OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Ean Miller

01239018

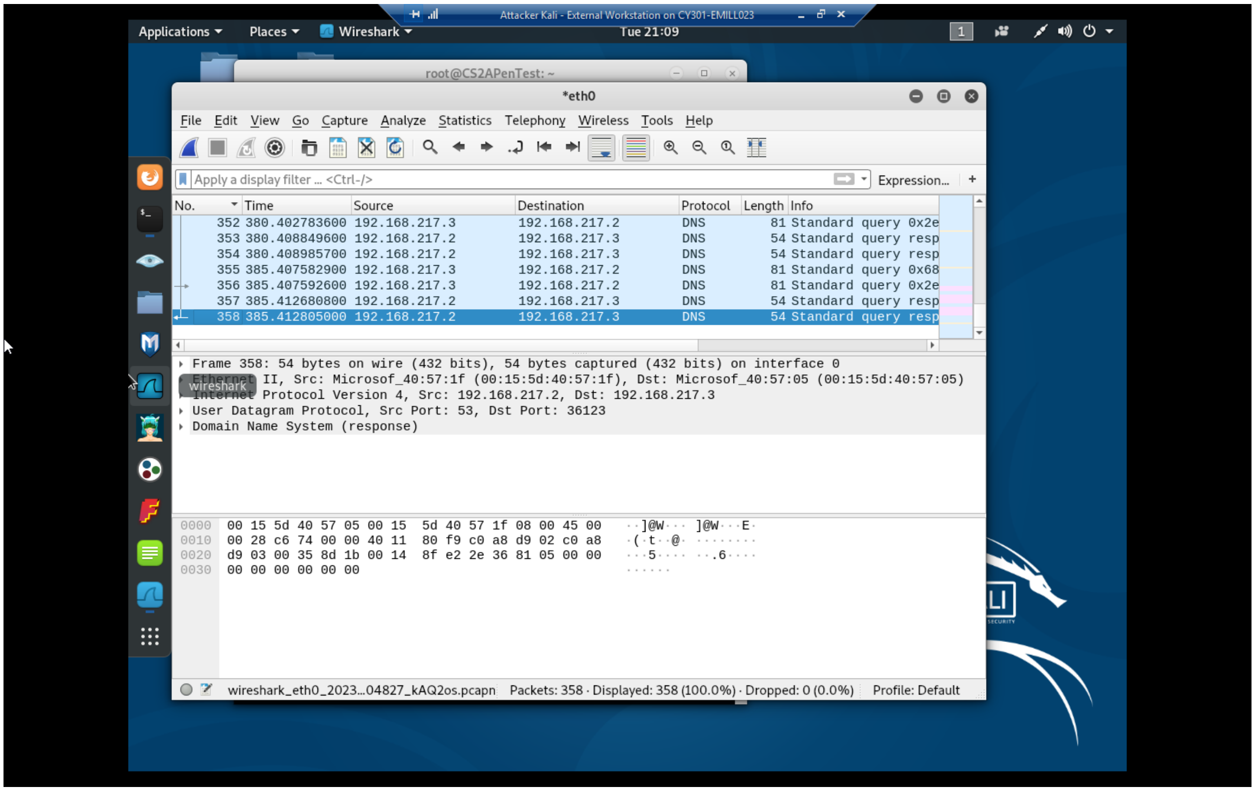
Task A --- Get started with Wireshark

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.

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


Attacker Kali - External Workstation on CY301-EMILL023
Applications
Places
Wireshark
Tue 21:09
root@CS2APenTest: ~
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
wireshark

```
No.   Time          Source          Destination     Protocol Length Info
  352 380.402783600 192.168.217.3   192.168.217.2   DNS        81 Standard query 0x2e
  353 380.408849600 192.168.217.2   192.168.217.3   DNS        54 Standard query resp
  354 380.408985700 192.168.217.2   192.168.217.3   DNS        54 Standard query resp
  355 385.407582900 192.168.217.3   192.168.217.2   DNS        81 Standard query 0x68
  356 385.407592600 192.168.217.3   192.168.217.2   DNS        81 Standard query 0x2e
  357 385.412680800 192.168.217.2   192.168.217.3   DNS        54 Standard query resp
  358 385.412805000 192.168.217.2   192.168.217.3   DNS        54 Standard query resp
```

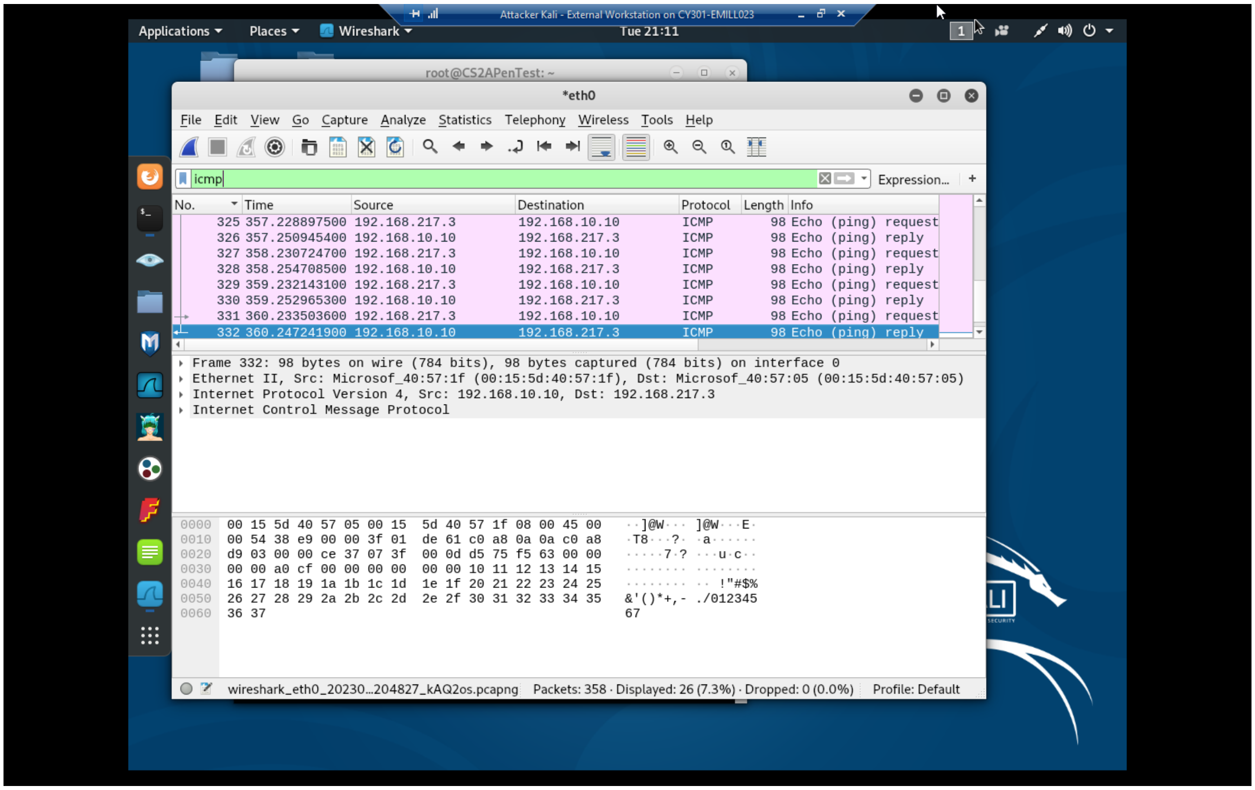
```
▸ Frame 358: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof_40:57:05 (00:15:5d:40:57:05)
▸ Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
▸ User Datagram Protocol, Src Port: 53, Dst Port: 36123
▸ Domain Name System (response)
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W···  ]@W···E·
0010  00 28 c6 74 00 00 40 11  80 f9 c0 a8 d9 02 c0 a8   ·(·t··@·  ········
0020  d9 03 00 35 8d 1b 00 14  8f e2 2e 36 81 05 00 00   ···5····  ···.6···
0030  00 00 00 00 00 00                                  ······
```

wireshark_eth0_2023...04827_kAQ2os.pcapn   Packets: 358 · Displayed: 358 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

Wire shark has captured 358 packets

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


Attacker Kali - External Workstation on CY301-EMILL023
Applications
Places
Wireshark
Tue 21:11
root@CS2APenTest: ~
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

icmp

No.	Time	Source	Destination	Protocol	Length	Info
325	357.228897500	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) request
326	357.250945400	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) reply
327	358.230724700	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) request
328	358.254708500	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) reply
329	359.232143100	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) request
330	359.252965300	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) reply
331	360.233503600	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) request
332	360.247241900	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) reply

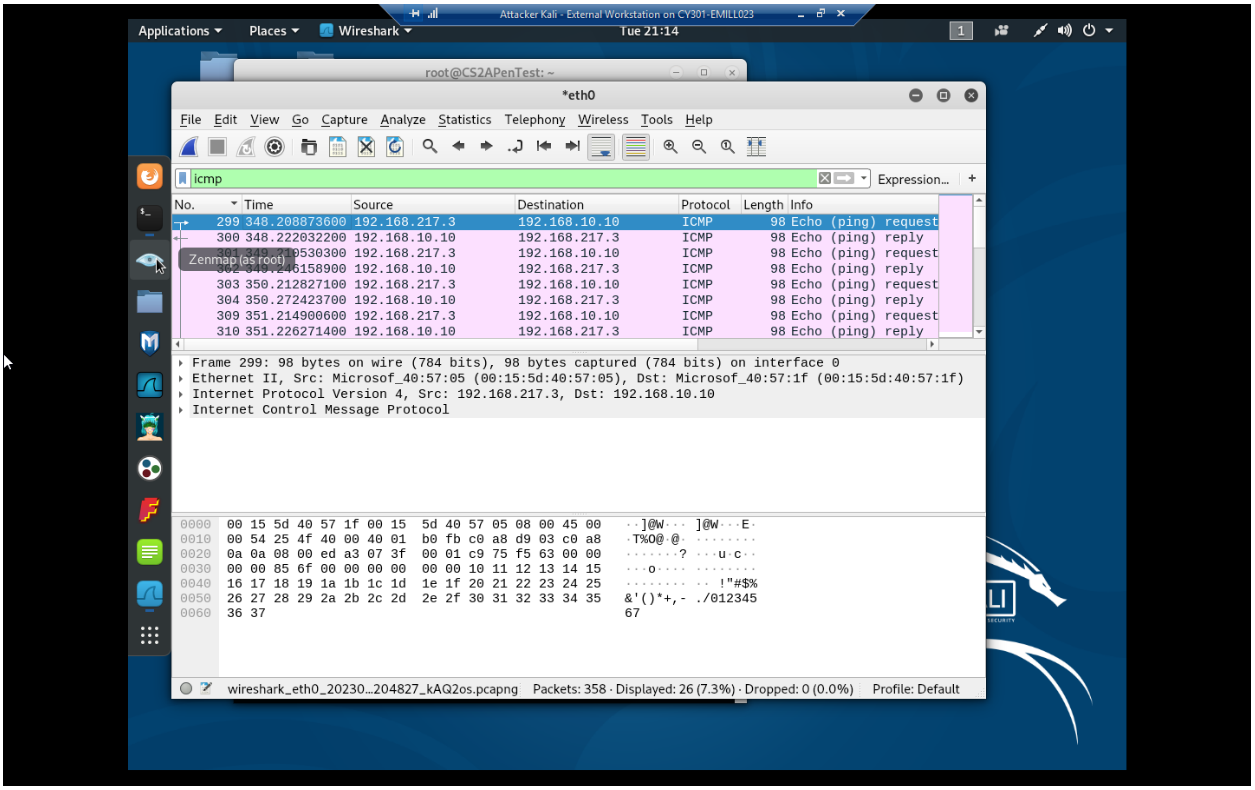
```
Frame 332: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof_40:57:05 (00:15:5d:40:57:05)
Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W···  ]@W···E·
0010  00 54 38 e9 00 00 3f 01  de 61 c0 a8 0a 0a c0 a8   ·T8···?·  ·a······
0020  d9 03 00 00 ce 37 07 3f  00 0d d5 75 f5 63 00 00   ·····7·?  ···u·c··
0030  00 00 a0 cf 00 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
```

wireshark_eth0_20230...204827_kAQ2os.pcapng Packets: 358 · Displayed: 26 (7.3%) · Dropped: 0 (0.0%) Profile: Default

Wireshark has captured 33 packets with the protocol ICMP

Q3. Select an Echo (replay) 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?



Applications
Places
Wireshark
Attacker Kali - External Workstation on CY301-EMILL023
Tue 21:14
root@CS2APenTest: ~
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
Zenmap (as root)

```
icmp
```

```
No.    Time          Source          Destination     Protocol  Length Info
  299 348.208873600 192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request
  300 348.222032200 192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply
  301 349.210530300 192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request
  302 349.246158900 192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply
  303 350.212827100 192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request
  304 350.272423700 192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply
  309 351.214900600 192.168.217.3   192.168.10.10   ICMP          98 Echo (ping) request
  310 351.226271400 192.168.10.10   192.168.217.3   ICMP          98 Echo (ping) reply
```

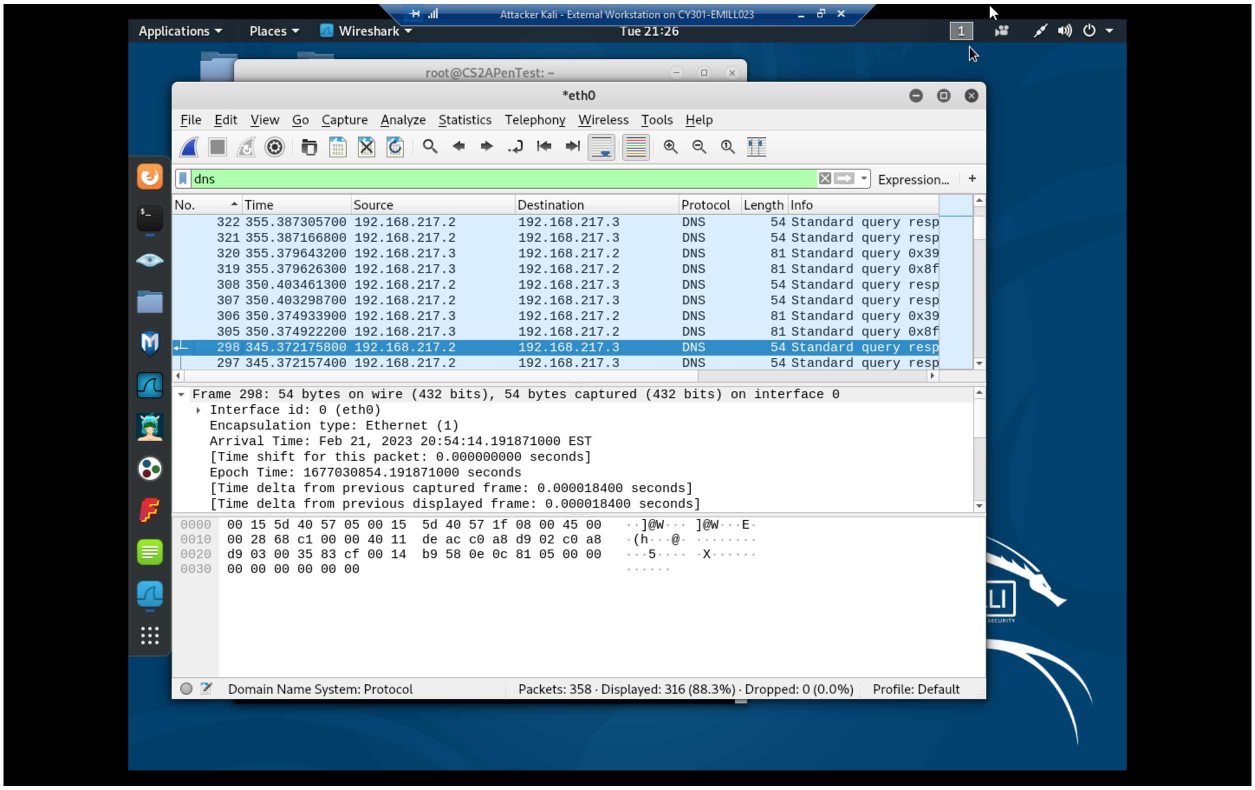
```
Frame 299: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Microsof_40:57:05 (00:15:5d:40:57:05), Dst: Microsof_40:57:1f (00:15:5d:40:57:1f)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
Internet Control Message Protocol
```

```
0000  00 15 5d 40 57 1f 00 15  5d 40 57 05 08 00 45 00   ··]@W···  ]@W···E·
0010  00 54 25 4f 40 00 40 01  b0 fb c0 a8 d9 03 c0 a8   ·T%O@·@·  ········
0020  0a 0a 08 00 ed a3 07 3f  00 01 c9 75 f5 63 00 00   ·······?  ···u·c··
0030  00 00 85 6f 00 00 00 00  00 00 10 11 12 13 14 15   ···o····  ········
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
```

wireshark_eth0_20230…204827_kAQ2os.pcapng · Packets: 358 · Displayed: 26 (7.3%) · Dropped: 0 (0.0%) · Profile: Default

I chose packet number 299 and the source IP is 192.168.217.3 and the destination IP is 192.168.10.10, and the sequence number is 1/256 and the size of the data is 98 bytes or 784 bits, and the response time is 348.208873600 seconds

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



```
dns
```

```
No.    Time           Source          Destination     Protocol Length Info
   322 355.387305700 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
   321 355.387166800 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
   320 355.379643200 192.168.217.3   192.168.217.2   DNS         81 Standard query 0x39
   319 355.379626300 192.168.217.3   192.168.217.2   DNS         81 Standard query 0x8f
   308 350.403461300 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
   307 350.403298700 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
   306 350.374933900 192.168.217.3   192.168.217.2   DNS         81 Standard query 0x39
   305 350.374922200 192.168.217.3   192.168.217.2   DNS         81 Standard query 0x8f
   298 345.372175800 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
   297 345.372157400 192.168.217.2   192.168.217.3   DNS         54 Standard query resp
```

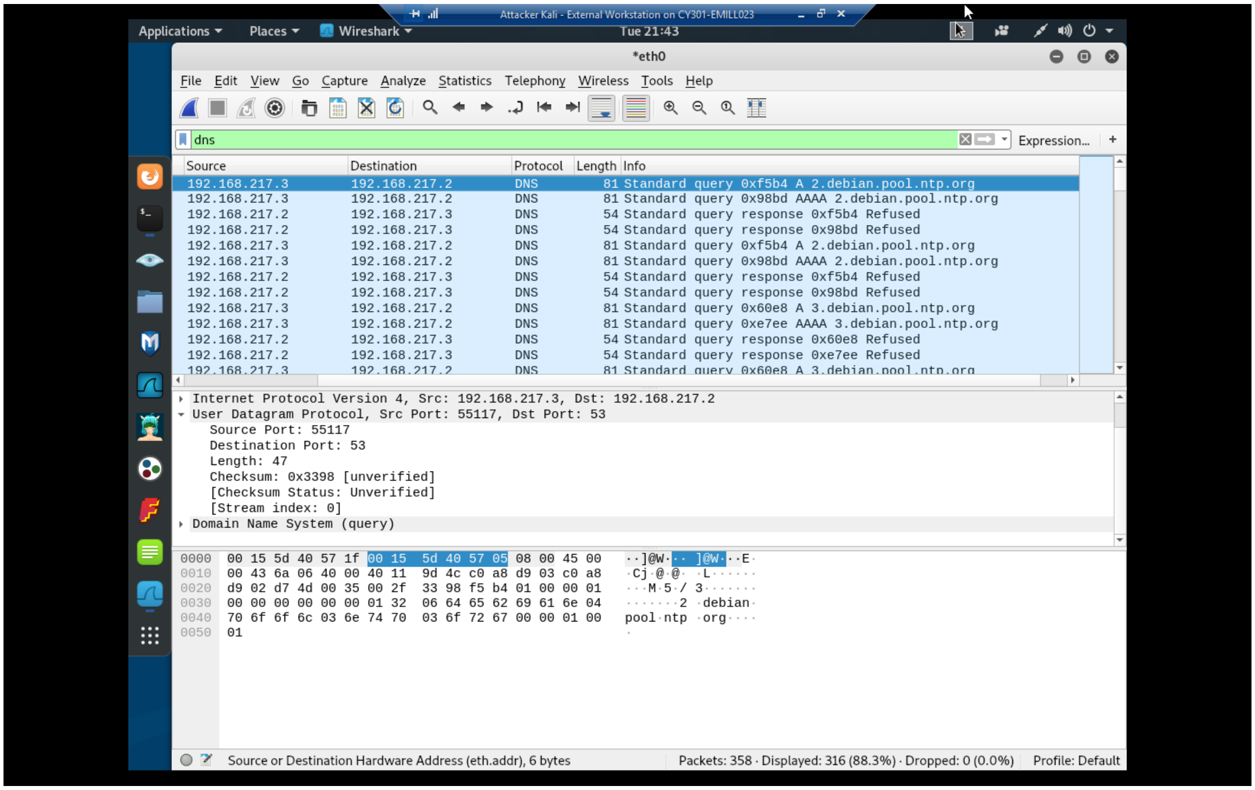
```
Frame 298: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 21, 2023 20:54:14.191871000 EST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1677030854.191871000 seconds
  [Time delta from previous captured frame: 0.000018400 seconds]
  [Time delta from previous displayed frame: 0.000018400 seconds]
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W··· ]@W···E·
0010  00 28 68 c1 00 00 40 11  de ac c0 a8 d9 02 c0 a8   ·(h···@· ········
0020  d9 03 00 35 83 cf 00 14  b9 58 0e 0c 81 05 00 00   ···5···· ·X······
0030  00 00 00 00 00 00                                  ······
```

Domain Name System: Protocol   Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)   Profile: Default

The amount of packets that are displayed is 322 packets

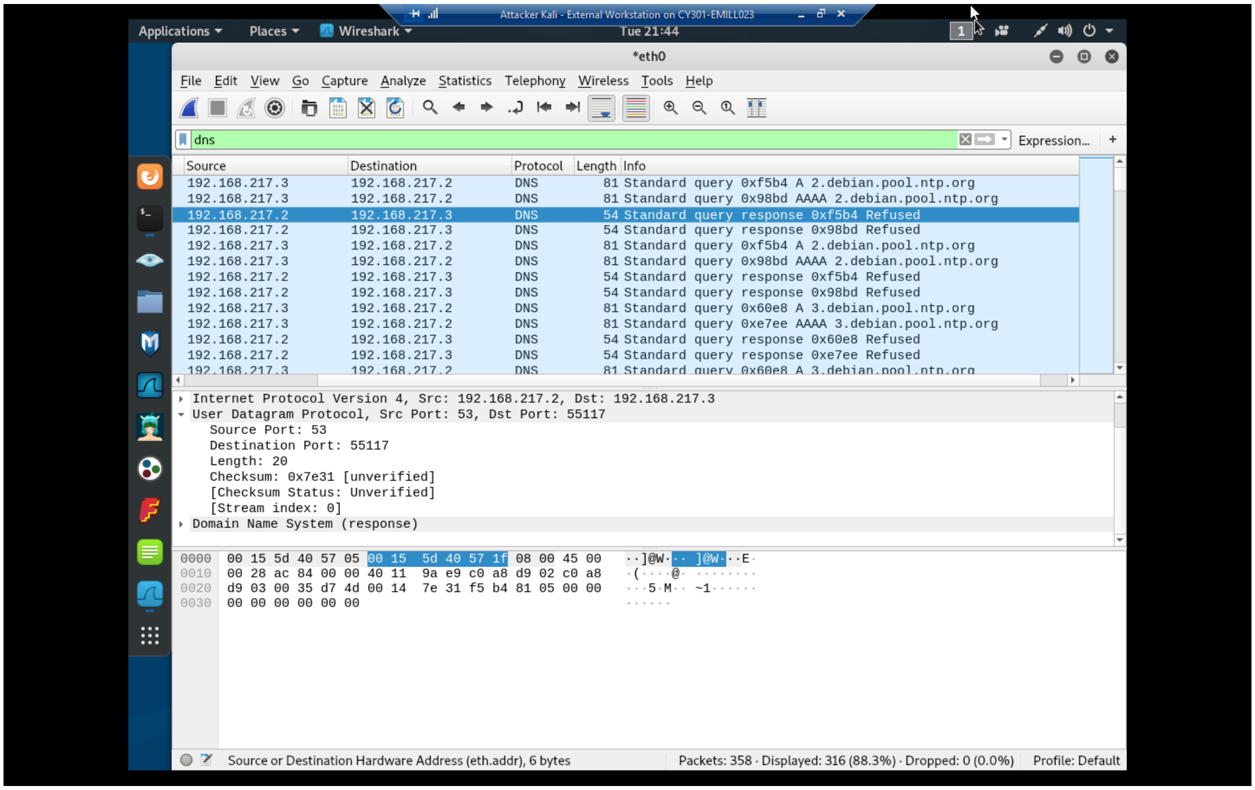
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: **IP:port**.


Attacker Kali - External Workstation on CY301-EMILL023
Applications
Places
Wireshark
Tue 21:43
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...

```
Source          Destination     Protocol Length Info
192.168.217.3   192.168.217.2   DNS      81 Standard query 0xf5b4 A 2.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS      81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xf5b4 Refused
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x98bd Refused
192.168.217.3   192.168.217.2   DNS      81 Standard query 0xf5b4 A 2.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS      81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xf5b4 Refused
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x98bd Refused
192.168.217.3   192.168.217.2   DNS      81 Standard query 0x60e8 A 3.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS      81 Standard query 0xe7ee AAAA 3.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x60e8 Refused
192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xe7ee Refused
192.168.217.3   192.168.217.2   DNS      81 Standard query 0x60e8 A 3.debian.pool.ntp.org

Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
User Datagram Protocol, Src Port: 55117, Dst Port: 53
    Source Port: 55117
    Destination Port: 53
    Length: 47
    Checksum: 0x3398 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)

0000  00 15 5d 40 57 1f 00 15  5d 40 57 05 08 00 45 00   ··]@W··· ]@W···E·
0010  00 43 6a 06 40 00 40 11  9d 4c c0 a8 d9 03 c0 a8   ·Cj·@·@·  ·L······
0020  d9 02 d7 4d 00 35 00 2f  33 98 f5 b4 01 00 00 01   ···M·5·/ 3·······
0030  00 00 00 00 00 00 01 32  06 64 65 62 69 61 6e 04   ·······2 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp ·org····
0050  01                                                 ·

Source or Destination Hardware Address (eth.addr), 6 bytes    Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)    Profile: Default
```

The domain name of this packet is Standard query 0xf5b4 A 2.debian.pool.ntp.org, the source IP and port number is 192.168.217.3:55117 and the destination IP and port number is 192.168.217.2:53

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?


Attacker Kali - External Workstation on CY301-EMILL023
Applications
Places
Wireshark
Tue 21:44
1
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

dns

```
Source          Destination     Protocol Length Info
192.168.217.3   192.168.217.2   DNS       81 Standard query 0xf5b4 A 2.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS       81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xf5b4 Refused
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x98bd Refused
192.168.217.3   192.168.217.2   DNS       81 Standard query 0xf5b4 A 2.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS       81 Standard query 0x98bd AAAA 2.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xf5b4 Refused
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x98bd Refused
192.168.217.3   192.168.217.2   DNS       81 Standard query 0x60e8 A 3.debian.pool.ntp.org
192.168.217.3   192.168.217.2   DNS       81 Standard query 0xe7ee AAAA 3.debian.pool.ntp.org
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x60e8 Refused
192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xe7ee Refused
192.168.217.3   192.168.217.2   DNS       81 Standard query 0x60e8 A 3.debian.pool.ntp.org
```

```
▸ Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
▾ User Datagram Protocol, Src Port: 53, Dst Port: 55117
    Source Port: 53
    Destination Port: 55117
    Length: 20
    Checksum: 0x7e31 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▸ Domain Name System (response)
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W··· ]@W···E·
0010  00 28 ac 84 00 00 40 11  9a e9 c0 a8 d9 02 c0 a8   ·(····@· ········
0020  d9 03 00 35 d7 4d 00 14  7e 31 f5 b4 81 05 00 00   ···5·M·· ~1······
0030  00 00 00 00 00 00                                   ······
```

Source or Destination Hardware Address (eth.addr), 6 bytes   Packets: 358 · Displayed: 316 (88.3%) · Dropped: 0 (0.0%)   Profile: Default

The source IP and port number is 192.168.217.2:53 and the destination IP and port number is 192.168.217.3:55117, the message is “Refused” with a flag of 0x8105