

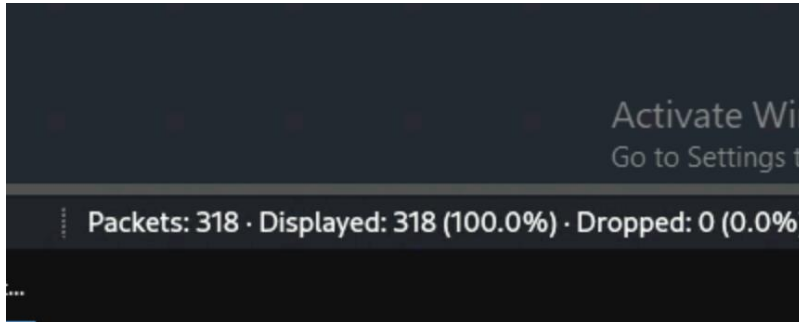
OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
Assignment #2 Traffic Tracing and Sniffing

Celeste Meraz-Luna
01302562

Task A: Get Started with Wireshark

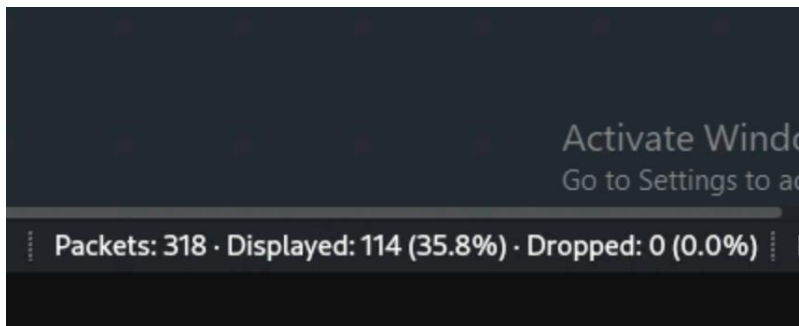
Q1. How many packets are captured in total? How many packets are displayed?

318 packets were captured and displayed in total.



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

After applying the “ICMP” filter 318 packets were captured and 114 packets were 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?

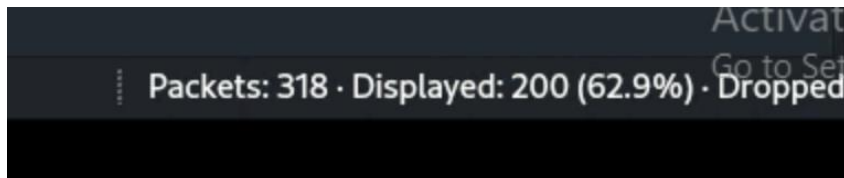
Under the IPV4 header the Source IP: 192.168.10.18, Destination IP 192.168.217.3

Under the ICMP header the Sequence Number: 1 (0x0001), Size of Data: 40 bytes, Response Time: 3.263 ms.

```
[Header checksum status: Unverified]
Source Address: 192.168.10.18
Destination Address: 192.168.217.3
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0xb7a9 [correct]
[Checksum Status: Good]
Identifier (BE): 22711 (0x58b7)
Identifier (LE): 46936 (0xb758)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Request frame: 1]
[Response time: 3.263 ms]
Timestamp from icmp data: Sep 24, 2025 00:09:5
[Timestamp from icmp data (relative): 0.003302]
Data (40 bytes)
```

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

After applying the “DNS” filter 318 packets were captured, and 200 packets were 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? Please express in the format: IP:port.

The domain name is under the Queries header: spocs.getpocket.com

The source IP and port 192.168.217.3:48086

The destination IP and port 192.168.217.2:53

```

e 47: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface eth0, id 0
rnet II, Src: Microsoft_40:57:27 (00:15:5d:40:57:27), Dst: Microsoft_40:57:38 (00:15:5d:40:57:38)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
User Datagram Protocol, Src Port: 48086, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x4bf5
Flags: 0x0100 Standard query
0... .. = Response: Message is a query
.000 0... .. = Opcode: Standard query (0)
... ..0... .. = Truncated: Message is not truncated
... ..1... .. = Recursion desired: Do query recursively
... ..0... .. = Z: reserved (0)
... ..0... .. = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Series
spocs.getpocket.com: type A, class IN
[Response In: 49]

```

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?

I found the responding packet by looking for the same transaction ID: 0x4bf5.

The source IP and port: 192.168.217.2:53

The destination IP and port: 192.168.217.3:48086

The standard query response is “Refused.”

Time	Source	Destination	Protocol	Length	Info
46	19.329118200	192.168.217.2	DNS	54	Standard query response 0
47	19.373347700	192.168.217.3	DNS	79	Standard query 0x4bf5 A s
48	19.373367700	192.168.217.3	DNS	79	Standard query 0x3214 AA
49	19.379614400	192.168.217.2	DNS	54	Standard query response 0
50	19.379624000	192.168.217.2	DNS	54	Standard query response 0
53	20.297899600	192.168.217.3	DNS	95	Standard query 0x9856 A c

```

Frame 49: 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: 48086
Domain Name System (response)
Transaction ID: 0x4bf5
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
... ..0... .. = Non-authenticated data: Unacceptable
... ..0101 = Reply code: Refused (5)
Questions: 0
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
[Request In: 47]
[Time: 0.006266700 seconds]

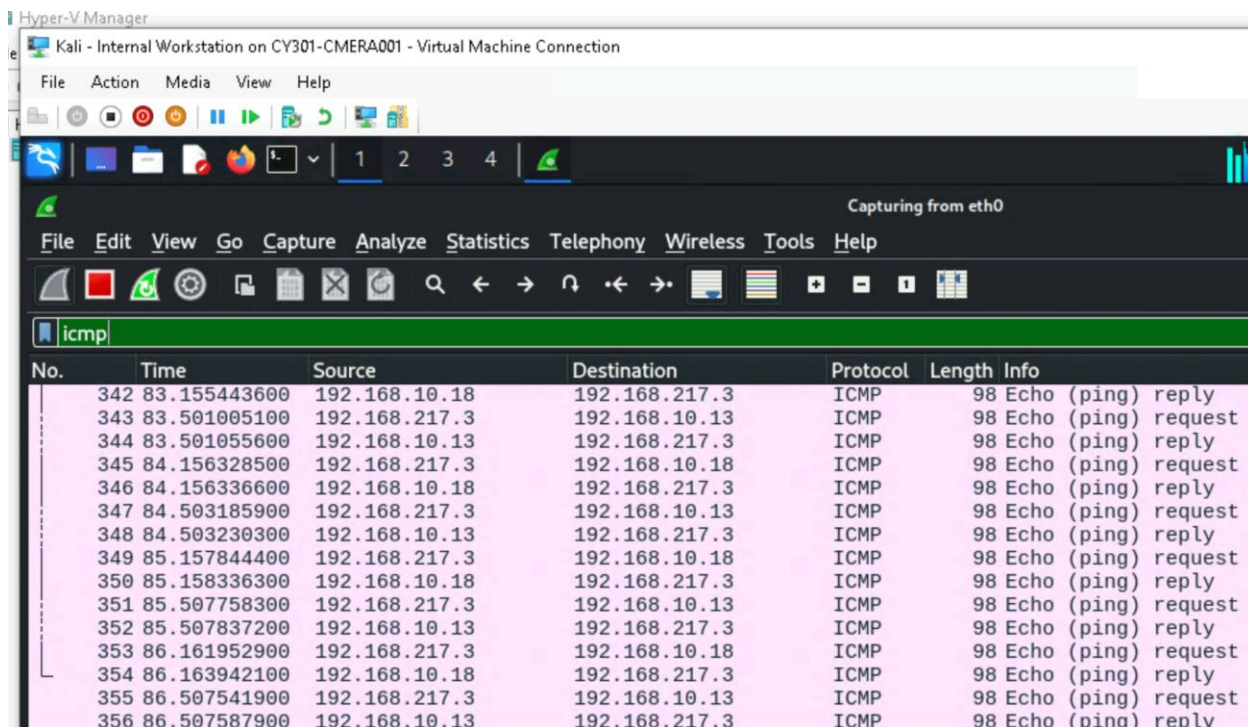
```

Task B: Sniff LAN Traffic

Q1: Sniff ICMP Traffic

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

I applied the ICMP filter to display the active ICMP traffic.



No.	Time	Source	Destination	Protocol	Length	Info
342	83.155443600	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply
343	83.501005100	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
344	83.501055600	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply
345	84.156328500	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
346	84.156336600	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply
347	84.503185900	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
348	84.503230300	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply
349	85.157844400	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
350	85.158336300	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply
351	85.507758300	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
352	85.507837200	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply
353	86.161952900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
354	86.163942100	192.168.10.18	192.168.217.3	ICMP	98	Echo (ping) reply
355	86.507541900	192.168.217.3	192.168.10.13	ICMP	98	Echo (ping) request
356	86.507587900	192.168.10.13	192.168.217.3	ICMP	98	Echo (ping) reply

- 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.

I applied the filter `icmp.type == 8 && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18`. This filter displays the ICMP requests from external Kali VM and goes to the Ubuntu 64-bit VM.

Hyper-V Manager

Kali - Internal Workstation on CY301-CMERA001 - Virtual Machine Connection

File Action Media View Help

Minimize all open windows and show the desktop *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp.type == 8 && ip.src == 192.168.217.3 && ip.dst == 192.168.10.18

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
5	1.001475900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
9	2.009770100	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
13	3.008336200	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
17	4.009604300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
21	5.010690800	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
25	6.012932900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
31	7.014865600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
35	8.016107300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
39	9.017651900	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
43	10.020036600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
47	11.021936000	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
51	12.023963300	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
55	13.026069600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request
59	14.042666600	192.168.217.3	192.168.10.18	ICMP	98	Echo (ping) request

Q2: Sniff FTP Traffic

- a. On External Kali I used the FTP 192.168.10.18 command to access the FTP server.

```
(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>
```

- b. Using the FTP filter, I was able to find the USER and PASS of the credentials submitted in the FTP Server. The USER: student and PASS: password

Time	Source	Destination	Protocol	Length	Info
112 25.775518200	192.168.10.18	192.168.217.3	FTP	86	Response: 220 (vsFTPD 3.6
136 31.402430600	192.168.217.3	192.168.10.18	FTP	80	Request: USER student
138 31.402562500	192.168.10.18	192.168.217.3	FTP	100	Response: 331 Please spec
162 36.905080000	192.168.10.18	192.168.217.3	FTP	80	Response: 421 Timeout.
190 43.065027700	192.168.217.3	192.168.10.18	FTP	81	Request: PASS password
191 43.075217800	192.168.10.18	192.168.217.3	FTP	89	Response: 230 Login succe
193 43.078849900	192.168.217.3	192.168.10.18	FTP	72	Request: SYST
196 43.084113900	192.168.10.18	192.168.217.3	FTP	85	Response: 215 UNIX Type:
197 43.085867500	192.168.217.3	192.168.10.18	FTP	72	Request: FEAT
198 43.094591900	192.168.10.18	192.168.217.3	FTP	81	Response: 211-Features:
199 43.094599800	192.168.10.18	192.168.217.3	FTP	87	Response: EPRT
200 43.094607200	192.168.10.18	192.168.217.3	FTP	110	Response: PASV

```

Frame 136: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface eth0, id 0
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: 49398, Dst Port: 21, Seq: 1, Ack: 21, Len: 14
File Transfer Protocol (FTP)
  USER student\r\n
    Request command: USER
    Request arg: student
[Current working directory: ]

```

- c. This time I used the ftp.request.command to filter out the USER and PASS. MY midas and uin number are shown as the USER and PASS.

Time	Source	Destination	Protocol	Length	Info
368 85.029932200	192.168.217.3	192.168.10.18	FTP	81	Request: USER cmera001
496 115.035303300	192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01302562
619 143.362089200	192.168.217.3	192.168.10.18	FTP	81	Request: USER cmera001
663 153.752772900	192.168.217.3	192.168.10.18	FTP	81	Request: PASS 01302562

```

Frame 368: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface eth0, id 0
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: 49892, Dst Port: 21, Seq: 1, Ack: 21, Len: 14
File Transfer Protocol (FTP)
  USER cmera001\r\n
    Request command: USER
    Request arg: cmera001
[Current working directory: ]

```