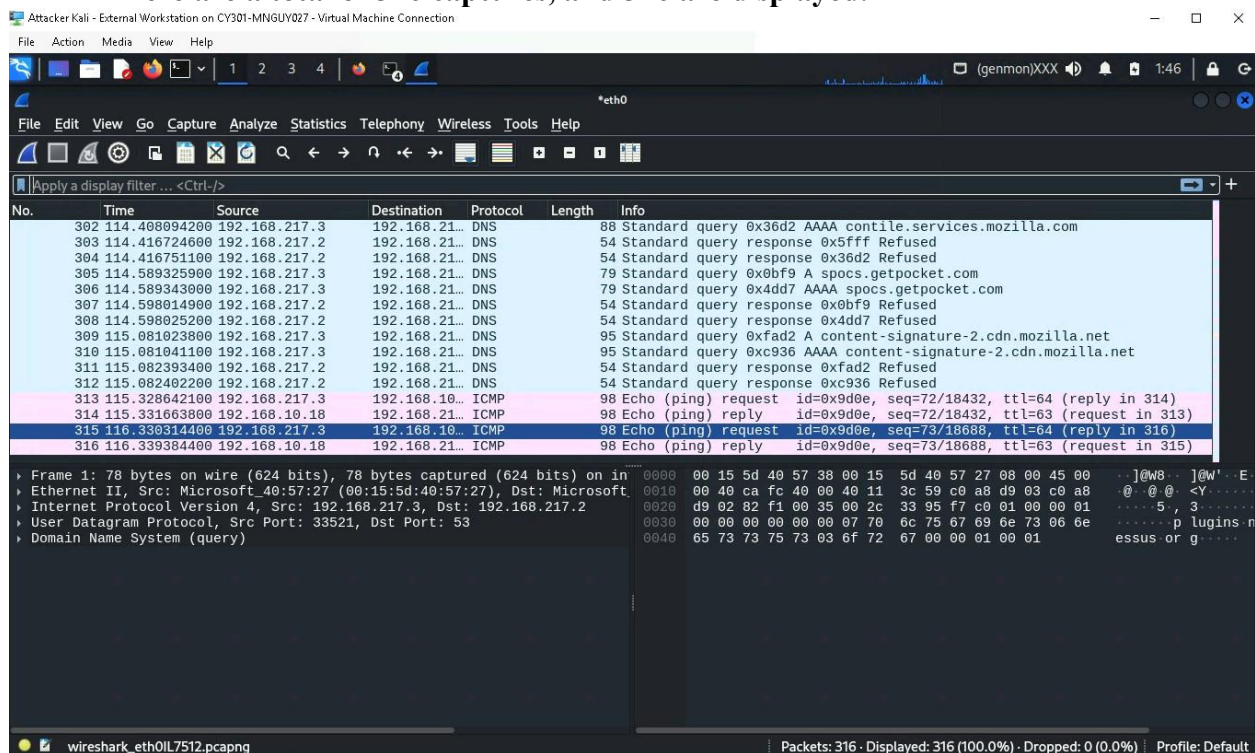
Tip: Please power on the pfsense VM and DO NOT revert to a previous checkpoint. You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface “eth0”.
2. Open a new terminal then ping Ubuntu VM for 5 – 10 seconds.
3. Stop capturing (the red button on the tool bar).

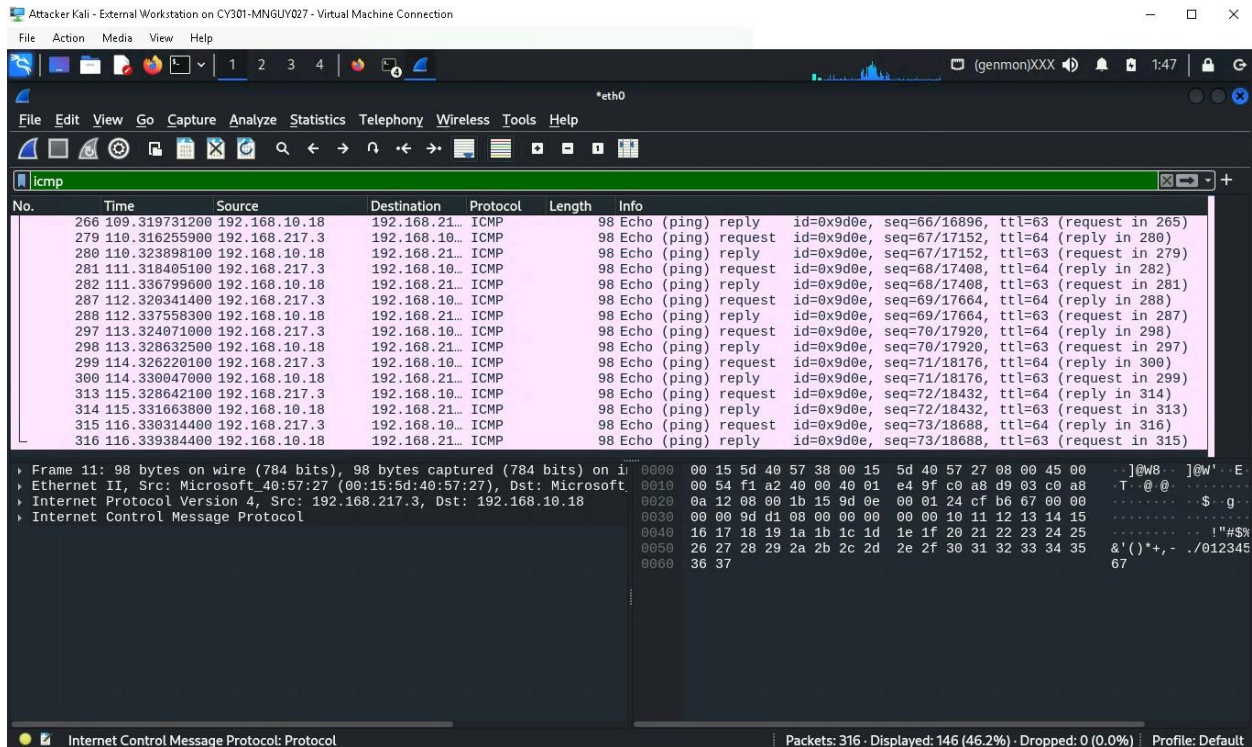
Now, answer the following questions. You need to provide a screenshot that contains the answers to each question

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

There are a total of 316 captures, and 316 are displayed.



2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question **There are a total of 316 captures, and 146 are displayed.**



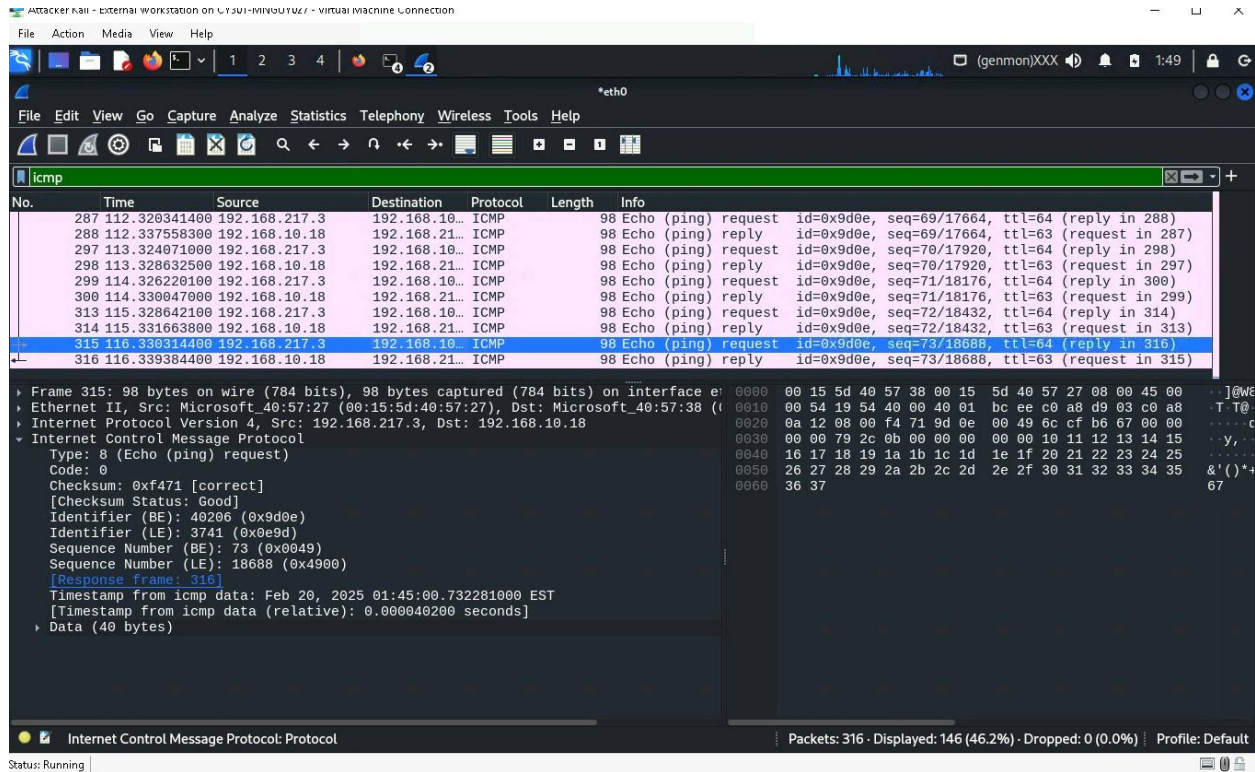
- Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

Source ip: 192.168.217.3 Destination ip: 192.168.10.18

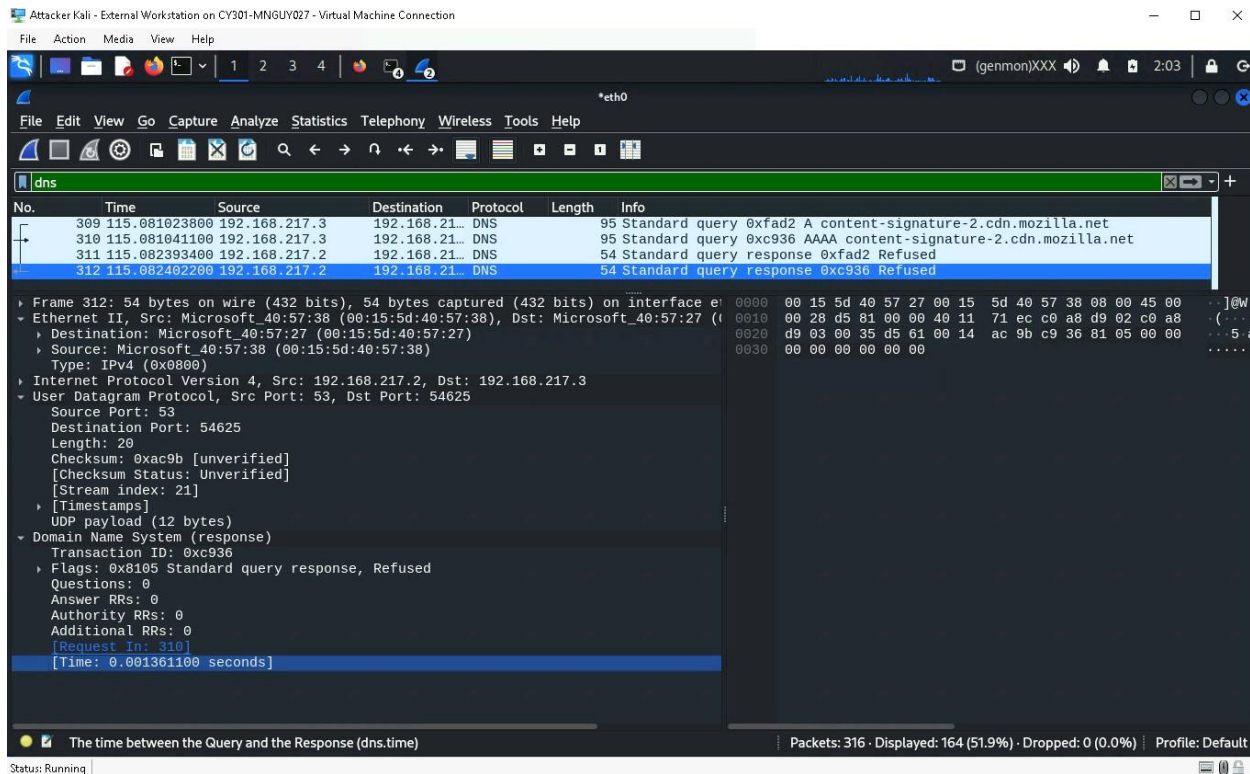
Sequence number: 73

Size: 40 Bytes

Response time: 0.000040200 s



4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed? **There are 164 packets 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?
Domain name: Transaction ID:0xc936
Source ip: 192.168.217.3:54625 Destination: 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: 192.168.217.2:53 Destination: 192.168.217.3:54625. The message from the server says refused.



Task B: Sniff LAN traffic

In this task, you will be acting as an ATTACKER who sniffs the regular communications between peers (External Attacker Kali and Ubuntu) by using either Wireshark or tshark on Internal Attacker Kali VM. I would recommend you keeping the Wireshark/tshark running on Internal Kali all the time.

IMPORTANT NOTES!

* Because the current Hyper-V setting does not “broadcast” the communication between hosts in the same network, we need to enable port mirroring to allow Internal Kali to “see” other's communication. To be specific, you need to put the sniffer (Internal Kali) as the mirroring Destination, and the target VMs are mirroring Source (Figure 2). Since each VM has two network adapters, one for regular connection and the other is 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”

** Since each Windows 10 Host Machine has 20G memory. We need to adjust the assigned Memory for

Internal Kali and External Kali from 8192 to 4096 MB to support 4 VM running simultaneously. Figure 1 Required VMs for this assignment Figure 2 How to configure port mirroring in Hyper-V Select the first

Network Adaptor, then click “Advanced Features”

1. Sniff ICMP traffic (10 + 10 = 20 points)

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

The screenshot shows the Wireshark interface with the following data:

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|--|
| 44 | 21.831626900 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1442/41477, ttl=64 (request ... |
| 45 | 22.034581700 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1443/41733, ttl=63 (reply in... |
| 46 | 22.034589700 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1443/41733, ttl=64 (request ... |
| 47 | 23.035302300 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1444/41989, ttl=63 (reply in... |
| 48 | 23.035312900 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1444/41989, ttl=64 (request ... |
| 49 | 24.037617800 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1445/42245, ttl=63 (reply in... |
| 50 | 24.038128000 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1445/42245, ttl=64 (request ... |
| 51 | 25.038286400 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1446/42501, ttl=63 (reply in... |
| 52 | 25.040325400 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1446/42501, ttl=64 (request ... |
| 53 | 26.039830500 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1447/42757, ttl=63 (reply in... |
| 54 | 26.039837800 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1447/42757, ttl=64 (request ... |
| 55 | 27.045772800 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1448/43013, ttl=63 (reply in... |
| 56 | 27.046560300 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1448/43013, ttl=64 (request ... |
| 57 | 28.044123200 | 192.168.217.3 | 192.168.10.18 | ICMP | 98 | Echo (ping) request id=0x9d0e, seq=1449/43269, ttl=63 (reply in... |
| 58 | 28.044146700 | 192.168.10.18 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0x9d0e, seq=1449/43269, ttl=64 (request ... |

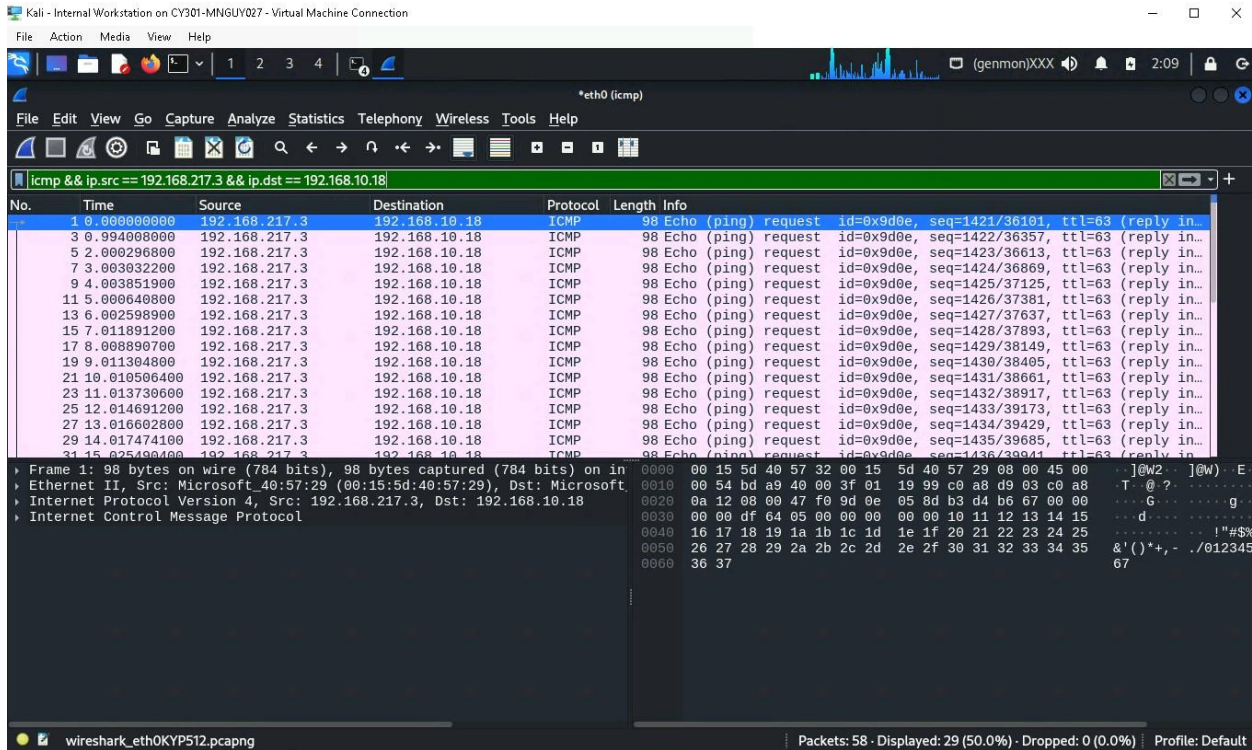
Packet details for Frame 1:

- Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface eth0
- Ethernet II, Src: Microsoft_08:00:00:00:00:00 (08:00:00:00:00:00), Dst: Microsoft_08:00:00:00:00:00
- Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
- Internet Control Message Protocol

Hex dump and ASCII view of the ICMP Echo (ping) request:

```
0000 00 15 5d 40 57 32 00 15 5d 40 57 29 08 00 45 00  ..]@w2... ]@W)  E
0001 00 54 bd a9 40 00 3f 01 19 99 c0 a8 d9 03 c0 a8  T.@? .....
0002 0a 12 08 00 47 f0 9d 0e 05 8d b3 d4 b6 67 00 00  ..d.....g....
0003 00 00 df 64 05 00 00 00 00 00 10 11 12 13 14 15  ....d.....!#$%
0004 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ....&'()*+,-./012345
0005 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  ....67
0006 36 37
```

B. Apply proper display or capture filter on Internal Kali VM that ONLY displays ICMP request originated from External Kali VM and goes to Ubuntu 64-bit VM



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

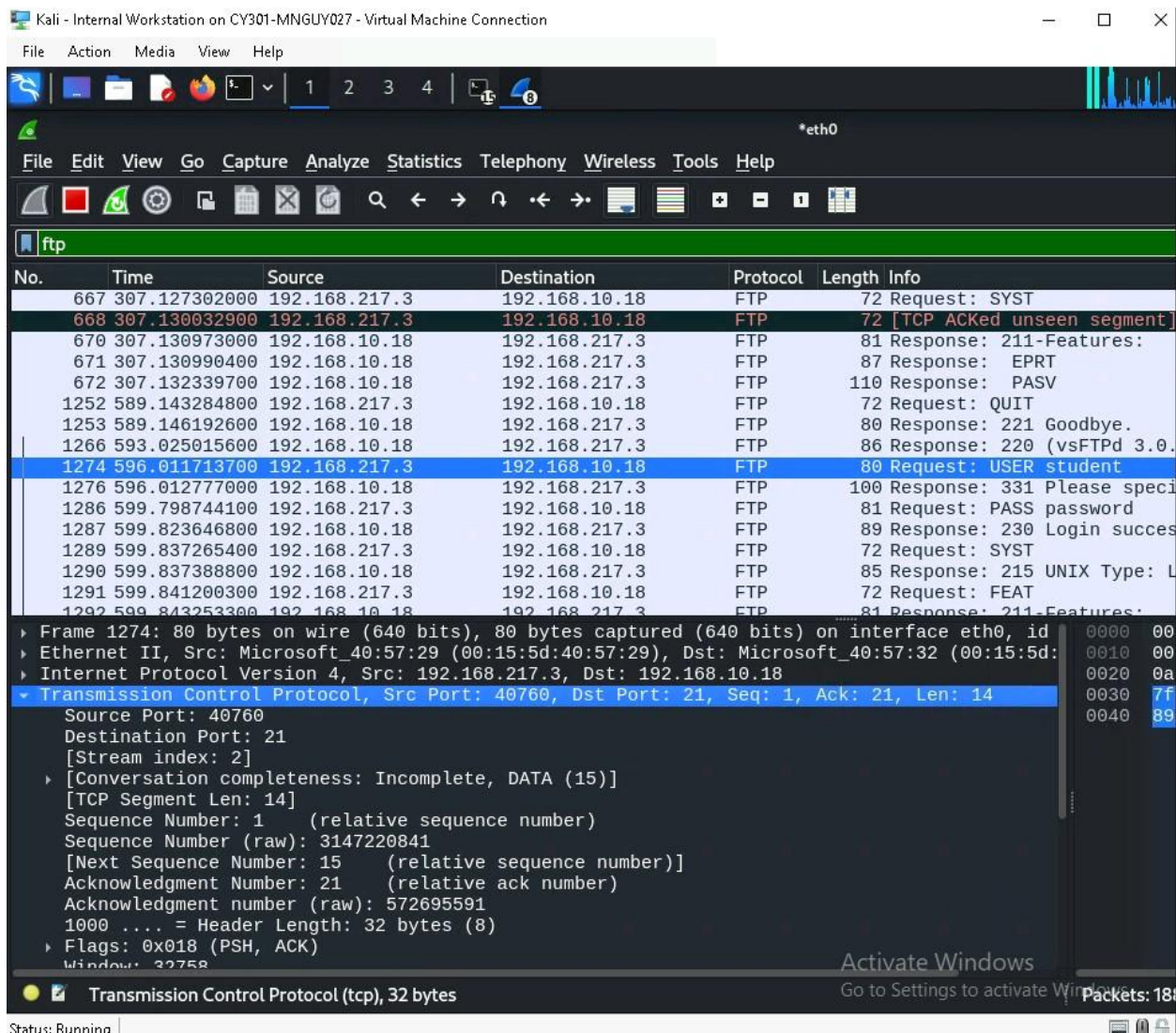
- A. Ubuntu VM is also serving as an FTP server inside the LAN network. Now, you need to use External Kali to access this FTP server by using the command: `ftp [ip_addr of ubuntu VM]`. The username for the FTP server is `cyse301`, and the password is `password`. You can follow the steps below to access the FTP server.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.

(root@kali)-[~]
#
```

- B. Unfortunately, Internal Kali, the attacker, is also sniffing to 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 screenshot and explain how you find the password.



FTP is an unencrypted protocol, meaning login credentials are sent in plain text. By sniffing traffic on Internal Kali, we intercepted the FTP login request. Using Wireshark, we captured the USER and PASS commands. The password “password” was visible in clear text in the packet capture.

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-MNGUY027 - Virtual Machine Connection

File Action Media View Help

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ftp

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------|---------------|---------------|----------|--------|----------------------------|
| 2092 | 974.348728100 | 192.168.217.3 | 192.168.10.18 | FTP | 80 | Request: USER student |
| 2094 | 974.349754600 | 192.168.10.18 | 192.168.217.3 | FTP | 100 | Response: 331 Please speci |
| 2102 | 977.685908500 | 192.168.217.3 | 192.168.10.18 | FTP | 81 | Request: PASS password |
| 2103 | 977.704968000 | 192.168.10.18 | 192.168.217.3 | FTP | 89 | Response: 230 Login succes |
| 2105 | 977.710837100 | 192.168.217.3 | 192.168.10.18 | FTP | 72 | Request: SYST |
| 2106 | 977.710844900 | 192.168.10.18 | 192.168.217.3 | FTP | 85 | Response: 215 UNIX Type: L |
| 2107 | 977.716062100 | 192.168.217.3 | 192.168.10.18 | FTP | 72 | Request: FEAT |
| 2108 | 977.716858700 | 192.168.10.18 | 192.168.217.3 | FTP | 81 | Response: 211-Features: |
| 2109 | 977.716866300 | 192.168.10.18 | 192.168.217.3 | FTP | 87 | Response: EPRT |
| 2111 | 977.720213500 | 192.168.10.18 | 192.168.217.3 | FTP | 110 | Response: PASV |
| 2282 | 1058.0853357... | 192.168.10.18 | 192.168.217.3 | FTP | 86 | Response: 220 (vsFTPd 3.0. |
| 2294 | 1063.5434459... | 192.168.217.3 | 192.168.10.18 | FTP | 81 | Request: USER mnguy027 |
| 2296 | 1063.5443971... | 192.168.10.18 | 192.168.217.3 | FTP | 100 | Response: 331 Please speci |
| 2356 | 1092.3830361... | 192.168.217.3 | 192.168.10.18 | FTP | 81 | Request: PASS 01277464 |
| 2364 | 1096.0452236... | 192.168.10.18 | 192.168.217.3 | FTP | 88 | Response: 530 Login incorr |

▶ Frame 2294: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0000 00
 ▶ Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft_40:57:32 (00:15:5d: 0010 00
 ▶ Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18 0020 0a
 ▶ Transmission Control Protocol, Src Port: 40210, Dst Port: 21, Seq: 1, Ack: 21, Len: 15 0030 7f
 Source Port: 40210 0040 a1
 Destination Port: 21 0050 0a
 [Stream index: 4]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 15]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1243834941
 [Next Sequence Number: 16 (relative sequence number)]
 Acknowledgment Number: 21 (relative ack number)
 Acknowledgment number (raw): 3546433030
 1000 ... = Header Length: 32 bytes (8)
 ▶ Flags: 0x018 (PSH, ACK)
 Window: 32768

Transmission Control Protocol (tcp), 32 bytes

Status: Running

Packets: 24

Task C – Extra credit: Steal files with Wireshark (15 points)

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.

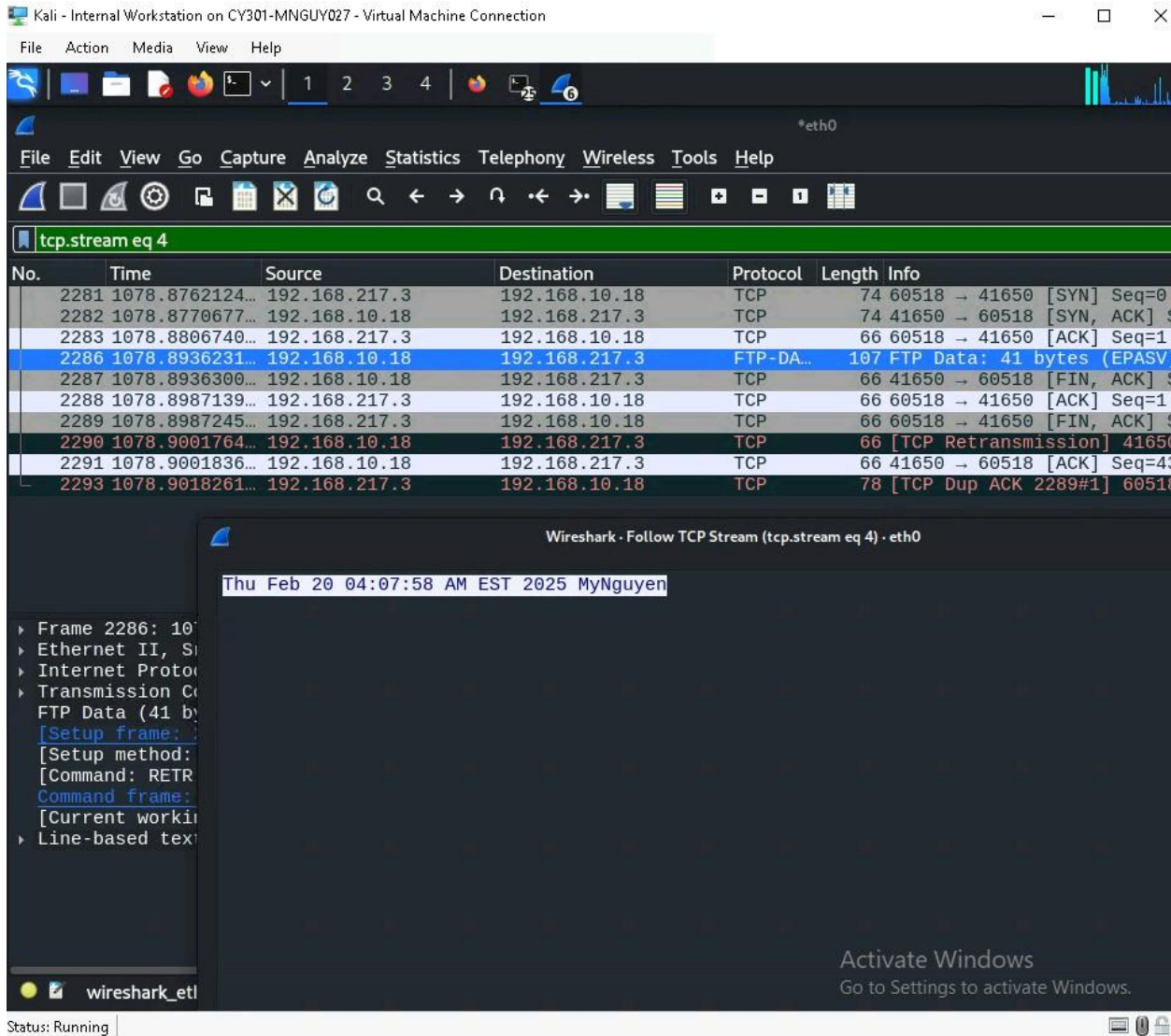
```
student@ubuntu: ~
student@ubuntu:~$ echo -e "$(date) MyNguyen" > mnguy027.txt
student@ubuntu:~$ ls
Desktop  Downloads          mnguy027.txt  Pictures  snap  Videos
Documents  examples.desktop  Music        Public    Templates  VMshare
student@ubuntu:~$ cat mnguy027.txt
Thu Feb 20 04:07:58 AM EST 2025 MyNguyen
student@ubuntu:~$
```

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.

```
root@kali: ~
File Actions Edit View Help
Destination Protocol Length Info
(root@kali)-[~]
# ftp 192.168.10.18
Connected to 192.168.10.18.
220 (vsFTPd 3.0.5)
Name (192.168.10.18:root): student
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get mnguy027.txt
local: mnguy027.txt remote: mnguy027.txt
229 Entering Extended Passive Mode (|||41650|)
150 Opening BINARY mode data connection for mnguy027.txt (41 bytes).
100% |*****| 41 400.39 KiB/s 00:00 ETA
226 Transfer complete.
41 bytes received in 00:00 (6.37 KiB/s)
ftp>
```

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. Below is an example.

