Fall 2022: ITIS 6167/8167: Network Security
Project 2: VPN

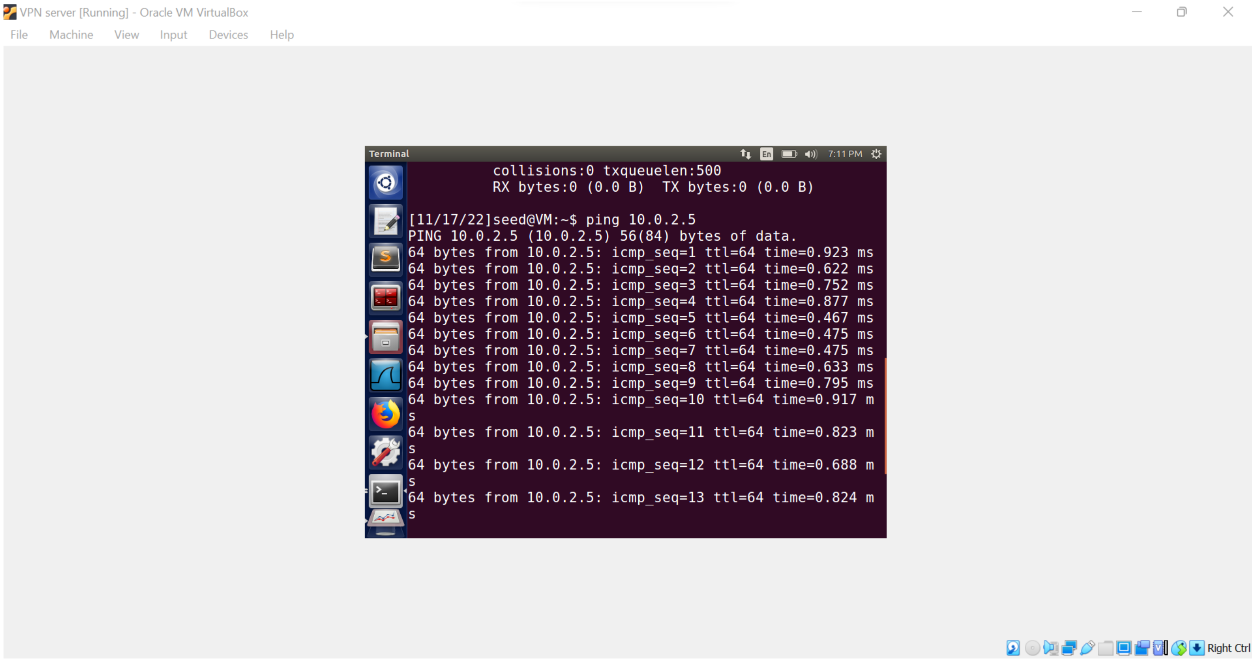
Professor: Dr. Michael Young

Student Name:Sireesha Ponnaganti
Student ID: 801310488
Student Email : sponnaga@uncc.edu

Answers:

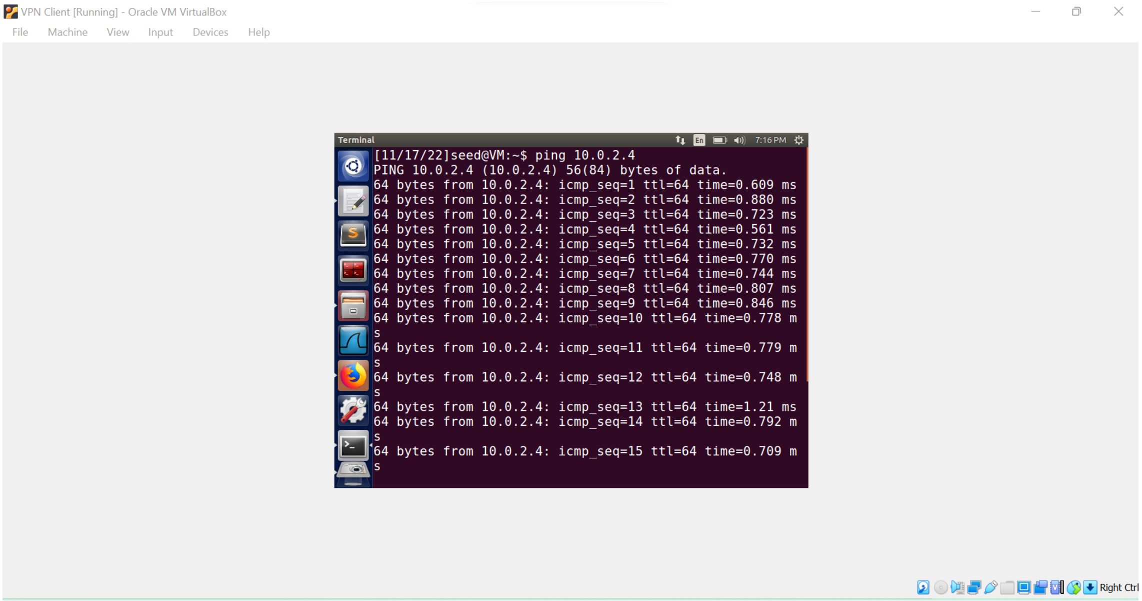
A) Take screenshots of the following:

a. The VPN Server pinging the VPN Client’s enp0s3 interface (recall Step 14)



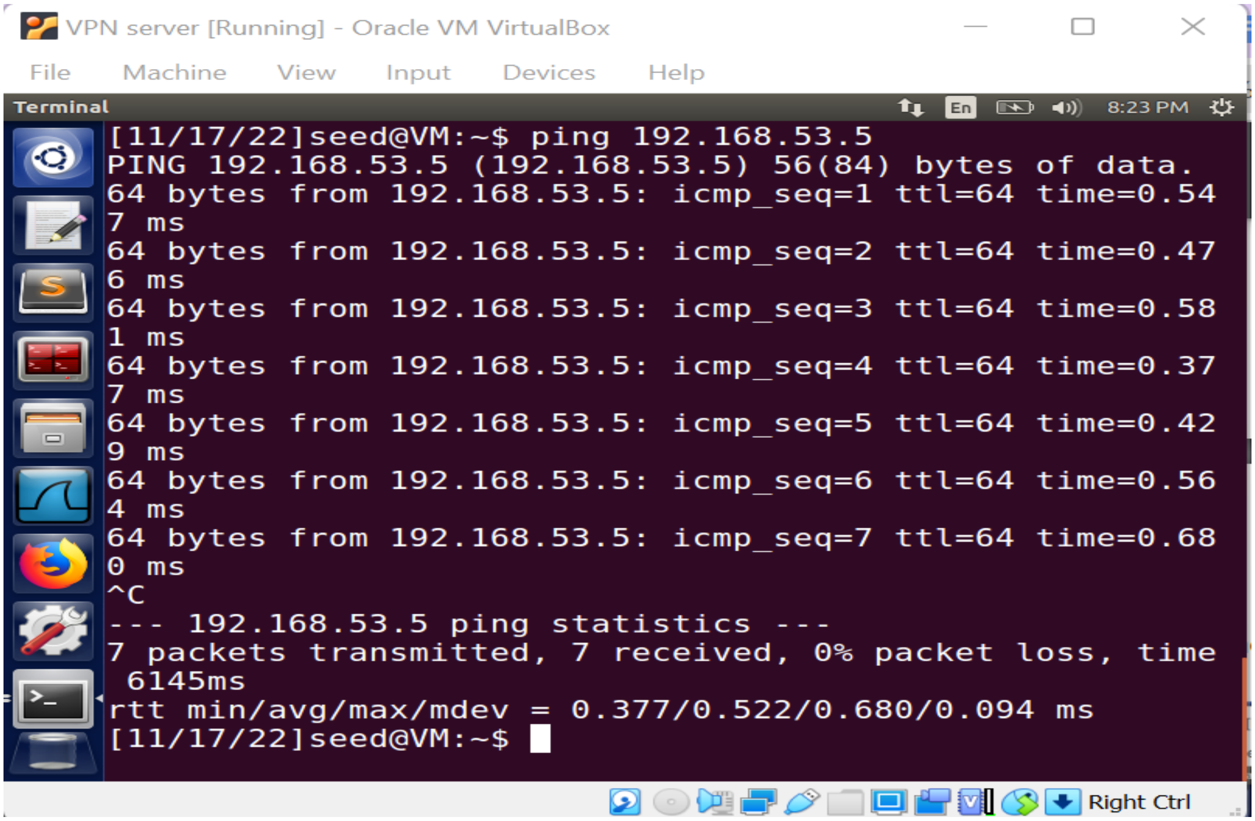
```
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

[11/17/22]seed@VM:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_seq=1 ttl=64 time=0.923 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=64 time=0.622 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=64 time=0.752 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=64 time=0.877 ms
64 bytes from 10.0.2.5: icmp_seq=5 ttl=64 time=0.467 ms
64 bytes from 10.0.2.5: icmp_seq=6 ttl=64 time=0.475 ms
64 bytes from 10.0.2.5: icmp_seq=7 ttl=64 time=0.475 ms
64 bytes from 10.0.2.5: icmp_seq=8 ttl=64 time=0.633 ms
64 bytes from 10.0.2.5: icmp_seq=9 ttl=64 time=0.795 ms
64 bytes from 10.0.2.5: icmp_seq=10 ttl=64 time=0.917 m
s
64 bytes from 10.0.2.5: icmp_seq=11 ttl=64 time=0.823 m
s
64 bytes from 10.0.2.5: icmp_seq=12 ttl=64 time=0.688 m
s
64 bytes from 10.0.2.5: icmp_seq=13 ttl=64 time=0.824 m
s
```

b. The VPN Client pinging the VPN Server's enp0s3 interface (recall Step 14)



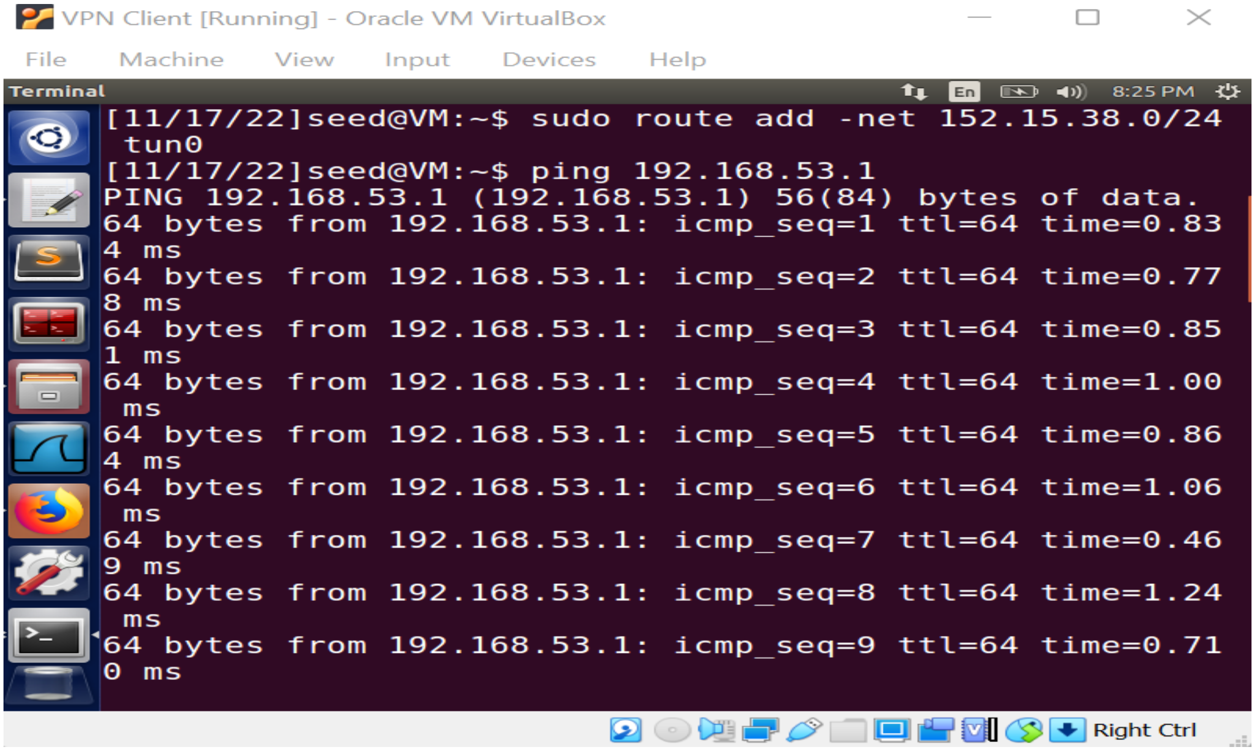
```
[11/17/22]seed@VM:~$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.609 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.880 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.723 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.561 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.732 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.770 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.744 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.807 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.846 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.778 m
s
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=0.779 m
s
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.748 m
s
64 bytes from 10.0.2.4: icmp_seq=13 ttl=64 time=1.21 ms
64 bytes from 10.0.2.4: icmp_seq=14 ttl=64 time=0.792 m
s
64 bytes from 10.0.2.4: icmp_seq=15 ttl=64 time=0.709 m
s
```

c. The VPN Server pinging the VPN Client's tun0 interface (recall Step 40)



```
[11/17/22]seed@VM:~$ ping 192.168.53.5
PING 192.168.53.5 (192.168.53.5) 56(84) bytes of data.
64 bytes from 192.168.53.5: icmp_seq=1 ttl=64 time=0.54
7 ms
64 bytes from 192.168.53.5: icmp_seq=2 ttl=64 time=0.47
6 ms
64 bytes from 192.168.53.5: icmp_seq=3 ttl=64 time=0.58
1 ms
64 bytes from 192.168.53.5: icmp_seq=4 ttl=64 time=0.37
7 ms
64 bytes from 192.168.53.5: icmp_seq=5 ttl=64 time=0.42
9 ms
64 bytes from 192.168.53.5: icmp_seq=6 ttl=64 time=0.56
4 ms
64 bytes from 192.168.53.5: icmp_seq=7 ttl=64 time=0.68
0 ms
^C
--- 192.168.53.5 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time
 6145ms
rtt min/avg/max/mdev = 0.377/0.522/0.680/0.094 ms
[11/17/22]seed@VM:~$
```

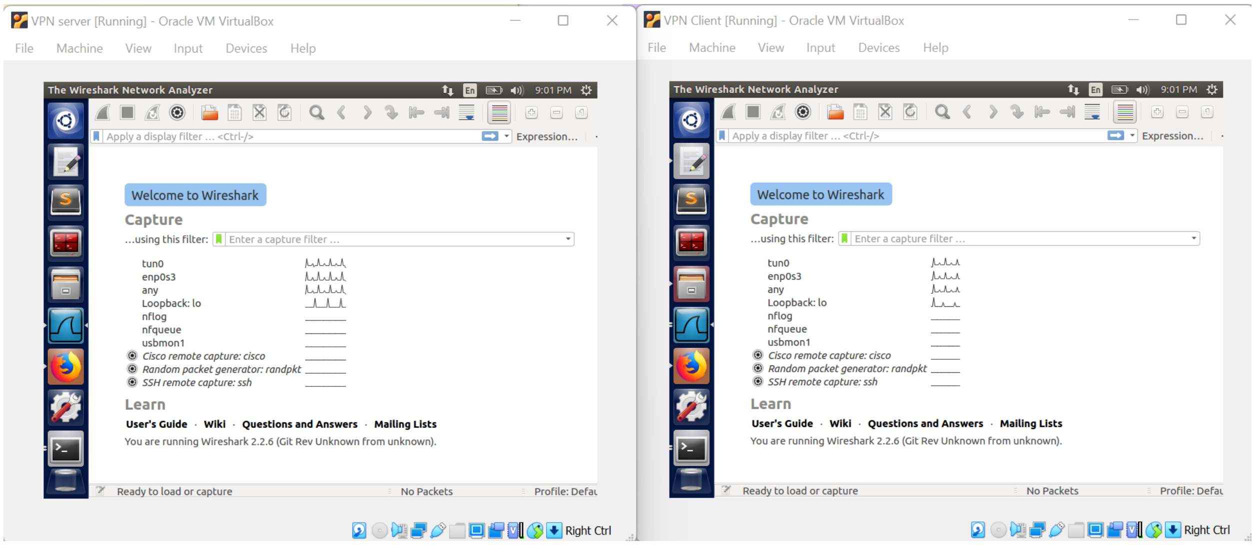
d. The VPN Client pinging the VPN Server’s tun0 interface (recall Step 40)


VPN Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
En
8:25 PM
Right Ctrl

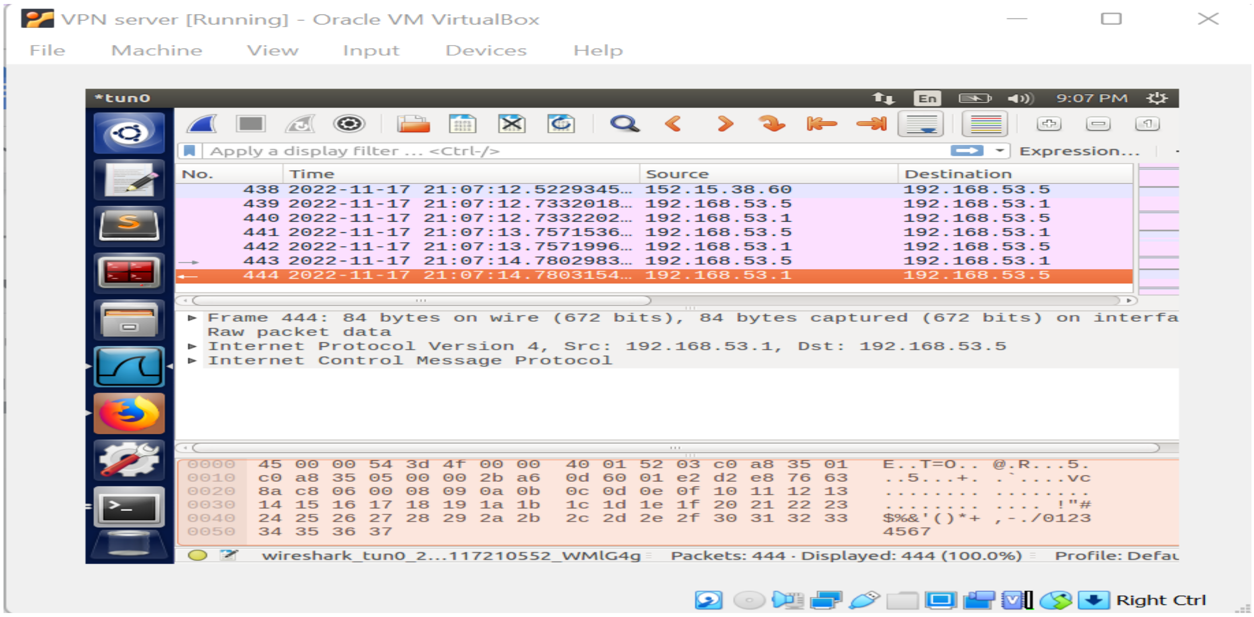
```
[11/17/22]seed@VM:~$ sudo route add -net 152.15.38.0/24
 tun0
[11/17/22]seed@VM:~$ ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
64 bytes from 192.168.53.1: icmp_seq=1 ttl=64 time=0.83
4 ms
64 bytes from 192.168.53.1: icmp_seq=2 ttl=64 time=0.77
8 ms
64 bytes from 192.168.53.1: icmp_seq=3 ttl=64 time=0.85
1 ms
64 bytes from 192.168.53.1: icmp_seq=4 ttl=64 time=1.00
 ms
64 bytes from 192.168.53.1: icmp_seq=5 ttl=64 time=0.86
4 ms
64 bytes from 192.168.53.1: icmp_seq=6 ttl=64 time=1.06
 ms
64 bytes from 192.168.53.1: icmp_seq=7 ttl=64 time=0.46
9 ms
64 bytes from 192.168.53.1: icmp_seq=8 ttl=64 time=1.24
 ms
64 bytes from 192.168.53.1: icmp_seq=9 ttl=64 time=0.71
0 ms
```

B) Follow the below steps, then answer the question that follows:

a. Open Wireshark on both the VPN Server and VPN Client

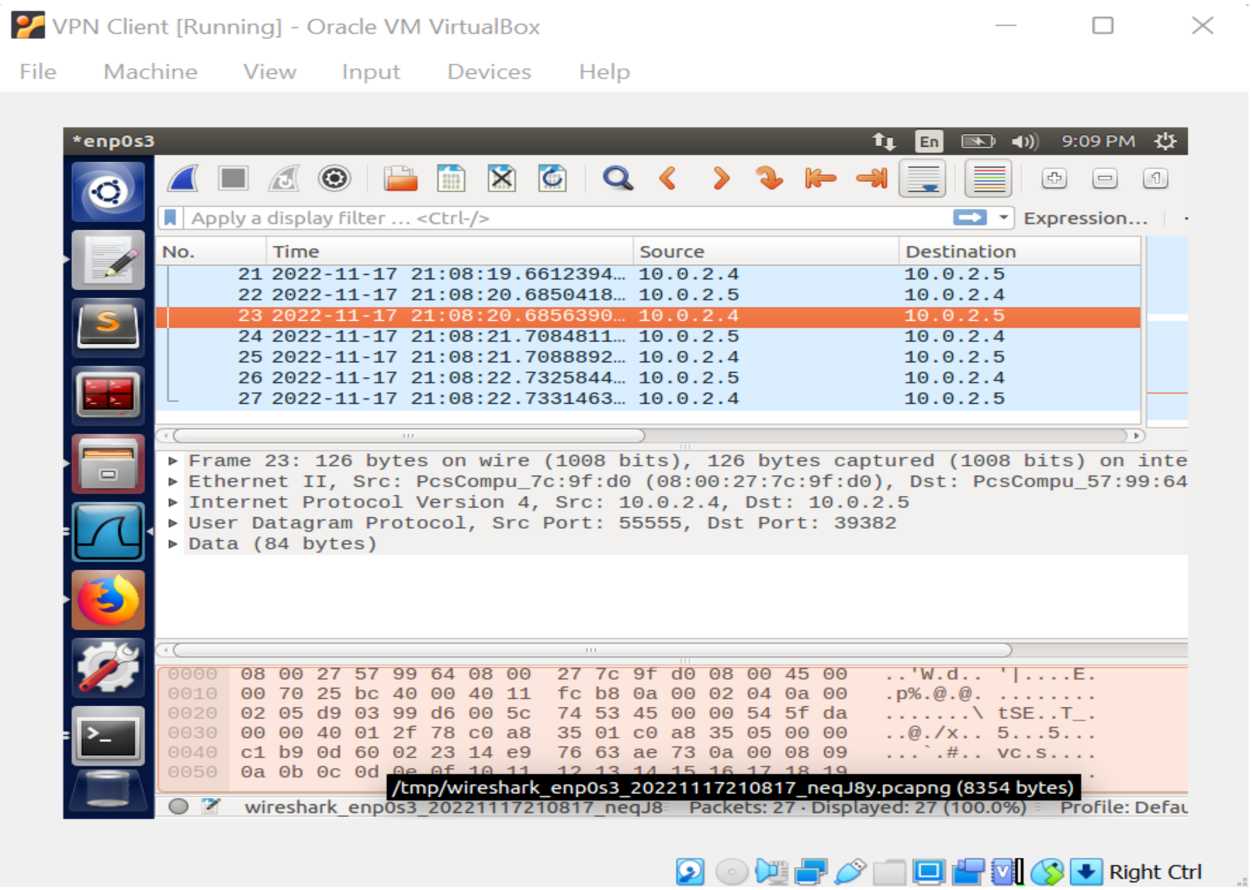

VPN server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer
9:01 PM
Apply a display filter … <Ctrl-/>
Expression…
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
tun0
enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).
Ready to load or capture
No Packets
Profile: Defau
Right Ctrl
VPN Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer
9:01 PM
Apply a display filter … <Ctrl-/>
Expression…
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
tun0
enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).
Ready to load or capture
No Packets
Profile: Defau
Right Ctrl

b. On the VPN Server's Wireshark, listen to the tun0 interface


VPN server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*tun0
En 9:07 PM
Apply a display filter … <Ctrl-/>
Expression…
Right Ctrl

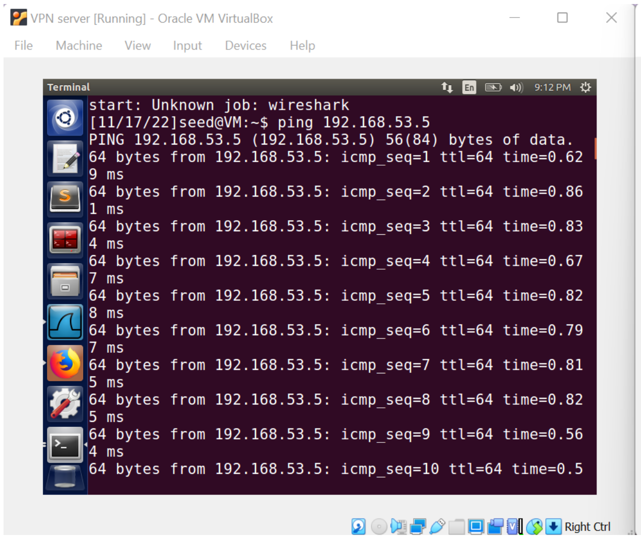
```
No.  Time                          Source           Destination
 438 2022-11-17 21:07:12.5229345…  152.15.38.60     192.168.53.5
 439 2022-11-17 21:07:12.7332018…  192.168.53.5     192.168.53.1
 440 2022-11-17 21:07:12.7332202…  192.168.53.1     192.168.53.5
 441 2022-11-17 21:07:13.7571536…  192.168.53.5     192.168.53.1
 442 2022-11-17 21:07:13.7571996…  192.168.53.1     192.168.53.5
 443 2022-11-17 21:07:14.7802983…  192.168.53.5     192.168.53.1
 444 2022-11-17 21:07:14.7803154…  192.168.53.1     192.168.53.5

▸ Frame 444: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interfa
  Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.53.1, Dst: 192.168.53.5
▸ Internet Control Message Protocol

0000  45 00 00 54 3d 4f 00 00  40 01 52 03 c0 a8 35 01   E..T=O.. @.R...5.
0010  c0 a8 35 05 00 00 2b a6  0d 60 01 e2 d2 e8 76 63   ..5...+. .`....vc
0020  8a c8 06 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   ........ ........
0030  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ ....  !"#
0040  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0050  34 35 36 37                                        4567

wireshark_tun0_2…117210552_WMlG4g   Packets: 444 · Displayed: 444 (100.0%)   Profile: Defau
```

c. On the VPN Client's Wireshark, listen to the enps0s3 interface

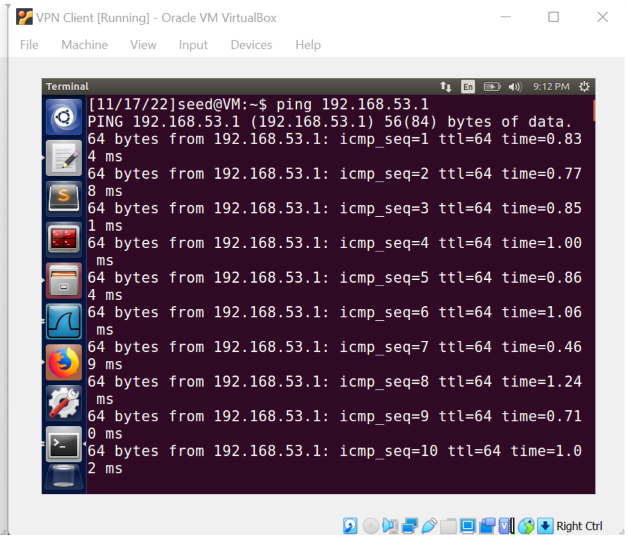

VPN Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
En 9:09 PM
Apply a display filter … <Ctrl-/>
Expression…
Right Ctrl

```
No.  Time                          Source     Destination
  21 2022-11-17 21:08:19.6612394…  10.0.2.4   10.0.2.5
  22 2022-11-17 21:08:20.6850418…  10.0.2.5   10.0.2.4
  23 2022-11-17 21:08:20.6856390…  10.0.2.4   10.0.2.5
  24 2022-11-17 21:08:21.7084811…  10.0.2.5   10.0.2.4
  25 2022-11-17 21:08:21.7088892…  10.0.2.4   10.0.2.5
  26 2022-11-17 21:08:22.7325844…  10.0.2.5   10.0.2.4
  27 2022-11-17 21:08:22.7331463…  10.0.2.4   10.0.2.5

▸ Frame 23: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on inte
▸ Ethernet II, Src: PcsCompu_7c:9f:d0 (08:00:27:7c:9f:d0), Dst: PcsCompu_57:99:64
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
▸ User Datagram Protocol, Src Port: 55555, Dst Port: 39382
▸ Data (84 bytes)

0000  08 00 27 57 99 64 08 00  27 7c 9f d0 08 00 45 00   ..'W.d.. '|....E.
0010  00 70 25 bc 40 00 40 11  fc b8 0a 00 02 04 0a 00   .p%.@.@. ........
0020  02 05 d9 03 99 d6 00 5c  74 53 45 00 00 54 5f da   .......\ tSE..T_.
0030  00 00 40 01 2f 78 c0 a8  35 01 c0 a8 35 05 00 00   ..@./x.. 5...5...
0040  c1 b9 0d 60 02 23 14 e9  76 63 ae 73 0a 00 08 09   ...`.#.. vc.s....
0050  0a 0b 0c 0d 0e 0f 10 11  12 13 14 15 16 17 18 19                    .
/tmp/wireshark_enp0s3_20221117210817_neqJ8y.pcapng (8354 bytes)

wireshark_enp0s3_20221117210817_neqJ8   Packets: 27 · Displayed: 27 (100.0%)   Profile: Defau
```

d. Have the VPN Server ping the VPN Client's tun0 interface's IP address.

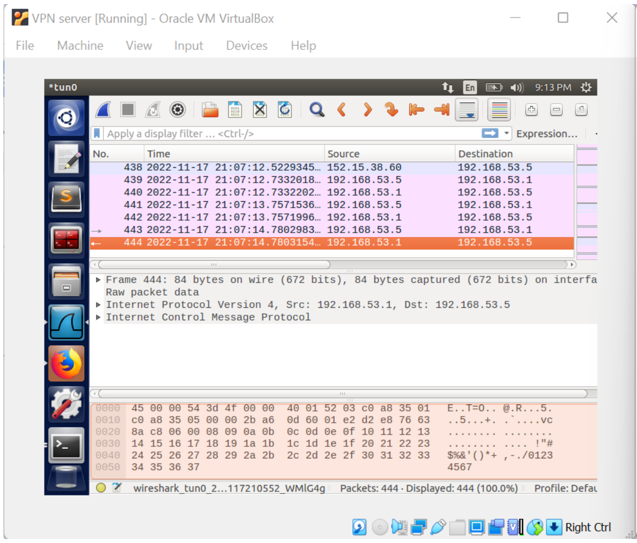


```
start: Unknown job: wireshark
[11/17/22]seed@VM:~$ ping 192.168.53.5
PING 192.168.53.5 (192.168.53.5) 56(84) bytes of data.
64 bytes from 192.168.53.5: icmp_seq=1 ttl=64 time=0.62
9 ms
64 bytes from 192.168.53.5: icmp_seq=2 ttl=64 time=0.86
1 ms
64 bytes from 192.168.53.5: icmp_seq=3 ttl=64 time=0.83
4 ms
64 bytes from 192.168.53.5: icmp_seq=4 ttl=64 time=0.67
7 ms
64 bytes from 192.168.53.5: icmp_seq=5 ttl=64 time=0.82
8 ms
64 bytes from 192.168.53.5: icmp_seq=6 ttl=64 time=0.79
7 ms
64 bytes from 192.168.53.5: icmp_seq=7 ttl=64 time=0.81
5 ms
64 bytes from 192.168.53.5: icmp_seq=8 ttl=64 time=0.82
5 ms
64 bytes from 192.168.53.5: icmp_seq=9 ttl=64 time=0.56
4 ms
64 bytes from 192.168.53.5: icmp_seq=10 ttl=64 time=0.5
```

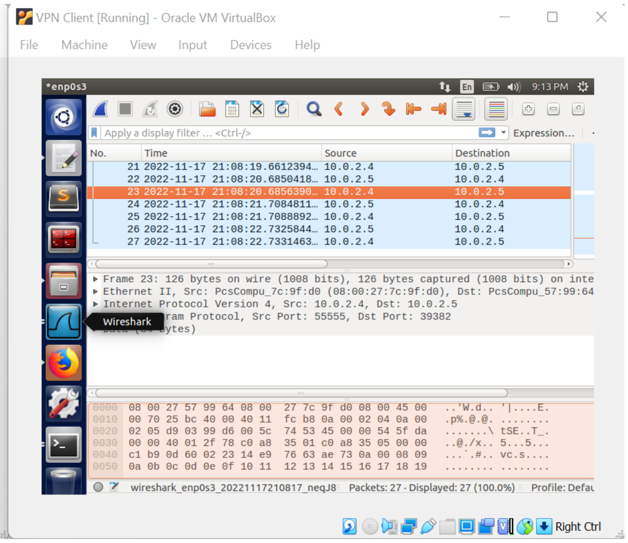


```
[11/17/22]seed@VM:~$ ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
64 bytes from 192.168.53.1: icmp_seq=1 ttl=64 time=0.83
4 ms
64 bytes from 192.168.53.1: icmp_seq=2 ttl=64 time=0.77
8 ms
64 bytes from 192.168.53.1: icmp_seq=3 ttl=64 time=0.85
1 ms
64 bytes from 192.168.53.1: icmp_seq=4 ttl=64 time=1.00
 ms
64 bytes from 192.168.53.1: icmp_seq=5 ttl=64 time=0.86
4 ms
64 bytes from 192.168.53.1: icmp_seq=6 ttl=64 time=1.06
 ms
64 bytes from 192.168.53.1: icmp_seq=7 ttl=64 time=0.46
9 ms
64 bytes from 192.168.53.1: icmp_seq=8 ttl=64 time=1.24
 ms
64 bytes from 192.168.53.1: icmp_seq=9 ttl=64 time=0.71
0 ms
64 bytes from 192.168.53.1: icmp_seq=10 ttl=64 time=1.0
2 ms
```

e. Take screenshots of what you see on Wireshark on both the VPN Server and VPN Client


VPN server [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
*tun0
En
9:13 PM
Apply a display filter ... <Ctrl-/>
Expression...
Right Ctrl

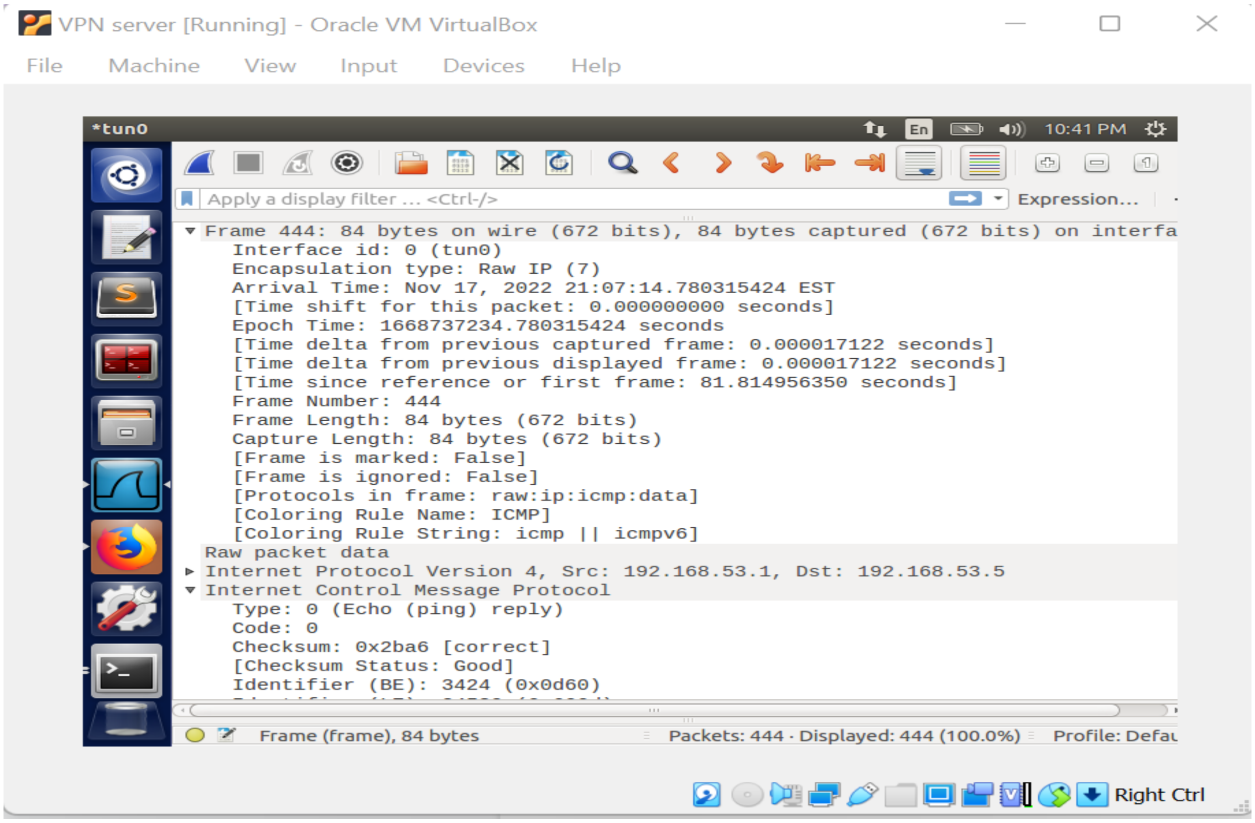
```
No.  Time                            Source          Destination
 438 2022-11-17 21:07:12.5229345…   152.15.38.60    192.168.53.5
 439 2022-11-17 21:07:12.7332018…   192.168.53.5    192.168.53.1
 440 2022-11-17 21:07:12.7332202…   192.168.53.1    192.168.53.5
 441 2022-11-17 21:07:13.7571536…   192.168.53.5    192.168.53.1
 442 2022-11-17 21:07:13.7571996…   192.168.53.1    192.168.53.5
 443 2022-11-17 21:07:14.7802983…   192.168.53.5    192.168.53.1
 444 2022-11-17 21:07:14.7803154…   192.168.53.1    192.168.53.5

▸ Frame 444: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interfa
  Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.53.1, Dst: 192.168.53.5
▸ Internet Control Message Protocol

0000  45 00 00 54 3d 4f 00 00  40 01 52 03 c0 a8 35 01   E..T=O.. @.R...5.
0010  c0 a8 35 05 00 00 2b a6  0d 60 01 e2 d2 e8 76 63   ..5...+. .`....vc
0020  8a c8 06 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   ........ ........
0030  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0040  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0050  34 35 36 37                                        4567

wireshark_tun0_2...117210552_WMlG4g   Packets: 444 · Displayed: 444 (100.0%)   Profile: Defau
```



```
No.  Time                            Source      Destination
  21 2022-11-17 21:08:19.6612394…   10.0.2.4    10.0.2.5
  22 2022-11-17 21:08:20.6850418…   10.0.2.5    10.0.2.4
  23 2022-11-17 21:08:20.6856390…   10.0.2.4    10.0.2.5
  24 2022-11-17 21:08:21.7084811…   10.0.2.5    10.0.2.4
  25 2022-11-17 21:08:21.7088892…   10.0.2.4    10.0.2.5
  26 2022-11-17 21:08:22.7325844…   10.0.2.5    10.0.2.4
  27 2022-11-17 21:08:22.7331463…   10.0.2.4    10.0.2.5

▸ Frame 23: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on inte
▸ Ethernet II, Src: PcsCompu_7c:9f:d0 (08:00:27:7c:9f:d0), Dst: PcsCompu_57:99:64
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 10.0.2.5
               ram Protocol, Src Port: 55555, Dst Port: 39382
               ytes)

0000  08 00 27 57 99 64 08 00  27 7c 9f d0 08 00 45 00   ..'W.d.. '|....E.
0010  00 70 25 bc 40 00 40 11  fc b8 0a 00 02 04 0a 00   .p%.@.@. ........
0020  02 05 d9 03 99 d6 00 5c  74 53 45 00 00 54 5f da   .......\ tSE..T_.
0030  00 00 40 01 2f 78 c0 a8  35 01 c0 a8 35 05 00 00   ..@./x.. 5...5...
0040  c1 b9 0d 60 02 23 14 e9  76 63 ae 73 0a 00 08 09   ...`.#.. vc.s....
0050  0a 0b 0c 0d 0e 0f 10 11  12 13 14 15 16 17 18 19   ........ ........

wireshark_enp0s3_20221117210817_neqJ8   Packets: 27 · Displayed: 27 (100.0%)   Profile: Defau
```

Question:Based on what you see on Wireshark on both virtual machines, how does VPN tunneling hide an IP packet within another IP packet? Please explain using the screenshots you took.

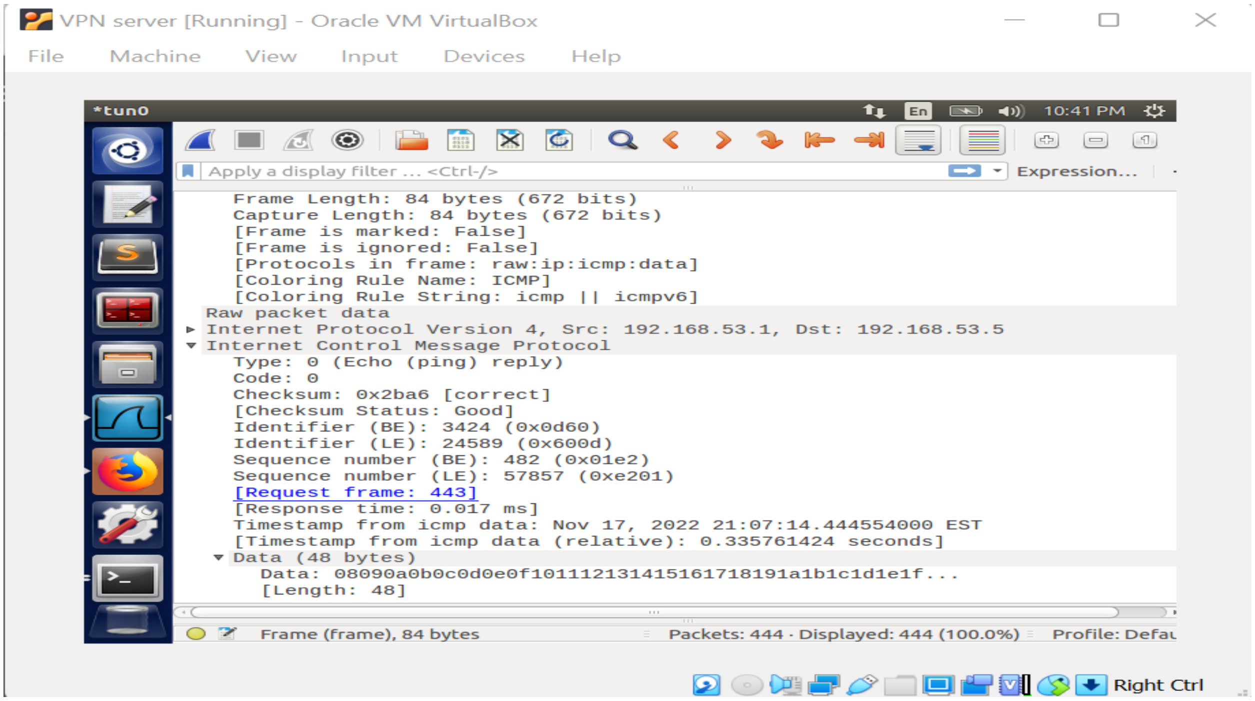
Answer:The ICMP request as well as ICMP reply between both the tun0 IP addresses of the VPN Client and VPN Server are visible in the tun0 Wireshark capture. Because of Wireshark connection we used to collect the information is tun0, we can view the tun0 IP addresses between both machines here. We are unable to view the same traffic while attempting to perform the same on the VPN Client's enp0s5 interface. Using a tunnel is a way to send a foreign protocol through a network that wouldn't typically support it. With the use of tunneling protocols, you could, for instance, transfer another protocol via IP in the IP datagram's "data" section. The majority of tunneling protocols work at layer 4, which means they are implemented as an alternative protocol to TCP or UDP. The communication in our current case took place over tun0 IP. This packet transfers the original packet over layer 4 while encasing it in its payload. This packet is decapsulated and then forwarded onto the internal network at the destination. Now that the VPN server's address is the packet's source address, responses can return to it. The packets that are being transferred between the enps0s5 interfaces of the VPN Client and VPN Server are visible. The VPN inserts the frame through into data field when an ICMP request is sent. The screenshots that follow demonstrate the way it is enclosed.


VPN server [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
*tun0
En
10:41 PM
Apply a display filter … <Ctrl-/>
Expression…
Right Ctrl

```
▾ Frame 444: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interfa
    Interface id: 0 (tun0)
    Encapsulation type: Raw IP (7)
    Arrival Time: Nov 17, 2022 21:07:14.780315424 EST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1668737234.780315424 seconds
    [Time delta from previous captured frame: 0.000017122 seconds]
    [Time delta from previous displayed frame: 0.000017122 seconds]
    [Time since reference or first frame: 81.814956350 seconds]
    Frame Number: 444
    Frame Length: 84 bytes (672 bits)
    Capture Length: 84 bytes (672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.53.1, Dst: 192.168.53.5
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x2ba6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3424 (0x0d60)
```

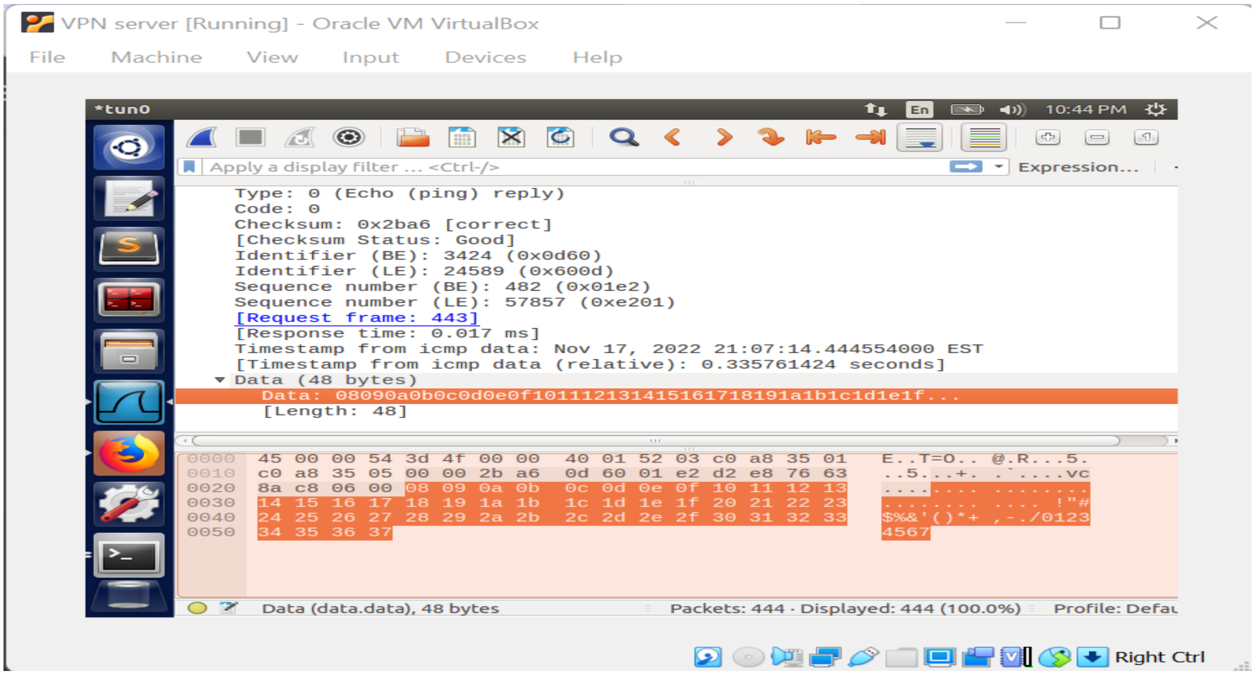
```
Frame (frame), 84 bytes          Packets: 444 · Displayed: 444 (100.0%)    Profile: Defau
```

Figure B(e):VPN Server’s tun0 interface packet


VPN server [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
*tun0
En
10:41 PM
Apply a display filter … <Ctrl-/>
Expression…
Right Ctrl

```
    Frame Length: 84 bytes (672 bits)
    Capture Length: 84 bytes (672 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: raw:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
  Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.53.1, Dst: 192.168.53.5
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x2ba6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3424 (0x0d60)
    Identifier (LE): 24589 (0x600d)
    Sequence number (BE): 482 (0x01e2)
    Sequence number (LE): 57857 (0xe201)
    [Request frame: 443]
    [Response time: 0.017 ms]
    Timestamp from icmp data: Nov 17, 2022 21:07:14.444554000 EST
    [Timestamp from icmp data (relative): 0.335761424 seconds]
  ▾ Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]

Frame (frame), 84 bytes        Packets: 444 · Displayed: 444 (100.0%)    Profile: Defau
```

Figure B(e1):VPN Server’s tun0 interface packet

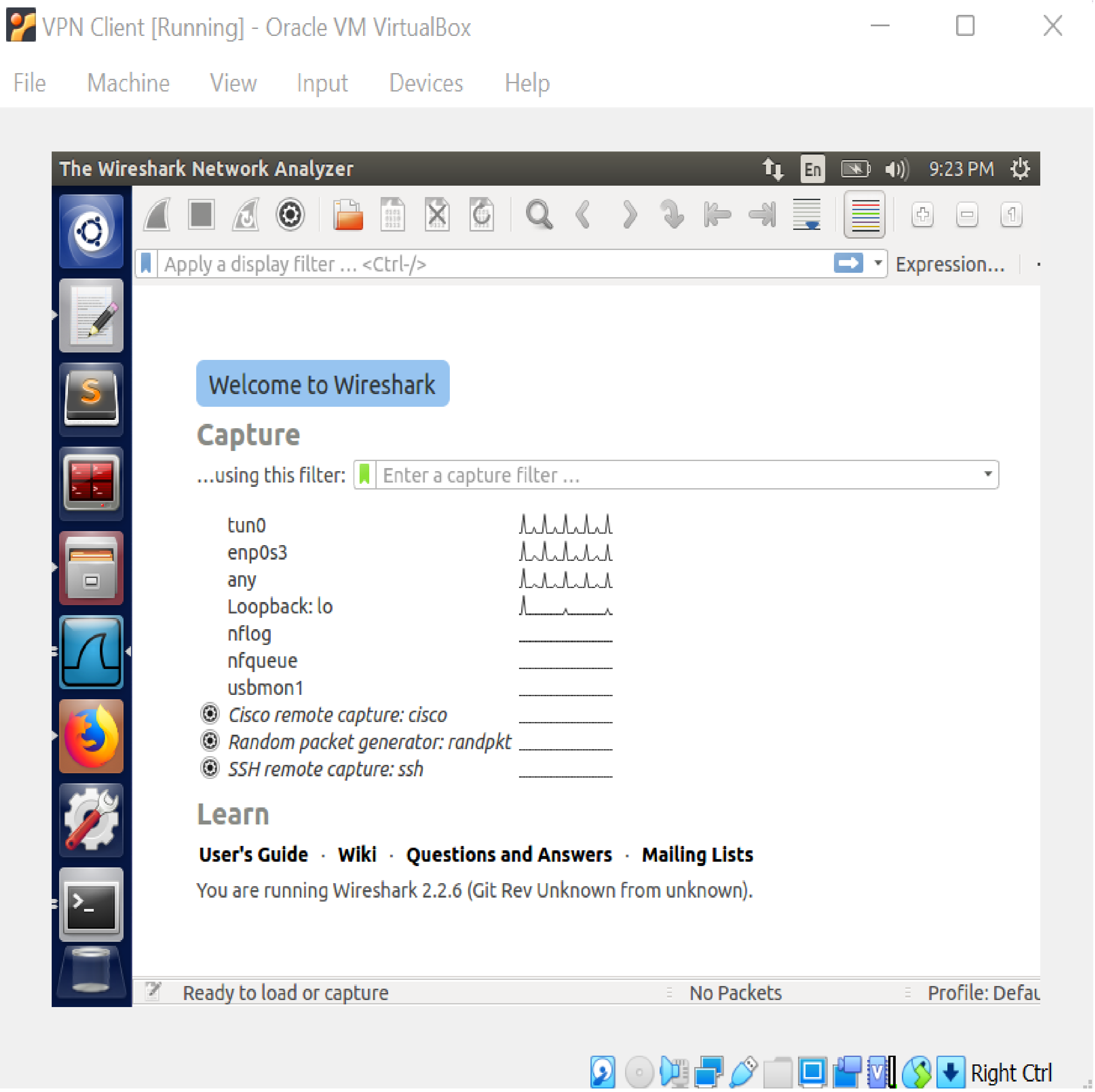

VPN server [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
*tun0
En
10:44 PM
Apply a display filter … <Ctrl-/>
Expression…
Right Ctrl

```
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x2ba6 [correct]
    [Checksum Status: Good]
    Identifier (BE): 3424 (0x0d60)
    Identifier (LE): 24589 (0x600d)
    Sequence number (BE): 482 (0x01e2)
    Sequence number (LE): 57857 (0xe201)
    [Request frame: 443]
    [Response time: 0.017 ms]
    Timestamp from icmp data: Nov 17, 2022 21:07:14.444554000 EST
    [Timestamp from icmp data (relative): 0.335761424 seconds]
  ▾ Data (48 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 48]

0000  45 00 00 54 3d 4f 00 00  40 01 52 03 c0 a8 35 01   E..T=O.. @.R...5.
0010  c0 a8 35 05 00 00 2b a6  0d 60 01 e2 d2 e8 76 63   ..5...+. .`....vc
0020  8a c8 06 00 08 09 0a 0b  0c 0d 0e 0f 10 11 12 13   ........ ........
0030  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ........ .... !"#
0040  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0050  34 35 36 37                                        4567

Data (data.data), 48 bytes     Packets: 444 · Displayed: 444 (100.0%)    Profile: Defau
```

Figure B(e2):VPN Client’s enp0s5 interface packet

C) Follow the below steps, then answer the question that follows:

a. Open Wireshark on your VPN Client



VPN Client [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
The Wireshark Network Analyzer
En
9:23 PM
Expression...
Right Ctrl

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

tun0
enp0s3
any
Loopback: lo
nflog
nfqueue
usbmon1
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh

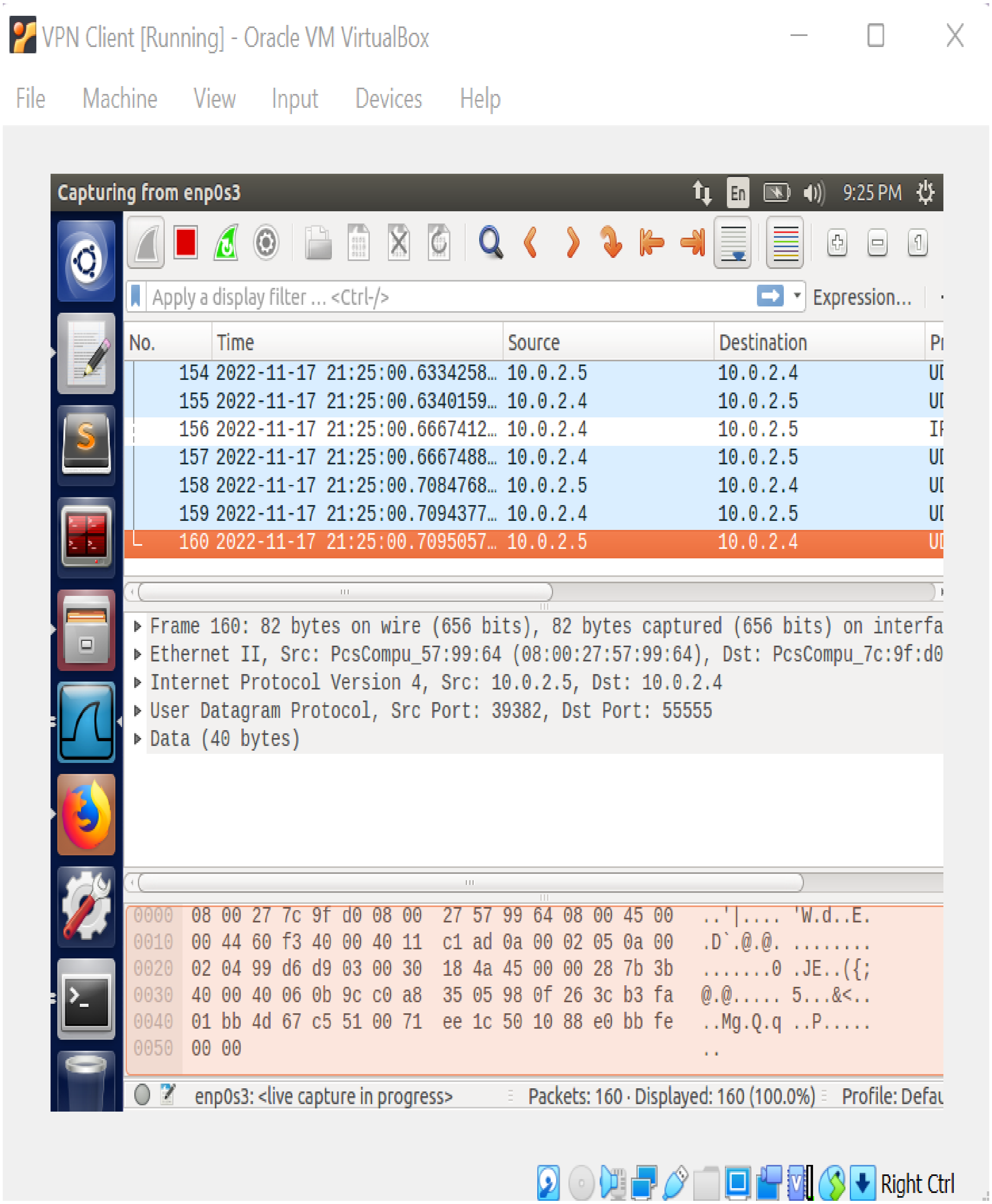
Learn

User's Guide · **Wiki** · **Questions and Answers** · **Mailing Lists**

You are running Wireshark 2.2.6 (Git Rev Unknown from unknown).

Ready to load or capture   No Packets   Profile: Defau

b. Listen to the enps0s3 interface



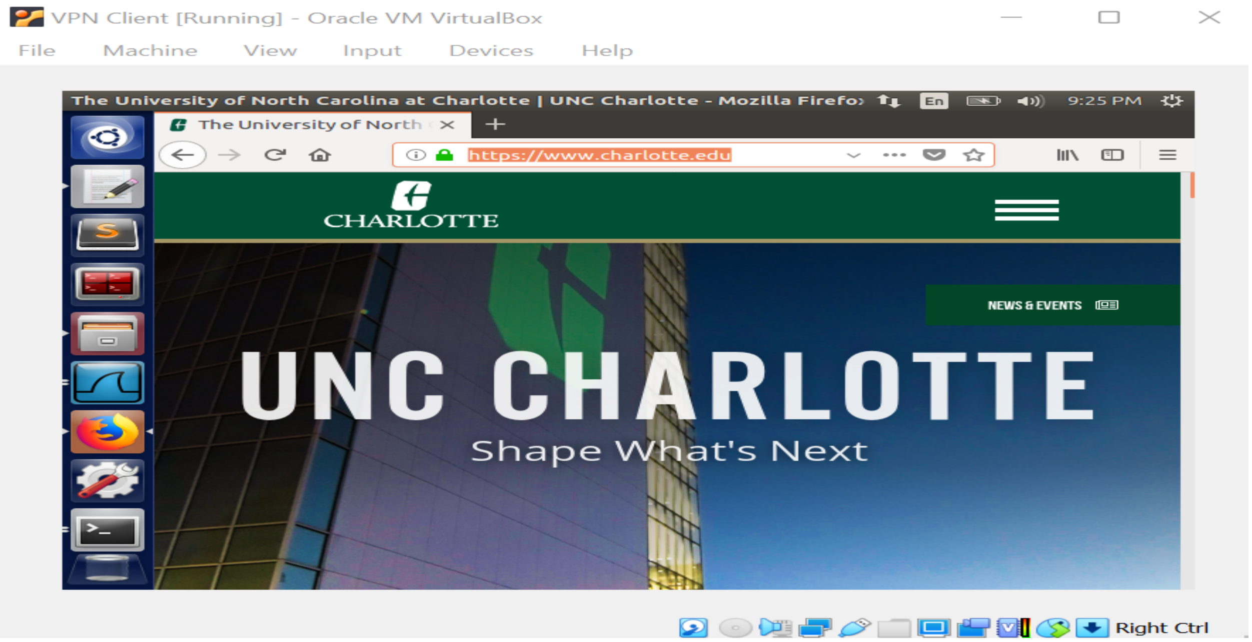
```
No.    Time                             Source      Destination  Pr
   154 2022-11-17 21:25:00.6334258…  10.0.2.5    10.0.2.4     UI
   155 2022-11-17 21:25:00.6340159…  10.0.2.4    10.0.2.5     UI
   156 2022-11-17 21:25:00.6667412…  10.0.2.4    10.0.2.5     IF
   157 2022-11-17 21:25:00.6667488…  10.0.2.4    10.0.2.5     UI
   158 2022-11-17 21:25:00.7084768…  10.0.2.5    10.0.2.4     UI
   159 2022-11-17 21:25:00.7094377…  10.0.2.4    10.0.2.5     UI
   160 2022-11-17 21:25:00.7095057…  10.0.2.5    10.0.2.4     UI
```

```
▸ Frame 160: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interfa
▸ Ethernet II, Src: PcsCompu_57:99:64 (08:00:27:57:99:64), Dst: PcsCompu_7c:9f:d0
▸ Internet Protocol Version 4, Src: 10.0.2.5, Dst: 10.0.2.4
▸ User Datagram Protocol, Src Port: 39382, Dst Port: 55555
▸ Data (40 bytes)
```

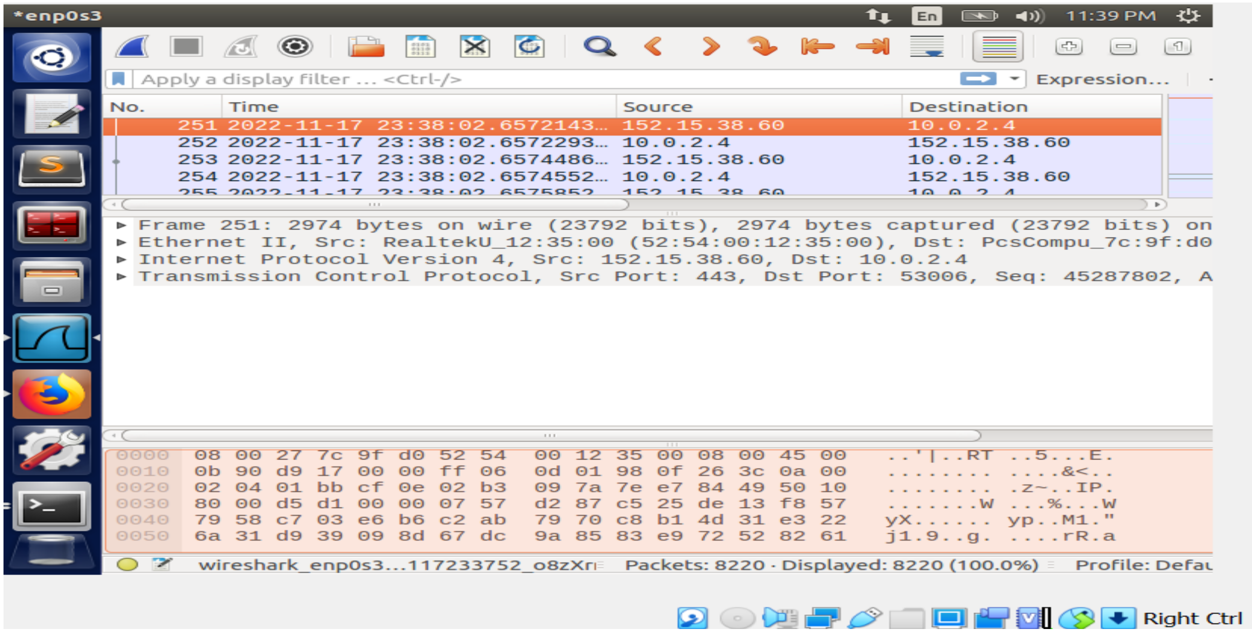
```
0000  08 00 27 7c 9f d0 08 00  27 57 99 64 08 00 45 00   ..'|.... 'W.d..E.
0010  00 44 60 f3 40 00 40 11  c1 ad 0a 00 02 05 0a 00   .D`.@.@. ........
0020  02 04 99 d6 d9 03 00 30  18 4a 45 00 00 28 7b 3b   .......0 .JE..({;
0030  40 00 40 06 0b 9c c0 a8  35 05 98 0f 26 3c b3 fa   @.@..... 5...&<..
0040  01 bb 4d 67 c5 51 00 71  ee 1c 50 10 88 e0 bb fe   ..Mg.Q.q ..P.....
0050  00 00                                              ..
```

enp0s3: <live capture in progress>   Packets: 160 · Displayed: 160 (100.0%)   Profile: Defau

c. Visit the blocked webpage


VPN Client [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
The University of North Carolina at Charlotte | UNC Charlotte - Mozilla Firefox
En
9:25 PM
The University of North
https://www.charlotte.edu
CHARLOTTE
NEWS & EVENTS
UNC CHARLOTTE
Shape What's Next
Right Ctrl

d. Take screenshot(s) of what you see on Wireshark



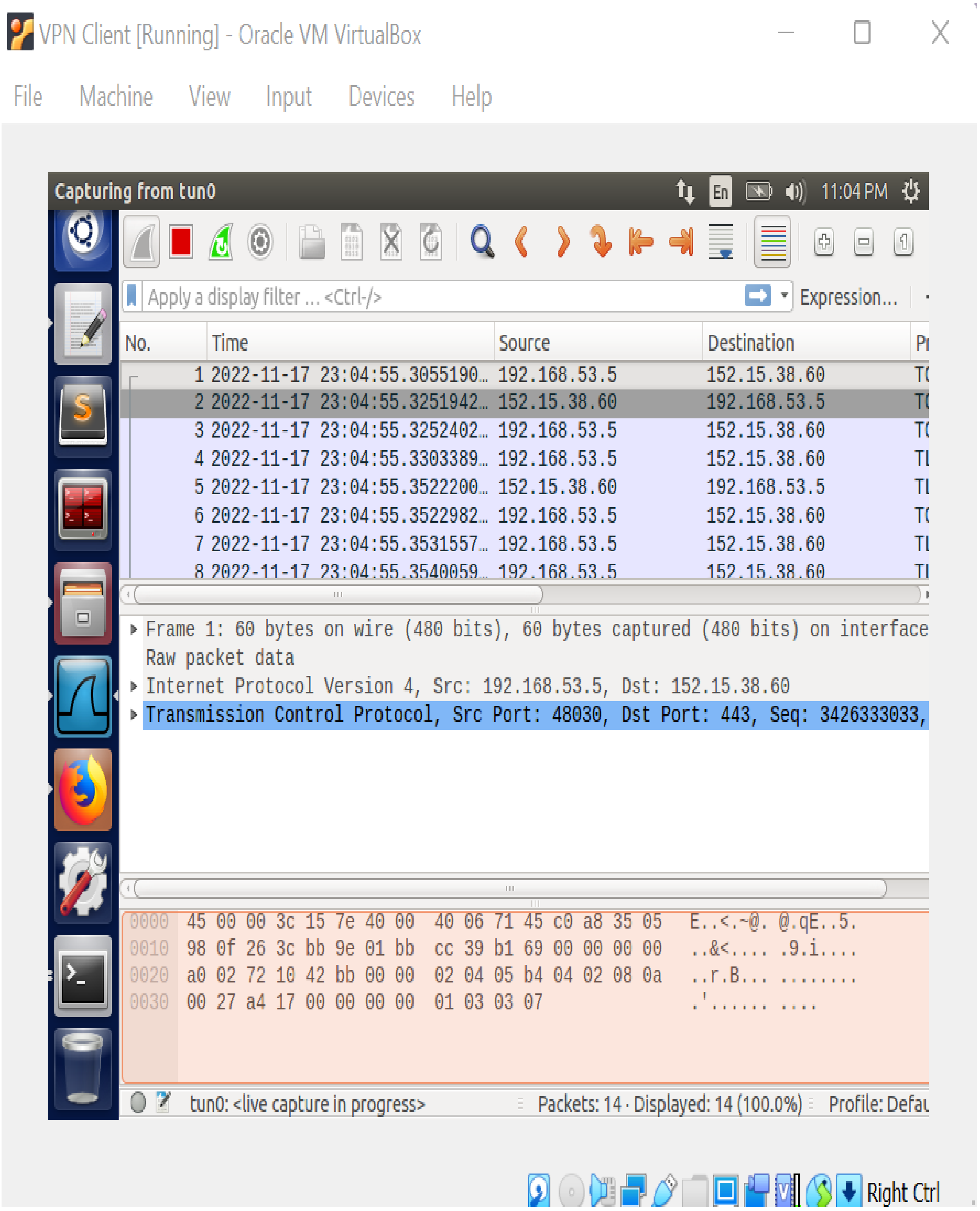
```
No.   Time                            Source          Destination
  251 2022-11-17 23:38:02.6572143…    152.15.38.60    10.0.2.4
  252 2022-11-17 23:38:02.6572293…    10.0.2.4        152.15.38.60
  253 2022-11-17 23:38:02.6574486…    152.15.38.60    10.0.2.4
  254 2022-11-17 23:38:02.6574552…    10.0.2.4        152.15.38.60
```

```
▸ Frame 251: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on
▸ Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_7c:9f:d0
▸ Internet Protocol Version 4, Src: 152.15.38.60, Dst: 10.0.2.4
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 53006, Seq: 45287802, A
```

```
0000  08 00 27 7c 9f d0 52 54  00 12 35 00 08 00 45 00   ..'|..RT ..5...E.
0010  0b 90 d9 17 00 00 ff 06  0d 01 98 0f 26 3c 0a 00   ........ ....&<..
0020  02 04 01 bb cf 0e 02 b3  09 7a 7e e7 84 49 50 10   ........ .z~..IP.
0030  80 00 d5 d1 00 00 07 57  d2 87 c5 25 de 13 f8 57   .......W ...%...W
0040  79 58 c7 03 e6 b6 c2 ab  79 70 c8 b1 4d 31 e3 22   yX...... yp..M1."
0050  6a 31 d9 39 09 8d 67 dc  9a 85 83 e9 72 52 82 61   j1.9..g. ....rR.a
```

wireshark_enp0s3…117233752_o8zXr   Packets: 8220 · Displayed: 8220 (100.0%)   Profile: Defau

e. Next listen to the tun0 interface



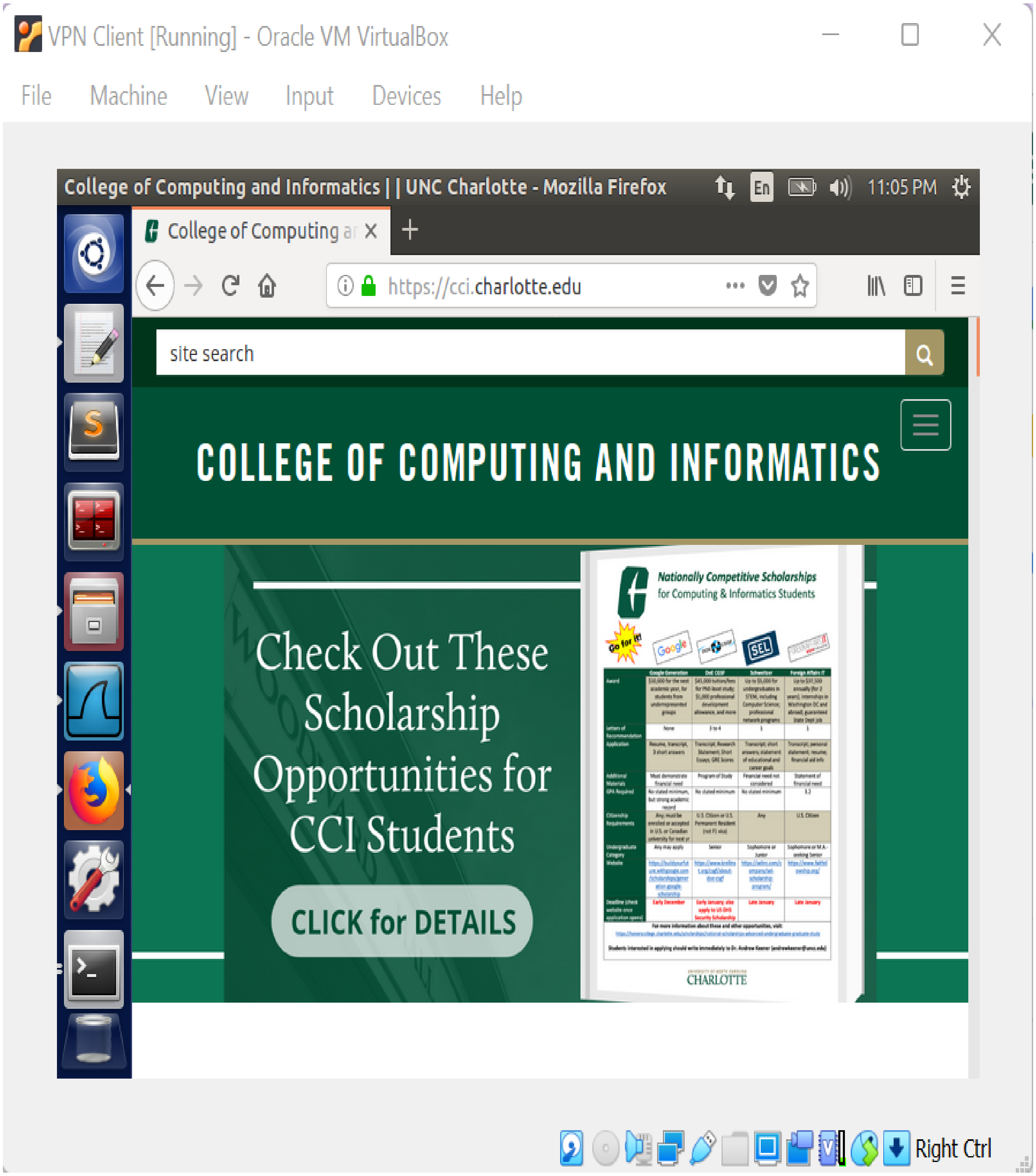
```
No.  Time                              Source          Destination     Pr
   1 2022-11-17 23:04:55.3055190…  192.168.53.5    152.15.38.60    TC
   2 2022-11-17 23:04:55.3251942…  152.15.38.60    192.168.53.5    TC
   3 2022-11-17 23:04:55.3252402…  192.168.53.5    152.15.38.60    TC
   4 2022-11-17 23:04:55.3303389…  192.168.53.5    152.15.38.60    TL
   5 2022-11-17 23:04:55.3522200…  152.15.38.60    192.168.53.5    TL
   6 2022-11-17 23:04:55.3522982…  192.168.53.5    152.15.38.60    TC
   7 2022-11-17 23:04:55.3531557…  192.168.53.5    152.15.38.60    TL
   8 2022-11-17 23:04:55.3540059…  192.168.53.5    152.15.38.60    TL
```

```
▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
  Raw packet data
▸ Internet Protocol Version 4, Src: 192.168.53.5, Dst: 152.15.38.60
▸ Transmission Control Protocol, Src Port: 48030, Dst Port: 443, Seq: 3426333033,
```

```
0000  45 00 00 3c 15 7e 40 00  40 06 71 45 c0 a8 35 05   E..<.~@. @.qE..5.
0010  98 0f 26 3c bb 9e 01 bb  cc 39 b1 69 00 00 00 00   ..&<.... .9.i....
0020  a0 02 72 10 42 bb 00 00  02 04 05 b4 04 02 08 0a   ..r.B... ........
0030  00 27 a4 17 00 00 00 00  01 03 03 07               .'...... ....
```

tun0: <live capture in progress>   Packets: 14 · Displayed: 14 (100.0%)   Profile: Defau

f. Visit the blocked webpage again


VPN Client [Running] - Oracle VM VirtualBox

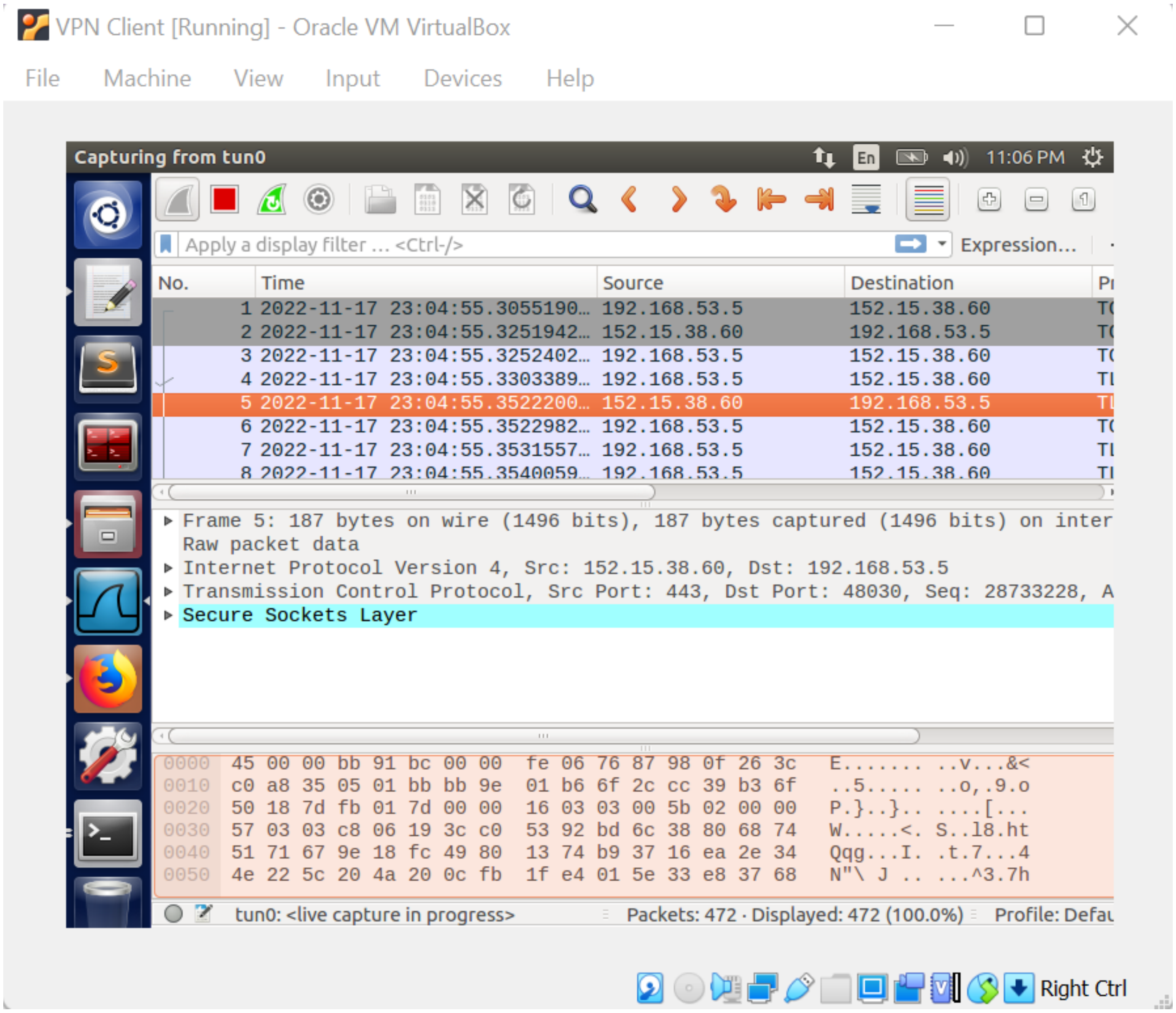
College of Computing and Informatics | | UNC Charlotte - Mozilla Firefox

https://cci.charlotte.edu

COLLEGE OF COMPUTING AND INFORMATICS

Check Out These Scholarship Opportunities for CCI Students

g. Take screenshot(s) of what you see on Wireshark



```
No.  Time                          Source          Destination     Pr
   1 2022-11-17 23:04:55.3055190… 192.168.53.5    152.15.38.60    TC
   2 2022-11-17 23:04:55.3251942… 152.15.38.60    192.168.53.5    TC
   3 2022-11-17 23:04:55.3252402… 192.168.53.5    152.15.38.60    TC
   4 2022-11-17 23:04:55.3303389… 192.168.53.5    152.15.38.60    TL
   5 2022-11-17 23:04:55.3522200… 152.15.38.60    192.168.53.5    TL
   6 2022-11-17 23:04:55.3522982… 192.168.53.5    152.15.38.60    TC
   7 2022-11-17 23:04:55.3531557… 192.168.53.5    152.15.38.60    TL
   8 2022-11-17 23:04:55.3540059… 192.168.53.5    152.15.38.60    TL
```

```
▶ Frame 5: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on inter
  Raw packet data
▶ Internet Protocol Version 4, Src: 152.15.38.60, Dst: 192.168.53.5
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 48030, Seq: 28733228, A
▶ Secure Sockets Layer
```

```
0000  45 00 00 bb 91 bc 00 00  fe 06 76 87 98 0f 26 3c   E....... ..v...&<
0010  c0 a8 35 05 01 bb bb 9e  01 b6 6f 2c cc 39 b3 6f   ..5..... ..o,.9.o
0020  50 18 7d fb 01 7d 00 00  16 03 03 00 5b 02 00 00   P.}..}.. ....[...
0030  57 03 03 c8 06 19 3c c0  53 92 bd 6c 38 80 68 74   W.....<. S..l8.ht
0040  51 71 67 9e 18 fc 49 80  13 74 b9 37 16 ea 2e 34   Qqg...I. .t.7...4
0050  4e 22 5c 20 4a 20 0c fb  1f e4 01 5e 33 e8 37 68   N"\ J .. ...^3.7h
```

```
tun0: <live capture in progress>    Packets: 472 · Displayed: 472 (100.0%)    Profile: Defau
```

Question: How is the VPN Client able to access the webpage that's blocked by its firewall? Please explain using the screenshots you took.

Answer: Observe that only packets were transferred between the tun0 interfaces of the VPN Client and VPN Server so when website was browsed in the aforementioned figures. As shown in the lines of the collected file in the figures above, traffic was sent over the tunnel when we activated the network's restricted website according to how the VPN channel was configured. In the same way that the source of the request is via tunnel, the source of the response is likewise through the tunnel, and the website is produced. By doing this, we get over the limitations imposed by the current network. This demonstrates that the packets were transmitted over the VPN tunnel when the VPN Client attempted to contact the website so that they could be encapsulated and afterwards forwarded to the website. On enp0s5, but not on tun0, we likely added a rules to restrict the IP address of the website. Through the VPN tunnel the with tun0 IP address, the VPN Client will visit the web. It won't be possible to access the webpage via tun0 if we really add a rule to block tun0 IP address.

References:

IBM(2021, Aug 9).Encapsulating security payload.https://www.ibm.com/docs/en/i/7.4?topic=protocols-encapsulating-security-payload

SENTIA(2020, Mar 27).Wireshark and Encapsulation.https://www.sentiatechblog.com/ans-exercise-2-2-tcpdump-wireshark-and-encapsulation

StackExchange(2021, Mar 21).Forwarding Traffic from TUN interface to XX.https://serverfault.com/questions/1057790/forwarding-traffic-from-tun-interface-to-xx

geeksforgeeks(2022, Mar 10). What is Encapsulating Security Payload.https://www.geeksforgeeks.org/what-is-encapsulating-security-payload/