CYSE 301: Cybersecurity Technique and Operations

Assignment 2: Traffic Tracing and Sniffing

- **Task A – Get started with Wireshark**

Jason Rivers

01236524

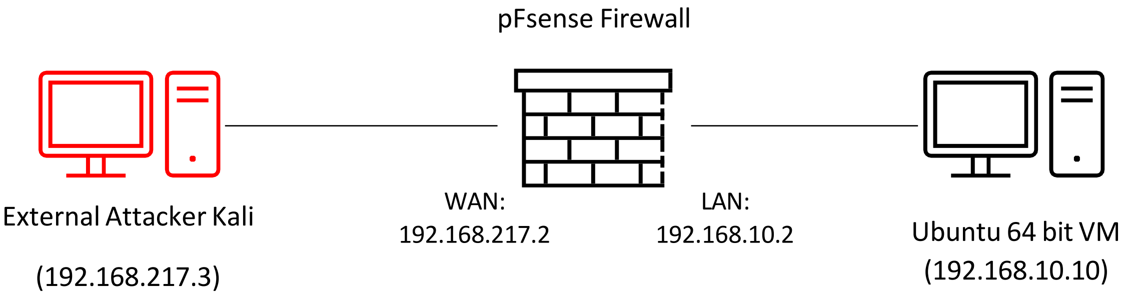
This document covers the first half of the assignment #2. The second half will be released after the complete discussion of Computer Network. Student needs to submit a report that covers both halves.

Each student needs to login into the **CCIA virtual environment** to complete this assignment.

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.*

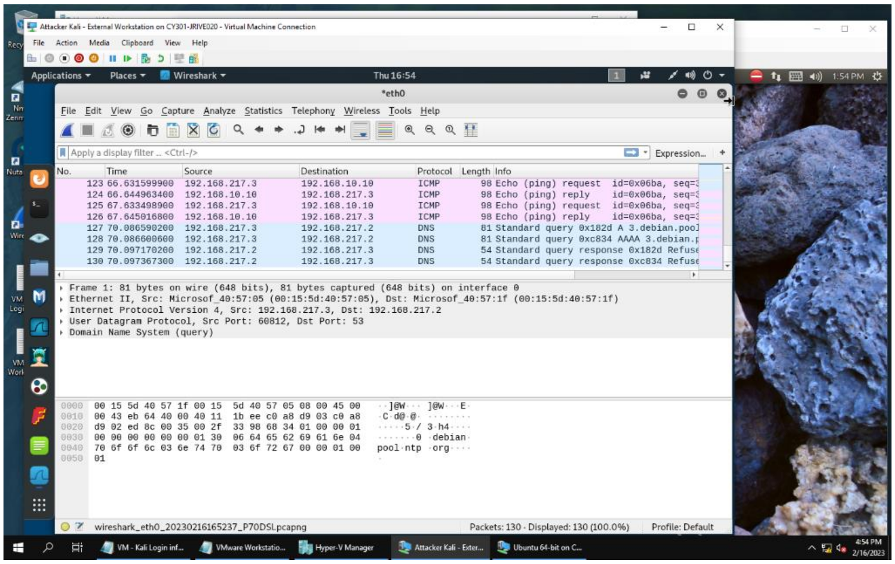


You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface "eth0".
2. Open a new terminal then ping Ubuntu VM for 5 – 10 seocnds.
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.

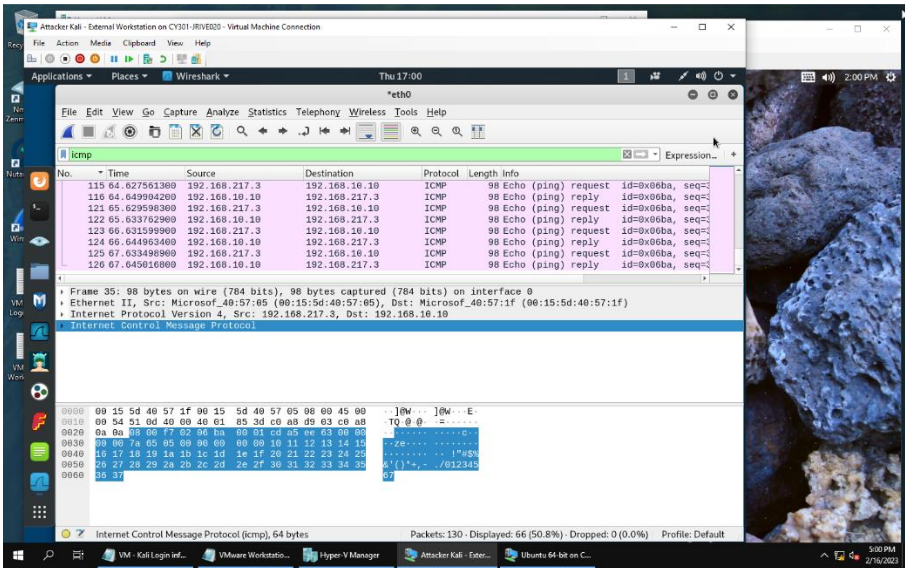
Q1. How many packets are captured in total? How many packets are displayed?


Attacker Kali - External Workstation on CY301-JR9VE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Thu 16:54
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
VM - Kali Login inf…
VMware Workstatio…
Hyper-V Manager
Attacker Kali - Exter…
Ubuntu 64-bit on C…

```
No.    Time          Source          Destination     Protocol Length Info
   123 66.631599900  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
   124 66.644963400  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3
   125 67.633498900  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
   126 67.645016800  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3
   127 70.086590200  192.168.217.3   192.168.217.2   DNS        81 Standard query 0x182d A 3.debian.pool
   128 70.086600600  192.168.217.3   192.168.217.2   DNS        81 Standard query 0xc834 AAAA 3.debian.p
   129 70.097170200  192.168.217.2   192.168.217.3   DNS        54 Standard query response 0x182d Refuse
   130 70.097367300  192.168.217.2   192.168.217.3   DNS        54 Standard query response 0xc834 Refuse

▸ Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 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: 192.168.217.2
▸ User Datagram Protocol, Src Port: 60812, Dst Port: 53
▸ 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 eb 64 40 00 40 11  1b ee c0 a8 d9 03 c0 a8   ·C·d@·@· ········
0020  d9 02 ed 8c 00 35 00 2f  33 98 68 34 01 00 00 01   ·····5·/ 3·h4····
0030  00 00 00 00 00 00 01 30  06 64 65 62 69 61 6e 04   ·······0 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp ·org····
0050  01                                                 ·

wireshark_eth0_20230216165237_P70DSL.pcapng     Packets: 130 · Displayed: 130 (100.0%)     Profile: Default
```

It captured 130 packets in all, and currently displays all of them because there is no filter yet.

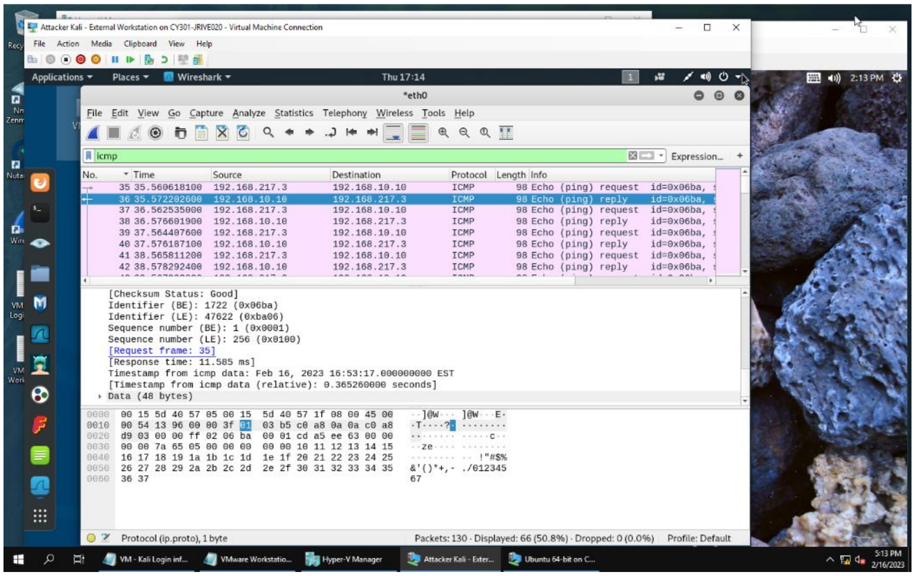
Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).


Attacker Kali - External Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Thu 17:00
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
VM - Kali Login inf... VMware Workstatio... Hyper-V Manager Attacker Kali - Exter... Ubuntu 64-bit on C...

```
No.    Time          Source          Destination     Protocol Length Info
  115 64.627561300  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
  116 64.649904200  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3
  121 65.629598300  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
  122 65.633762900  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3
  123 66.631599900  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
  124 66.644963400  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3
  125 67.633498900  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba, seq=3
  126 67.645016800  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba, seq=3

› Frame 35: 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 51 0d 40 00 40 01  85 3d c0 a8 d9 03 c0 a8   ·TQ·@·@·  ·=······
0020  0a 0a 08 00 f7 02 06 ba  00 01 cd a5 ee 63 00 00   ········  ·····c··
0030  00 00 7a 65 05 00 00 00  00 00 10 11 12 13 14 15   ··ze····  ········
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

Internet Control Message Protocol (icmp), 64 bytes    Packets: 130 · Displayed: 66 (50.8%) · Dropped: 0 (0.0%)    Profile: Default
```

There are 130 packets captures, but because we have applied the ICMP filter, only 66 (half) of them are displayed.

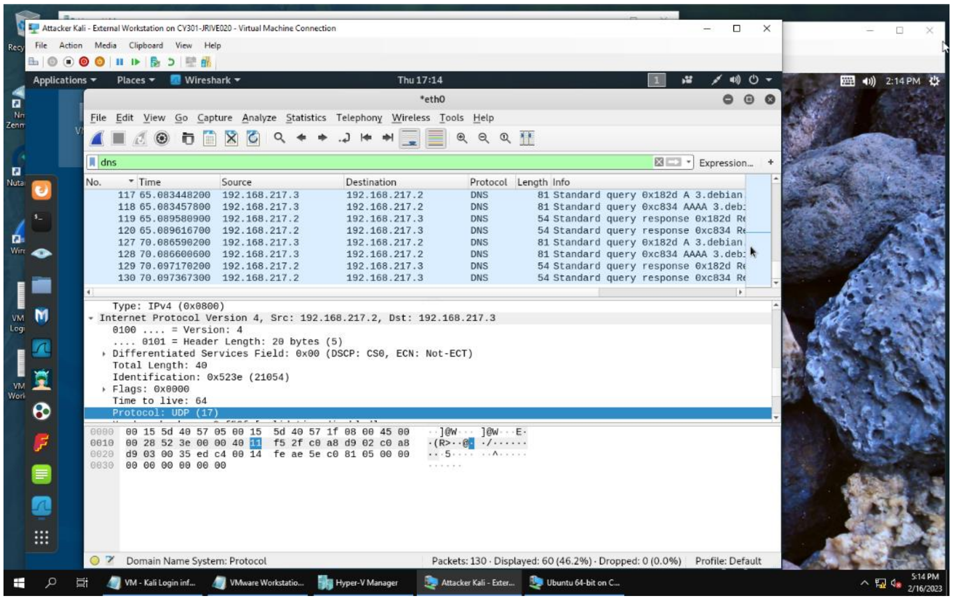
Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?


Attacker Kali - External Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Thu 17:14
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
VM - Kali Login inf... VMware Workstatio... Hyper-V Manager Attacker Kali - Exter... Ubuntu 64-bit on C...

```
No.    Time          Source          Destination     Protocol Length Info
   35 35.560618100  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba,
   36 35.572202600  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba,
   37 36.562535000  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba,
   38 36.576601900  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba,
   39 37.564407600  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba,
   40 37.576187100  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba,
   41 38.565811200  192.168.217.3   192.168.10.10   ICMP       98 Echo (ping) request  id=0x06ba,
   42 38.578292400  192.168.10.10   192.168.217.3   ICMP       98 Echo (ping) reply    id=0x06ba,

    [Checksum Status: Good]
    Identifier (BE): 1722 (0x06ba)
    Identifier (LE): 47622 (0xba06)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 35]
    [Response time: 11.585 ms]
    Timestamp from icmp data: Feb 16, 2023 16:53:17.000000000 EST
    [Timestamp from icmp data (relative): 0.365260000 seconds]
  › Data (48 bytes)

0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W···  ]@W···E·
0010  00 54 13 96 00 00 3f 01  03 b5 c0 a8 0a 0a c0 a8   ·T····?·  ········
0020  d9 03 00 00 ff 02 06 ba  00 01 cd a5 ee 63 00 00   ········  ·····c··
0030  00 00 7a 65 05 00 00 00  00 00 10 11 12 13 14 15   ··ze····  ········
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

Protocol (ip.proto), 1 byte    Packets: 130 · Displayed: 66 (50.8%) · Dropped: 0 (0.0%)    Profile: Default
```

(Assuming replay in the questions is supposed to be reply) The source of this packet is 192.168.10.10, destination is 192.168.217.3. The sequence number showed (BE) 1, and (LE) 256, and the size was 48 bytes. Response time was 11.585 ms.

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


Attacker Kali - External Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Thu 17:14
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
VM - Kali Login inf... VMware Workstatio... Hyper-V Manager Attacker Kali - Exter... Ubuntu 64-bit on C...
5:14 PM 2/16/2023

Filter: dns

```
No.  Time          Source          Destination     Protocol Length Info
 117 65.083448200  192.168.217.3   192.168.217.2   DNS      81 Standard query 0x182d A 3.debian
 118 65.083457800  192.168.217.3   192.168.217.2   DNS      81 Standard query 0xc834 AAAA 3.deb:
 119 65.089580900  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x182d Re
 120 65.089616700  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xc834 Re
 127 70.086590200  192.168.217.3   192.168.217.2   DNS      81 Standard query 0x182d A 3.debian
 128 70.086600600  192.168.217.3   192.168.217.2   DNS      81 Standard query 0xc834 AAAA 3.deb:
 129 70.097170200  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x182d Re
 130 70.097367300  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xc834 Re
```

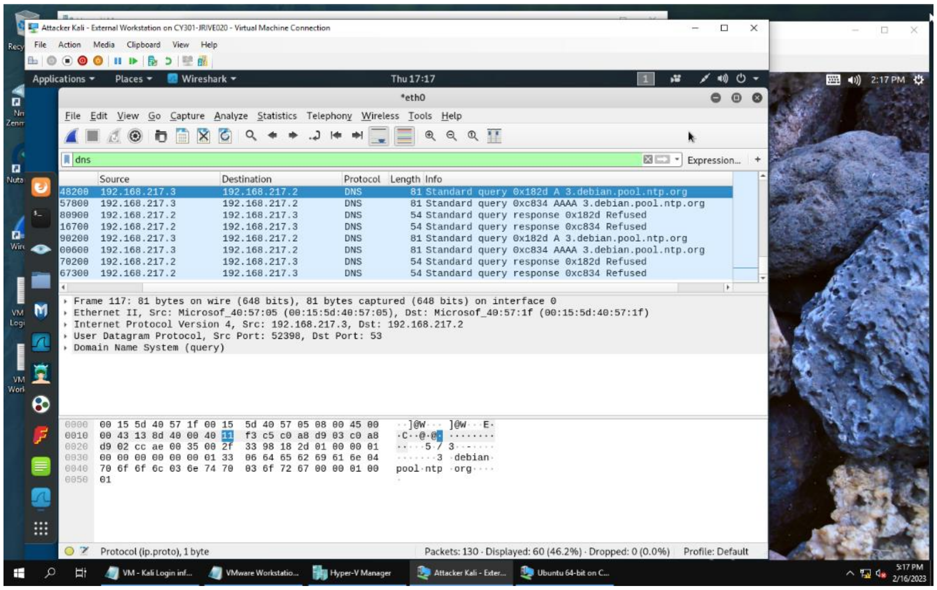
```
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168.217.3
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x523e (21054)
  ▸ Flags: 0x0000
    Time to live: 64
    Protocol: UDP (17)
```

```
0000  00 15 5d 40 57 05 00 15  5d 40 57 1f 08 00 45 00   ··]@W··· ]@W···E·
0010  00 28 52 3e 00 00 40 11  f5 2f c0 a8 d9 02 c0 a8   ·(R>··@· ·/······
0020  d9 03 00 35 ed c4 00 14  fe ae 5e c0 81 05 00 00   ···5···· ··^·····
0030  00 00 00 00 00 00                                  ······
```

Domain Name System: Protocol   Packets: 130 · Displayed: 60 (46.2%) · Dropped: 0 (0.0%)   Profile: Default

60 DNS packets are 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.**


Attacker Kali - External Workstation on CY301-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Thu 17:17
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
VM - Kali Login inf... VMware Workstatio... Hyper-V Manager Attacker Kali - Exter... Ubuntu 64-bit on C...
5:17 PM 2/16/2023

Filter: dns

```
       Source          Destination     Protocol Length Info
48200  192.168.217.3   192.168.217.2   DNS      81 Standard query 0x182d A 3.debian.pool.ntp.org
57800  192.168.217.3   192.168.217.2   DNS      81 Standard query 0xc834 AAAA 3.debian.pool.ntp.org
80900  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x182d Refused
16700  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xc834 Refused
90200  192.168.217.3   192.168.217.2   DNS      81 Standard query 0x182d A 3.debian.pool.ntp.org
00600  192.168.217.3   192.168.217.2   DNS      81 Standard query 0xc834 AAAA 3.debian.pool.ntp.org
70200  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0x182d Refused
67300  192.168.217.2   192.168.217.3   DNS      54 Standard query response 0xc834 Refused
```

```
▸ Frame 117: 81 bytes on wire (648 bits), 81 bytes captured (648 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: 192.168.217.2
▸ User Datagram Protocol, Src Port: 52398, Dst Port: 53
▸ 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 13 8d 40 00 40 11  f3 c5 c0 a8 d9 03 c0 a8   ·C··@·@· ········
0020  d9 02 cc ae 00 35 00 2f  33 98 18 2d 01 00 00 01   ·····5·/ 3··-····
0030  00 00 00 00 00 00 01 33  06 64 65 62 69 61 6e 04   ·······3 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp ·org····
0050  01                                                 ·
```

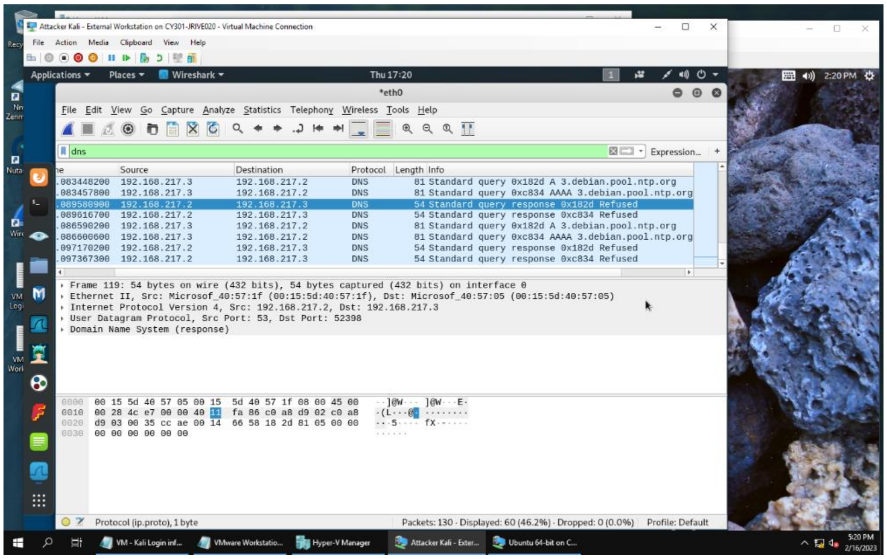
Protocol (ip.proto), 1 byte   Packets: 130 · Displayed: 60 (46.2%) · Dropped: 0 (0.0%)   Profile: Default

The query is trying to resolve the debian.pool.ntp.org domain name.

Source: 192.168.217.3:52398

Dst: 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-JRIVE020 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark
Thu 17:20
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression…
Protocol (ip.proto), 1 byte
Packets: 130 · Displayed: 60 (46.2%) · Dropped: 0 (0.0%)
Profile: Default
VM - Kali Login inf…
VMware Workstatio…
Hyper-V Manager
Attacker Kali - Exter…
Ubuntu 64-bit on C…
2:20 PM
5:20 PM
2/16/2023

```
ne           Source          Destination     Protocol Length Info
.083448200   192.168.217.3   192.168.217.2   DNS        81 Standard query 0x182d A 3.debian.pool.ntp.org
.083457800   192.168.217.3   192.168.217.2   DNS        81 Standard query 0xc834 AAAA 3.debian.pool.ntp.org
.089580900   192.168.217.2   192.168.217.3   DNS        54 Standard query response 0x182d Refused
.089616700   192.168.217.2   192.168.217.3   DNS        54 Standard query response 0xc834 Refused
.086590200   192.168.217.3   192.168.217.2   DNS        81 Standard query 0x182d A 3.debian.pool.ntp.org
.086600600   192.168.217.3   192.168.217.2   DNS        81 Standard query 0xc834 AAAA 3.debian.pool.ntp.org
.097170200   192.168.217.2   192.168.217.3   DNS        54 Standard query response 0x182d Refused
.097367300   192.168.217.2   192.168.217.3   DNS        54 Standard query response 0xc834 Refused
```

```
› Frame 119: 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: 52398
› 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 4c e7 00 00 40 11  fa 86 c0 a8 d9 02 c0 a8   ·(L···@·········
0020  d9 03 00 35 cc ae 00 14  66 58 18 2d 81 05 00 00   ···5····fX·-····
0030  00 00 00 00 00 00                                  ······
```

Source: 192.168.217.2:53
Dst: 192.168.217.3:52398

The message was that the query was refused.