

# Fall 2023: ITIS 6167/8167: Network Security

## Project 3: VPN

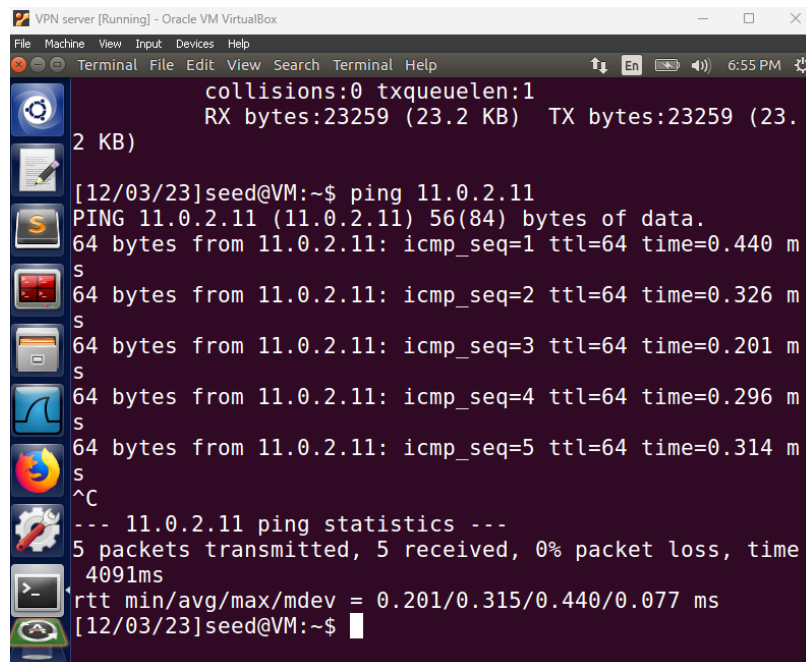
Divyansh Jain

801364884

03-Dec-2023

A) Take screenshots of the following:

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



```
collisions:0 txqueuelen:1
RX bytes:23259 (23.2 KB) TX bytes:23259 (23.2 KB)

[12/03/23]seed@VM:~$ ping 11.0.2.11
PING 11.0.2.11 (11.0.2.11) 56(84) bytes of data:
64 bytes from 11.0.2.11: icmp_seq=1 ttl=64 time=0.440 m
s
64 bytes from 11.0.2.11: icmp_seq=2 ttl=64 time=0.326 m
s
64 bytes from 11.0.2.11: icmp_seq=3 ttl=64 time=0.201 m
s
64 bytes from 11.0.2.11: icmp_seq=4 ttl=64 time=0.296 m
s
64 bytes from 11.0.2.11: icmp_seq=5 ttl=64 time=0.314 m
s
^C
--- 11.0.2.11 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
4091ms
rtt min/avg/max/mdev = 0.201/0.315/0.440/0.077 ms
[12/03/23]seed@VM:~$
```

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

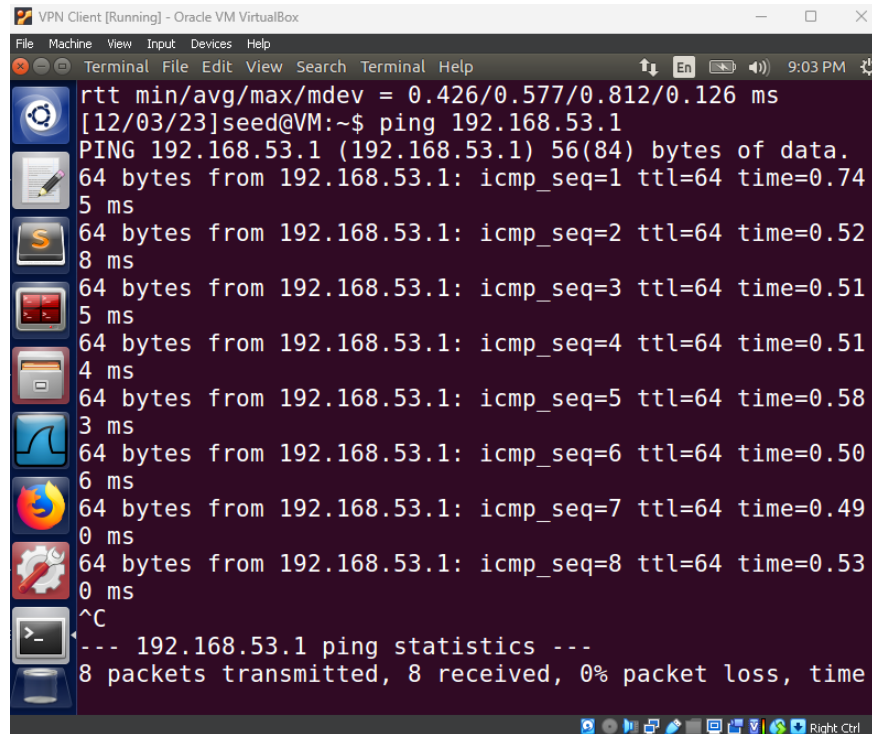
```
VPN Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
arrier:0
collisions:0 txqueuelen:1
RX bytes:21309 (21.3 KB) TX bytes:21309 (21.3 KB)

[12/03/23]seed@VM:~$ ping 11.0.2.10
PING 11.0.2.10 (11.0.2.10) 56(84) bytes of data.
64 bytes from 11.0.2.10: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 11.0.2.10: icmp_seq=2 ttl=64 time=0.331 ms
64 bytes from 11.0.2.10: icmp_seq=3 ttl=64 time=0.294 ms
64 bytes from 11.0.2.10: icmp_seq=4 ttl=64 time=0.526 ms
64 bytes from 11.0.2.10: icmp_seq=5 ttl=64 time=0.288 ms
^C
--- 11.0.2.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time
4063ms
rtt min/avg/max/mdev = 0.288/0.493/1.028/0.281 ms
[12/03/23]seed@VM:~$
```

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

```
VPN server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[12/03/23]seed@VM:~$ sudo route add -net 192.168.53.0/24 tun0
[12/03/23]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=0.694 ms
64 bytes from 192.168.53.5: icmp_seq=2 ttl=64 time=0.505 ms
64 bytes from 192.168.53.5: icmp_seq=3 ttl=64 time=0.526 ms
64 bytes from 192.168.53.5: icmp_seq=4 ttl=64 time=0.411 ms
64 bytes from 192.168.53.5: icmp_seq=5 ttl=64 time=0.541 ms
64 bytes from 192.168.53.5: icmp_seq=6 ttl=64 time=0.537 ms
64 bytes from 192.168.53.5: icmp_seq=7 ttl=64 time=0.515 ms
64 bytes from 192.168.53.5: icmp_seq=8 ttl=64 time=0.787 ms
64 bytes from 192.168.53.5: icmp_seq=9 ttl=64 time=0.421 ms
```

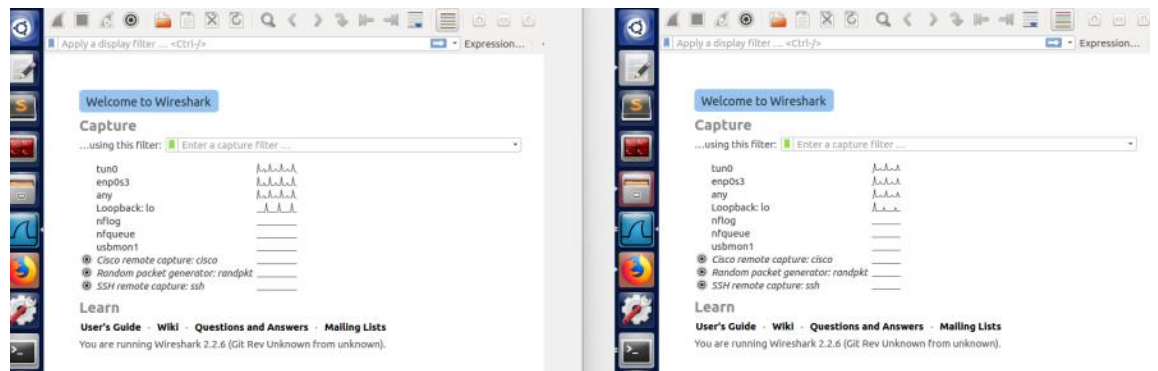
- d. The VPN Client ping the VPN Server's tun0 interface (recall Step 40)



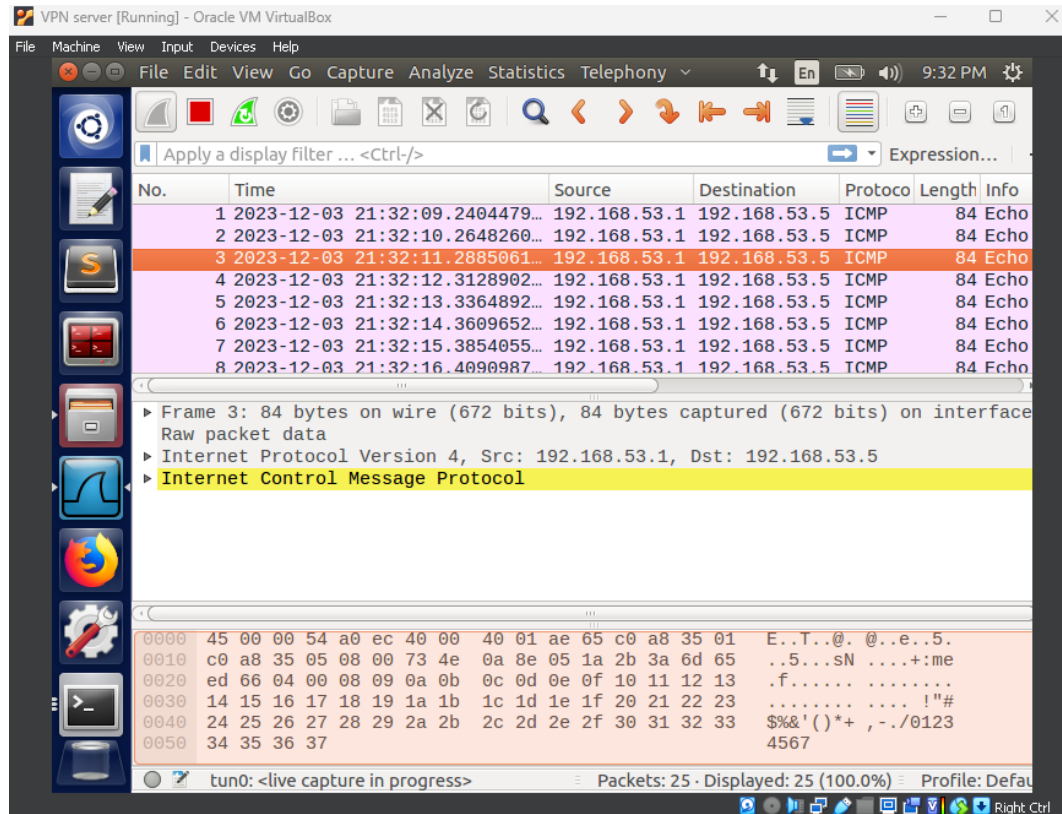
```
VPN Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal File Edit View Search Terminal Help
rtt min/avg/max/mdev = 0.426/0.577/0.812/0.126 ms
[12/03/23]seed@VM:~$ ping 192.168.53.1
PING 192.168.53.1 (192.168.53.1) 56(84) bytes of data.
64 bytes from 192.168.53.1: icmp_seq=1 ttl=64 time=0.745 ms
64 bytes from 192.168.53.1: icmp_seq=2 ttl=64 time=0.528 ms
64 bytes from 192.168.53.1: icmp_seq=3 ttl=64 time=0.515 ms
64 bytes from 192.168.53.1: icmp_seq=4 ttl=64 time=0.514 ms
64 bytes from 192.168.53.1: icmp_seq=5 ttl=64 time=0.583 ms
64 bytes from 192.168.53.1: icmp_seq=6 ttl=64 time=0.506 ms
64 bytes from 192.168.53.1: icmp_seq=7 ttl=64 time=0.490 ms
64 bytes from 192.168.53.1: icmp_seq=8 ttl=64 time=0.530 ms
^C
--- 192.168.53.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time
```

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

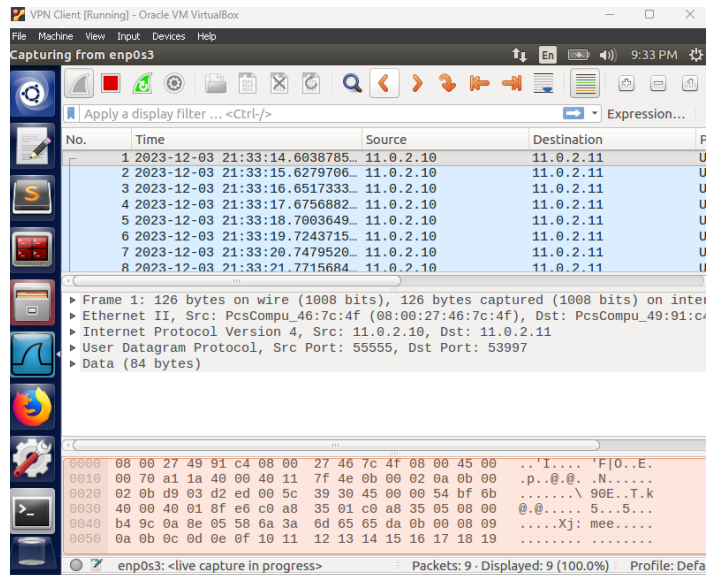
**a. Open Wireshark on both the VPN Server and VPN Client.**



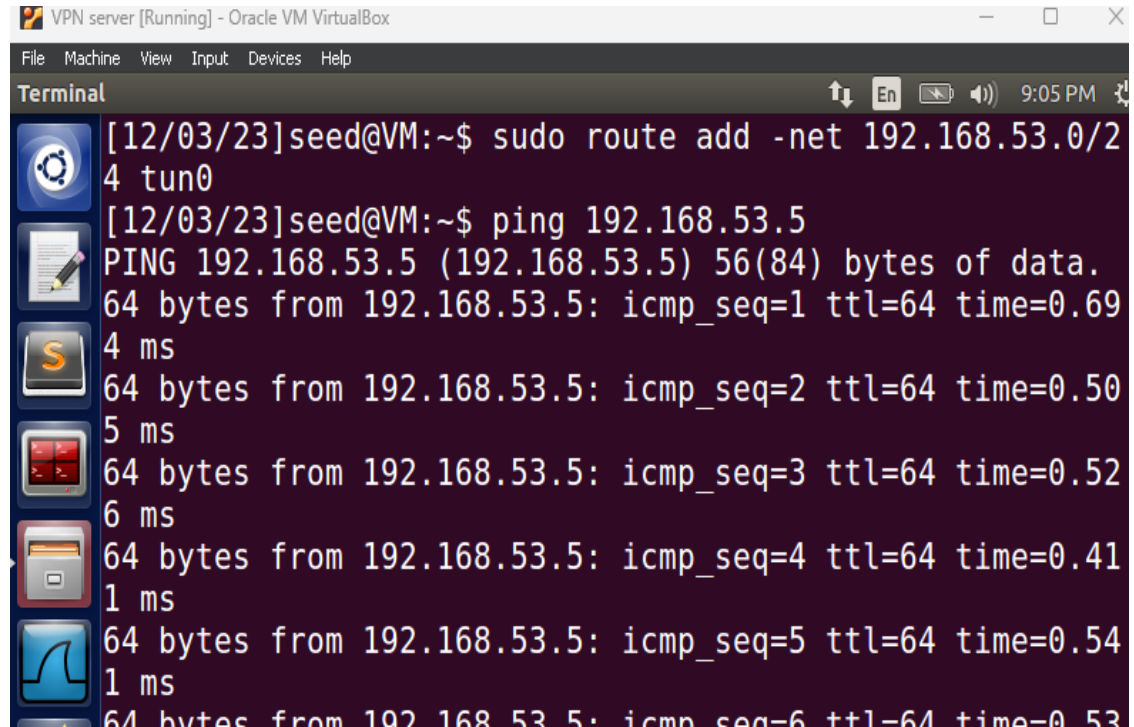
**b. On the VPN Server's Wireshark, listen to the tun0 interface**



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



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



```
VPN server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
[12/03/23]seed@VM:~$ sudo route add -net 192.168.53.0/24 tun0
[12/03/23]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=0.694 ms
64 bytes from 192.168.53.5: icmp_seq=2 ttl=64 time=0.505 ms
64 bytes from 192.168.53.5: icmp_seq=3 ttl=64 time=0.526 ms
64 bytes from 192.168.53.5: icmp_seq=4 ttl=64 time=0.411 ms
64 bytes from 192.168.53.5: icmp_seq=5 ttl=64 time=0.541 ms
64 bytes from 192.168.53.5: icmp_seq=6 ttl=64 time=0.531 ms
```

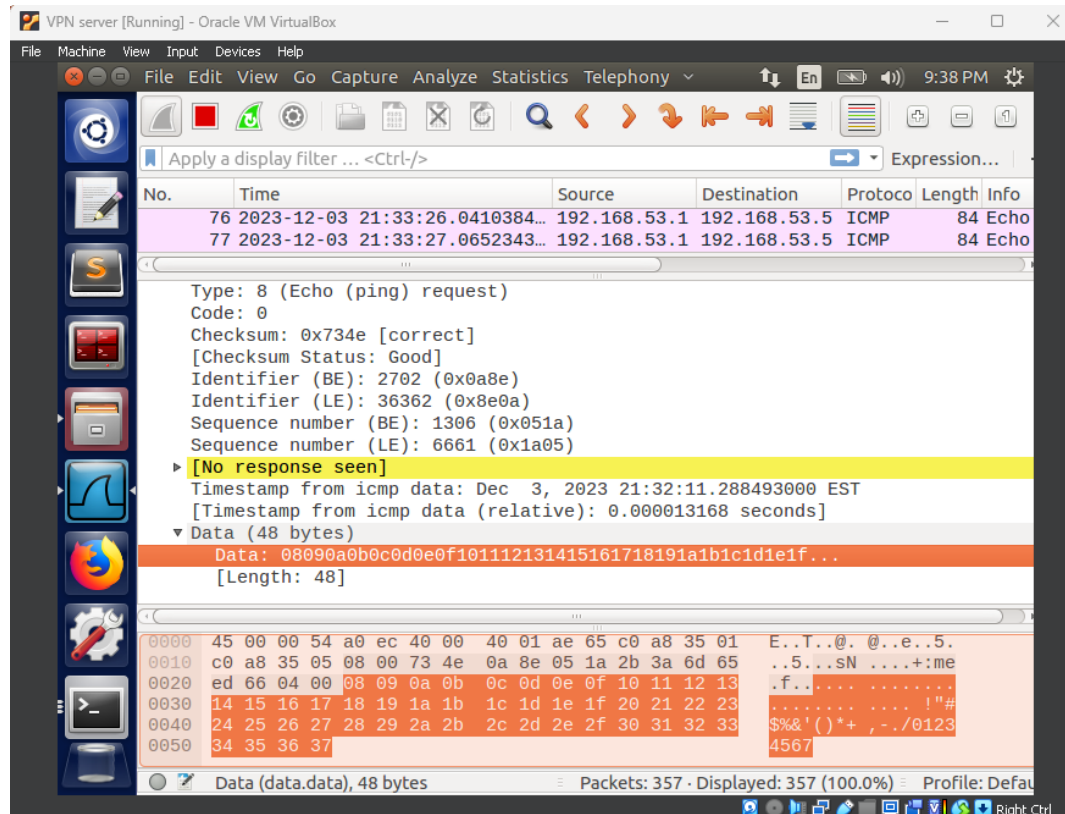
- e. Take screenshots of what you see on Wireshark on both the VPN Server and VPN Client

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.

The examination of the Wireshark capture on the tun0 interface unveils the intricate exchange of ICMP requests and replies between the VPN Client and VPN Server, complete with the distinctive tun0 IP addresses assigned to each. However, the attempt to replicate this analysis on the VPN Client's enp0s5 interface proves unproductive, as the corresponding traffic remains elusive. This discrepancy underscores the unique characteristics of tunneling, a technique employed to facilitate the transmission of non-native protocols across networks that might not inherently support them.

Tunneling protocols, typically operating at layer 4, present themselves as viable alternatives to conventional TCP or UDP methods. In our specific scenario, the communication channels are established over the tun0 IP. Here, the original packet undergoes a process of encapsulation, being enveloped within another packet at layer 4. Subsequently, at the destination, this encapsulated packet is carefully decapsulated and seamlessly forwarded into the internal network. Notably, the VPN server's address takes on the role of the source in this intricate process, ensuring that responses can traverse the network back to the origin.

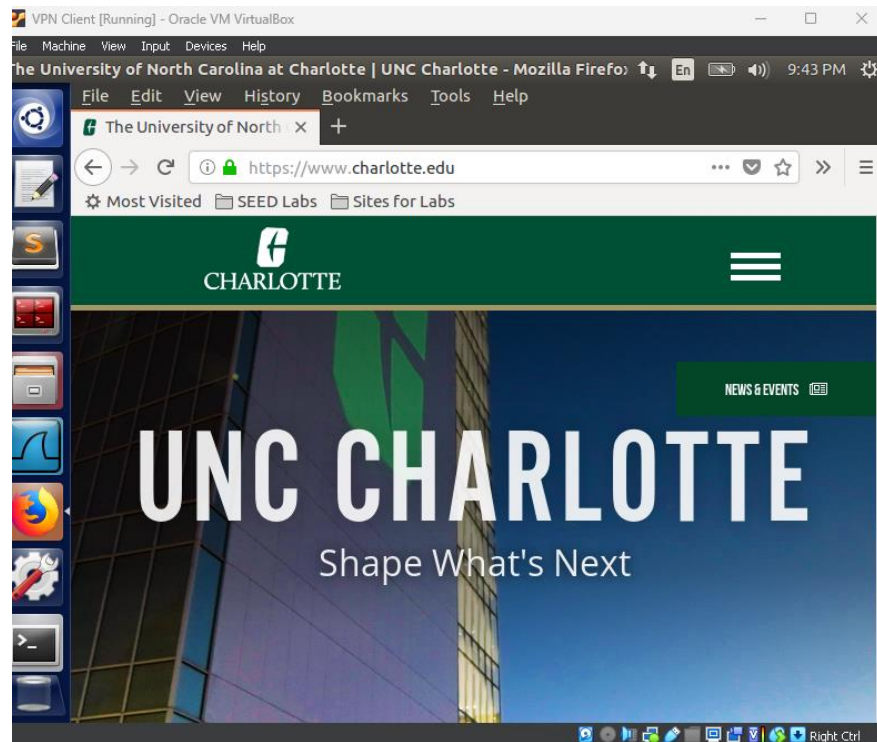
Concurrently, the ongoing exchange of packets between the enp0s5 interfaces of the VPN Client and VPN Server remains observable. Significantly, when an ICMP request is dispatched, the VPN ingeniously inserts the frame into the data field, a critical step vividly illustrated in the accompanying screenshots. This methodical encapsulation and decapsulation dance encapsulate the essence of how the VPN seamlessly transfers information between these network interfaces, revealing a nuanced interplay between tunneled communication and conventional packet exchange.



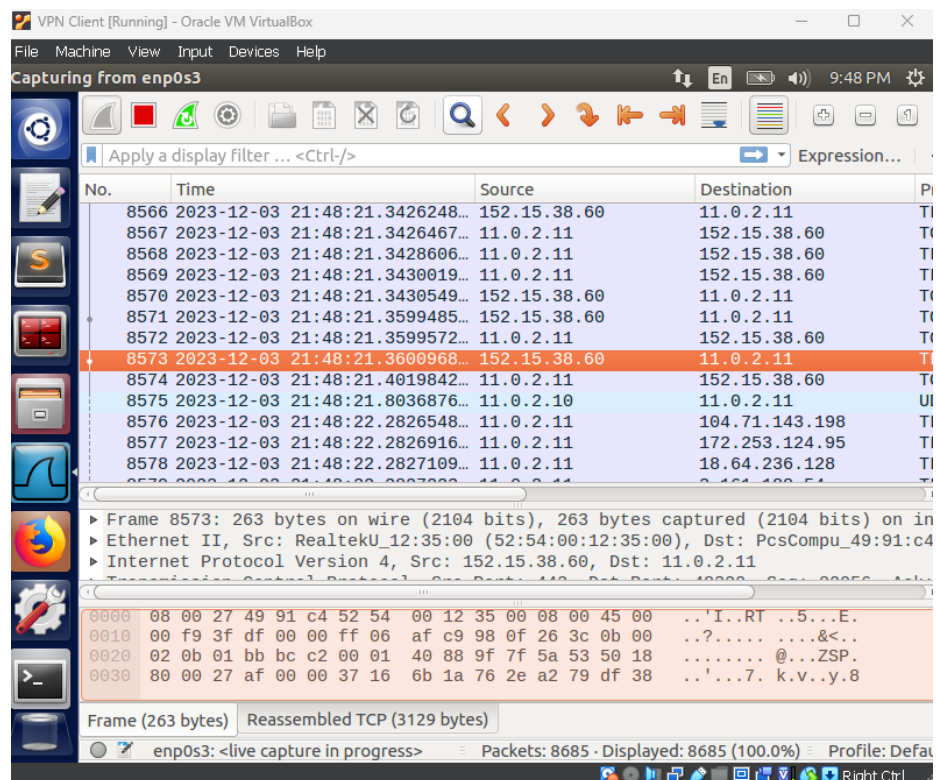




c. Visit the blocked webpage

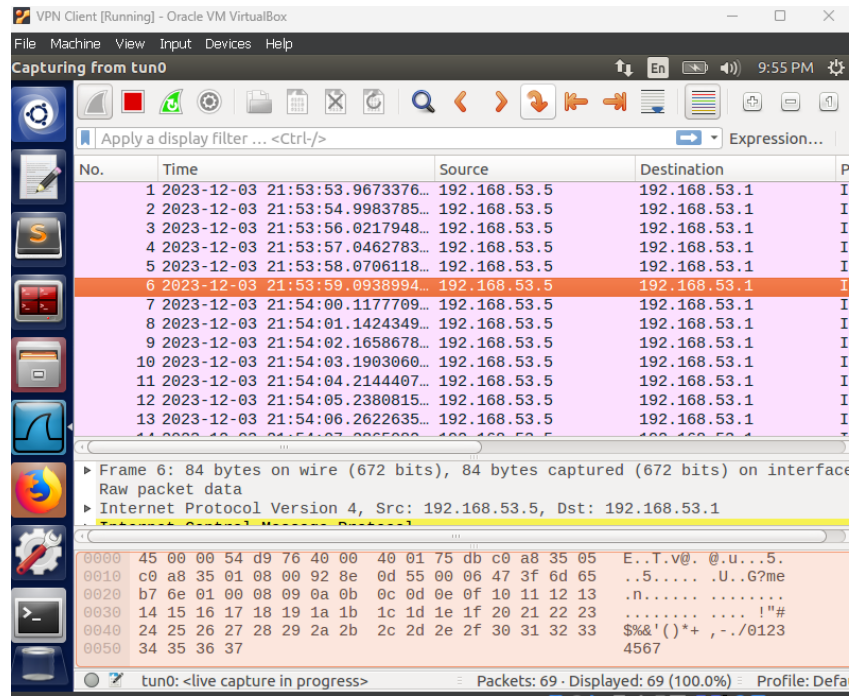


d. Take screenshot(s) of what you see on Wireshark

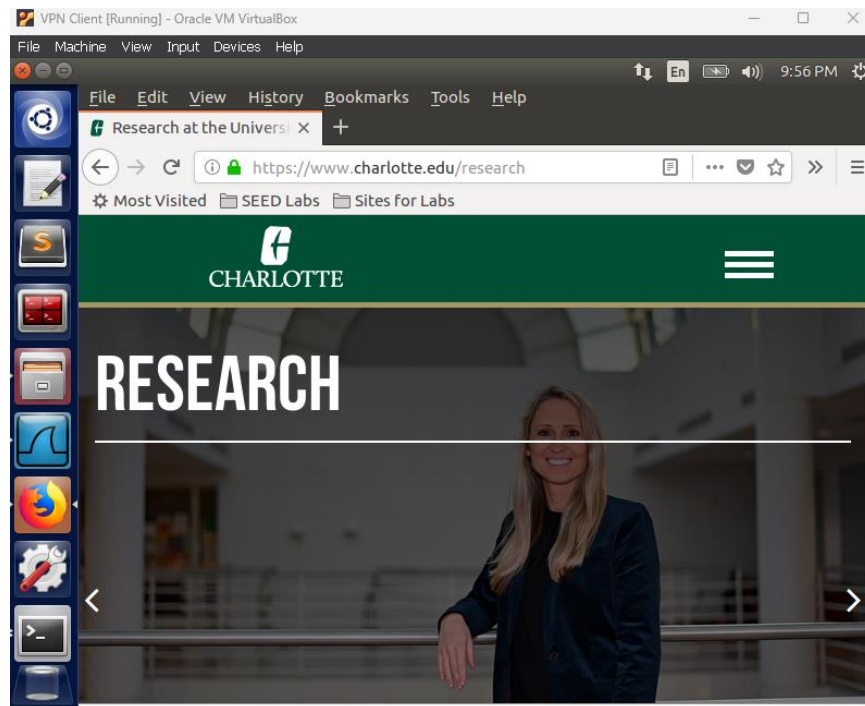




e. Next listen to the tun0 interface



f. Visit the blocked webpage again

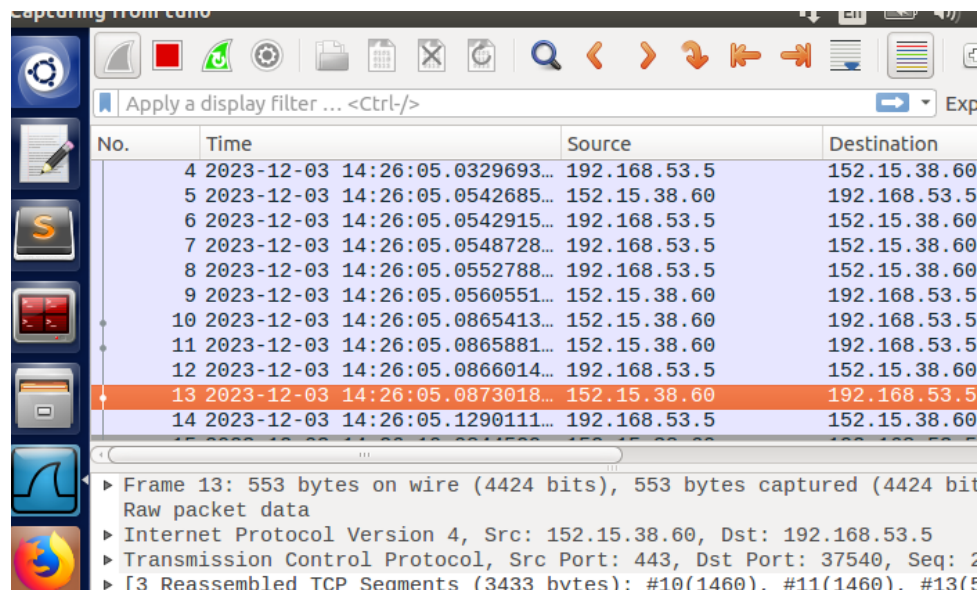


g. Take screenshot(s) of what you see on Wireshark

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

The figures unmistakably illustrate a pattern of packet exchange confined to the tun0 interfaces of both the VPN Client and VPN Server during the browsing activity. Delving into the lines of the collected file, a clear narrative emerges: upon the initiation of the network's restricted website, the orchestrated flow of traffic adhered to the predetermined route over the tunnel, meticulously configured within the VPN channel. Noteworthy is the fact that both the originating request and the ensuing response were channeled through the tunnel, ensuring seamless accessibility to the targeted website. This deliberate routing strategy serves as an effective means to navigate and overcome the inherent limitations imposed by the existing network infrastructure.

As the VPN Client endeavors to establish a connection with the website, a series of packets traverse the VPN tunnel, undergoing a process of encapsulation and subsequent forwarding. Notably, it appears that rules were instituted to restrict the IP address of the website, specifically on the enp0s5 interface rather than on tun0. Through the VPN tunnel, characterized by the tun0 IP address, the VPN Client successfully accesses the web. However, it's crucial to acknowledge that the addition of a rule designed to block the tun0 IP address would, in turn, render access to the webpage via tun0 unattainable. This nuanced interplay of strategic routing and rule implementation underscores the intricacies of network management in the context of VPN configurations and traffic handling.



No.	Time	Source	Destination
4	2023-12-03 14:26:05.0329693...	192.168.53.5	152.15.38.60
5	2023-12-03 14:26:05.0542685...	152.15.38.60	192.168.53.5
6	2023-12-03 14:26:05.0542915...	192.168.53.5	152.15.38.60
7	2023-12-03 14:26:05.0548728...	192.168.53.5	152.15.38.60
8	2023-12-03 14:26:05.0552788...	192.168.53.5	152.15.38.60
9	2023-12-03 14:26:05.0560551...	152.15.38.60	192.168.53.5
10	2023-12-03 14:26:05.0865413...	152.15.38.60	192.168.53.5
11	2023-12-03 14:26:05.0865881...	152.15.38.60	192.168.53.5
12	2023-12-03 14:26:05.0866014...	192.168.53.5	152.15.38.60
13	2023-12-03 14:26:05.0873018...	152.15.38.60	192.168.53.5
14	2023-12-03 14:26:05.1290111...	192.168.53.5	152.15.38.60

Frame 13: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface  
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: 37540, Seq: 2  
[3 Reassembled TCP Segments (3433 bytes): #10(1460), #11(1460), #13(523)]