

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?

The screenshot shows the Wireshark interface with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
19	7.827292800	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0
20	8.827171700	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request id=0
21	8.829314000	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply id=0
22	10.782834400	192.168.217.3	192.168.217.2	DNS	78	Standard query 0xc2f1 A p
23	10.782845300	192.168.217.3	192.168.217.2	DNS	78	Standard query 0xf7f0 AAA
24	10.783884500	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0
25	10.783893900	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0
26	15.783736500	192.168.217.3	192.168.217.2	DNS	78	Standard query 0xc2f1 A p
27	15.783762500	192.168.217.3	192.168.217.2	DNS	78	Standard query 0xf7f0 AAA
28	15.796566700	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0
29	15.796574400	192.168.217.2	192.168.217.3	DNS	54	Standard query response 0

Packet details for Frame 1:

- Frame 1: 62 bytes on wire (496 bits), 62 bytes captured on interface eth0
- Ethernet II, Src: Microsoft\_40:57:27 (00:15:5d:40:57:27), Dst: 08:00:00:00:00:00
- Internet Protocol Version 6, Src: fe80::cf01:6444:5b00:0000, Dst: fe80::9f6e:54ff:0000:0000
- Internet Control Message Protocol v6, Type: Echo (ping) reply

Wireshark status bar: Packets: 29 · Displayed: 29 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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)

Attacker Kali - External Workstation on CY301-RALAR002 - Virtual Machine Connection

File Action Media View Help

Wireshark - Protocol Hierarchy Statistics - eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	29	100.0	2438	1,234
Ethernet	100.0	29	16.7	406	205
Internet Protocol Version 6	3.4	1	1.6	40	20
Internet Control Message Protocol v6	3.4	1	0.3	8	4
Internet Protocol Version 4	89.7	26	21.3	520	263
User Datagram Protocol	27.6	8	2.6	64	32
Domain Name System	27.6	8	7.9	192	97
Internet Control Message Protocol	62.1	18	47.3	1152	583
Address Resolution Protocol	6.9	2	2.3	56	28

No display filter.

Close Copy Protocols Help

Internet Control Message Protocol: Protocol      Packets: 29 · Displayed: 29 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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?

The screenshot shows the Wireshark interface with packet 3 selected. The packet list pane on the left shows the following details:

No.	Time
1	0.000000000
2	0.802334400
3	0.805707400
4	1.804316900
5	1.820926200
6	2.816497900
7	2.818612200
8	3.818096200
9	3.827374600
10	4.819889500
11	4.821621900
12	5.821268800
13	5.840913600

The packet details pane for packet 3 shows the following structure:

- Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 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)
- Internet Protocol Version 4, Src: 192.168.10.18, Dst: 192.168.217.3
- Internet Control Message Protocol

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 15 5d 40 57 27 00 15 5d 40 57 38 08 00 45 00  --]@w'-- ]@w8-E-
0010 00 54 12 c4 00 00 3f 01 04 7f c0 a8 0a 12 c0 a8  .T....?.....
0020 d9 03 00 00 15 29 7f 41 00 01 c7 a8 f9 66 00 00  .....)A....f..
0030 00 00 e1 b1 0a 00 00 00 00 00 10 11 12 13 14 15  .....)A....f..
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....)A....f..
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 67
```

The packet bytes pane also shows the following information:

- Internet Protocol Version 4 (ip), 20 bytes
- Show packet bytes

The status bar at the bottom of the window shows: Packets: 29 - Displayed: 29 (100.0%) - Dropped: 0 (0.0%) Profile: Default

Source IP: 192.168.10.18  
Destination IP: 192.168.217.3

Attacker Kali - External Workstation on CY301-RALAR002 - Virtual Machine Connection

File Action Media View Help

Wireshark - Packet 3 - eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time
1	0.000000000
2	0.802334400
3	0.805707400
4	1.804316900
5	1.820926200
6	2.816497900
7	2.818612200
8	3.818096200
9	3.827374600
10	4.819889500
11	4.821621900
12	5.821268800
13	5.840913600

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 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)  
Internet Protocol Version 4, Src: 192.168.10.18, Dst: 192.168.217.3  
Internet Control Message Protocol  
Type: 0 (Echo (ping) reply)  
Code: 0  
Checksum: 0x1529 [correct]  
[Checksum Status: Good]  
Identifier (BE): 32577 (0x7f41)  
Identifier (LE): 16767 (0x417f)  
Sequence Number (BE): 1 (0x0001)  
Sequence Number (LE): 256 (0x0100)  
[Request frame: 2]  
[Response time: 3.373 ms]  
Timestamp from icmp data: Sep 29, 2024 15:21:43.700897000 EDT  
[Timestamp from icmp data (relative): 0.003404700 seconds]  
Data (40 bytes)

```
0020 d9 03 00 00 15 29 7f 41 00 01 c7 a8 f9 66 00 00  ....)-A . . . . f . .
0030 00 00 e1 b1 0a 00 00 00 00 00 10 11 12 13 14 15  . . . . .
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  . . . . . !"#$$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
```

Sequence Number (big endian representation) (icmp.seq), 2 bytes

✓ Show packet bytes

Close Help

Internet Control Message Protocol: Protocol

Packets: 29 - Displayed: 29 (100.0%) - Dropped: 0 (0.0%) Profile: Default

**Sequence numbers: 0x0001 and 0x0100**

**Data size: 40 bytes**

Attacker Kali - External Workstation on CY301-RALAR002 - Virtual Machine Connection

File Action Media View Help

Wireshark - Packet 3 - eth0

No.	Time
1	0.000000000
2	0.802334400
3	0.805707400
4	1.804316900
5	1.820926200
6	2.816497900
7	2.818612200
8	3.818096200
9	3.827374600
10	4.819889500
11	4.821621900
12	5.821268800
13	5.840913600

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 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)  
Internet Protocol Version 4, Src: 192.168.10.18, Dst: 192.168.217.3  
Internet Control Message Protocol  
Type: 0 (Echo (ping) reply)  
Code: 0  
Checksum: 0x1529 [correct]  
[Checksum Status: Good]  
Identifier (BE): 32577 (0x7f41)  
Identifier (LE): 16767 (0x417f)  
Sequence Number (BE): 1 (0x0001)  
Sequence Number (LE): 256 (0x0100)  
[Request frame: 2]  
[Response time: 3.373 ms]  
Timestamp from icmp data: Sep 29, 2024 15:21:43.700897000 EDT  
[Timestamp from icmp data (relative): 0.003404700 seconds]  
Data (40 bytes)

0030	00 00 e1 b1 0a 00 00 00 00 00	10 11 12 13 14 15	.....
0040	16 17 18 19 1a 1b 1c 1d 1e 1f	20 21 22 23 24 25	..... !"#\$%
0050	26 27 28 29 2a 2b 2c 2d 2e 2f	30 31 32 33 34 35	&'()*+,-./012345
0060	36 37		67

No.: 3 · Time: 0.805707400 · Source: 192.168.10.18 · Destination: 192.168.217....h: 98 · Info: Echo (ping) reply id=0x7f41, seq=1/256, ttl=63 (request in 2)

✓ Show packet bytes

Close Help

Internet Control Message Protocol: Protocol      Packets: 29 · Displayed: 29 (100.0%) · Dropped: 0 (0.0%)      Profile: Default

Response time: 3.373 ms

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

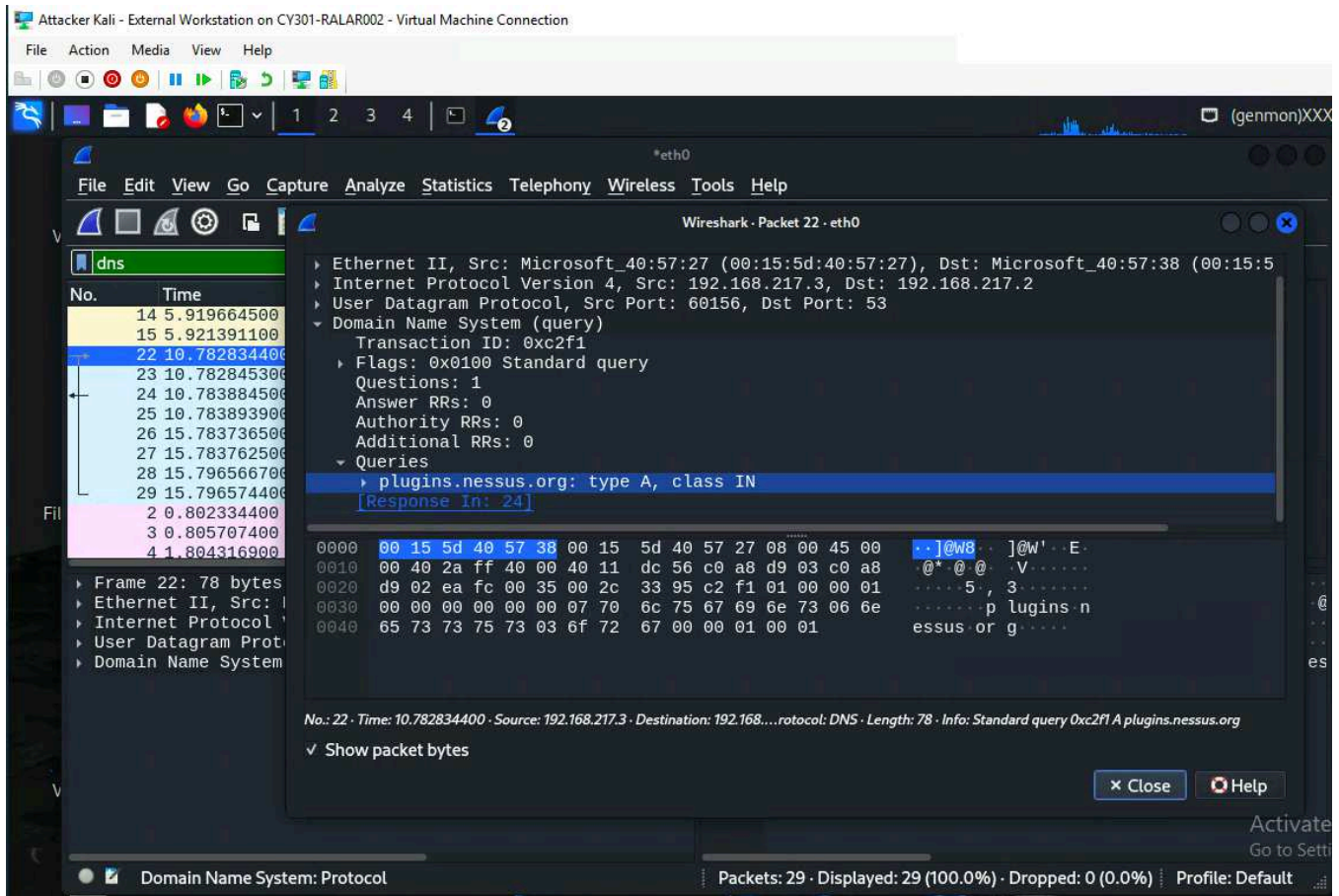
The screenshot shows the Wireshark interface with a display filter of 'dns' applied. The packet list on the left shows several packets, with packet 3 selected. The protocol hierarchy statistics table on the right shows the following data:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s
Frame	100.0	29	100.0	2438	1,234
Ethernet	100.0	29	16.7	406	205
Internet Protocol Version 6	3.4	1	1.6	40	20
Internet Control Message Protocol v6	3.4	1	0.3	8	4
Internet Protocol Version 4	89.7	26	21.3	520	263
User Datagram Protocol	27.6	8	2.6	64	32
Domain Name System	27.6	8	7.9	192	97
Internet Control Message Protocol	62.1	18	47.3	1152	583
Address Resolution Protocol	6.9	2	2.3	56	28

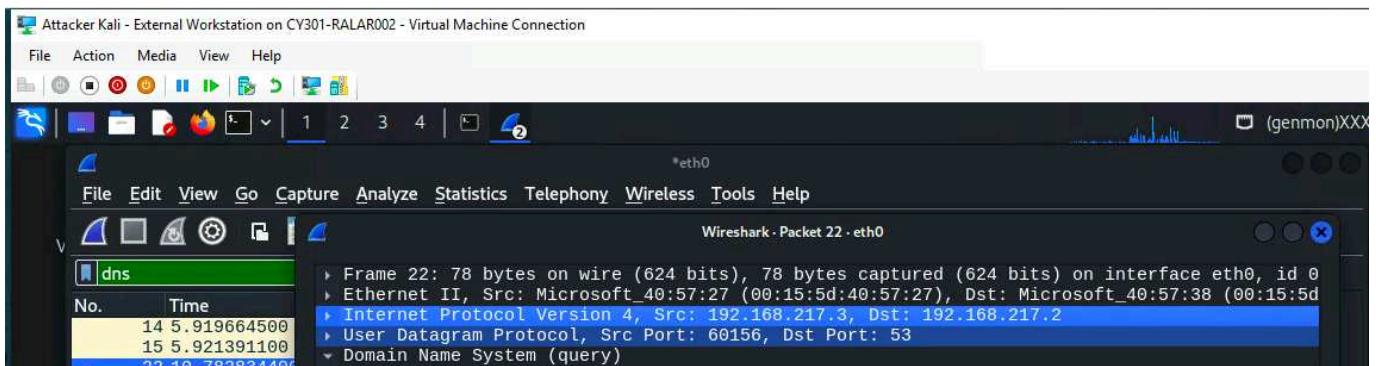
The status bar at the bottom indicates: Packets: 29 · Displayed: 29 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

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?

The screenshot shows the Wireshark interface with the following details:

- Packet List:** Packet 24 is selected, showing a Domain Name System (response) with a transaction ID of 0xc2f1.
- Packet Details:** The selected packet is a Domain Name System (response) with the following structure:
  - Transaction ID: 0xc2f1
  - Flags: 0x8105 Standard query response, Refused
  - Questions: 0
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - [Request In: 22]
  - [Time: 0.001050100 seconds]
- Packet Bytes:** The raw data of the packet is displayed in hexadecimal and ASCII. The first 20 bytes correspond to the IP header and payload, showing the source IP 192.168.217.2 and destination IP 192.168.217.3.

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

Attacker Kali - External Workstation on CY301-RALAR002 - Virtual Machine Connection

File Action Media View Help

Wireshark · Packet 24 · eth0

No.	Time
14	5.919664500
15	5.921391100
22	10.782834400
23	10.782845300
24	10.783884500
25	10.783893900
26	15.783736500
27	15.783762500
28	15.796566700
29	15.796574400
2	0.802334400
3	0.805707400
4	1.804316900

Frame 24: 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)
- Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
- User Datagram Protocol, Src Port: 53, Dst Port: 60156
- Domain Name System (response)
  - Transaction ID: 0xc2f1
  - Flags: 0x8105 Standard query response, Refused
  - Questions: 0
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - [Request In: 22]
  - [Time: 0.001050100 seconds]

```
0000  00 15 5d 40 57 27 00 15 5d 40 57 38 08 00 45 00  ..]@W'.. ]@W8..E.
0010  00 28 97 f6 00 00 40 11 af 77 c0 a8 d9 02 c0 a8  -(...@..w.....
0020  d9 03 00 35 ea fc 00 14 9d 45 c2 f1 81 05 00 00  ..5...E...
0030  00 00 00 00 00 00
```

Flags (dns.flags), 2 bytes

Show packet bytes

Close Help

Domain Name System: Protocol

Packets: 29 · Displayed: 29 (100.0%) · Dropped: 0 (0.0%) Profile: Default

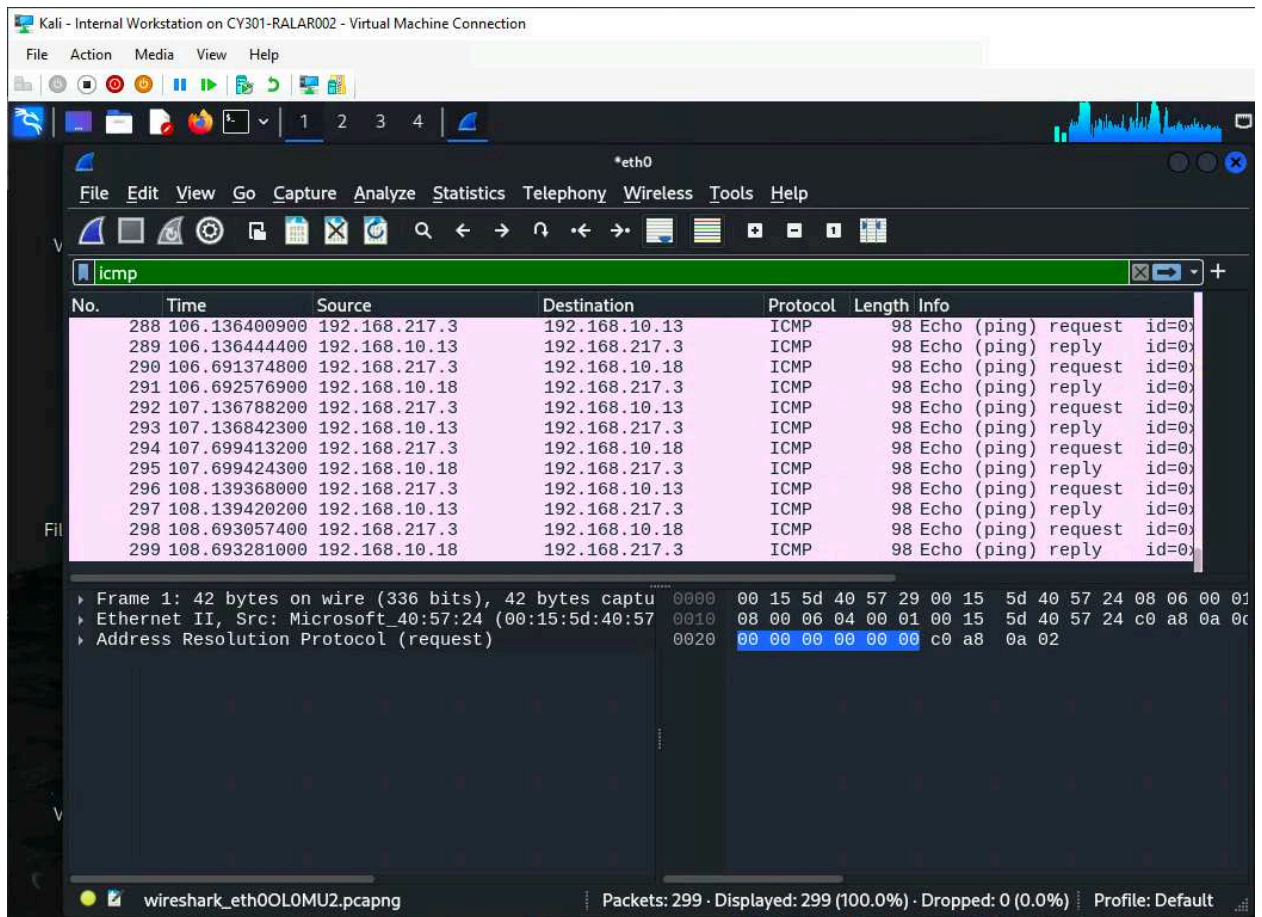
The standard query response was refused by the DNS

# Task B

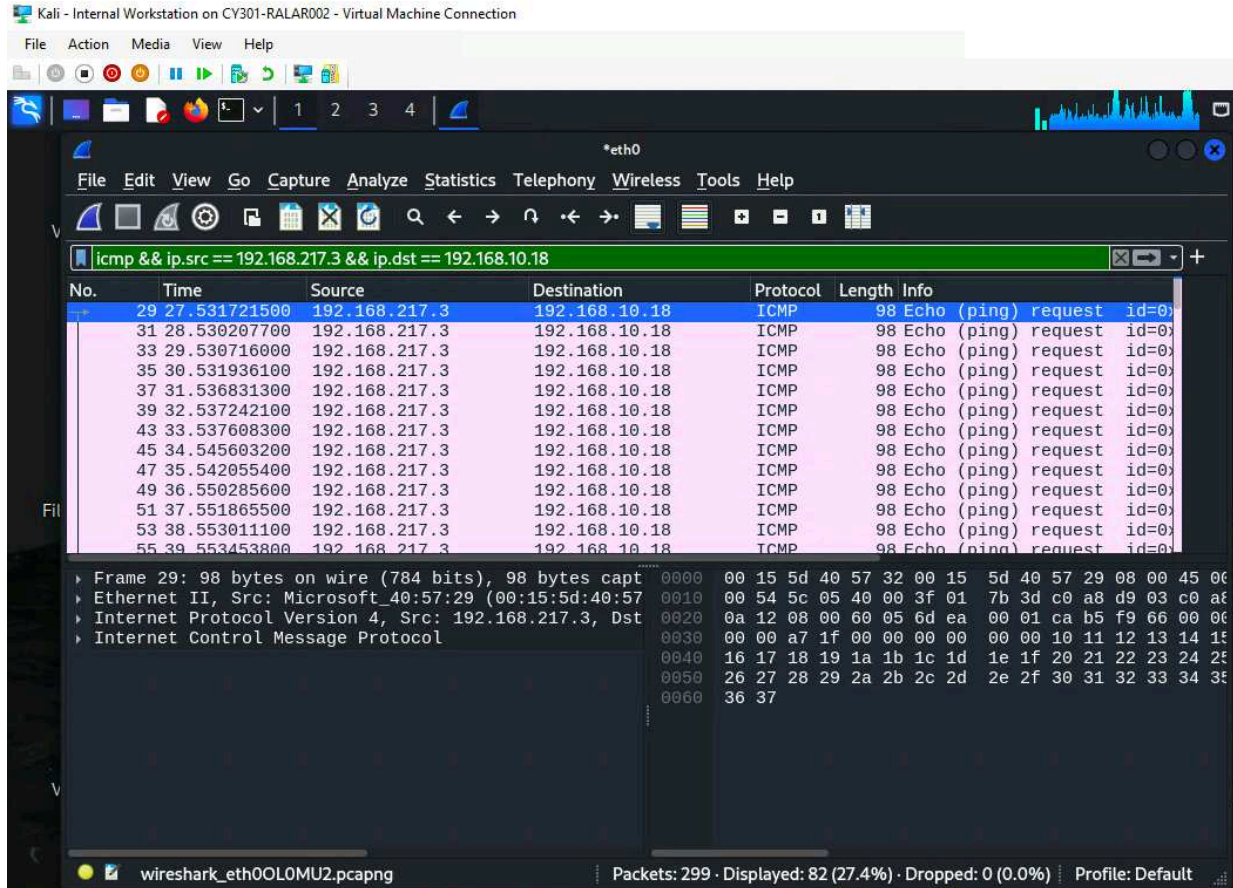
## 1. Sniff ICMP traffic:

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

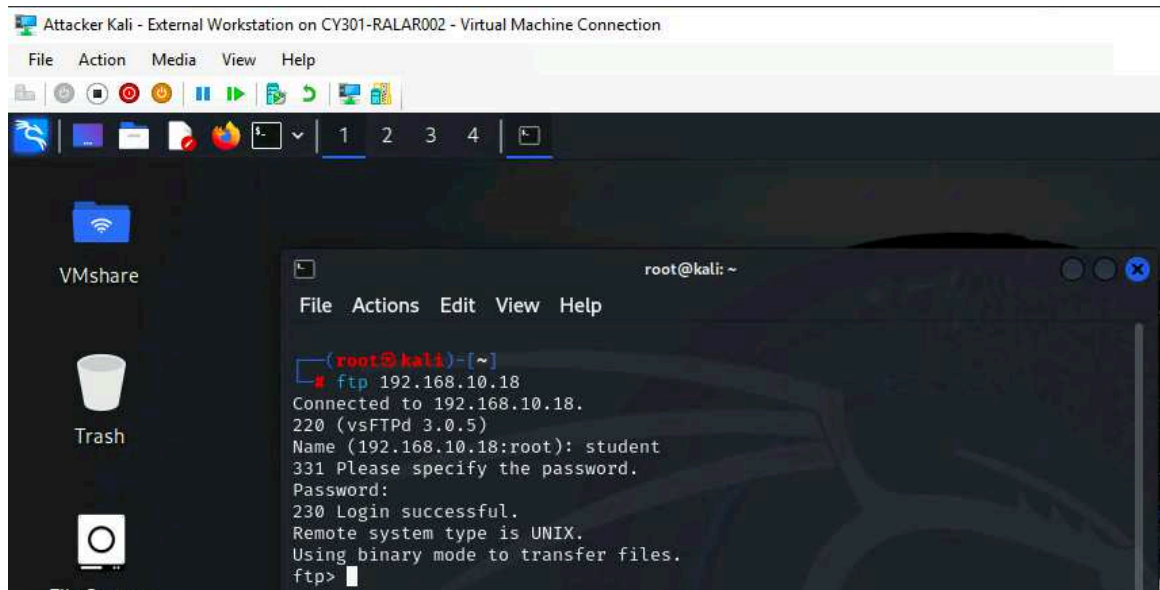


- b. Apply a proper display or capture filter on the internal Kali VM that ONLY displays the ICMP request that originated from the external Kali VM and goes to the Ubuntu 64-bit VM

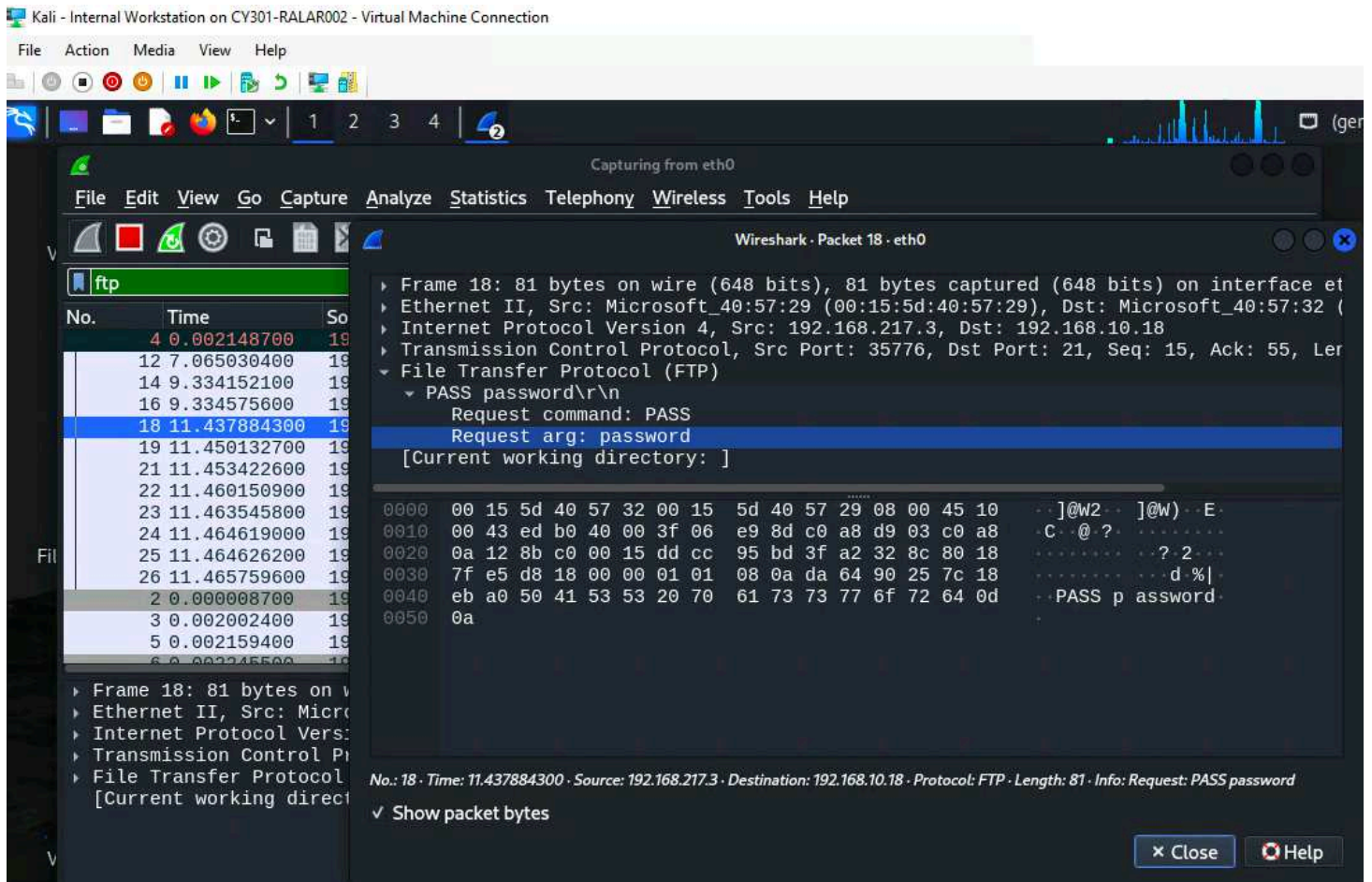


## 2. Sniff FTP traffic:

- 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

Wireshark - Packet 16 - eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source
7	5.068253100	Microsoft_40:57:29
8	5.068539800	Microsoft_40:57:29
14	33.484500200	Microsoft_40:57:29
15	33.485015500	Microsoft_40:57:29
24	108.748671400	Microsoft_40:57:29
25	108.749019100	Microsoft_40:57:29
1	0.000000000	192.168.217.3
2	0.002346800	192.168.217.3
12	28.338035800	192.168.217.3
16	45.095224200	192.168.217.3
18	45.095494500	192.168.217.3
20	103.487314200	192.168.217.3
22	106.848243800	192.168.217.3
3	0.002354200	192.168.217.3
4	0.004665100	192.168.217.3

Frame 16: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0  
 Ethernet II, Src: Microsoft\_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft\_40:57:32 (00:15:5d: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: 4  
 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  ..]@w2.. ]@w) --E-
0010 00 43 73 c2 40 00 3f 06 63 7c c0 a8 d9 03 c0 a8  -Cs_@.? c|.....
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  .....g..|.....
0040 eb c0 55 53 45 52 20 72 61 6c 61 72 30 30 32 0d  -USER ralar002-
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

Kali - Internal Workstation on CY301-RALAR002 - Virtual Machine Connection

File Action Media View Help

Wireshark - Packet 20 - eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source
7	5.068253100	Microsoft_40:57:29
8	5.068539800	Microsoft_40:57:29
14	33.484500200	Microsoft_40:57:29
15	33.485015500	Microsoft_40:57:29
24	108.748671400	Microsoft_40:57:29
25	108.749019100	Microsoft_40:57:29
1	0.000000000	192.168.217.3
2	0.002346800	192.168.217.3
12	28.338035800	192.168.217.3
16	45.095224200	192.168.217.3
18	45.095494500	192.168.217.3
20	103.487314200	192.168.217.3
22	106.848243800	192.168.217.3
3	0.002354200	192.168.217.3
4	0.004665100	192.168.217.3

Frame 20: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0  
 Ethernet II, Src: Microsoft\_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft\_40:57:32 (00:15:5d: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, Len: 4  
 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  ..]@w2.. ]@w) --E-
0010 00 43 73 c4 40 00 3f 06 63 7a c0 a8 d9 03 c0 a8  -Cs_@.? cz.....
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  .....h..|.....
0040 2d 36 50 41 53 53 20 30 31 31 39 39 37 34 31 0d  -6PASS 01199741-
0050 0a
  
```

Request command (ftp.request.command), 4 bytes

Show packet bytes

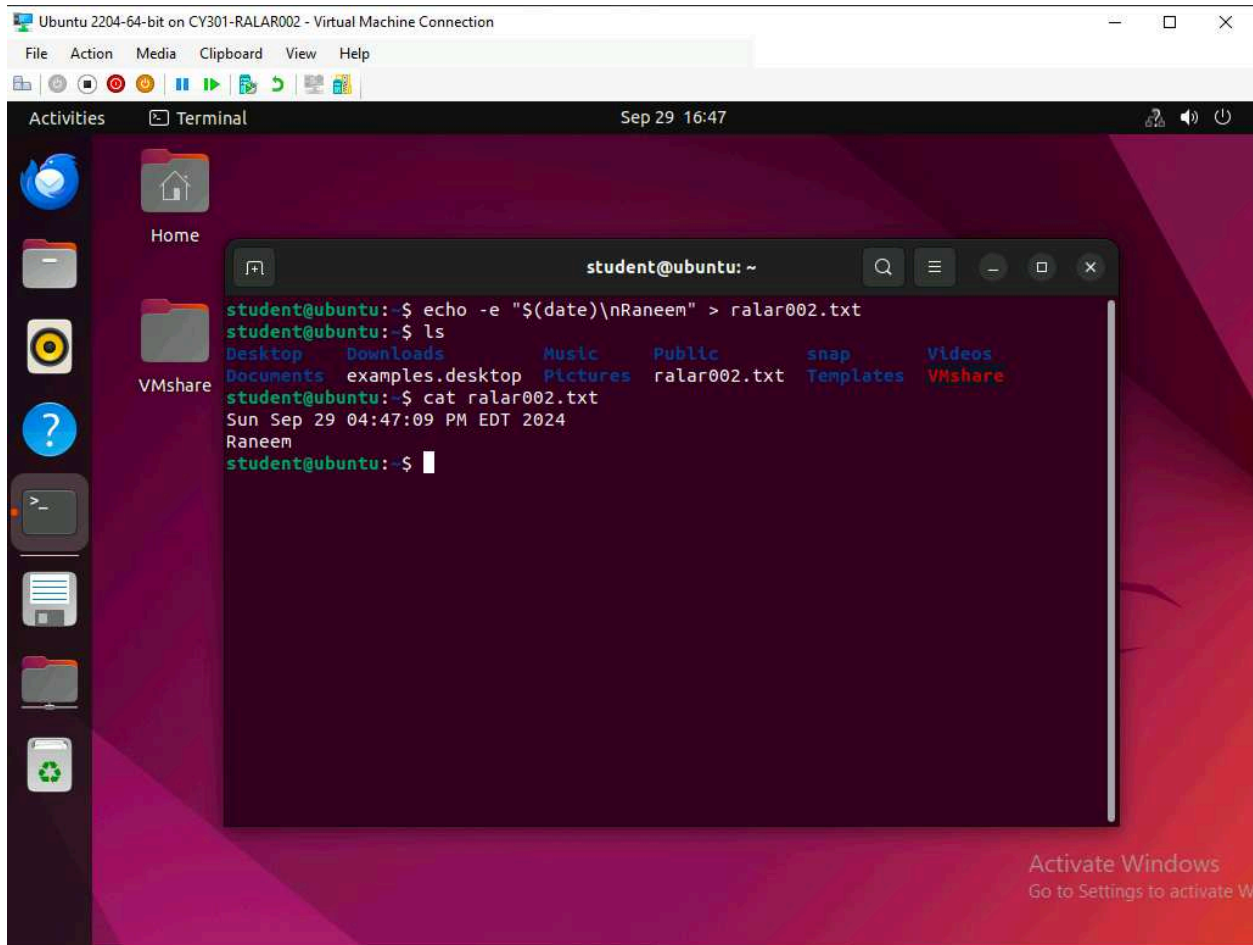
Close Help

File Transfer Protocol (FTP): Protocol

Packets: 25 - Displayed: 25 (100.0%) - Dropped: 0 (0.0%) | Profile: Default

# Task C- Extra Credit

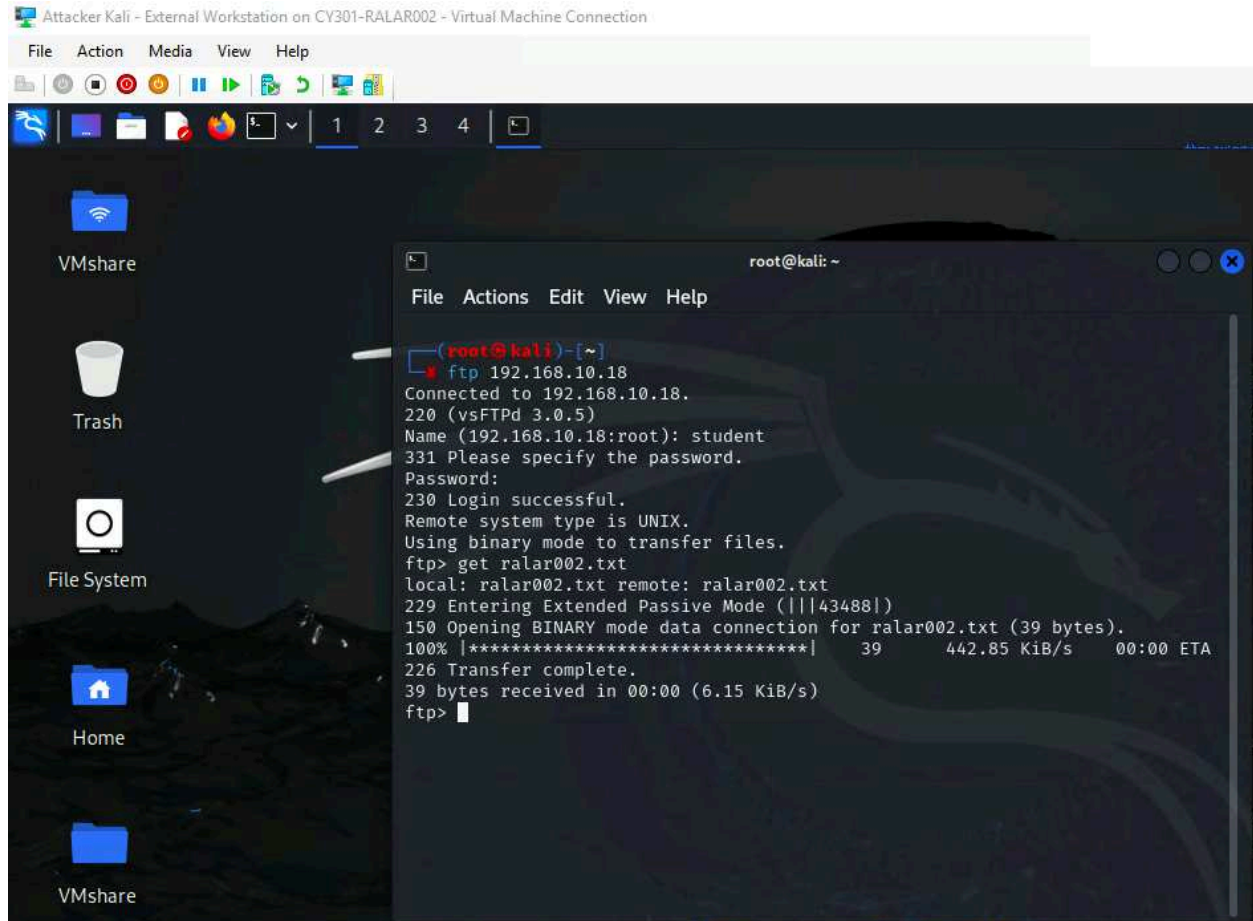
Login to Ubuntu VM, and create a file in your home directory named “YOUR\_MIDAS.txt”. Put the current timestamp and your name in the file



The screenshot shows a terminal window titled "student@ubuntu: ~" with the following commands and output:

```
student@ubuntu:~$ echo -e "$(date)\nRaneem" > ralar002.txt
student@ubuntu:~$ ls
Desktop  Downloads  Music      Public     snap        Videos
Documents examples.desktop Pictures    ralar002.txt Templates  VMshare
student@ubuntu:~$ cat ralar002.txt
Sun Sep 29 04:47:09 PM EDT 2024
Raneem
student@ubuntu:~$
```

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

The screenshot shows the Wireshark interface in Kali Linux. The main window is titled "Wireshark · Follow TCP Stream (tcp.stream eq 2) · eth0". The left pane shows a list of captured packets, with packet 36 selected. The right pane shows the details of the selected packet, including the Transmission Control Protocol (TCP) segment. The "Follow TCP Stream" pane is active, showing the stream index and the content of the stream. The stream content is displayed as ASCII text, showing the beginning of a file transfer: "Sun Sep 29 04:47:09 PM EDT 2024 Raneem".

No.	Time	Source	Destination
36	360.537645400	192.168.1.1	192.168.1.2
32	360.526699400	192.168.1.2	192.168.1.1
33	360.527708300	192.168.1.1	192.168.1.2
34	360.529394900	192.168.1.2	192.168.1.1
37	360.537655500	192.168.1.1	192.168.1.2
39	360.543691200	192.168.1.2	192.168.1.1
40	360.543698800	192.168.1.1	192.168.1.2
41	360.543706000	192.168.1.2	192.168.1.1
42	360.545002300	192.168.1.1	192.168.1.2
44	360.546954700	192.168.1.2	192.168.1.1

Details of Frame 36:

- Frame 36: 105 bytes on wire (840 bytes captured) on interface eth0
- Ethernet II, Src: Mikrotik (08:00:0C:00:00:00), Dst: Mikrotik (08:00:0C:00:00:00)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
- Transmission Control Protocol, Seq: 373514400, Len: 105
- Source Port: 43488
- Destination Port: 373514400
- [Stream index: 2]
- [Conversation complete]
- [TCP Segment Len: 39]
- Sequence Number: 1
- Sequence Number (raw): 373514400

Follow TCP Stream (tcp.stream eq 2) - eth0

0 client pkts, 1 server pkt, 0 turns.

Entire conversation (39 bytes) Show data as ASCII Stream 2

Find: Find Next

Filter Out This Stream Print Save as... Back × Close Help