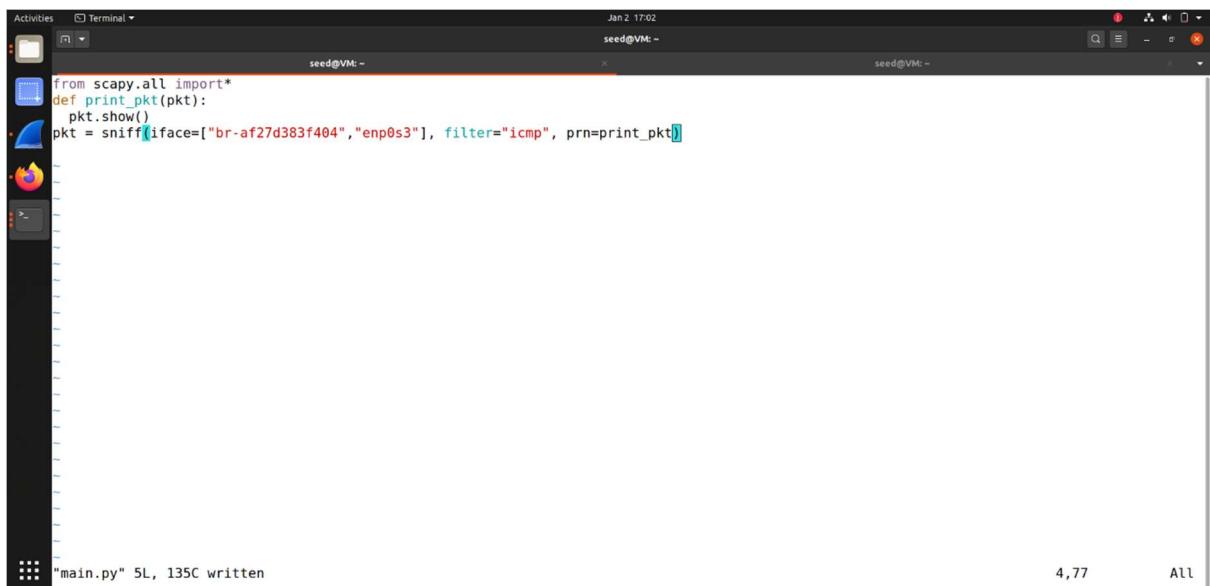


First Part:

All the codes in the first part are written in python



```
Activities Terminal Jan 2 17:02
seed@VM: ~
from scapy.all import*
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface=["br-af27d383f404","enp0s3"], filter="icmp", prn=print_pkt)

main.py 5L, 135C written
4,77 All
```

The code above will sniff the packets on the br-af27d383f404 interface

Task 1.1 A:

Capturing packets using root privileges:



```
Activities Terminal Jan 4 14:08
seed@VM: ~/volumes
[01/04/22]seed@VM:~/.../volumes$ sudo chmod a+x sniffer.py
[01/04/22]seed@VM:~/.../volumes$ sudo python3 sniffer.py
###[ Ethernet ]##
dst      = 52:54:00:12:35:02
src      = 08:00:27:e5:5e:55
type     = IPv4
###[ IP ]##
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 14149
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x4296
src      = 10.0.2.15
dst      = 142.251.37.196
'options  \
###[ ICMP ]##
type     = echo-request
code    = 0
checksum = 0xe914
id      = 0x1
seq     = 0x1
###[ Raw ]##
load    = '\x15\x9b\xd4a\x00\x00\x00\x00\x19\x01\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1
e\x1f !#$%&`(*+,-./01234567'
###[ Ethernet ]##
dst      = 08:00:27:e5:5e:55
src      = 52:54:00:12:35:02
```

```
[01/04/22]seed@VM:~/.../Labsetup$ ping www.google.com
PING www.google.com (142.251.37.196) 56(84) bytes of data.
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=1 ttl=117 time=80.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=2 ttl=117 time=44.4 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=3 ttl=117 time=48.5 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=4 ttl=117 time=46.9 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=5 ttl=117 time=51.9 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=6 ttl=117 time=54.5 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=7 ttl=117 time=52.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=8 ttl=117 time=56.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=9 ttl=117 time=58.4 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=10 ttl=117 time=50.1 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=11 ttl=117 time=60.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=12 ttl=117 time=53.0 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=13 ttl=117 time=43.7 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=14 ttl=117 time=56.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=15 ttl=117 time=115 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=16 ttl=117 time=49.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=17 ttl=117 time=44.3 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=18 ttl=117 time=50.6 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=19 ttl=117 time=65.1 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=20 ttl=117 time=53.6 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=21 ttl=117 time=64.4 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=22 ttl=117 time=55.1 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=23 ttl=117 time=47.9 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=24 ttl=117 time=47.4 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=25 ttl=117 time=45.8 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=26 ttl=117 time=50.6 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=27 ttl=117 time=59.3 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=28 ttl=117 time=48.7 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=29 ttl=117 time=47.2 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=30 ttl=117 time=44.5 ms
64 bytes from mrs09s15-in-f4.le100.net (142.251.37.196): icmp_seq=31 ttl=117 time=47.2 ms
```

Running the code with out root privilege :

```
[01/04/22]seed@VM:~/.../volumes$ python3 sniffer.py
Traceback (most recent call last):
  File "sniffer.py", line 11, in <module>
    pkt = sniff(iface=interfaces, filter='icmp',prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniff._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 894, in _run
    sniff_sockets.update(
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 895, in <genexpr>
    (L2socket(type=ETH_P_ALL, iface=ifname, *arg, **karg),
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(typ
e)) # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[01/04/22]seed@VM:~/.../volumes$
```

Task 1.1 B:

Code is written to capture ICMP packets:

```
Activities Terminal Jan 4 14:43
seed@VM: ~/volumes
from scapy.all import *

def print_pkt(pkt):
    if pkt[ICMP] is not None:
        if pkt[ICMP].type == 0 or pkt[ICMP].type == 8:
            print(f"\tsource: {pkt[IP].src}")
            print(f"\tdest: {pkt[IP].dst}")

        if pkt[ICMP].type == 0:
            print("ICMP type: echo-reply")

        if pkt[ICMP].type == 8:
            print("ICMP type: echo-request")

interfaces=['br-af27d383f404','enp0s3','lo']
pkt = sniff(iface=interfaces, filter='icmp', prn=print_pkt)

icmp.py" 25L, 580C
```

Running the code to capture ICMP packets ,on sending ping to google.com:

Ping to www.google.com:

```
Activities Terminal Jan 4 14:29
seed@VM: ~/volumes seed@VM: ~/volumes seed@VM: ~/volumes
[01/04/22]seed@VM:~/.../volumes$ ping www.google.com
PING www.google.com (142.250.180.100) 56(84) bytes of data.
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=1 ttl=115 time=49.2 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=2 ttl=115 time=50.8 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=3 ttl=115 time=50.5 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=4 ttl=115 time=52.2 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=5 ttl=115 time=51.6 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=6 ttl=115 time=51.0 ms
64 bytes from mil04s42-in-f4.1e100.net (142.250.180.100): icmp_seq=7 ttl=115 time=49.6 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6006ms
rtt min/avg/max/mdev = 49.168/50.680/52.168/0.974 ms
[01/04/22]seed@VM:~/.../volumes$
```

Task 1.1 B 2):

Capture Tcp packets:

Tcp packets captured on port 23 and host 10.0.2.15

Code used to capture tcp packets:

```
Activities Terminal Jan 4 15:19 • seed@VM: ~/volumes seed@VM: ~/volumes seed@VM: - seed@VM: ~/volumes
from scapy.all import *
def print_pkt(pkt):
    if pkt[TCP] is not None:
        print(f"\tsource: {pkt[IP].src}")
        print(f"\tdest: {pkt[IP].dst}")
        print(f"\tsource_port: {pkt[TCP].sport}")
        print(f"\tdest_port: {pkt[TCP].dport}")

interfaces=['br-af27d383f404','enp0s3','lo']
pkt = sniff(iface=interfaces, filter='tcp port 23 and src host 10.0.2.15',prn=print_pkt)

tcp.py 24L, 420C 18,72 All
```

Task 1.1 B 3):

Code used to send packets to specific subnet:

```
Activities Terminal Jan 4 15:31 • seed@VM: ~/volumes seed@VM: ~/volumes seed@VM: - seed@VM: ~/volumes seed@VM: ~/volumes seed@VM: ~/volumes seed@VM: ~/volumes
from scapy.all import *
ip=IP()
ip.dst='128.230.0.0/16'
send(ip,4)
send_subnet.py 6L, 69C 6,0-1 All
```

Code used to sniff packets on dest 128.230.0.0/16:

A screenshot of a terminal window titled "Activities Terminal". The window has multiple tabs, all labeled "seed@VM: ~/volumes". The code in the terminal is as follows:

```
from scapy.all import *
def print_pkt(pkt):
    pkt.show()

interfaces=['br-af27d383f404','enp0s3','lo']
pkt=sniff(iface=interfaces, filter='dst net 128.230.0.0/16',prn=print_pkt)
```

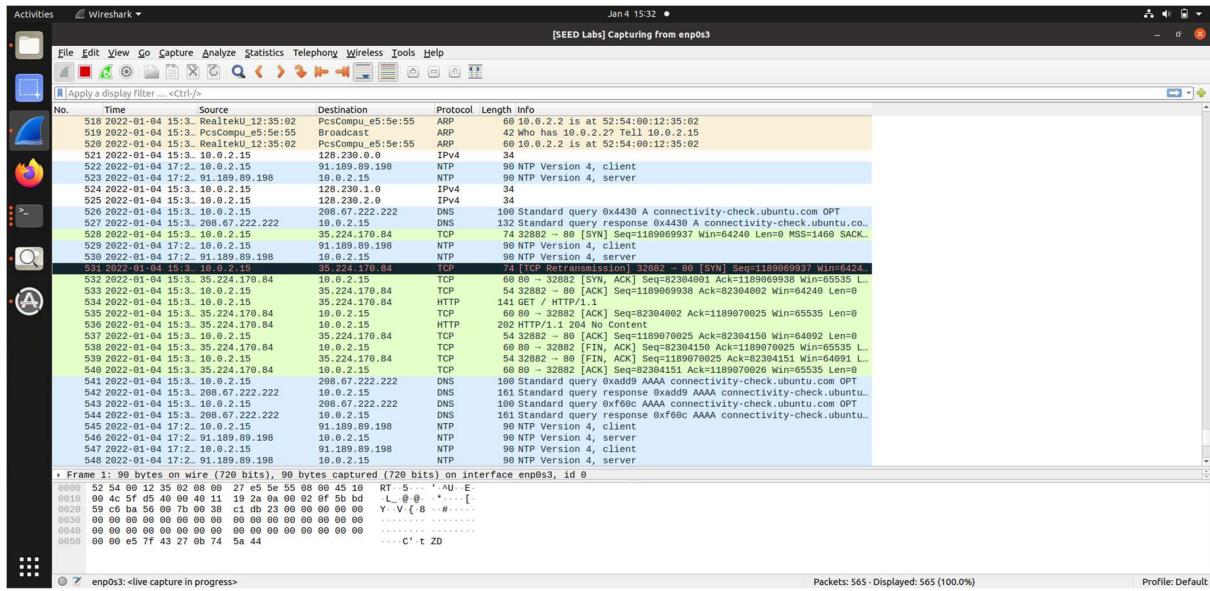
The status bar at the bottom shows "subnet.py" 12L, 186C, 1,8, and All.

Running the program to sniff packets:

A screenshot of a terminal window titled "Activities Terminal". The window has multiple tabs, all labeled "seed@VM: ~/volumes". The command run is "sudo python3 subnet.py". The output shows two captured Ethernet frames. The first frame is detailed below:

```
[01/04/22]seed@VM:~/.../volumes$ sudo python3 subnet.py
#[[ Ethernet
dst      = 52:54:00:12:35:02
src      = 08:00:27:e5:5e:55
type     = IPv4
#[[ IP ]#
version  = 4
ihl      = 5
tos      = 0x0
len      = 20
id       = 1
flags    =
frag    = 0
ttl      = 64
proto   = hopopt
chksum   = 0xedf4
src      = 10.0.2.15
dst      = 128.230.0.0
\options  \
#[[ Ethernet ]#
dst      = 52:54:00:12:35:02
src      = 08:00:27:e5:5e:55
type     = IPv4
#[[ IP ]#
version  = 4
ihl      = 5
tos      = 0x0
len      = 20
id       = 1
flags    =
```

Wireshark photo to show the Tcp packets being sniffed on the 128.230.0.0/16:



Task 1.2:

We will spoof ICMP echo request packets, and send them to another VM on the same network. We will use Wireshark to observe whether our request will be accepted by the receiver.

a.src is an arbitrary ip used for sending packet,

this code used to send packet from src to dest:

```

Activities Terminal Jan 6 14:21 •
seed@VM: ~ seed@VM: ~ seed@VM: ~
from scapy.all import *

a=IP()
a.src='10.0.2.1'
a.dst='10.0.2.3'
b=ICMP()
p=a/b
send(p)
-- INSERT --

```

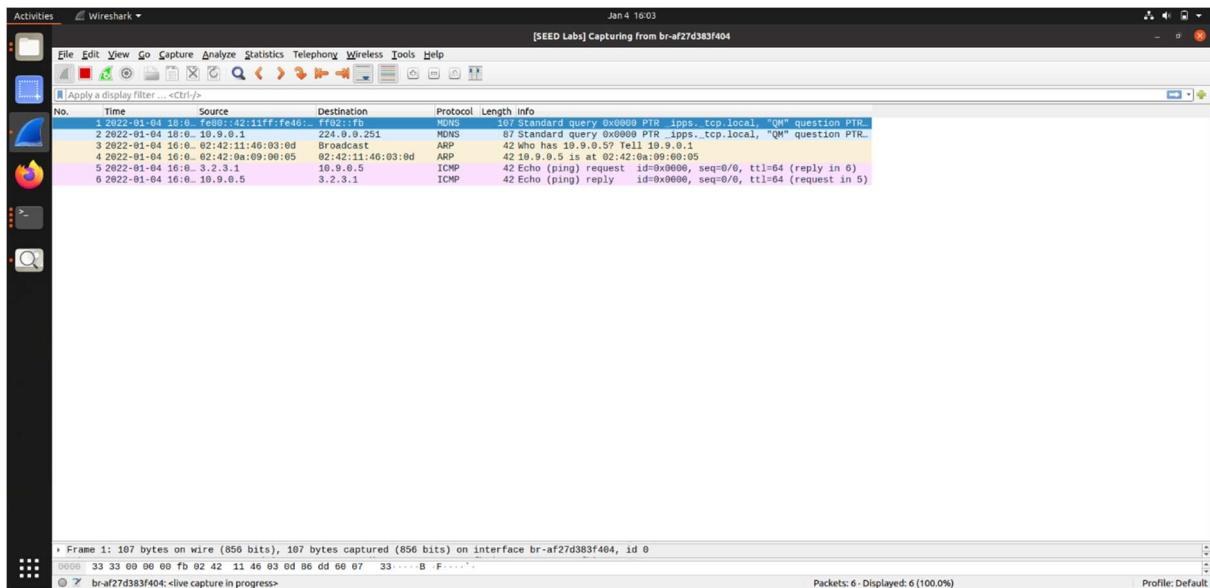
Spoofing the sent packet:

```
Activities Terminal Jan 4 16:03 seed@VM:~ seed@VM:~ Sent 1 packets.
version : BitField (4 bits)      = 4          (4)
ihl   : BitField (4 bits)      = None       (None)
tos   : XByteField            = 0          (0)
len   : ShortField             = None       (None)
id    : ShortField             = 1          (1)
flags : FlagsField (3 bits)     = <Flag 0 ()>
frag  : BitField (13 bits)     = 0          (0)
ttl   : ByteField              = 64         (64)
proto : ByteEnumField         = 0          (0)
checksum : XShortField        = None       (None)
src   : SourceIPField          = '3.2.3.1'  (None)
dst   : DestIPField            = '10.9.0.5' (None)
options : PacketListField      = []         ([])

[01/04/22]seed@VM:~$ sudo python3 spoofing_icmp.py .
Sent 1 packets.
version : BitField (4 bits)      = 4          (4)
ihl   : BitField (4 bits)      = None       (None)
tos   : XByteField            = 0          (0)
len   : ShortField             = None       (None)
id    : ShortField             = 1          (1)
flags : FlagsField (3 bits)     = <Flag 0 ()>
frag  : BitField (13 bits)     = 0          (0)
ttl   : ByteField              = 64         (64)
proto : ByteEnumField         = 0          (0)
checksum : XShortField        = None       (None)
src   : SourceIPField          = '3.2.3.1'  (None)
dst   : DestIPField            = '10.9.0.5' (None)
options : PacketListField      = []         ([])

[01/04/22]seed@VM:~$
```

As it appears on wireshark image below there is an echo request and an echo reply to spoofed packed that was sent:

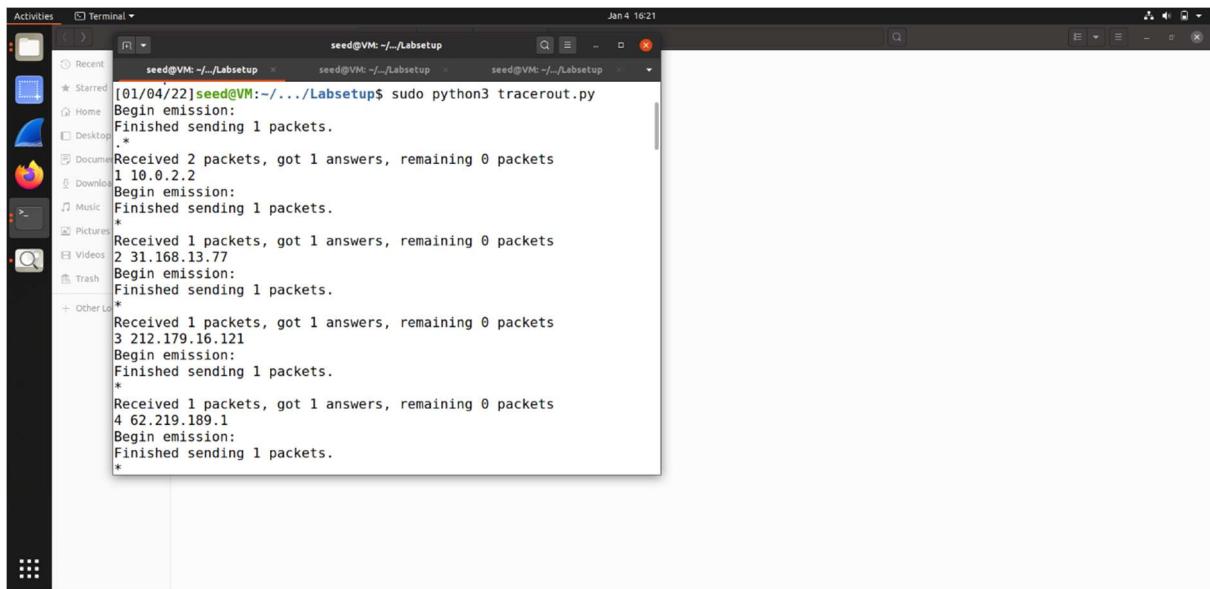


Task1.3:

In this task we estimate the distance of a data being sent from src to dest,
By using TCP/IP protocols

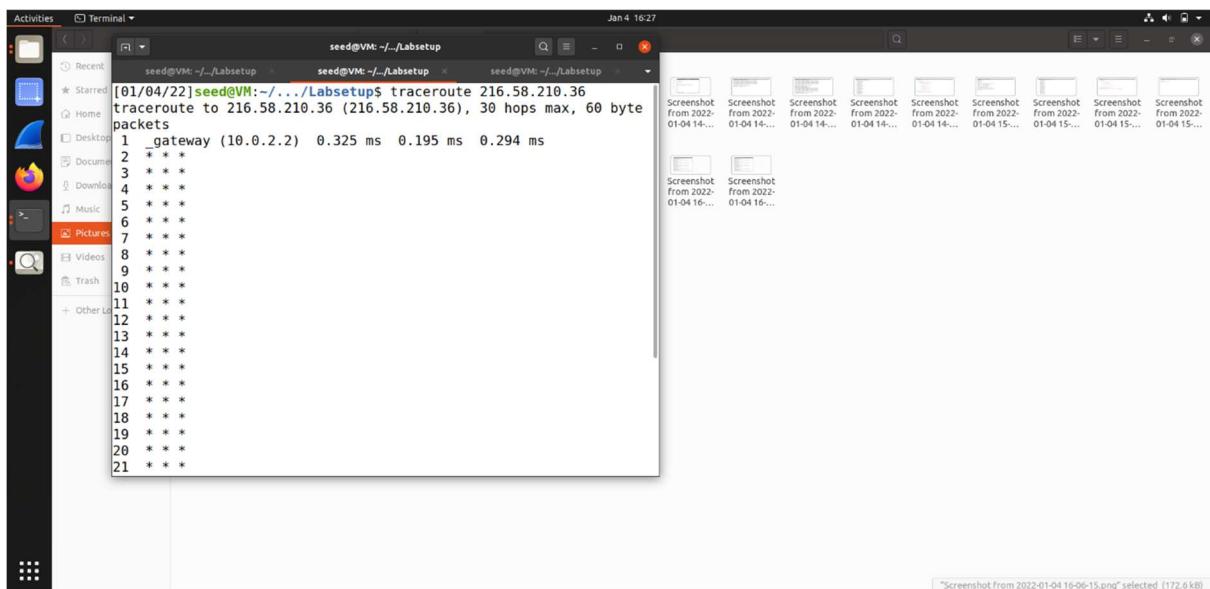
Tracerout program used to send packets over network from src to dest,

The path of the packet:



```
[01/04/22]seed@VM:~/.../Labsetup$ sudo python3 tracerout.py
Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets
1 10.0.2.2
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
2 31.168.13.77
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
3 212.179.16.121
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
4 62.219.189.1
Begin emission:
Finished sending 1 packets.
*
```

Estimated distance time at takes to arrive at dest on the network:



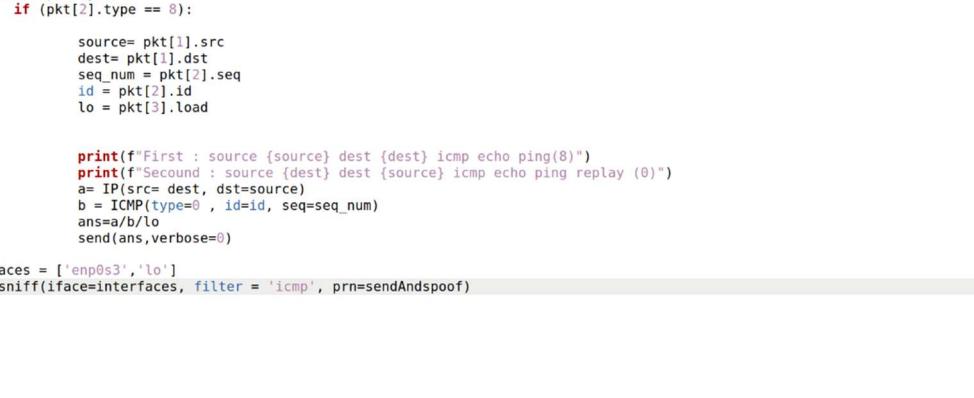
```
[01/04/22]seed@VM:~/.../Labsetup$ traceroute 216.58.210.36
traceroute to 216.58.210.36 (216.58.210.36), 30 hops max, 60 byte
packets
1 _gateway (10.0.2.2)  0.325 ms  0.195 ms  0.294 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
```

Task1.4:

In this task we have implemented sniff and then spoof program,

We have sent ping to 1.2.3.4, we have used the attacker container to response to the ARP protocol asking for a specific ip belongs to who.

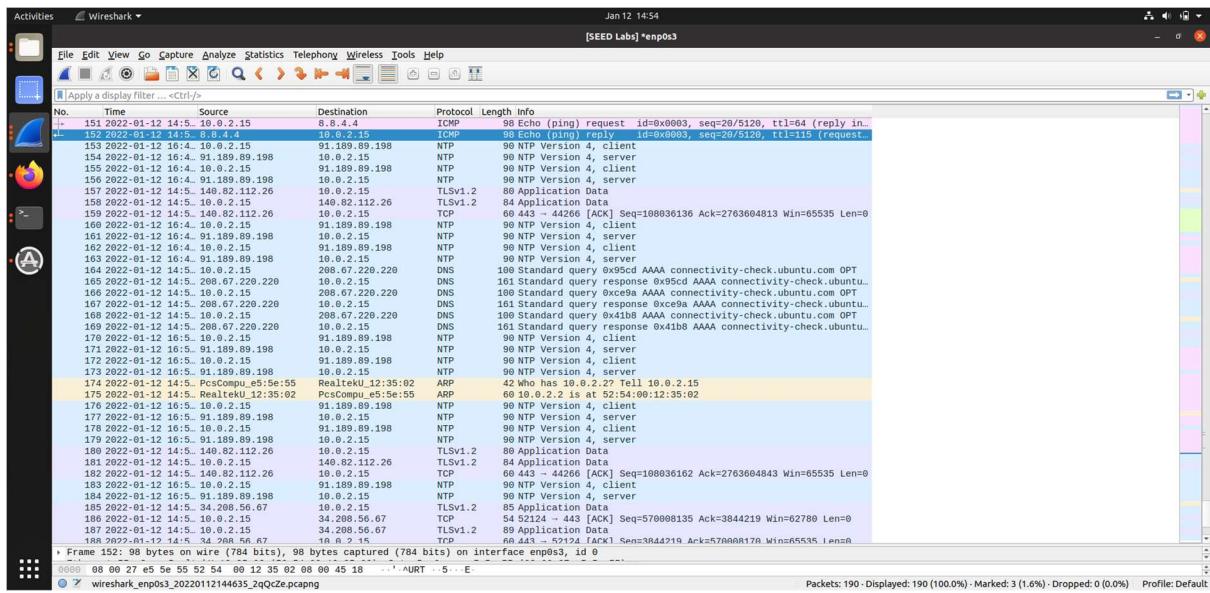
Running the program :



The screenshot shows a terminal window titled "Text Editor" with the file "sniffing_spooftg1.py" open. The code implements ICMP spoofing by sniffing for ICMP echo requests and sending ICMP echo replies with forged source and destination addresses. The terminal interface includes a sidebar with icons for file operations, search, and help.

```
1 from scapy.all import *
2
3 def sendAndspoof(pkt):
4     if (pkt[2].type == 8):
5
6         source= pkt[1].src
7         dest= pkt[1].dst
8         seq_num = pkt[2].seq
9         id = pkt[2].id
10        lo = pkt[3].load
11
12
13         print(f"First : source {source} dest {dest} icmp echo ping(8)")
14         print(f"Second : source {dest} dest {source} icmp echo ping replay (0)")
15         a= IP(src= dest, dst=source)
16         b = ICMP(type=0 , id=id, seq=seq_num)
17         ans=a/b/lo
18         send(ans,verbose=0)
19
20 interfaces = ['enp0s3','lo']
21 pkt = sniff(iface=interfaces, filter = 'icmp', prn=sendAndspoof)
```

as you can see on the wireshark image below the ARP asks who has this ip and the attacker gives a response to him that he acknowledges this ip.



Second part:

Task2:

packets captured by the sniff program:

running with pernicious mode=0

```
Activities Terminal Jan 11 05:44
seed@VM: ~/Labsetup
root@VM:~# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var volumes
root@VM:~# ls volumes
icmp.py send_subnet.py snif sniff sniff.c sniff.o sniffer.py sniffing_spoffing.py sp.py subnet.py tcp.py volumes
root@VM:~# ./sniff
bash: ./sniff: No such file or directory
root@VM:~# cd volumes
root@VM:/volumes# ./sniff
A Packet has been Captured
Source: 183.22.64.0
Destination: 64.1.107.129
A Packet has been Captured
Source: 74.87.64.0
Destination: 64.1.216.64
A Packet has been Captured
Source: 183.57.64.0
Destination: 64.1.107.94
A Packet has been Captured
Source: 74.88.64.0
Destination: 64.1.216.63
A Packet has been Captured
Source: 183.166.64.0
Destination: 64.1.106.241
A Packet has been Captured
Source: 74.89.64.0
Destination: 64.1.216.62
A Packet has been Captured
Source: 184.68.64.0
Destination: 64.1.106.83
A Packet has been Captured
Source: 74.90.64.0
Destination: 64.1.216.61
```

The program in the phot up is the captures being sent by ping 10.9.0.5:

```

[01/11/22] seed@VM:~/.../Labsetup$ docksh 7f82b86e44e9
root@VM:/# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.151 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.103 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.070 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=64 time=0.073 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=64 time=0.083 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=64 time=0.061 ms
64 bytes from 10.9.0.5: icmp_seq=9 ttl=64 time=0.053 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=64 time=0.046 ms
64 bytes from 10.9.0.5: icmp_seq=11 ttl=64 time=0.079 ms
^C
--- 10.9.0.5 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10241ms
rtt min/avg/max/mdev = 0.046/0.077/0.151/0.028 ms
root@VM:/# ping 10.0.2.3
PING 10.0.2.3 (10.0.2.3) 56(84) bytes of data.
64 bytes from 10.0.2.3: icmp_seq=1 ttl=64 time=0.388 ms
64 bytes from 10.0.2.3: icmp_seq=2 ttl=64 time=0.360 ms
64 bytes from 10.0.2.3: icmp_seq=3 ttl=64 time=0.518 ms
64 bytes from 10.0.2.3: icmp_seq=4 ttl=64 time=0.392 ms
64 bytes from 10.0.2.3: icmp_seq=5 ttl=64 time=0.536 ms
^C
--- 10.0.2.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4089ms
rtt min/avg/max/mdev = 0.360/0.438/0.536/0.073 ms
root@VM:/# 

```

packets captured by the sniff program:

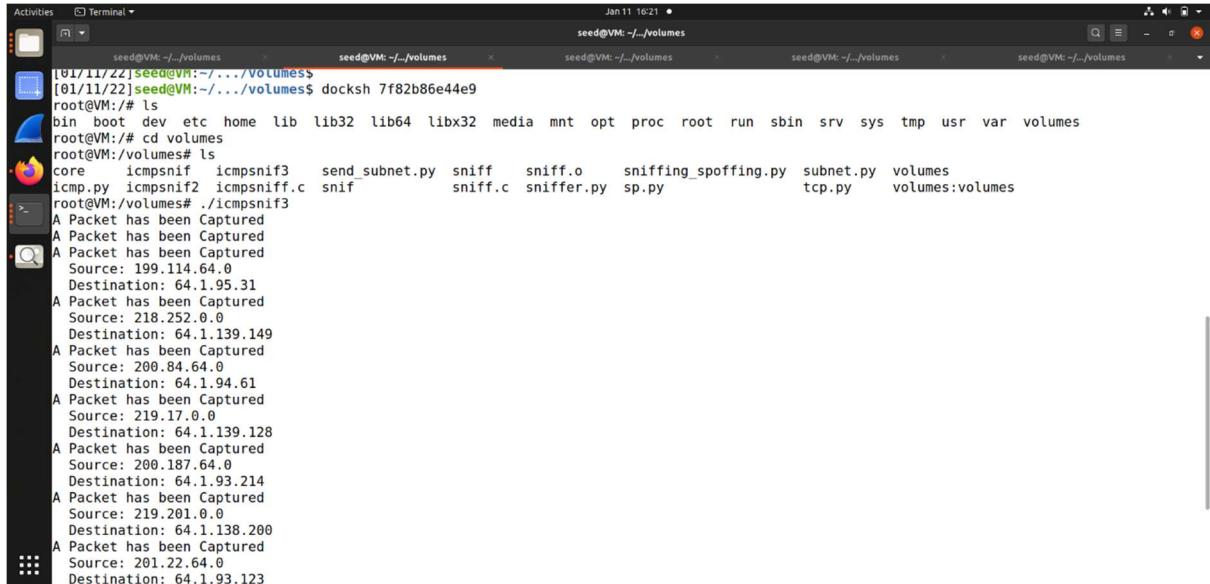
running with pernicious mode=1

```

[01/11/22] seed@VM:~/.../Labsetup$ docksh 7f82b86e44e9
root@VM:/# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var volumes
root@VM:/# ls volumes
icmp.py send_subnet.py snif sniff sniff.c sniff.o sniffer.py sniffing_spoffing.py sp.py subnet.py tcp.py volumes
root@VM:/# cd volumes
root@VM:/volumes# ./sniff
A Packet has been Captured
Source: 224.95.64.0
Destination: 64.1.66.56
A Packet has been Captured
Source: 74.157.64.0
Destination: 64.1.215.250
A Packet has been Captured
Source: 225.89.64.0
Destination: 64.1.65.62
A Packet has been Captured
Source: 74.158.64.0
Destination: 64.1.215.249
A Packet has been Captured
Source: 225.147.64.0
Destination: 64.1.65.4
A Packet has been Captured
Source: 74.159.64.0
Destination: 64.1.215.248
A Packet has been Captured
Source: 226.86.64.0
Destination: 64.1.64.65
A Packet has been Captured
Source: 74.160.64.0
Destination: 64.1.215.247
A Packet has been Captured

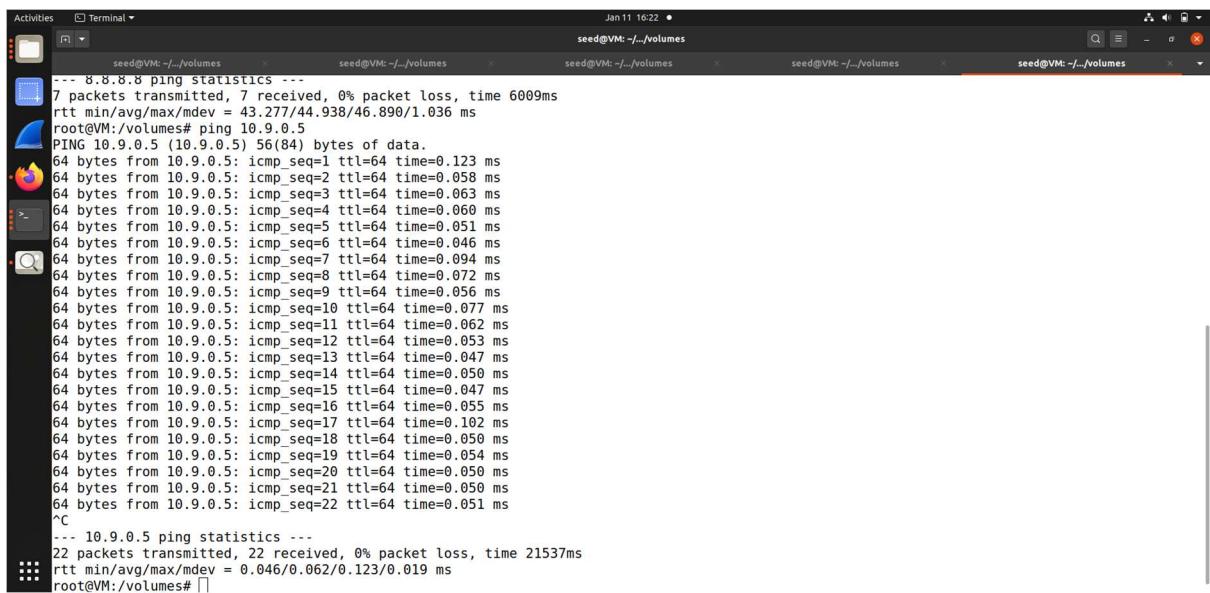
```

Program that captures icmp packets between two hosts on the network:



```
[01/11/22]seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes
[01/11/22]seed@VM:~/volumes$ docksh 7f82b86e44e9
root@VM:# ls
bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run sbin srv sys tmp usr var volumes
root@VM:# cd volumes
root@VM:/volumes# ls
core icmpsnif1 icmpsnif3 send_subnet.py sniff sniff.o sniffing_spoffing.py subnet.py volumes
icmp.py icmpsnif2 icmpsnif.c snif sniff.c sniffer.py sp.py tcp.py volumes:volumes
root@VM:/volumes# ./icmpsnif3
A Packet has been Captured
A Packet has been Captured
A Packet has been Captured
Source: 199.114.64.0
Destination: 64.1.95.31
A Packet has been Captured
Source: 218.252.0.0
Destination: 64.1.139.149
A Packet has been Captured
Source: 200.84.64.0
Destination: 64.1.94.61
A Packet has been Captured
Source: 219.17.0.0
Destination: 64.1.139.128
A Packet has been Captured
Source: 200.187.64.0
Destination: 64.1.93.214
A Packet has been Captured
Source: 219.201.0.0
Destination: 64.1.138.200
A Packet has been Captured
Source: 201.22.64.0
Destination: 64.1.93.123
```

Sending packets using ping 10.9.0.5:



```
Activities Terminal Jan 11 16:22 •
seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes      seed@VM:~/volumes
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 43.277/44.938/46.890/1.036 ms
root@VM:/volumes# ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.123 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.063 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.061 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.051 ms
64 bytes from 10.9.0.5: icmp_seq=6 ttl=64 time=0.046 ms
64 bytes from 10.9.0.5: icmp_seq=7 ttl=64 time=0.094 ms
64 bytes from 10.9.0.5: icmp_seq=8 ttl=64 time=0.072 ms
64 bytes from 10.9.0.5: icmp_seq=9 ttl=64 time=0.056 ms
64 bytes from 10.9.0.5: icmp_seq=10 ttl=64 time=0.077 ms
64 bytes from 10.9.0.5: icmp_seq=11 ttl=64 time=0.062 ms
64 bytes from 10.9.0.5: icmp_seq=12 ttl=64 time=0.053 ms
64 bytes from 10.9.0.5: icmp_seq=13 ttl=64 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=64 time=0.047 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=64 time=0.055 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=64 time=0.102 ms
64 bytes from 10.9.0.5: icmp_seq=18 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=19 ttl=64 time=0.054 ms
64 bytes from 10.9.0.5: icmp_seq=20 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=21 ttl=64 time=0.050 ms
64 bytes from 10.9.0.5: icmp_seq=22 ttl=64 time=0.051 ms
^C
--- 10.9.0.5 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21537ms
rtt min/avg/max/mdev = 0.046/0.062/0.123/0.019 ms
root@VM:/volumes#
```

We have used the pcap library which contains the main functions for the sniffing program:

1.pcap_open_live: to capture packets going on the network(network card)

2.pcap_compile: used for the packets filter

3.pcap_setfilter: used for packets filter

4.pcap_loop: for receiving packets

Question 2:

On order to capture packets on the network level(network card) we need to use raw socket,

To use Raw socket u need root privilage, using raw socket could be very sensitive in the term of the user.

Question 3:

When the promiscuous mode is off we can sniff only the packets that goes on our network card and was meant to be sent to us(to our network card),

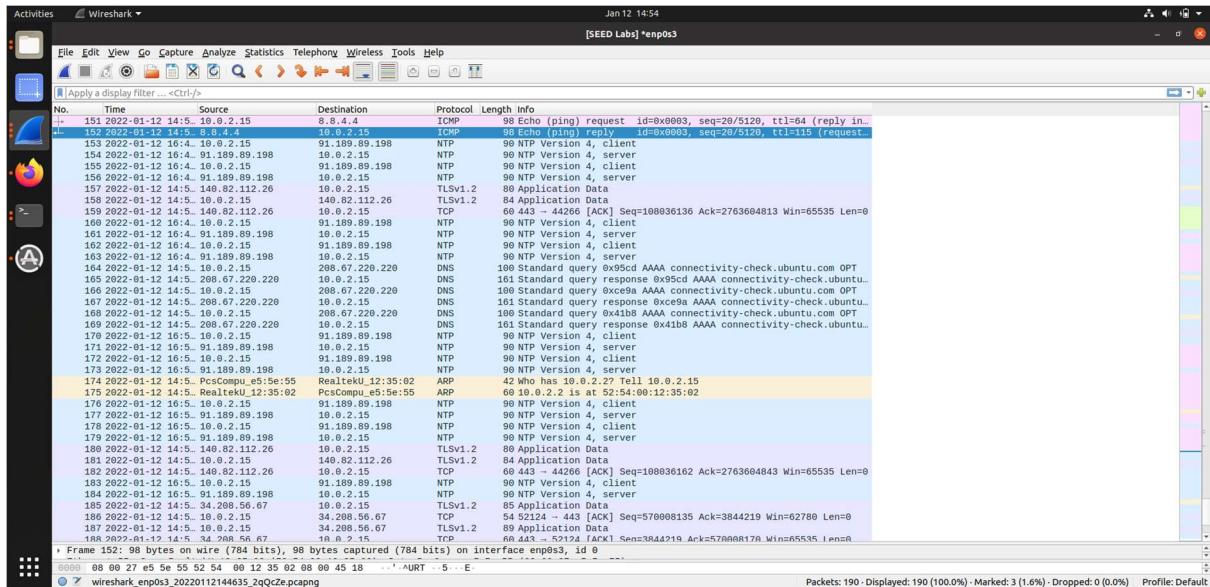
But if the promiscuous mode is on more packets can be captured by our network card which may not necessarily meant to be sent to our network card.

Program that captures TCP with a given range which is 1-100:

TCP program to capture tcp packets with a given port range:

Task2.2A:

Wireshark photo shows the packets that was spoofed,ping sent to 8.8.4.4



Task2.2B:

As seen on the photo below the packet has been spoofed successfully:

Question 4:

No, applying this on our code may cause an error on the code , so it will not work

Question 5:

Calculating checksum for the ip header is not needed ,

It's calculated by our operating system

Question 6:

Raw packets allows us to deal with packets and protocols on low level so it requires a root privilege,

It's up to the user to allow using raw sockets , because it could harm the system and could be dangerous

Task2.3-sniff and then spoof:

Ping sent to 1.3.3.4:

Running spoofing_icmp program to spoof ICMP request:

```

[01/12/22] seed@VM:~/.../volumes$ docksh 7f82b86e44e9
root@VM:/volumes# ./icmp_sniff
bash: ./icmp_sniff: No such file or directory
root@VM:/volumes# ./spoofing_icmp
RAW PACKET SENT
Sent from :1.3.3.4
TO: 255.255.255.255
root@VM:/volumes# ./spoofing_icmp
RAW PACKET SENT
Sent from :1.3.3.4
TO: 255.255.255.255
root@VM:/volumes# ./spoofing_icmp
RAW PACKET SENT
Sent from :1.3.3.4
TO: 255.255.255.255
root@VM:/volumes# ./spoofing_icmp
RAW PACKET SENT

```

We have tried our best to make it work but was just getting icmp request without replies as seen on the wireshark photo below:

