OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT 2: TRAFFIC TRACING AND SNIFFING

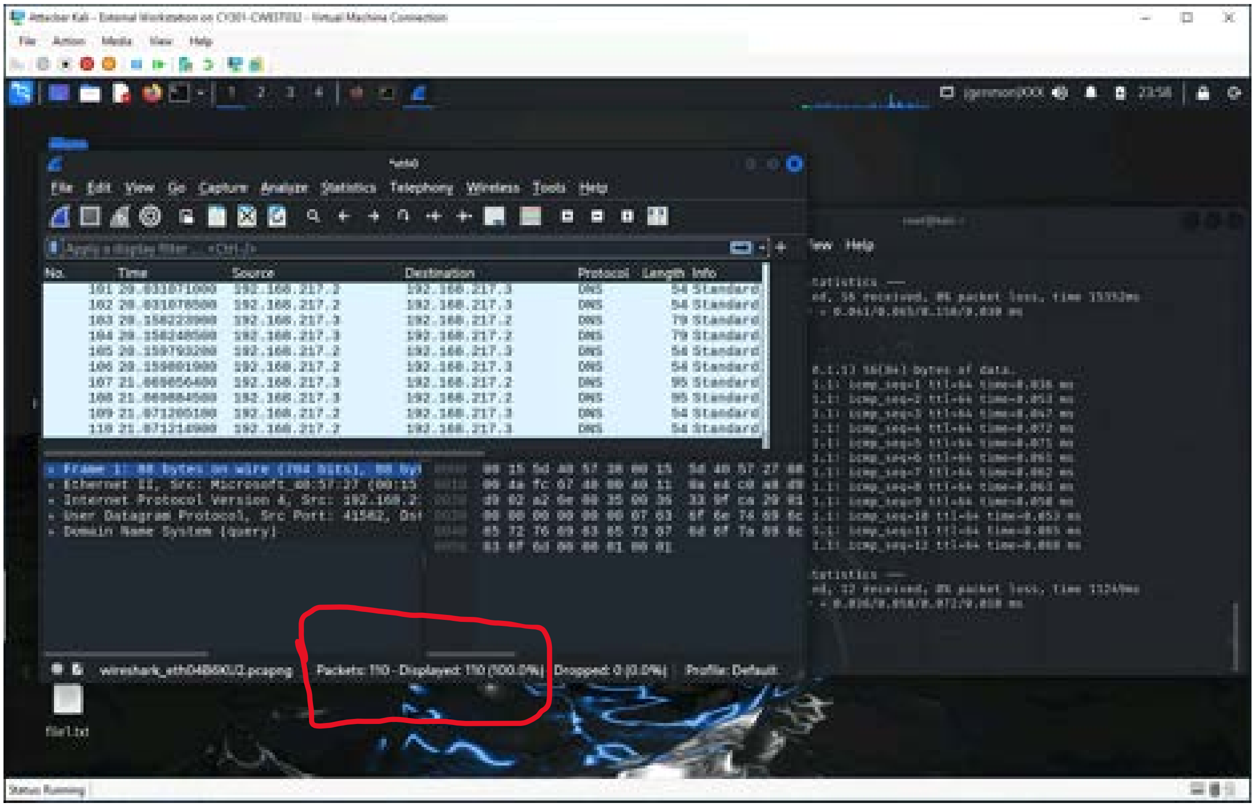
Chandler Aiden West

01226601

Below is the snippet of a sample lab report.

TASK A

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


Attacker Kali - External Workstation on CY301-CWEST02 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
file1.txt
Status: Running

```
No.   Time          Source            Destination       Protocol  Length Info
  101 20.031071000  192.168.217.2     192.168.217.3     DNS          54 Standard
  102 20.031078500  192.168.217.2     192.168.217.3     DNS          54 Standard
  103 20.158223900  192.168.217.3     192.168.217.2     DNS          79 Standard
  104 20.158240500  192.168.217.3     192.168.217.2     DNS          79 Standard
  105 20.159793200  192.168.217.2     192.168.217.3     DNS          54 Standard
  106 20.159801900  192.168.217.2     192.168.217.3     DNS          54 Standard
  107 21.069656400  192.168.217.3     192.168.217.2     DNS          95 Standard
  108 21.069604500  192.168.217.3     192.168.217.2     DNS          95 Standard
  109 21.071205100  192.168.217.2     192.168.217.3     DNS          54 Standard
  110 21.071214900  192.168.217.2     192.168.217.3     DNS          54 Standard
```

```
> Frame 1: 88 bytes on wire (704 bits), 88 by
> Ethernet II, Src: Microsoft_40:57:27 (00:15
> Internet Protocol Version 4, Src: 192.168.2
> User Datagram Protocol, Src Port: 41582, Dst
> Domain Name System (query)
```

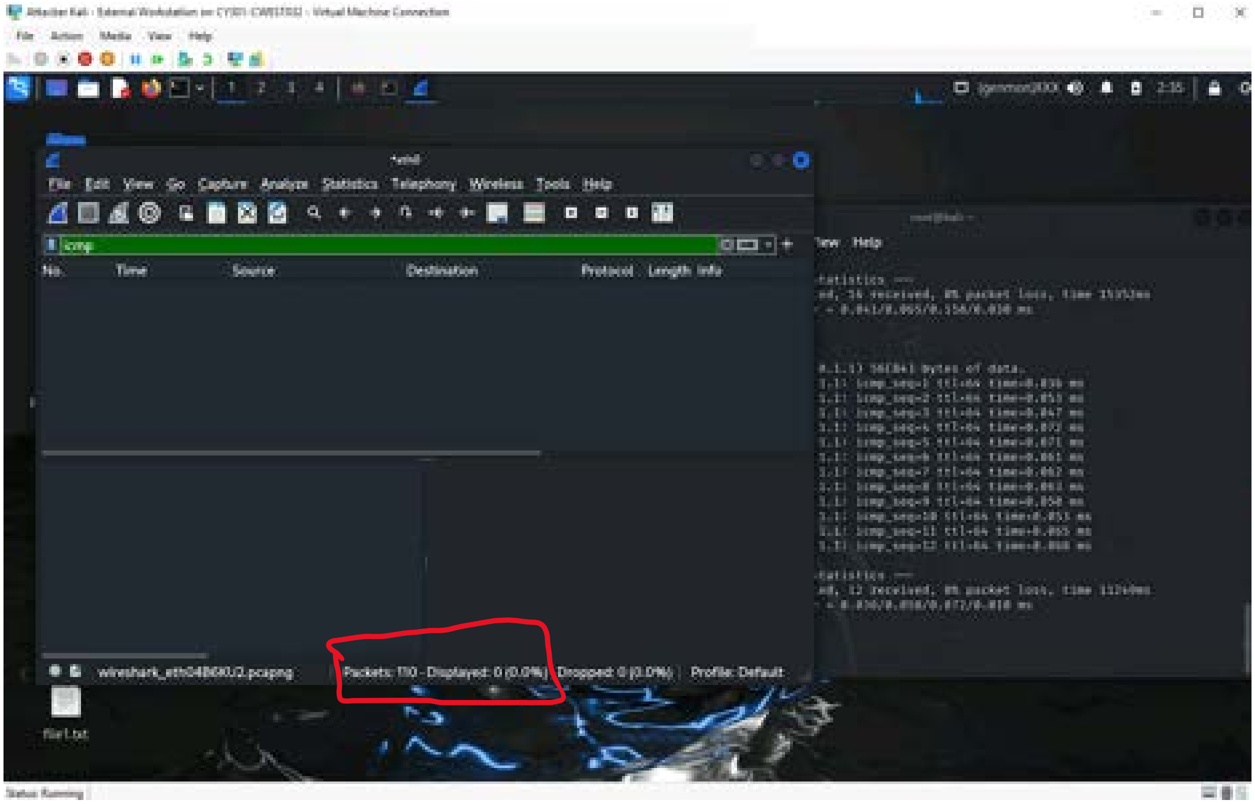
```
0000  00 15 5d 40 57 28 00 15  5d 40 57 27 08
0010  00 4a fc 07 40 00 40 11  8a e4 c0 a8 d9
0020  d9 02 a2 6e 00 35 00 36  33 9f ca 20 01
0030  00 00 00 00 00 00 07 63  6f 6e 74 69 6c
0040  65 72 76 69 63 65 73 07  6d 6f 7a 69 6c
0050  63 6f 6d 00 00 01 00 01
```

```
tatistics ---
ed, 16 received, 0% packet loss, time 15352ms
 = 0.041/0.065/0.116/0.030 ms

8.1.1) 56(84) bytes of data.
1.1: icmp_seq=1 ttl=64 time=0.036 ms
1.1: icmp_seq=2 ttl=64 time=0.053 ms
1.1: icmp_seq=3 ttl=64 time=0.047 ms
1.1: icmp_seq=4 ttl=64 time=0.072 ms
1.1: icmp_seq=5 ttl=64 time=0.071 ms
1.1: icmp_seq=6 ttl=64 time=0.051 ms
1.1: icmp_seq=7 ttl=64 time=0.062 ms
1.1: icmp_seq=8 ttl=64 time=0.063 ms
1.1: icmp_seq=9 ttl=64 time=0.058 ms
1.1: icmp_seq=10 ttl=64 time=0.053 ms
1.1: icmp_seq=11 ttl=64 time=0.065 ms
1.1: icmp_seq=12 ttl=64 time=0.060 ms

tatistics ---
ed, 12 received, 0% packet loss, time 11249ms
 = 0.036/0.058/0.072/0.010 ms
```

```
wireshark_eth04B6KU2.pcapng   Packets: 110 - Displayed: 110 (100.0%)   Dropped: 0 (0.0%)   Profile: Default
```

There are 110 packets captured in total and 110 packets displayed.

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


Attacker Kali - External Workstation on CYS01-CWS07032 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
file1.txt
Status: Running

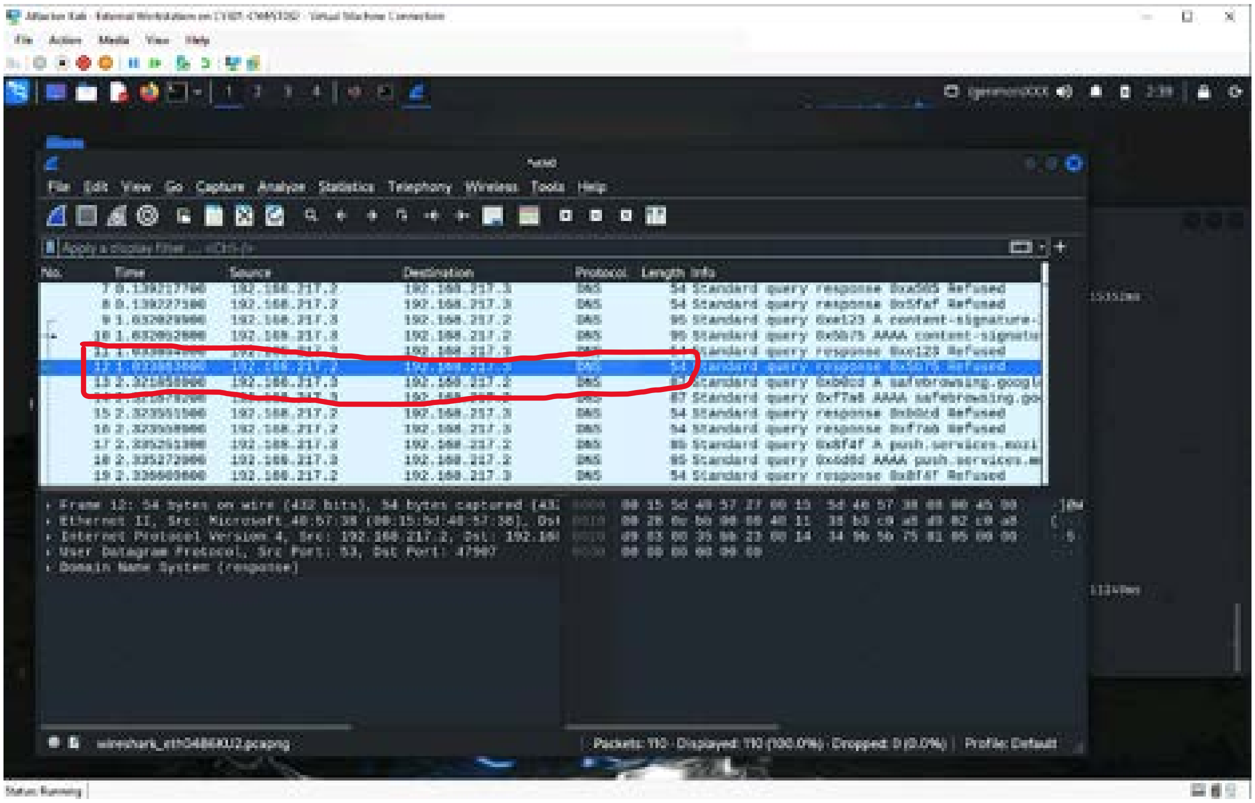
icmp

```
tatistics ---
ed, 16 received, 0% packet loss, time 15352ms
 = 0.041/0.065/0.156/0.030 ms

0.1.1) 56(84) bytes of data.
1.1: icmp_seq=1 ttl=64 time=0.036 ms
1.1: icmp_seq=2 ttl=64 time=0.053 ms
1.1: icmp_seq=3 ttl=64 time=0.047 ms
1.1: icmp_seq=4 ttl=64 time=0.072 ms
1.1: icmp_seq=5 ttl=64 time=0.071 ms
1.1: icmp_seq=6 ttl=64 time=0.061 ms
1.1: icmp_seq=7 ttl=64 time=0.062 ms
1.1: icmp_seq=8 ttl=64 time=0.063 ms
1.1: icmp_seq=9 ttl=64 time=0.058 ms
1.1: icmp_seq=10 ttl=64 time=0.053 ms
1.1: icmp_seq=11 ttl=64 time=0.065 ms
1.1: icmp_seq=12 ttl=64 time=0.060 ms

tatistics ---
ed, 12 received, 0% packet loss, time 11264ms
 = 0.036/0.058/0.072/0.010 ms
```

wireshark_eth04B6KU2.pcapng | Packets: 110 · Displayed: 0 (0.0%) | Dropped: 0 (0.0%) | Profile: Default

There are 110 packets captured and 0 packets displayed.

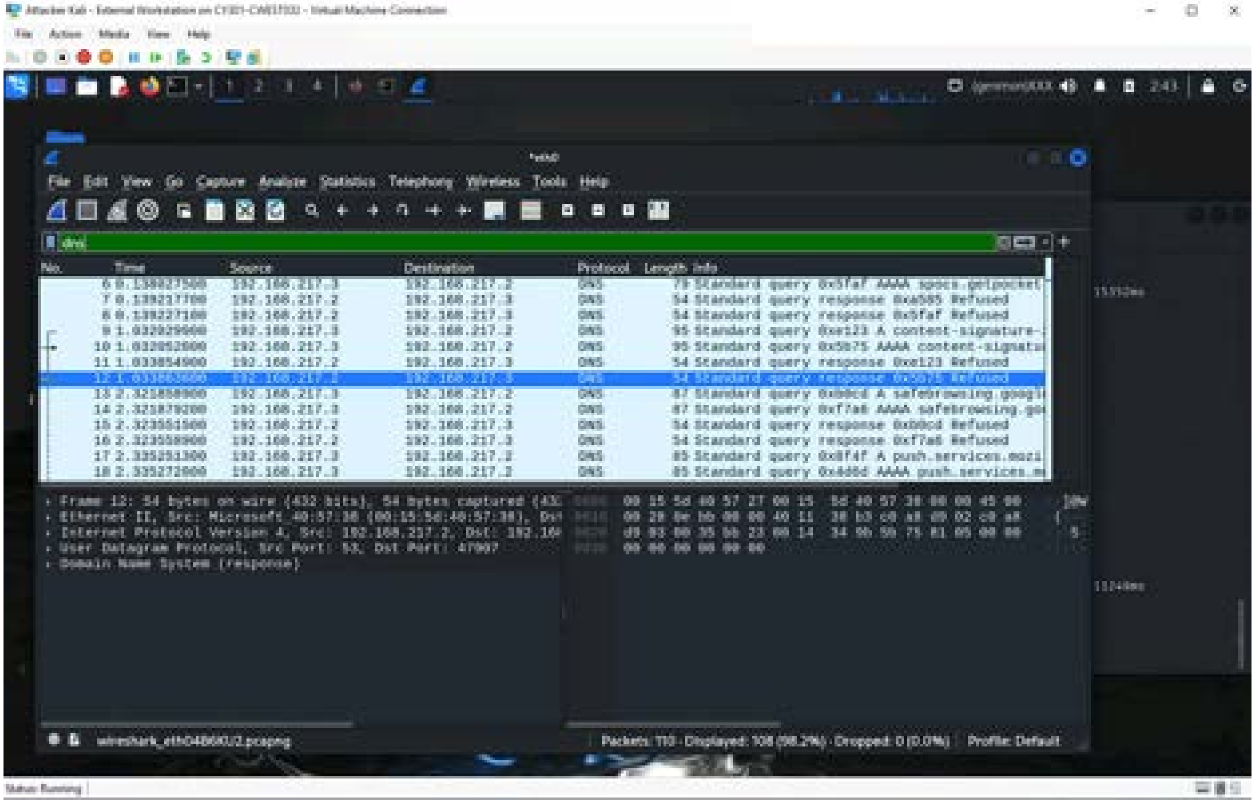
Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?



```
No.  Time          Source          Destination     Protocol  Length Info
   7 0.139217700   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xa505 Refused
   8 0.139227500   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x5faf Refused
   9 1.032029000   192.168.217.3   192.168.217.2   DNS       95 Standard query 0xe123 A content-signature-
  10 1.032052000   192.168.217.3   192.168.217.2   DNS       95 Standard query 0x5b75 AAAA content-signatu
  11 1.033034000   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xe123 Refused
  12 1.033053000   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x5b75 Refused
  13 2.321858000   192.168.217.3   192.168.217.2   DNS       87 Standard query 0xb0cd A safebrowsing.googl
  14 2.321878200   192.168.217.3   192.168.217.2   DNS       87 Standard query 0xf7a6 AAAA safebrowsing.go
  15 2.323551500   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xb0cd Refused
  16 2.323558000   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0xf7a6 Refused
  17 2.335251300   192.168.217.3   192.168.217.2   DNS       85 Standard query 0x8f4f A push.services.mozi
  18 2.335272000   192.168.217.3   192.168.217.2   DNS       85 Standard query 0xd8d AAAA push.services.m
  19 2.336003000   192.168.217.2   192.168.217.3   DNS       54 Standard query response 0x8f4f Refused

› Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (43
› Ethernet II, Src: Microsoft_40:57:38 (00:15:5d:40:57:38), Dst
› Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.168
› User Datagram Protocol, Src Port: 53, Dst Port: 47907
› Domain Name System (response)

0000  00 15 5d 40 57 27 00 15  5d 40 57 38 08 00 45 00
0010  00 28 0c b0 00 00 40 11  33 b3 c0 a8 d9 02 c0 a8
0020  d9 03 00 35 bb 23 00 14  34 9b 5b 75 81 05 00 00
0030  00 00 00 00 00 00

wireshark_eth0486KU2.pcapng     Packets: 110 · Displayed: 110 (100.0%) · Dropped: 0 (0.0%)  |  Profile: Default
```

Source IP: 192.168.217.2 Destination IP: 192.168.217.3 Sequence Number: 12 Size: 54 bytes

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



Attacker Kali - External Workstation on CY301-CWE57032 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Status: Running

```
No.    Time          Source           Destination      Protocol  Length Info
     6 0.138027500   192.168.217.3    192.168.217.2    DNS       79 Standard query 0x5faf AAAA spocs.getpocket
     7 0.139217700   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xa585 Refused
     8 0.139227100   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x5faf Refused
     9 1.032029000   192.168.217.3    192.168.217.2    DNS       95 Standard query 0xe123 A content-signature-
    10 1.032052000   192.168.217.3    192.168.217.2    DNS       95 Standard query 0x5b75 AAAA content-signatu
    11 1.033854900   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xe123 Refused
    12 1.033863600   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x5b75 Refused
    13 2.321858000   192.168.217.3    192.168.217.2    DNS       87 Standard query 0xb0cd A safebrowsing.googl
    14 2.321879200   192.168.217.3    192.168.217.2    DNS       87 Standard query 0xf7a6 AAAA safebrowsing.go
    15 2.323551500   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xb0cd Refused
    16 2.323558900   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xf7a6 Refused
    17 2.335251300   192.168.217.3    192.168.217.2    DNS       85 Standard query 0x8f4f A push.services.mozi
    18 2.335272000   192.168.217.3    192.168.217.2    DNS       85 Standard query 0x4d0d AAAA push.services.m
```

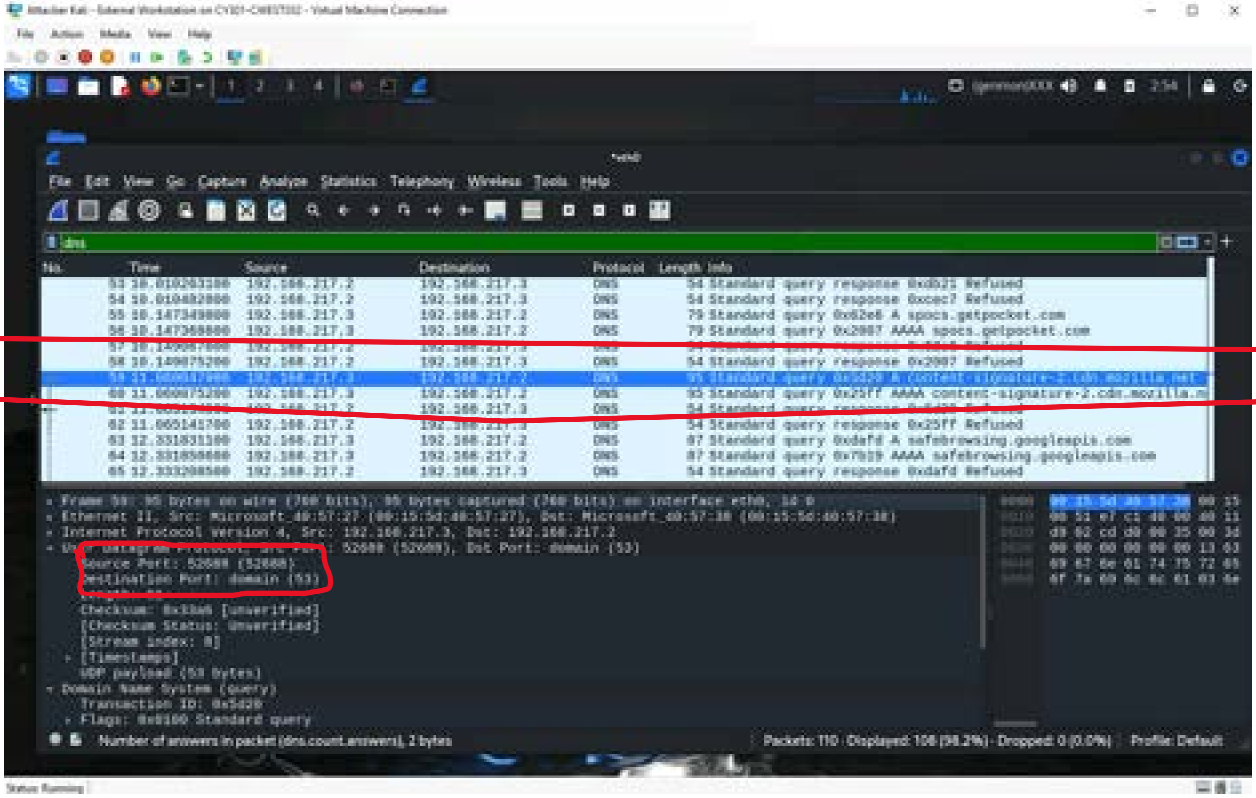
```
› Frame 12: 54 bytes on wire (432 bits), 54 bytes captured (43
› Ethernet II, Src: Microsoft_40:57:38 (00:15:5d:40:57:38), Dst
› Internet Protocol Version 4, Src: 192.168.217.2, Dst: 192.16
› User Datagram Protocol, Src Port: 53, Dst Port: 47907
› Domain Name System (response)
```

```
0000  00 15 5d 40 57 27 00 15  5d 40 57 38 08 00 45 00   ]@W
0010  00 28 0e bb 00 00 40 11  38 b3 c0 a8 d9 02 c0 a8   (
0020  d9 03 00 35 bb 23 00 14  34 9b 5b 75 81 05 00 00    5
0030  00 00 00 00 00 00
```

```
wireshark_eth04B6KU2.pcapng     Packets: 110 · Displayed: 108 (98.2%) · Dropped: 0 (0.0%)   Profile: Default
```

There are 110 packets and 108 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.

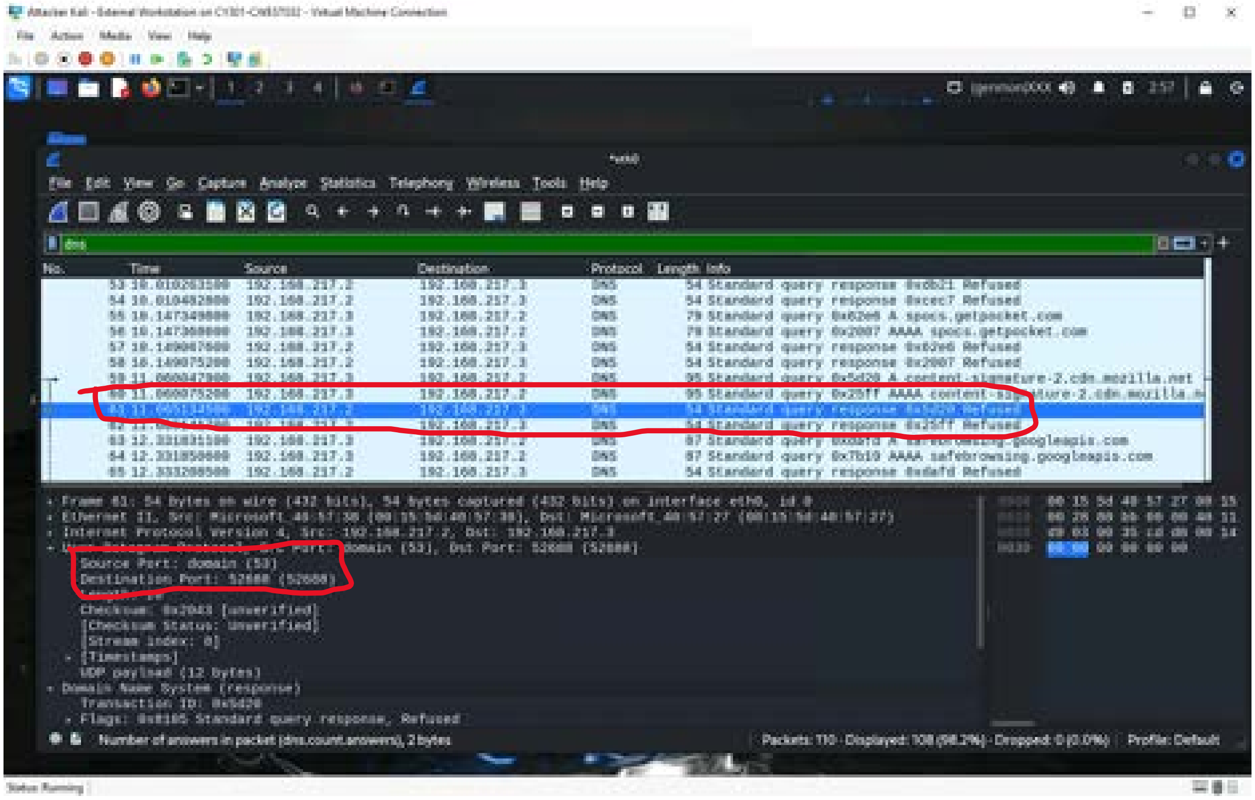


Attacker Kali - External Workstation on CY301-CWEST02 - Virtual Machine Connection
File Action Media View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time           Source          Destination     Protocol Length Info
53 10.010203100 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0xdb21 Refused
54 10.010482000 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0xcec7 Refused
55 10.147349000 192.168.217.3 192.168.217.2 DNS 79 Standard query 0x82e6 A spocs.getpocket.com
56 10.147360000 192.168.217.3 192.168.217.2 DNS 79 Standard query 0x2007 AAAA spocs.getpocket.com
57 10.149087000 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x82e6 Refused
58 10.149875200 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x2007 Refused
59 11.060817000 192.168.217.3 192.168.217.2 DNS 95 Standard query 0x5d20 A content-signature-2.cdn.mozilla.net
60 11.060875200 192.168.217.3 192.168.217.2 DNS 95 Standard query 0x25ff AAAA content-signature-2.cdn.mozilla.n
61 11.065131000 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x5d20 Refused
62 11.065141700 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0x25ff Refused
63 12.331831100 192.168.217.3 192.168.217.2 DNS 87 Standard query 0xdafd A safebrowsing.googleapis.com
64 12.331850800 192.168.217.3 192.168.217.2 DNS 87 Standard query 0x7b19 AAAA safebrowsing.googleapis.com
65 12.333208500 192.168.217.2 192.168.217.3 DNS 54 Standard query response 0xdafd Refused

> Frame 59: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface eth0, id 0
> Ethernet 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
v User Datagram Protocol, Src Port: 52688 (52688), Dst Port: domain (53)
    Source Port: 52688 (52688)
    Destination Port: domain (53)
    Length: 61
    Checksum: 0x33b6 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 8]
  > [Timestamps]
    UDP payload (53 bytes)
v Domain Name System (query)
    Transaction ID: 0x5d20
  > Flags: 0x0100 Standard query

0000  00 15 5d 40 57 38 00 15
0010  00 51 e7 c1 40 00 40 11
0020  d9 02 cd d0 00 35 00 3d
0030  00 00 00 00 00 00 13 63
0040  69 67 6e 61 74 75 72 65
0050  6f 7a 69 6c 6c 61 03 6e

Number of answers in packet (dns.count.answers), 2 bytes
Packets: 110 · Displayed: 108 (98.2%) · Dropped: 0 (0.0%)    Profile: Default
```

Domain Name: cdn.mozilla.net Source: 192.168.217.3:52688 Destination: 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-CWS57032 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Status: Running

```
No.   Time            Source           Destination      Protocol Length Info
   53 10.010203500   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xdb21 Refused
   54 10.010482800   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xcec7 Refused
   55 10.147349800   192.168.217.3    192.168.217.2    DNS       79 Standard query 0x62e6 A spocs.getpocket.com
   56 10.147368800   192.168.217.3    192.168.217.2    DNS       79 Standard query 0x2007 AAAA spocs.getpocket.com
   57 10.149067600   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x62e6 Refused
   58 10.149075200   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x2007 Refused
   59 11.060047900   192.168.217.3    192.168.217.2    DNS       95 Standard query 0x5d20 A content-signature-2.cdn.mozilla.net
   60 11.060075200   192.168.217.3    192.168.217.2    DNS       95 Standard query 0x25ff AAAA content-signature-2.cdn.mozilla.n
   61 11.065134500   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x5d20 Refused
   62 11.0[illegible]  192.168.217.2    192.168.217.3    DNS       54 Standard query response 0x25ff Refused
   63 12.331835100   192.168.217.3    192.168.217.2    DNS       87 Standard query 0xdafd A safebrowsing.googleapis.com
   64 12.331850800   192.168.217.3    192.168.217.2    DNS       87 Standard query 0x7b10 AAAA safebrowsing.googleapis.com
   65 12.333208500   192.168.217.2    192.168.217.3    DNS       54 Standard query response 0xdafd Refused
```

```
> Frame 61: 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
v User Datagram Protocol, Src Port: domain (53), Dst Port: 52688 (52688)
    Source Port: domain (53)
    Destination Port: 52688 (52688)
    Length: 20
    Checksum: 0x2043 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (12 bytes)
v Domain Name System (response)
    Transaction ID: 0x5d20
  > Flags: 0x8105 Standard query response, Refused
```

```
0000  00 15 5d 40 57 27 00 15
0010  00 28 00 bb 00 00 40 11
0020  d9 03 00 35 cd d0 00 14
0030  00 00 00 00 00 00
```

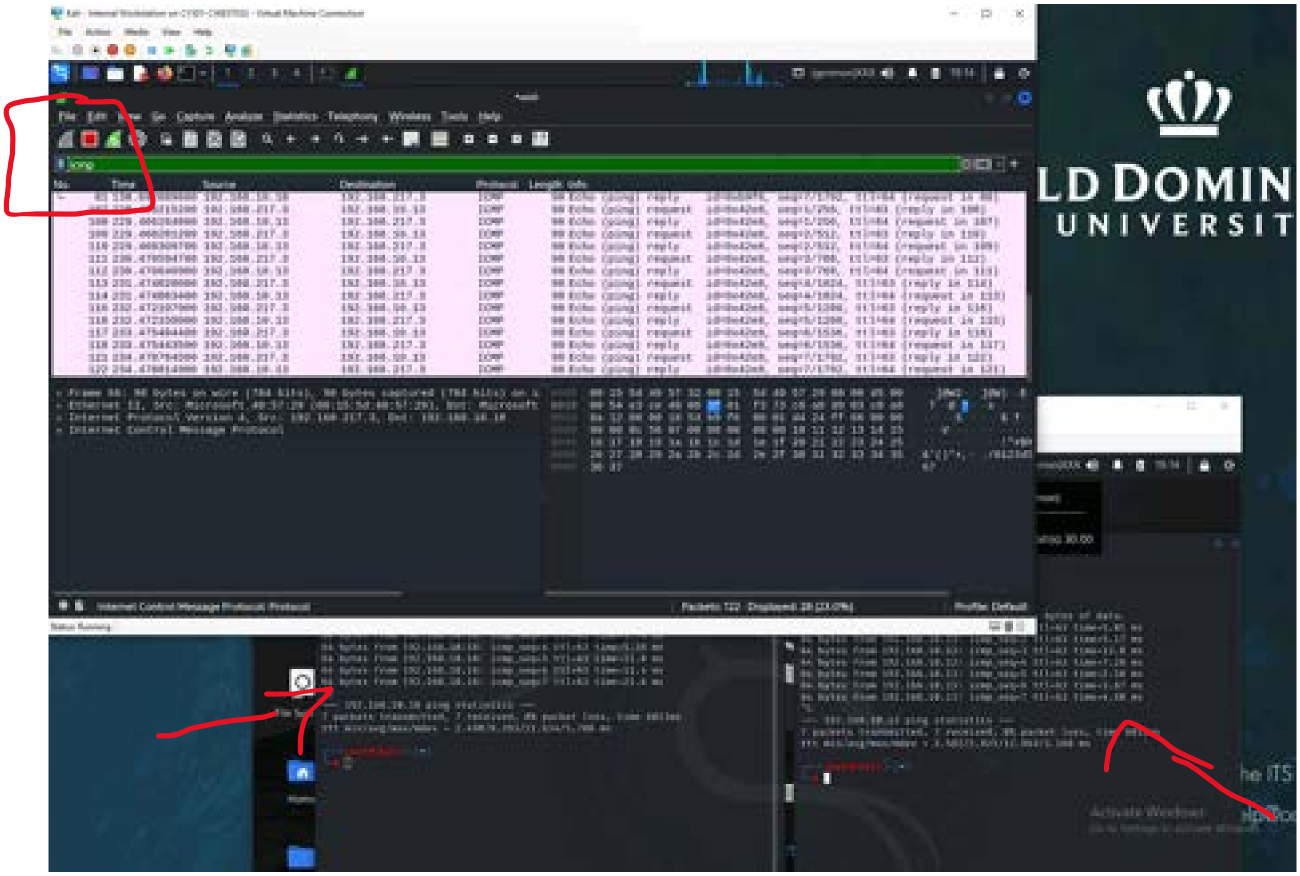
Number of answers in packet (dns.count.answers), 2 bytes   Packets: 110 · Displayed: 108 (98.2%) · Dropped: 0 (0.0%)   Profile: Default

Source: 192.168.217.2:53 Destination: 192.168.217.3:52688 Message: Refused

TASK B

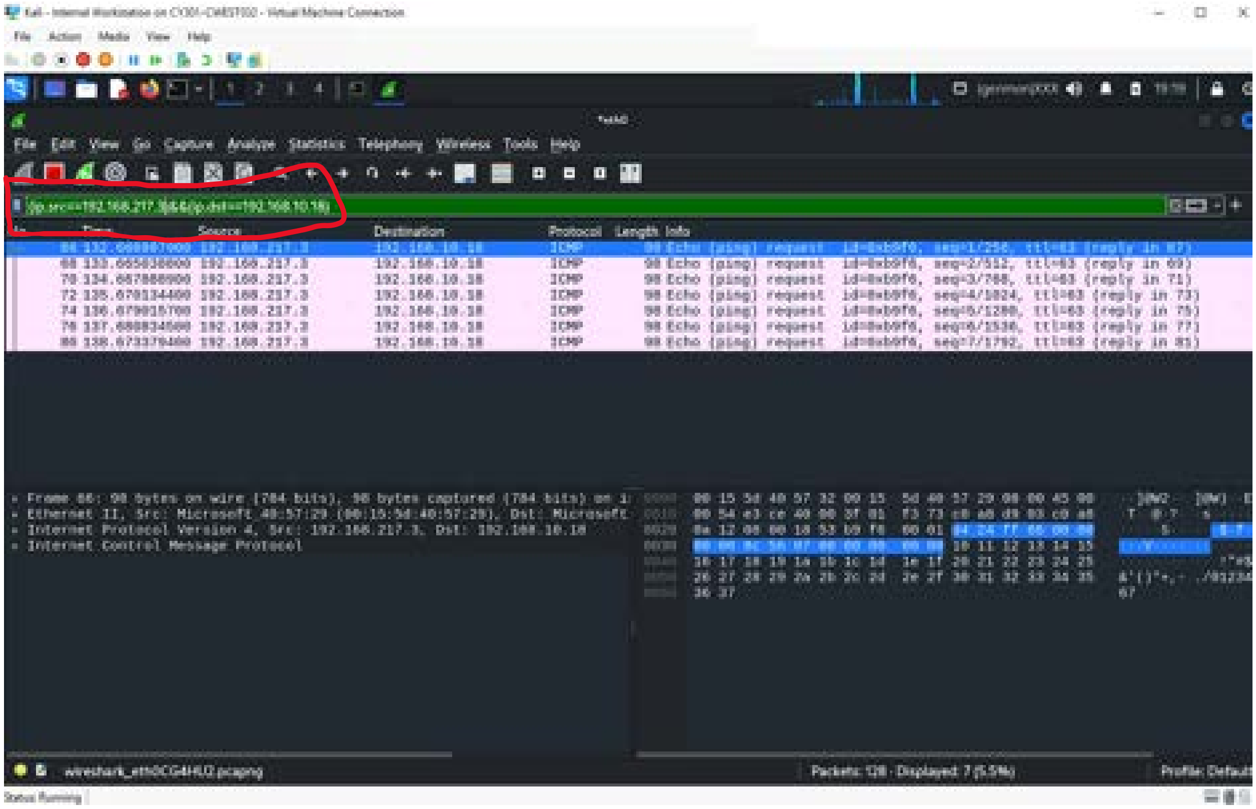
1. Sniff ICMP traffic

A:


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Destination Protocol Length Info
Internet Control Message Protocol: Protocol
Packets: 122 · Displayed: 28 (23.0%)
Profile: Default
Status: Running
Activate Windows

Pinged both Internal Kali and Ubuntu and applied the icmp filter to wireshark.

B:



Kali - Internal Workstation on CY301-CWEST02 - Virtual Machine Connection
File Action Media View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
*eth0
Status: Running

```
(ip.src==192.168.217.3)&&(ip.dst==192.168.10.18)
```

```
No.  Time           Source          Destination     Protocol  Length  Info
66   132.660887000  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=1/256, ttl=63 (reply in 67)
68   133.665038000  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=2/512, ttl=63 (reply in 69)
70   134.667888000  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=3/768, ttl=63 (reply in 71)
72   135.670134400  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=4/1024, ttl=63 (reply in 73)
74   136.670015700  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=5/1280, ttl=63 (reply in 75)
76   137.668834500  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=6/1536, ttl=63 (reply in 77)
80   138.673379400  192.168.217.3   192.168.10.18   ICMP      98      Echo (ping) request  id=0xb0f6, seq=7/1792, ttl=63 (reply in 83)
```

```
› Frame 66: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on i
› Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft_
› Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
› Internet Control Message Protocol
```

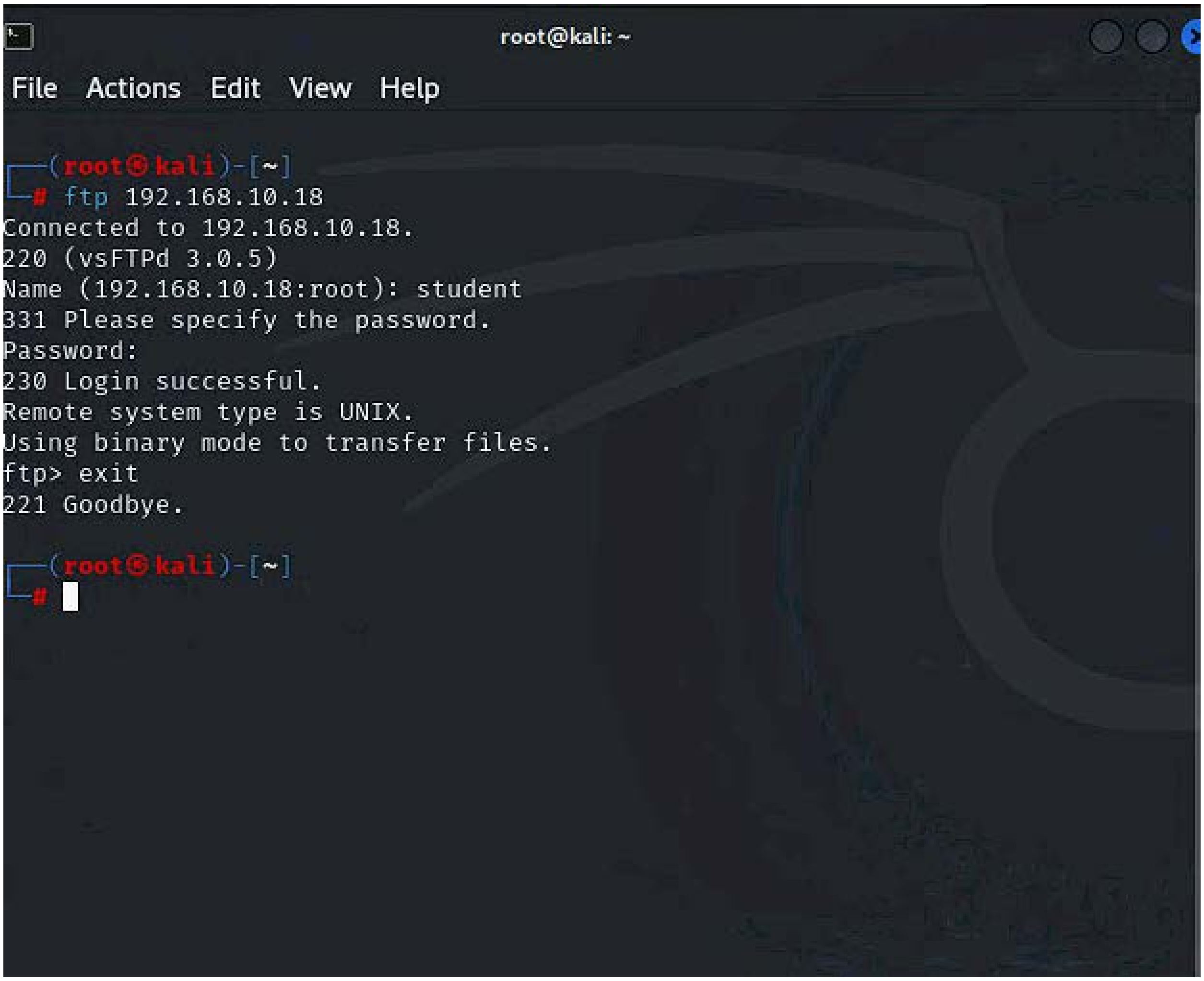
```
0000  00 15 5d 40 57 32 00 15  5d 40 57 29 08 00 45 00   ..]@W2.. ]@W)..E
0010  00 54 e3 ce 40 00 3f 01  f3 73 c0 a8 d9 03 c0 a8   .T..@.?. .s......
0020  0a 12 08 00 18 53 b0 f6  00 01 a4 24 ff 66 00 00   .....S.. ...$.f..
0030  00 00 8c 56 07 00 00 00  00 00 10 11 12 13 14 15   ...V.... ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

wireshark_eth0CG4HU2.pcapng   Packets: 128 · Displayed: 7 (5.5%)   Profile: Default

Put this in the filter to see data in between external kali and Ubuntu.

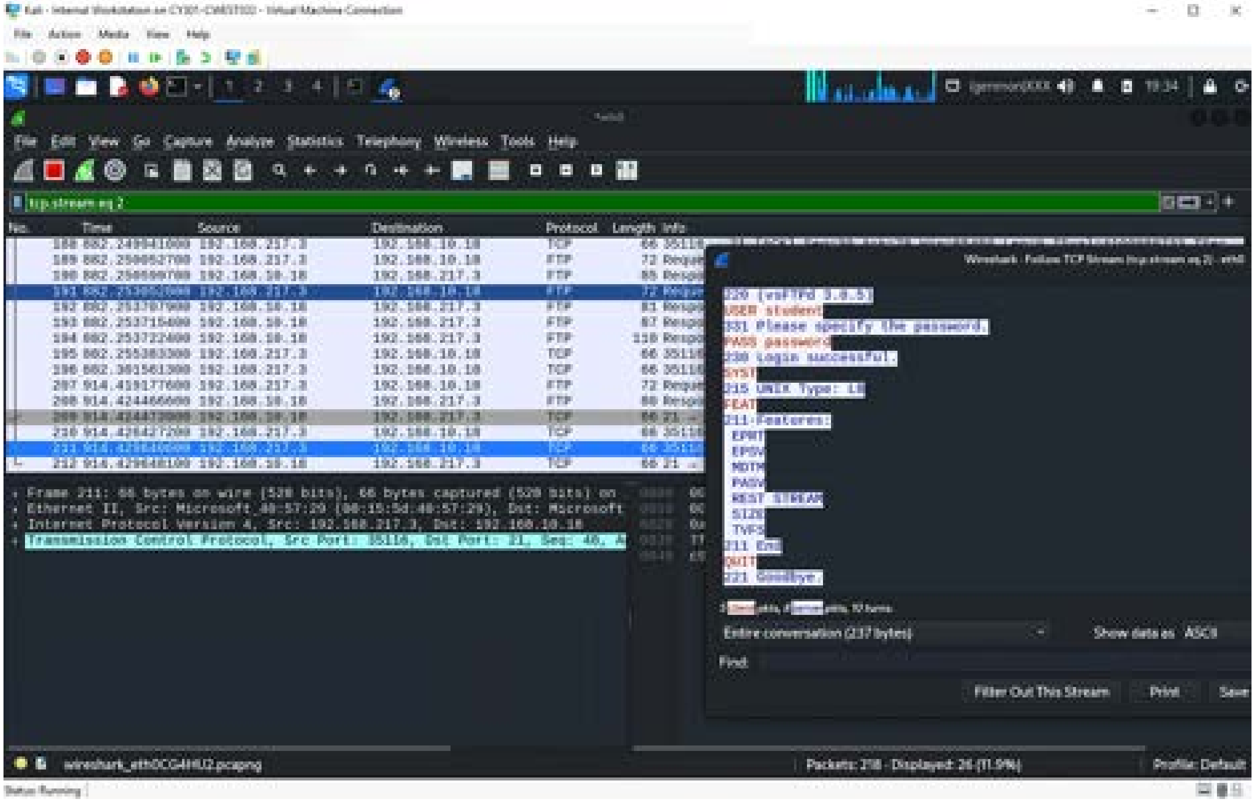
2. Sniff FTP traffic

A:



```
┌──(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:



tcp.stream eq 2

```
No.  Time           Source          Destination     Protocol Length Info
 188 882.249941000 192.168.217.3   192.168.10.18   TCP      66 3511…
 189 882.250052700 192.168.217.3   192.168.10.18   FTP      72 Reque…
 190 882.250500700 192.168.10.18   192.168.217.3   FTP      85 Respo…
 191 882.253052000 192.168.217.3   192.168.10.18   FTP      72 Reque…
 192 882.253707900 192.168.10.18   192.168.217.3   FTP      81 Respo…
 193 882.253715400 192.168.10.18   192.168.217.3   FTP      87 Respo…
 194 882.253722400 192.168.10.18   192.168.217.3   FTP     118 Respo…
 195 882.255383300 192.168.217.3   192.168.10.18   TCP      66 3511…
 196 882.301561300 192.168.217.3   192.168.10.18   TCP      66 3511…
 207 914.419177600 192.168.217.3   192.168.10.18   FTP      72 Reque…
 208 914.424466000 192.168.10.18   192.168.217.3   FTP      80 Respo…
 209 914.424473000 192.168.10.18   192.168.217.3   TCP      66 21 →
 210 914.426427200 192.168.217.3   192.168.10.18   TCP      66 3511…
 211 914.429640000 192.168.217.3   192.168.10.18   TCP      66 3511…
 212 914.429648100 192.168.10.18   192.168.217.3   TCP      66 21 →
```

```
› Frame 211: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
› Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft
› Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
› Transmission Control Protocol, Src Port: 35110, Dst Port: 21, Seq: 40, A
```

Wireshark · Follow TCP Stream (tcp.stream eq 2) · eth0

```
220 (vsFTPd 3.0.5)
USER student
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
FEAT
211-Features:
 EPRT
 EPSV
 MDTM
 PASV
 REST STREAM
 SIZE
 TVFS
211 End
QUIT
221 Goodbye.
```

Entire conversation (237 bytes)

Show data as ASCII

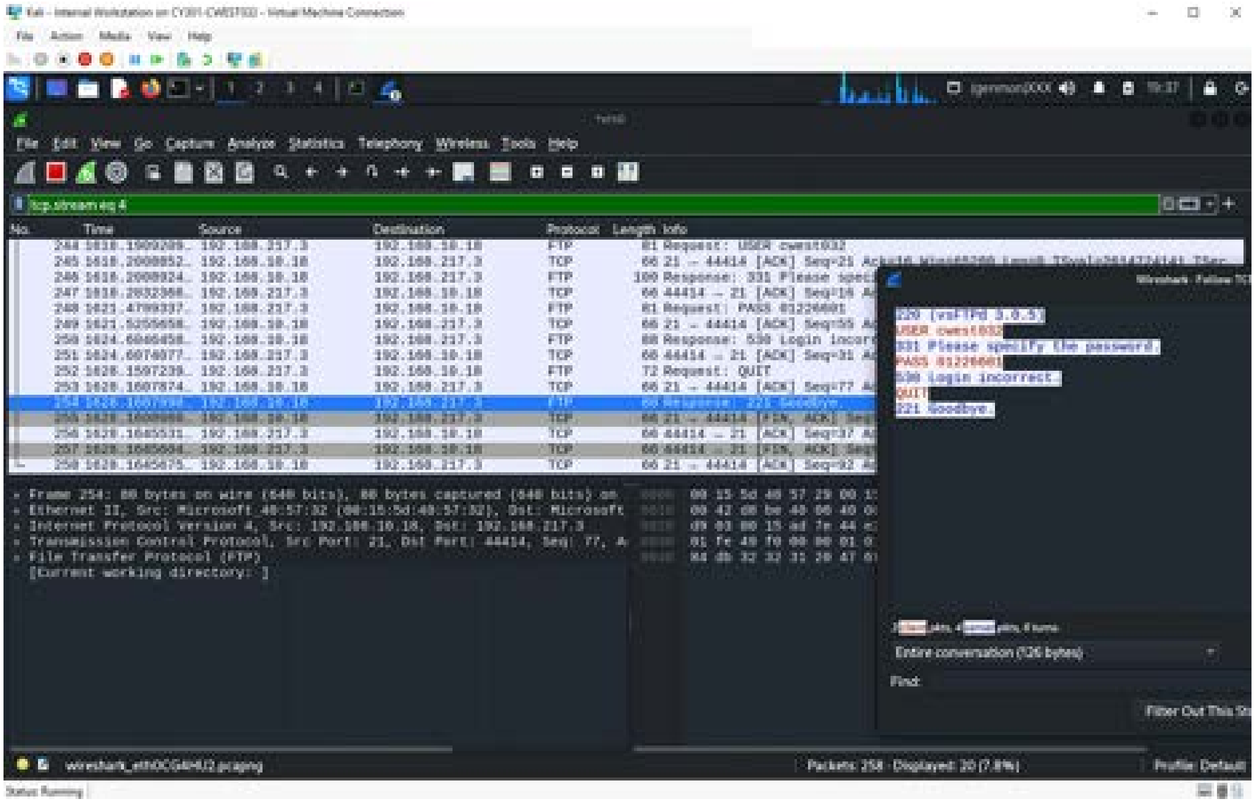
Packets: 218 · Displayed: 26 (11.9%)

Profile: Default

Kali - Internal Workstation on CY301-CW0STI03 - Virtual Machine Connection
File Action Media View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Find:
Filter Out This Stream
Print
Save
wireshark_eth0CG4HU2.pcapng
Status: Running

I captured the internal kali packets with wireshark and followed a tcp packet that went from external kalis ip to internal kali sip. Then it showed me what the username and password were for the connection.

C:



Kali - Internal Workstation on CY301-CWEST032 - Virtual Machine Connection

File Action Media View Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 4

```
No.   Time                Source           Destination      Protocol  Length Info
  244 1618.1980209…  192.168.217.3    192.168.10.18    FTP        81 Request: USER cwest032
  245 1618.2000852…  192.168.10.18    192.168.217.3    TCP        66 21 → 44414 [ACK] Seq=21 Ack=16 Win=65280 Len=0 TSval=2614772414 TSec
  246 1618.2000924…  192.168.10.18    192.168.217.3    FTP       100 Response: 331 Please speci
  247 1618.2032368…  192.168.217.3    192.168.10.18    TCP        66 44414 → 21 [ACK] Seq=16 A
  248 1621.4709337…  192.168.217.3    192.168.10.18    FTP        81 Request: PASS 01226601
  249 1621.5255658…  192.168.10.18    192.168.217.3    TCP        66 21 → 44414 [ACK] Seq=55 A
  250 1624.6066458…  192.168.10.18    192.168.217.3    FTP        88 Response: 530 Login incorr
  251 1624.6074077…  192.168.217.3    192.168.10.18    TCP        66 44414 → 21 [ACK] Seq=31 A
  252 1628.1597239…  192.168.217.3    192.168.10.18    FTP        72 Request: QUIT
  253 1628.1607874…  192.168.10.18    192.168.217.3    TCP        66 21 → 44414 [ACK] Seq=77 A
  254 1628.1607998…  192.168.10.18    192.168.217.3    FTP        80 Response: 221 Goodbye.
  255 1628.1608088…  192.168.10.18    192.168.217.3    TCP        66 21 → 44414 [FIN, ACK] Seq
  256 1628.1645531…  192.168.217.3    192.168.10.18    TCP        66 44414 → 21 [ACK] Seq=37 A
  257 1628.1645604…  192.168.217.3    192.168.10.18    TCP        66 44414 → 21 [FIN, ACK] Seq
  258 1628.1645675…  192.168.10.18    192.168.217.3    TCP        66 21 → 44414 [ACK] Seq=92 A
```

```
› Frame 254: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on
› Ethernet II, Src: Microsoft_40:57:32 (00:15:5d:40:57:32), Dst: Microsoft
› Internet Protocol Version 4, Src: 192.168.10.18, Dst: 192.168.217.3
› Transmission Control Protocol, Src Port: 21, Dst Port: 44414, Seq: 77, A
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000   00 15 5d 40 57 29 00 1
0010   00 42 d8 be 40 00 40 0
0020   d9 03 00 15 ad 7e 44 e
0030   01 fe 40 f0 00 00 01 0
0040   04 db 32 32 31 20 47 6
```

Wireshark · Follow TC

```
220 (vsFTPd 3.0.5)
USER cwest032
331 Please specify the password.
PASS 01226601
530 Login incorrect.
QUIT
221 Goodbye.
```

3 client pkts, 4 server pkts, 4 turns.

Entire conversation (126 bytes)

Find:

wireshark_eth0CG4HU2.pcapng

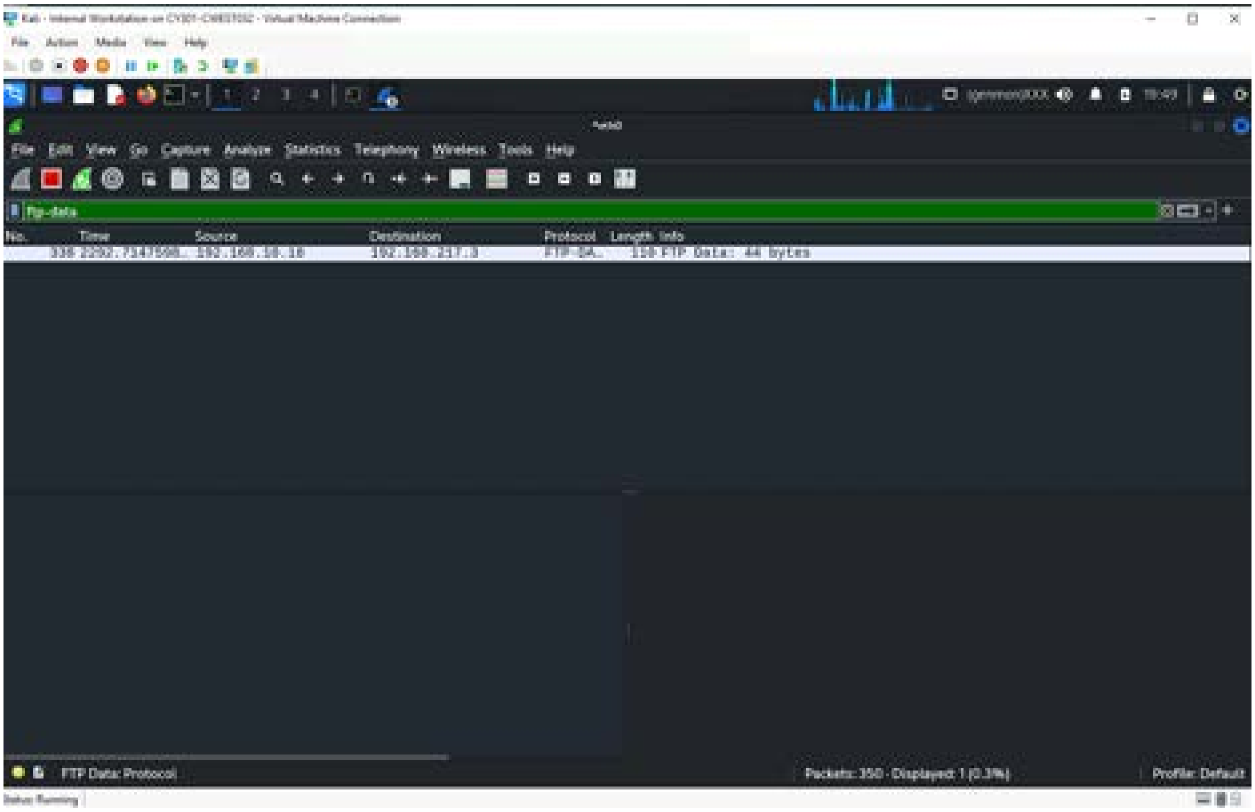
Packets: 258 · Displayed: 20 (7.8%)

Profile: Default

Status: Running

EXTRA CREDIT

1:



ftp-data

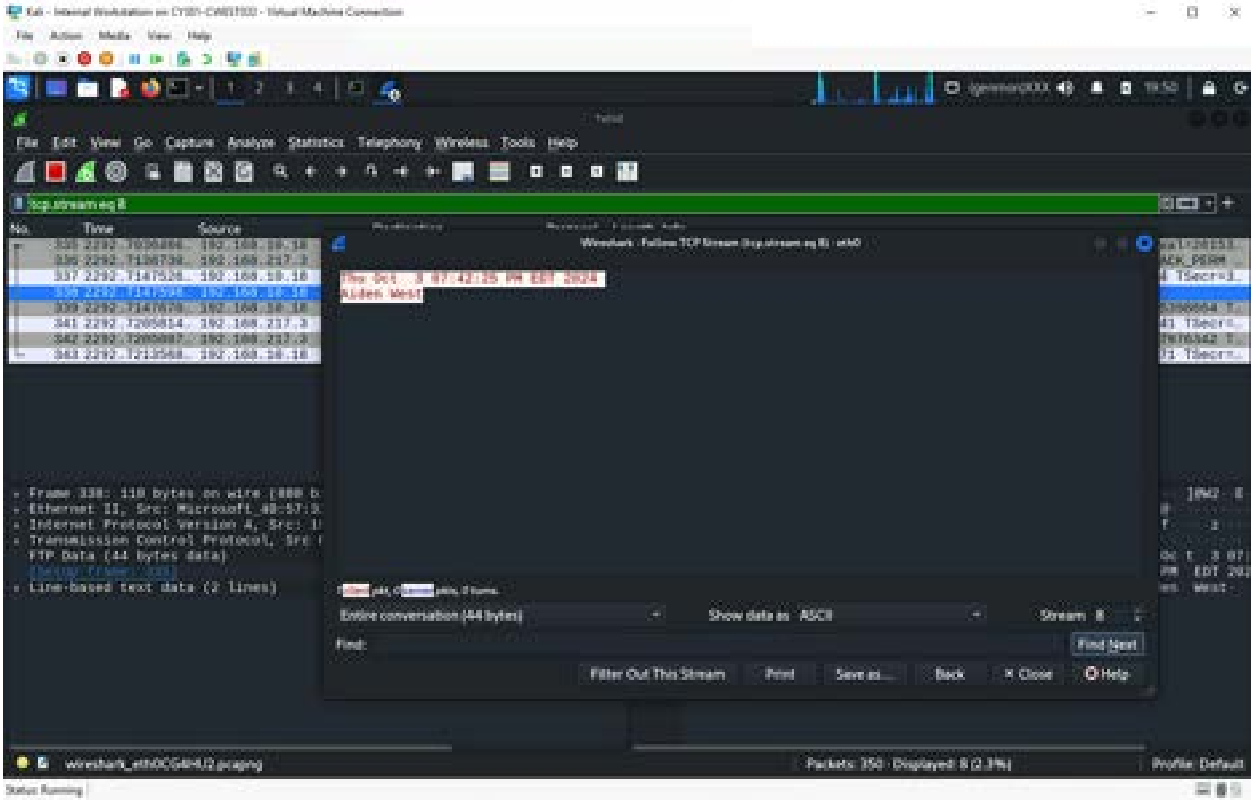
```
No.   Time               Source           Destination      Protocol  Length  Info
  338 2292.7147598…  192.168.10.18    192.168.217.3    FTP-DA…     110  FTP Data: 44 bytes
```

FTP Data: Protocol

Packets: 350 · Displayed: 1 (0.3%)

Profile: Default

2:



tcp.stream eq 8

```
No.   Time               Source
  335 2292.7035466…  192.168.10.18
  336 2292.7136736…  192.168.217.3
  337 2292.7147528…  192.168.10.18
  338 2292.7147598…  192.168.10.18
  339 2292.7147678…  192.168.10.18
  341 2292.7205814…  192.168.217.3
  342 2292.7205887…  192.168.217.3
  343 2292.7213568…  192.168.10.18
```

```
› Frame 338: 110 bytes on wire (880 b
› Ethernet II, Src: Microsoft_40:57:3
› Internet Protocol Version 4, Src: 1
› Transmission Control Protocol, Src
  FTP Data (44 bytes data)
  [Setup frame: 331]
› Line-based text data (2 lines)
```

Wireshark · Follow TCP Stream (tcp.stream eq 8) · eth0

```
Thu Oct  3 07:42:29 PM EDT 2024
Aiden West
```

Entire conversation (44 bytes)

Show data as ASCII

Stream 8

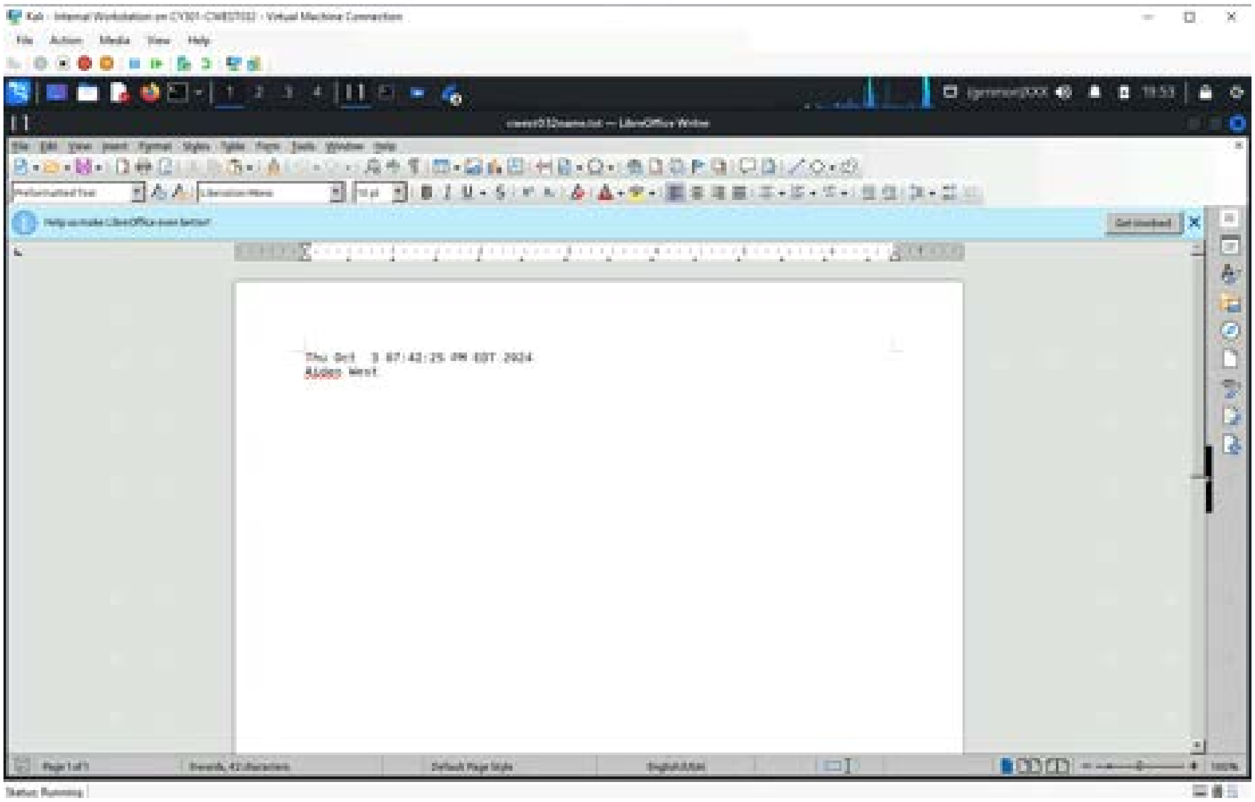
Find:

wireshark_eth0CG4HU2.pcapng

Packets: 350 · Displayed: 8 (2.3%)

Profile: Default

3:


Kali - Internal Workstation on CY301-CWEST032 - Virtual Machine Connection
File
Action
Media
View
Help
LibreOffice Writer
Help us make LibreOffice even better!
Get Involved
Default Page Style
Status: Running

```
Thu Oct  3 07:42:25 PM EDT 2024
Aiden West
```