

Computer Networks Security

Assignment 4

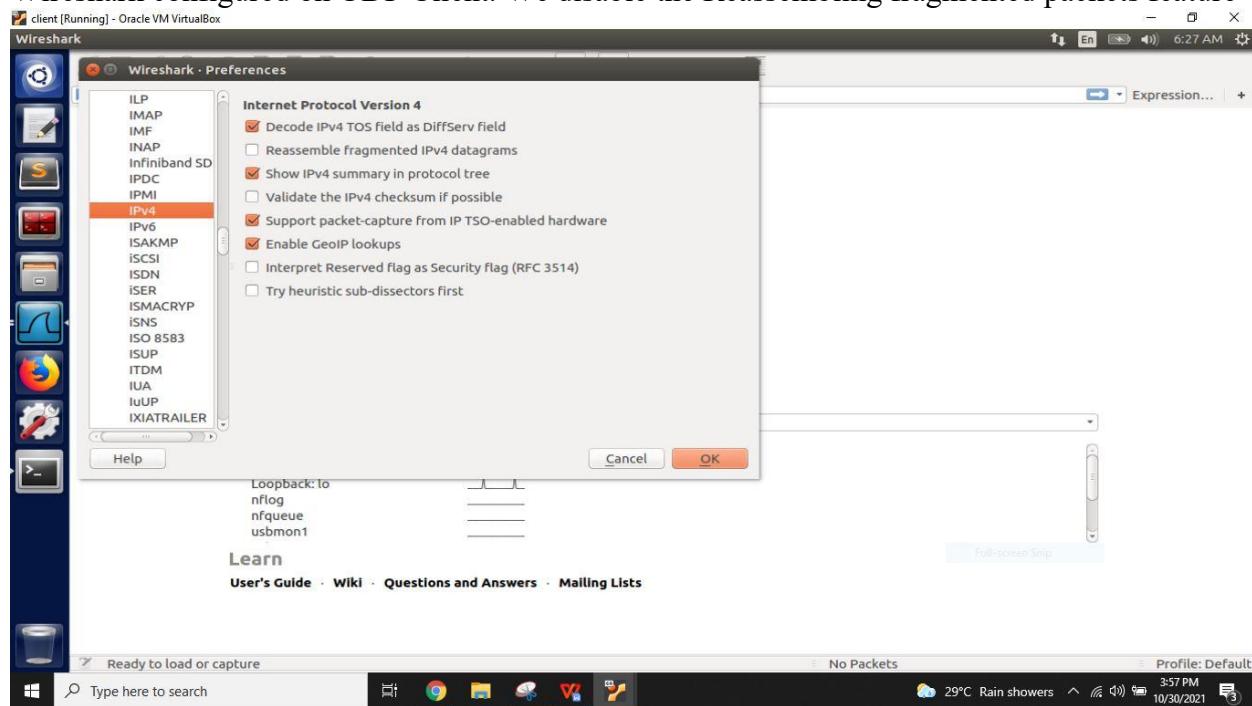
Name: Nikhil TM
SRN: PES1UG20CS821

Lab setup
Vm1:10.0.2.18
Vm2:10.0.2.19
Vm3:192.168.60.5

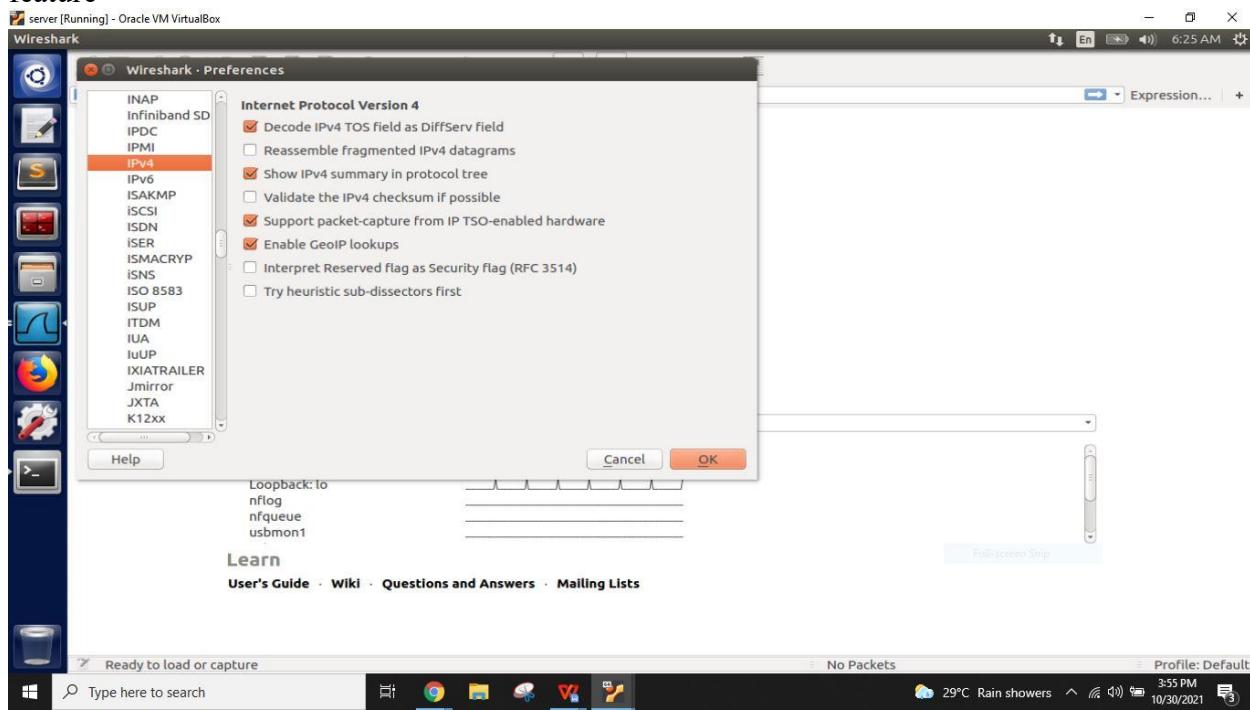
Task1: IP Fragmentation

Task 1a: UDP server

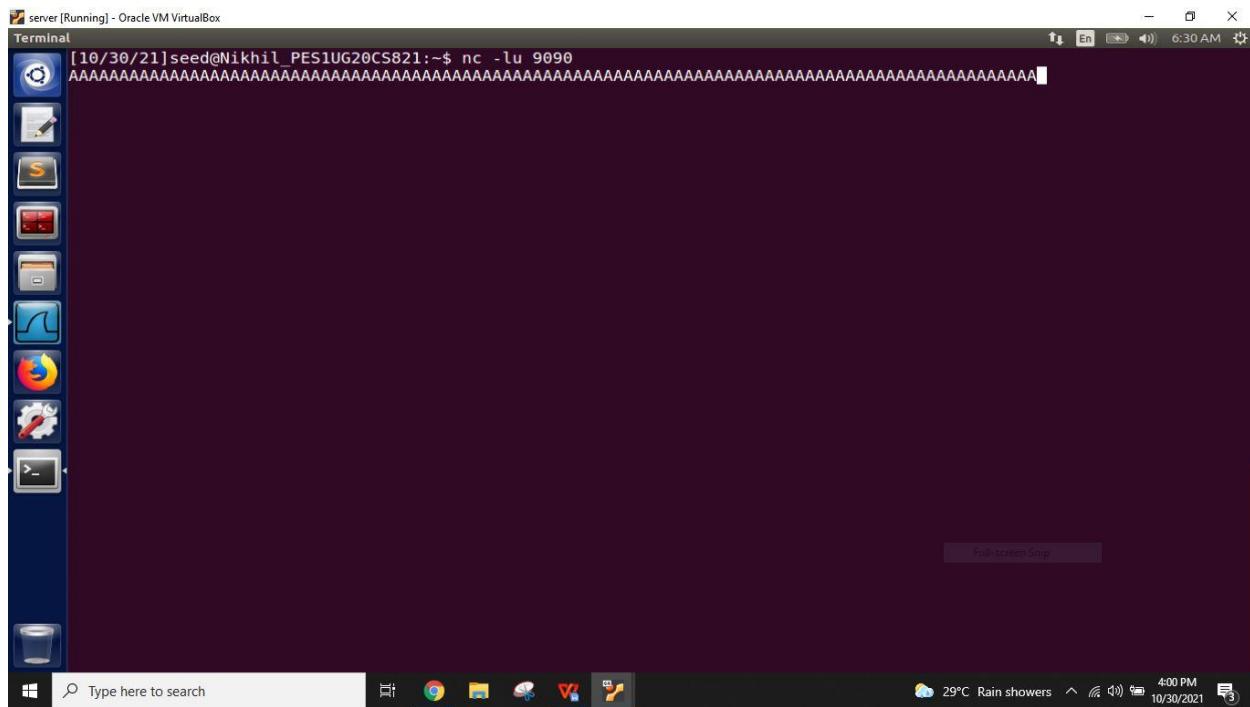
Wireshark configured on UDP Client. We disable the Reassembling fragmented packets feature



Wireshark configured on UDP Server also. We disable the Reassembling fragmented packets feature



Listen to the port 9090 on UDP Server using netcat



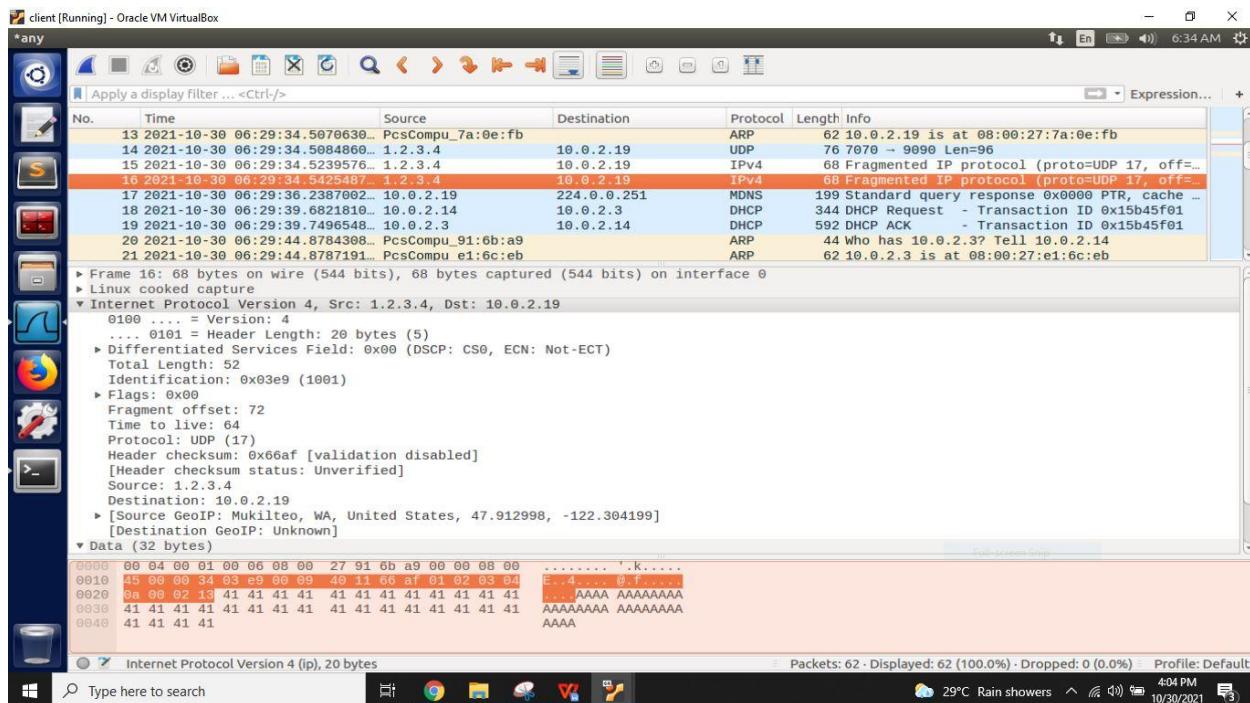
Run the Task1a.py on UDP client

```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:91:6b:a9
          inet addr:10.0.2.14 Bcast:10.0.2.255 Mask:255.255.255.0
             inet6 addr: fe80::b069:9ec0:5d23:9722/64 Scope:Link
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:468 errors:0 dropped:0 overruns:0 frame:0
             TX packets:371 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:182508 (182.5 KB) TX bytes:39671 (39.6 KB)

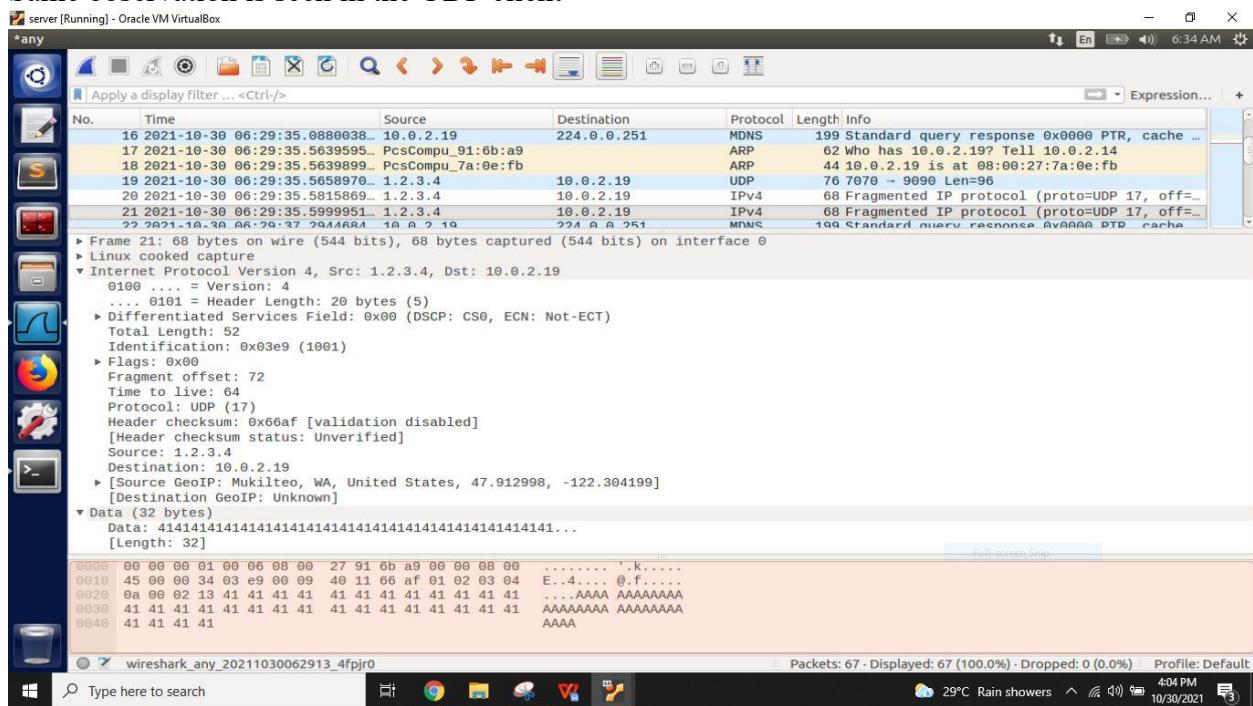
lo     Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
               UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:105 errors:0 dropped:0 overruns:0 frame:0
             TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1
             RX bytes:24056 (24.0 KB) TX bytes:24056 (24.0 KB)

[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.py
(gedit:2605): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

Use wireshark to capture the packets we can see that packets from source 1.2.3.4 is captured by 10.0.2.19 in the UDP client

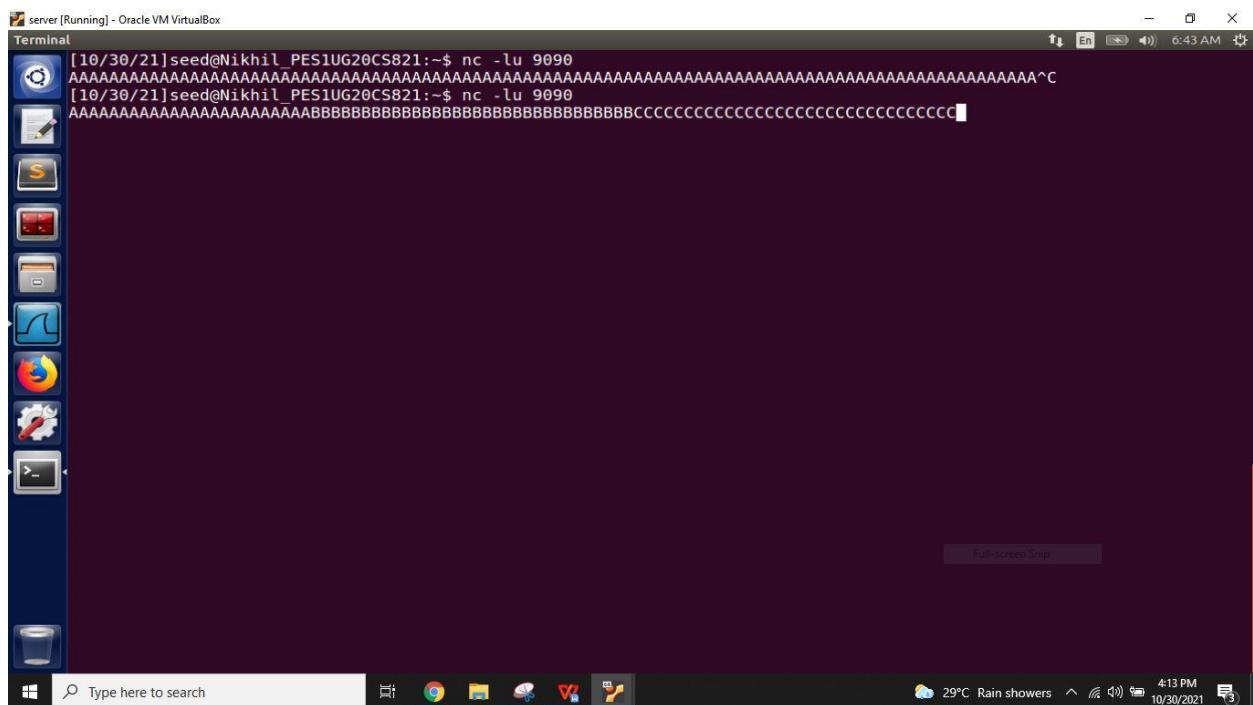


Same observation is seen in the UDP client



Task 1.b: IP Fragments with Overlapping Contents

Listen to port 9090 from UDP server through netcat



We considered k=15 and Running at the file task1.b on UDP Client.

[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ sudo gedit task1.py

(gedit:2605): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported

[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ sudo python task1.py

Finish Sending Packets!

[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ sudo gedit task1.py

** (gedit:3534): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported

[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ sudo gedit task1.b.py

(gedit:3591): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

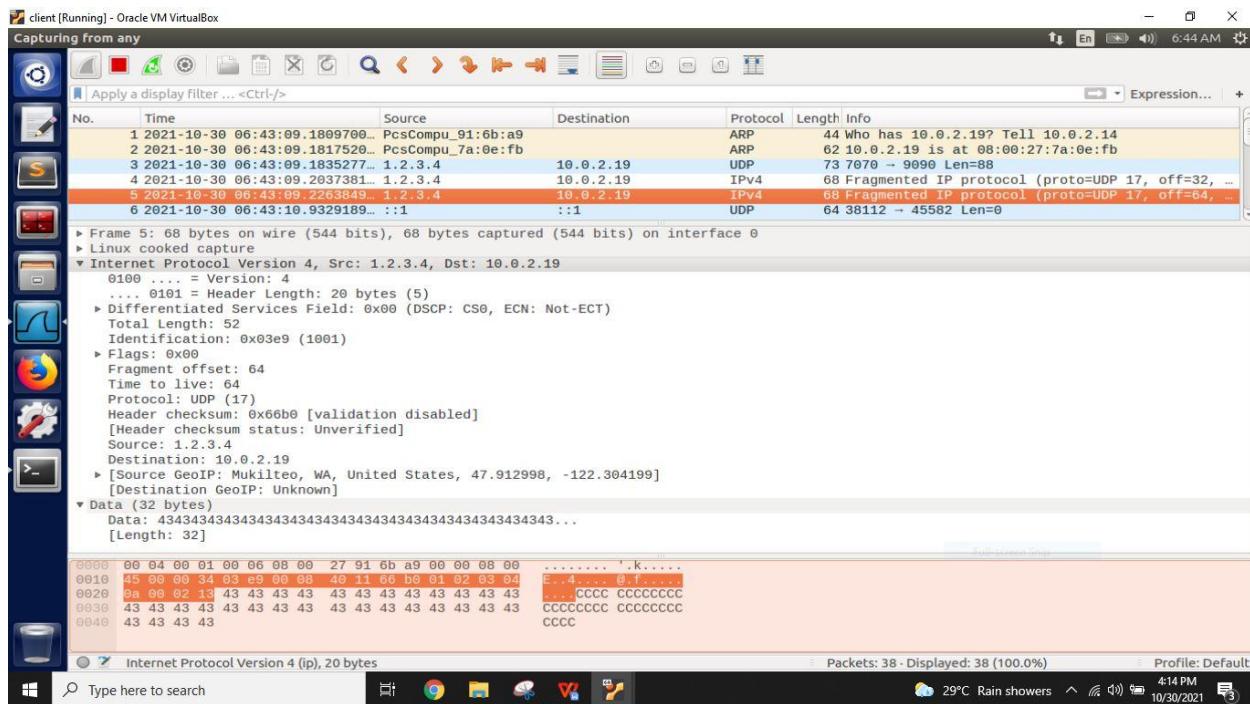
** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported

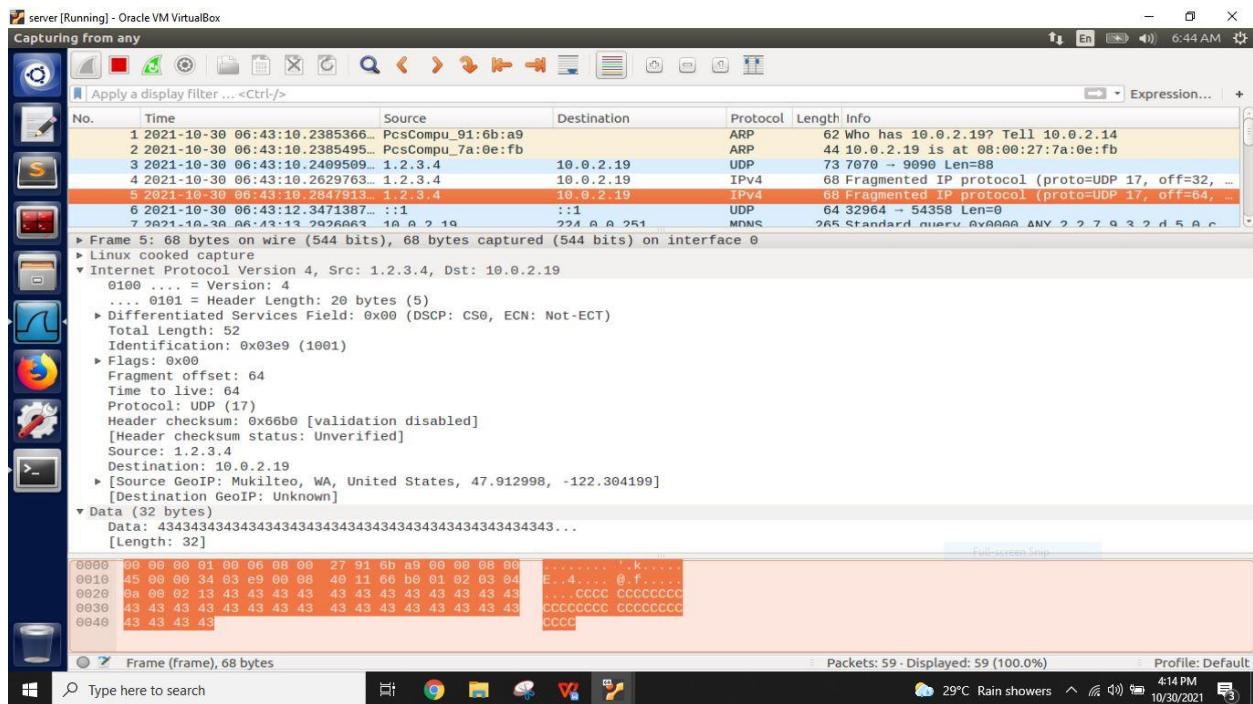
[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ sudo python task1.b.py

Finish Sending Packets!

[10/30/21]seed@Nikhil_PES1UG20CS821:~\$

Those packets are captured in the wireshark on both UDP client and server and we can see the same observation on both of the systems ans we can see length is 32





Now we send second fragment is first and then first fragment

We run the code in the UDP client and send the packets

```
client [Running] - Oracle VM VirtualBox
Terminal
** (gedit:2605): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.py

** (gedit:3534): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.b.py

(gedit:3591): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

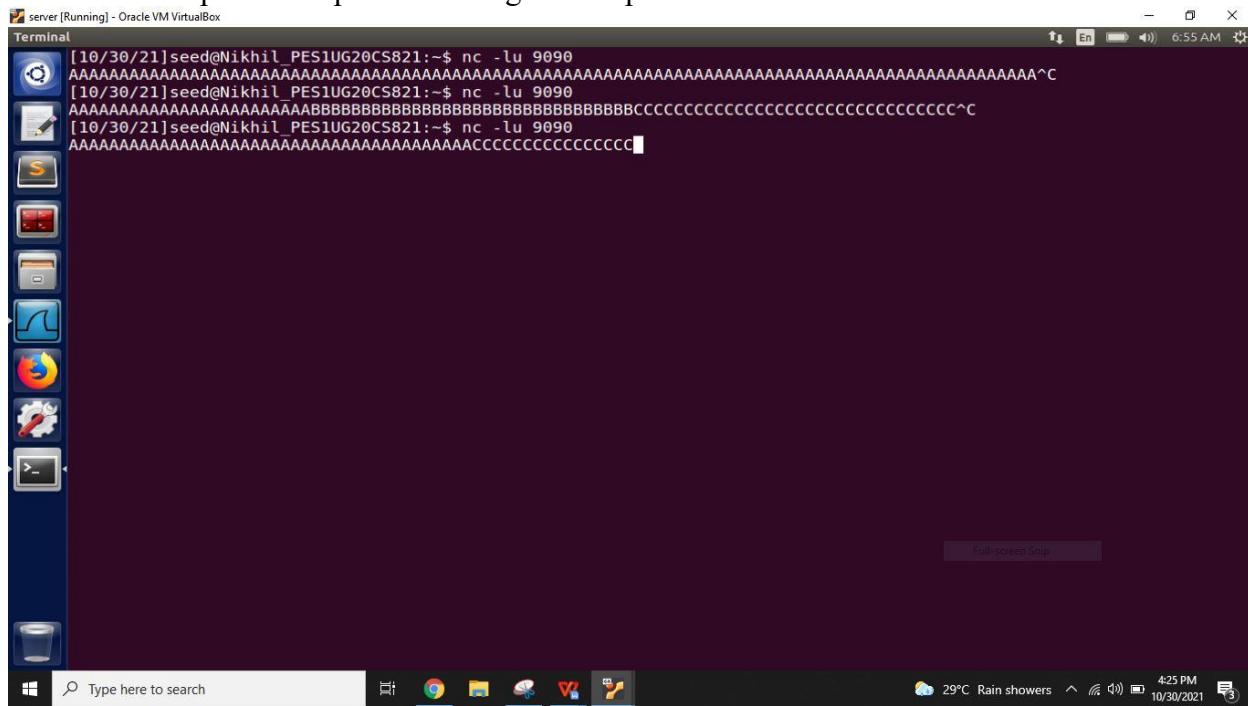
** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3591): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.b.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.b2.py

(gedit:4539): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:4539): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported

** (gedit:4539): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:4539): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.b2.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

UDP Server captures the packets through 9090 port and observation can be seen

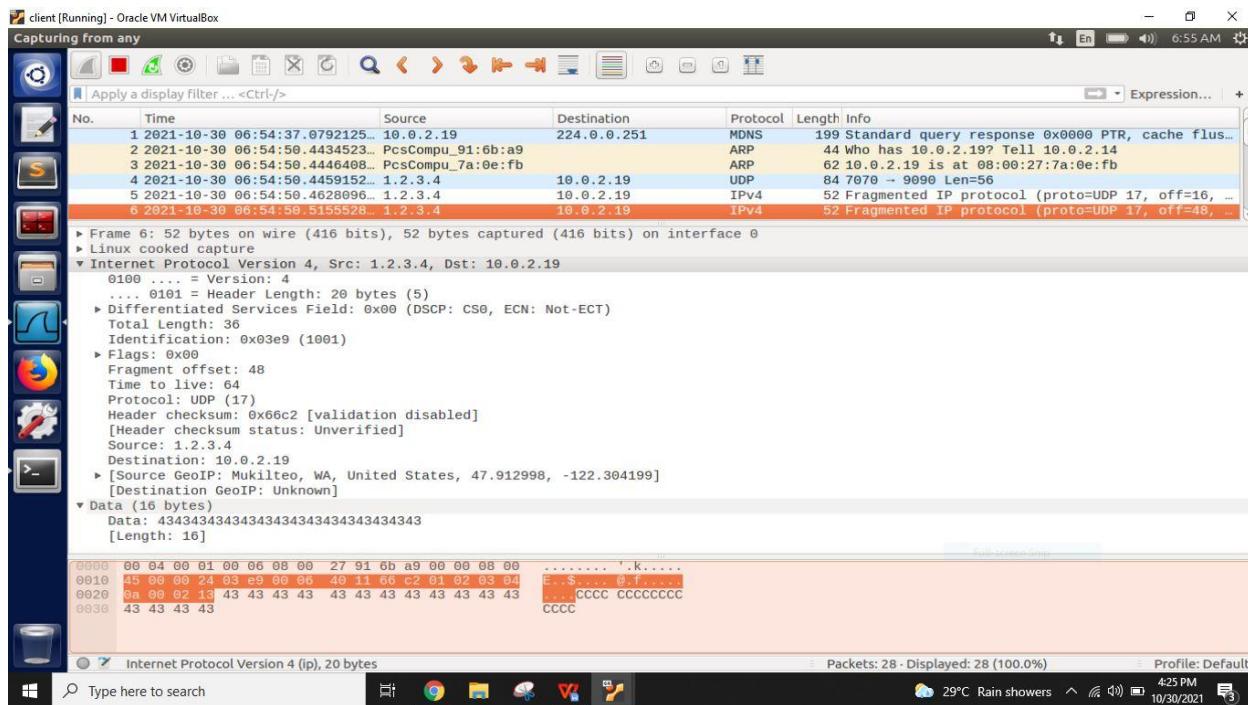


The screenshot shows a terminal window titled "server [Running] - Oracle VM VirtualBox". The terminal displays three lines of command-line output:

```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ nc -lu 9090
AAAAAAA^C
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ nc -lu 9090
AAAAAAA^C
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ nc -lu 9090
AAAAAAA^C
```

The terminal has a dark background with light-colored text. A vertical toolbar on the left contains icons for file operations, a terminal, a browser, and other utilities. The bottom of the screen shows a Windows-style taskbar with icons for File Explorer, Google Chrome, and others.

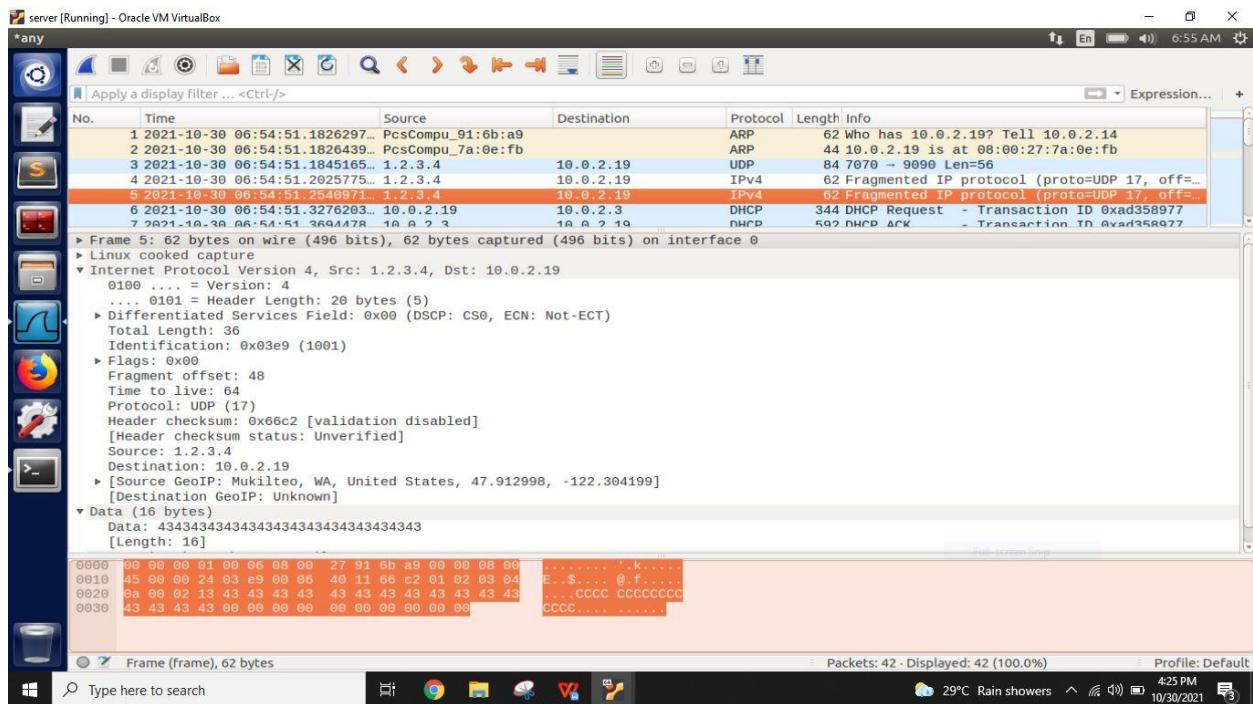
In this task also same observation see on both the client and server system which consists of UDP packets



The screenshot shows a Wireshark interface titled "client [Running] - Oracle VM VirtualBox". The "Capturing from any" tab is active. The packet list pane shows several UDP frames captured on interface 0:

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-10-30 06:54:37.0792125...	10.0.2.19	224.0.0.251	MDNS	199	Standard query response 0x0000 PTR, cache flus...
2	2021-10-30 06:54:58.4434523...	PcsCompu_91:6b:a9		ARP	44	Who has 10.0.2.19? Tell 10.0.2.14
3	2021-10-30 06:54:58.4446408...	PcsCompu_7a:0e:fb		ARP	62	10.0.2.19 is at 08:00:27:7a:0e:fb
4	2021-10-30 06:54:58.4459152...	1.2.3.4	10.0.2.19	UDP	84	7070 → 9090 Len=56
5	2021-10-30 06:54:58.4628096...	1.2.3.4	10.0.2.19	IPv4	52	Fragmented IP protocol (proto=UDP 17, off=16, ...)
6	2021-10-30 06:54:58.5155528...	1.2.3.4	10.0.2.19	IPv4	52	Fragmented IP protocol (proto=UDP 17, off=48, ...)

The details and bytes panes show the structure of the captured UDP frames. The bottom status bar indicates "Packets: 28 - Displayed: 28 (100.0%)".



Task 1.c: Sending a Super-Large Packet

Send super large packet from the UDP client using the file task1.c.py

```
client [Running] - Oracle VM VirtualBox
Terminal
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.c.py
(gedit:5044): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:5044): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:5044): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:5044): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.c.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

Those sent packets are captured by the UDP server using netcat

A screenshot of a Windows desktop environment. In the center is a terminal window titled "server [Running] - Oracle VM VirtualBox". The terminal displays several lines of text, likely representing captured network traffic or logs. The text includes: "[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ nc -lu 9090", followed by multiple lines of 'AAAAA' characters, and "[10/30/21]seed@Nikhil_PES1UG20CS821:~\$ nc -lu 9090" again. Below the terminal is a taskbar with various icons and a search bar. The system tray shows the date as 10/30/2021 and the time as 4:32 PM.

```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ nc -lu 9090
AAAAAAA
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ nc -lu 9090
```

Wireshark observation clearly shows that the huge number of packets are sent to the server (10.0.2.19)

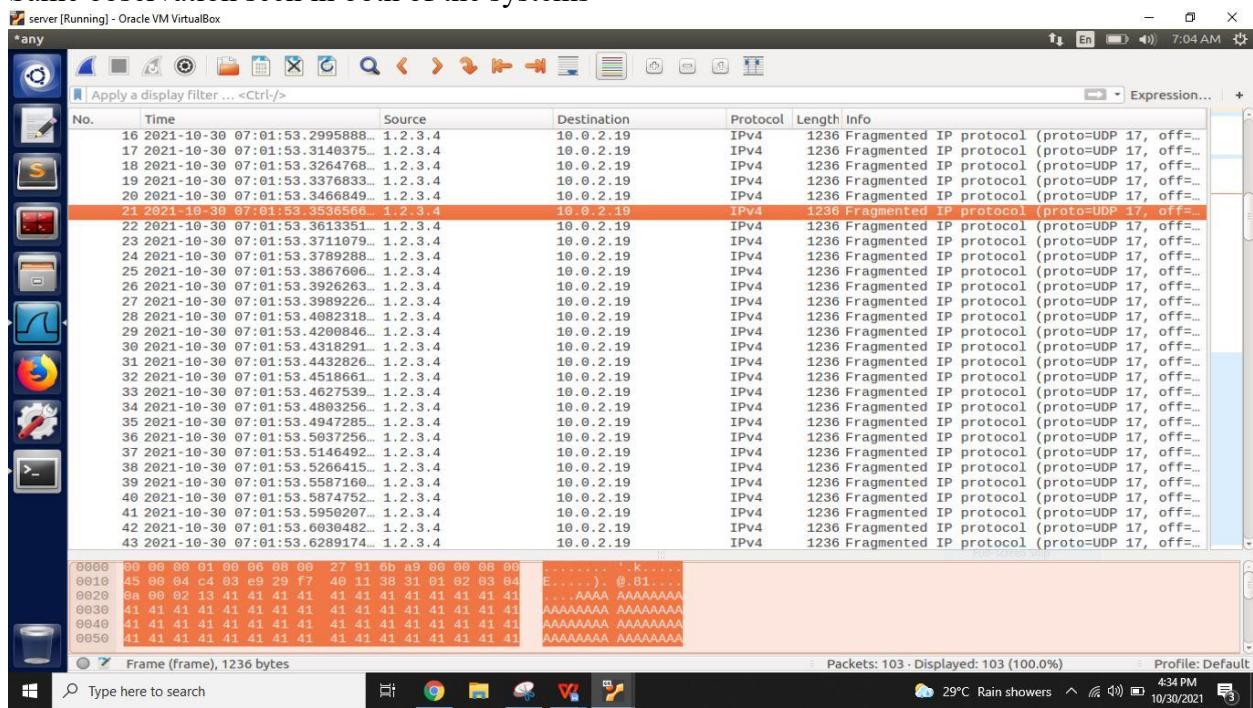
A screenshot of the Wireshark application, which is capturing network traffic from a client machine. The interface shows a list of 134 captured packets. The first few packets are highlighted in red, indicating they are the ones being analyzed. The packet details pane shows the raw hex and ASCII data for one of the selected packets. The selected packet's details are as follows:

No.	Time	Source	Destination	Protocol	Length	Info
10	2021-10-30 07:01:52.6710570...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=7208...)
11	2021-10-30 07:01:52.68357567...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=8408...)
12	2021-10-30 07:01:52.7032519...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=9608...)
13	2021-10-30 07:01:52.7251237...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1080...
14	2021-10-30 07:01:52.7393085...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1200...
15	2021-10-30 07:01:52.7536328...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1320...
16	2021-10-30 07:01:52.7718996...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1440...
17	2021-10-30 07:01:52.7861982...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1560...
18	2021-10-30 07:01:52.7986926...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1680...
19	2021-10-30 07:01:52.8099357...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1800...
20	2021-10-30 07:01:52.8190018...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=1920...
21	2021-10-30 07:01:52.8258293...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2040...
22	2021-10-30 07:01:52.8332936...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2160...
23	2021-10-30 07:01:52.8428198...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2280...
24	2021-10-30 07:01:52.8506451...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2400...
25	2021-10-30 07:01:52.8580287...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2520...
26	2021-10-30 07:01:52.8645847...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2640...
27	2021-10-30 07:01:52.8719974...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2760...
28	2021-10-30 07:01:52.8806140...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=2880...
29	2021-10-30 07:01:52.8924180...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3000...
30	2021-10-30 07:01:52.9039271...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3120...
31	2021-10-30 07:01:52.9139676...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3240...
32	2021-10-30 07:01:52.9238467...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3360...
33	2021-10-30 07:01:52.9336033...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3480...
34	2021-10-30 07:01:52.9516862...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3600...
35	2021-10-30 07:01:52.9661786...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3720...
36	2021-10-30 07:01:52.9758297...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3840...
37	2021-10-30 07:01:52.9856840...	1.2.3.4	10.0.2.19	IPv4	1236	1236 Fragmented IP protocol (proto=UDP 17, off=3960...

The packet details pane shows the raw hex and ASCII data for the selected packet (packet 10). The ASCII dump shows a series of 'A' characters.

```
0010 45 00 04 c4 03 e9 23 85 40 11 3e a3 01 02 03 04 E....# @.>.
0020 0a 00 02 13 41 41 41 41 41 41 41 41 41 41 41 41 ..AAA AAAA
0030 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAA AAAA
0040 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAA AAAA
0050 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAA AAAA
0060 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 ..AAA AAAA
```

Same observation seen in both of the systems



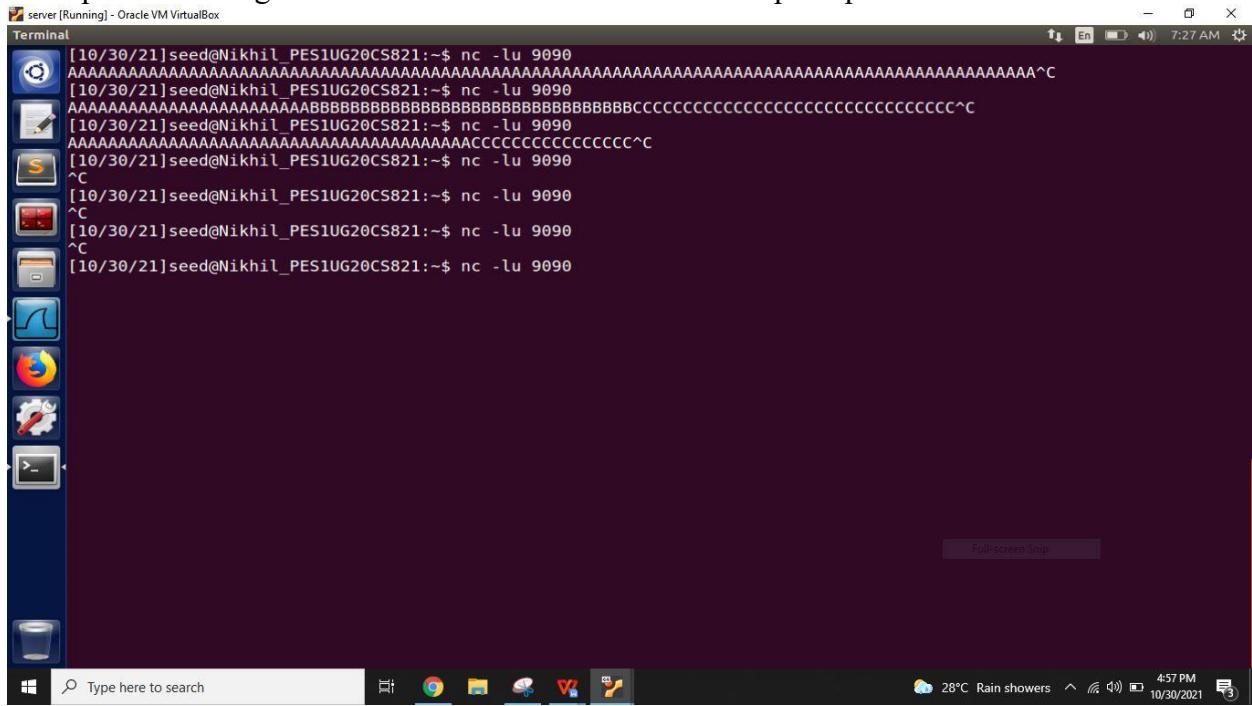
Task 1.d: Sending Incomplete IP Packet

In this task we send an incomplete packet from the UDP client

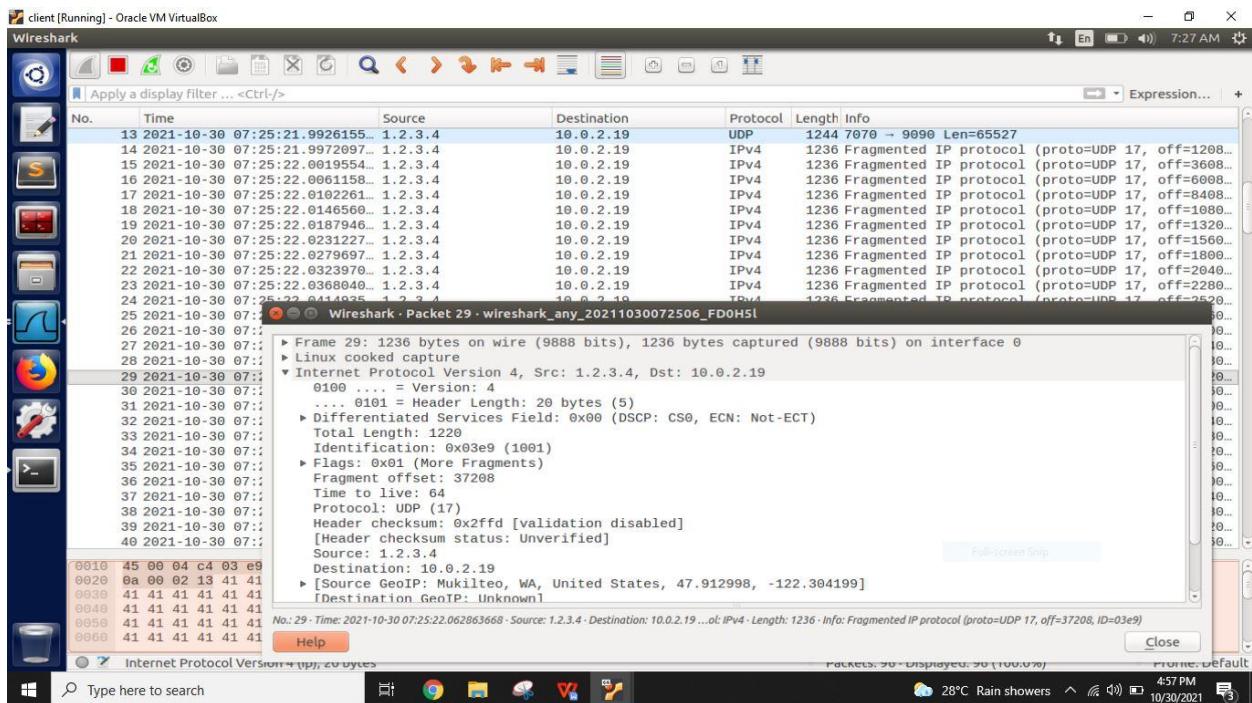
```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.d.py
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.d.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

The terminal window shows the execution of a Python script named `task1.d.py`. The output indicates that the script has finished sending incomplete packets. The system status bar at the bottom right shows the date as 10/30/2021, time as 4:56 PM, and weather as 28°C Rain showers.

As expected nothing is shown on the UDP server as no complete packet is sent



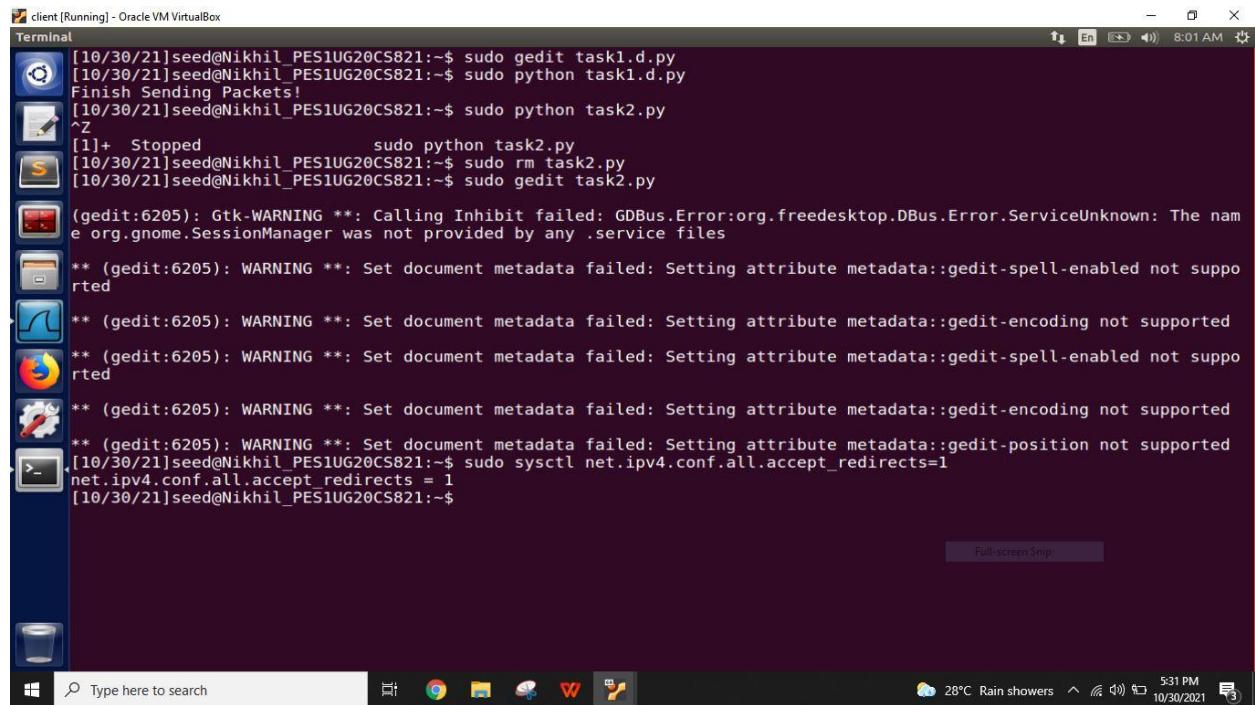
Wireshark has captured all the ip fragments



By sending incomplete packets we are going to flood the kernel memory and perform the dos attack

Task 2: ICMP Redirect Attack

Remove the countermeasure



A screenshot of a Linux desktop environment. At the top is a terminal window titled "client [Running] - Oracle VM VirtualBox". The terminal shows the following command-line session:

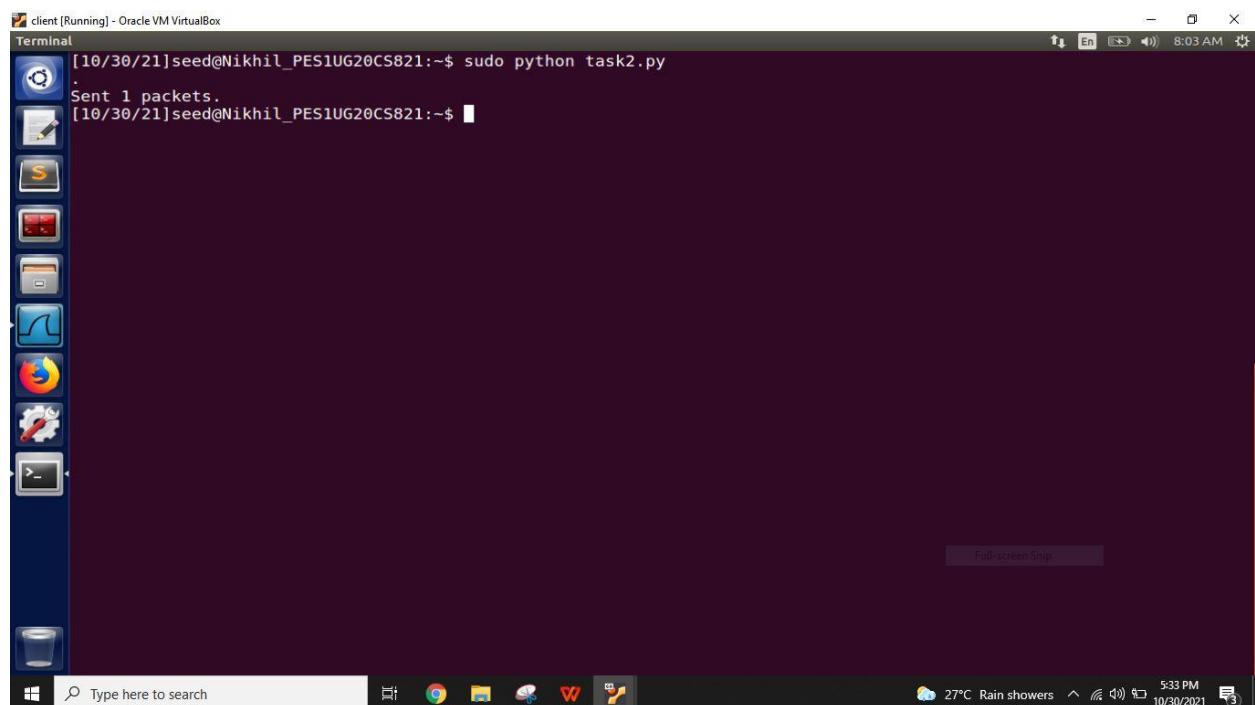
```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task1.d.py
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task1.d.py
Finish Sending Packets!
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task2.py
^Z
[1]+  Stopped                  sudo python task2.py
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo rm task2.py
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit task2.py

(gedit:6205): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files

** (gedit:6205): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:6205): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:6205): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:6205): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:6205): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo sysctl net.ipv4.conf.all.accept_redirects=1
net.ipv4.conf.all.accept_redirects = 1
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a docked application bar with icons for various applications like a file manager, terminal, and system tray. The taskbar at the bottom shows the Windows logo, a search bar, pinned icons for File Explorer, Edge, Mail, Photos, and Settings, and a system tray with weather information (28°C Rain showers), date (10/30/2021), and time (5:31 PM).

Send packet by running task2.py on the UDP client

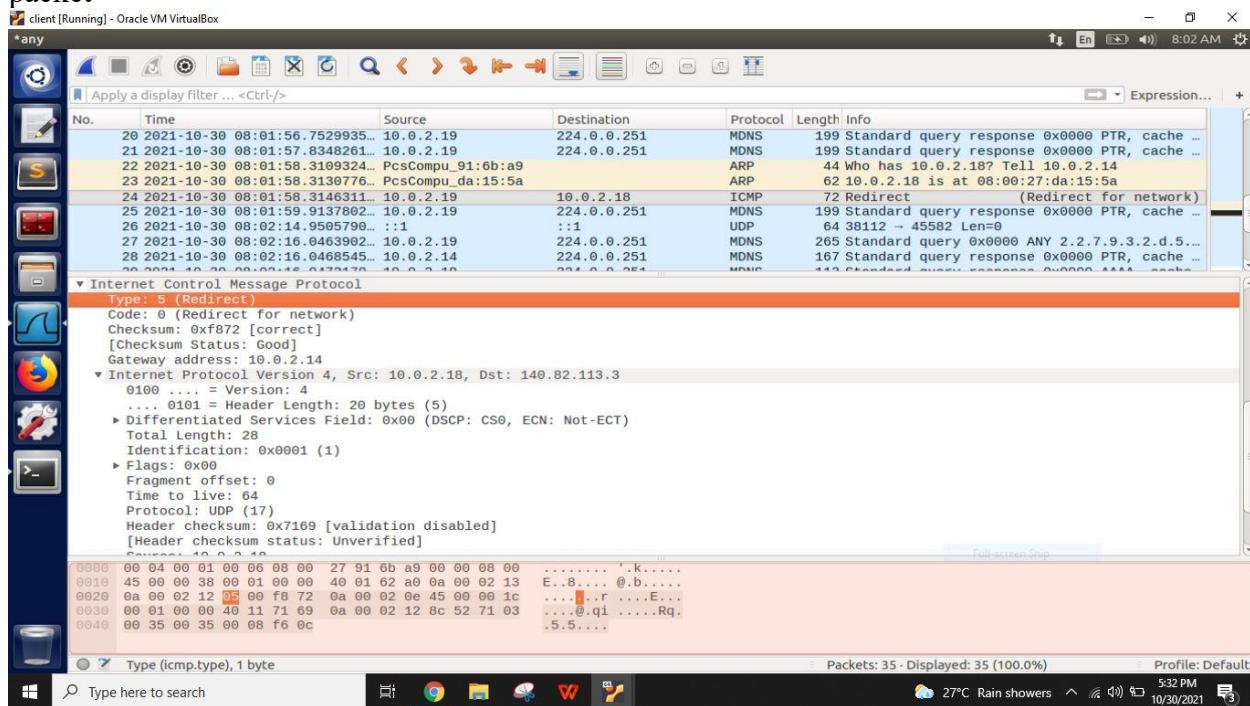


A screenshot of a Linux desktop environment, identical to the previous one, showing a terminal window titled "client [Running] - Oracle VM VirtualBox". The terminal shows the following command-line session:

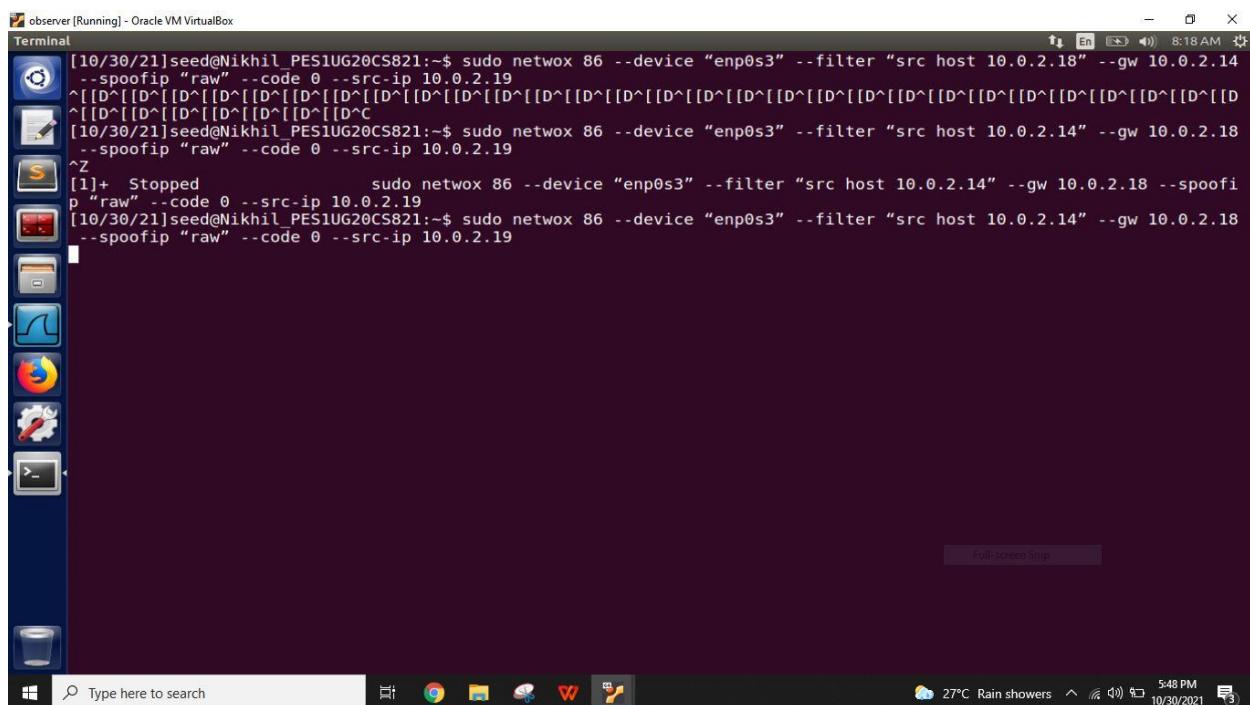
```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ sudo python task2.py
.
Sent 1 packets.
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

The desktop interface includes a docked application bar with icons for various applications like a file manager, terminal, and system tray. The taskbar at the bottom shows the Windows logo, a search bar, pinned icons for File Explorer, Edge, Mail, Photos, and Settings, and a system tray with weather information (27°C Rain showers), date (10/30/2021), and time (5:33 PM).

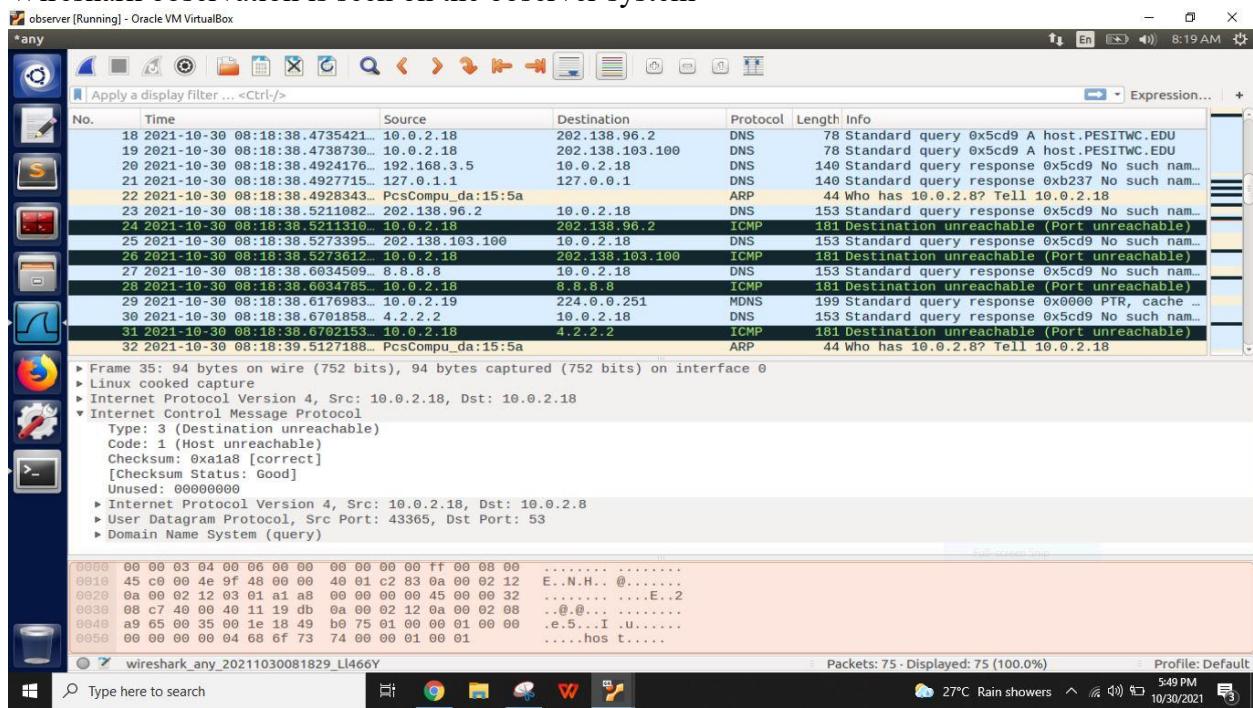
On wireshark we can see that icmp packet type is 5 which indicates the redirect of the icmp packet



Same above task we repeated but by using netwox tool. Run the netwox command in the UDP client



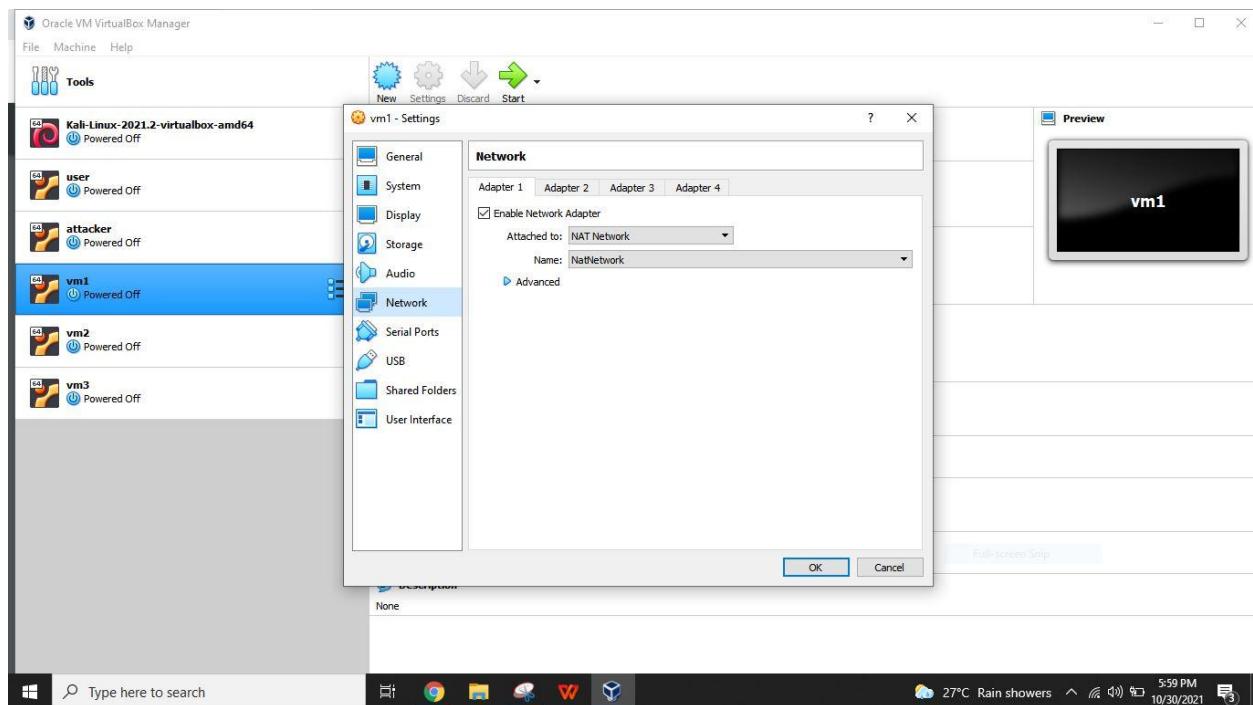
Wireshark observation is seen on the observer system



Task3: Routing and reverse Path filtering

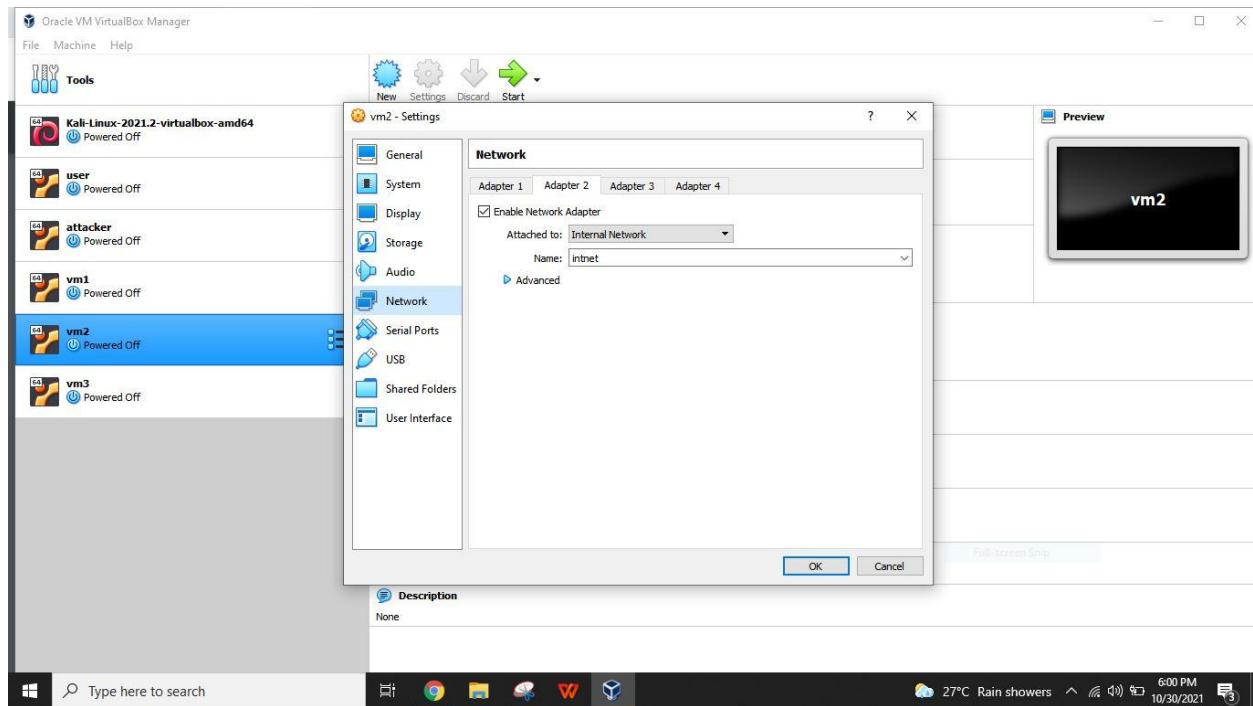
Task 3a: Network setup

Set one nat network interface on the vm1

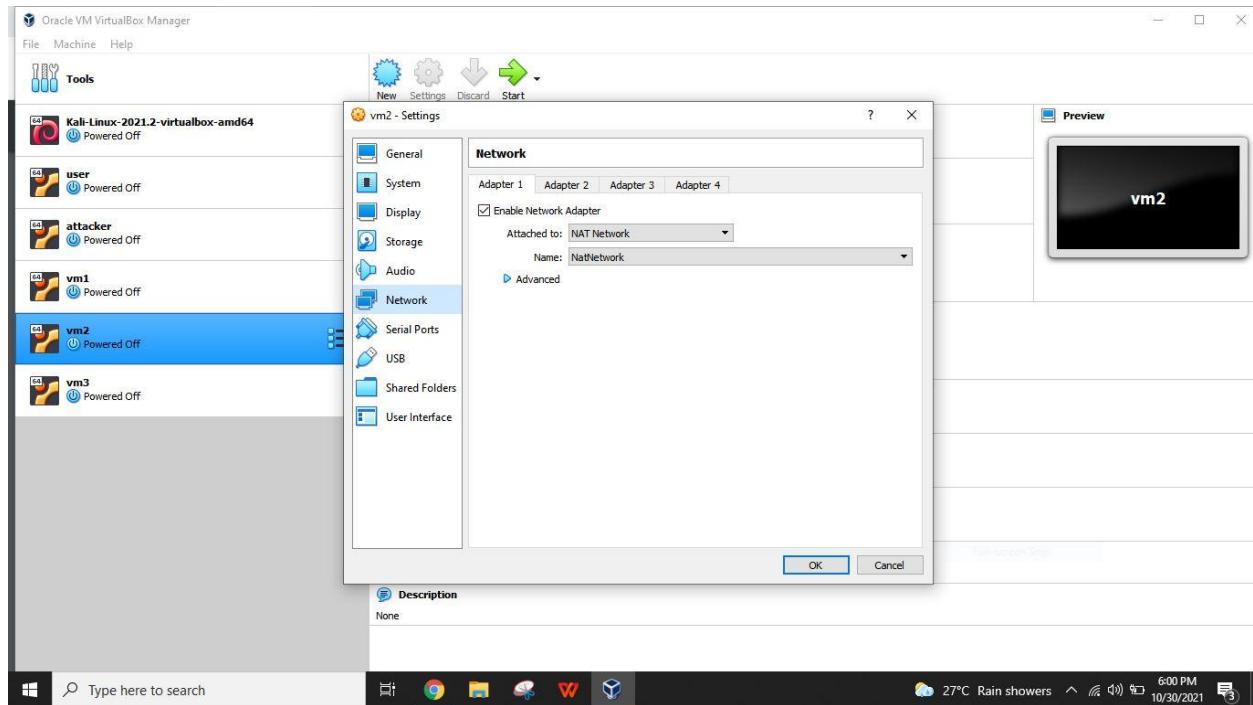


Set two interface in the vm2

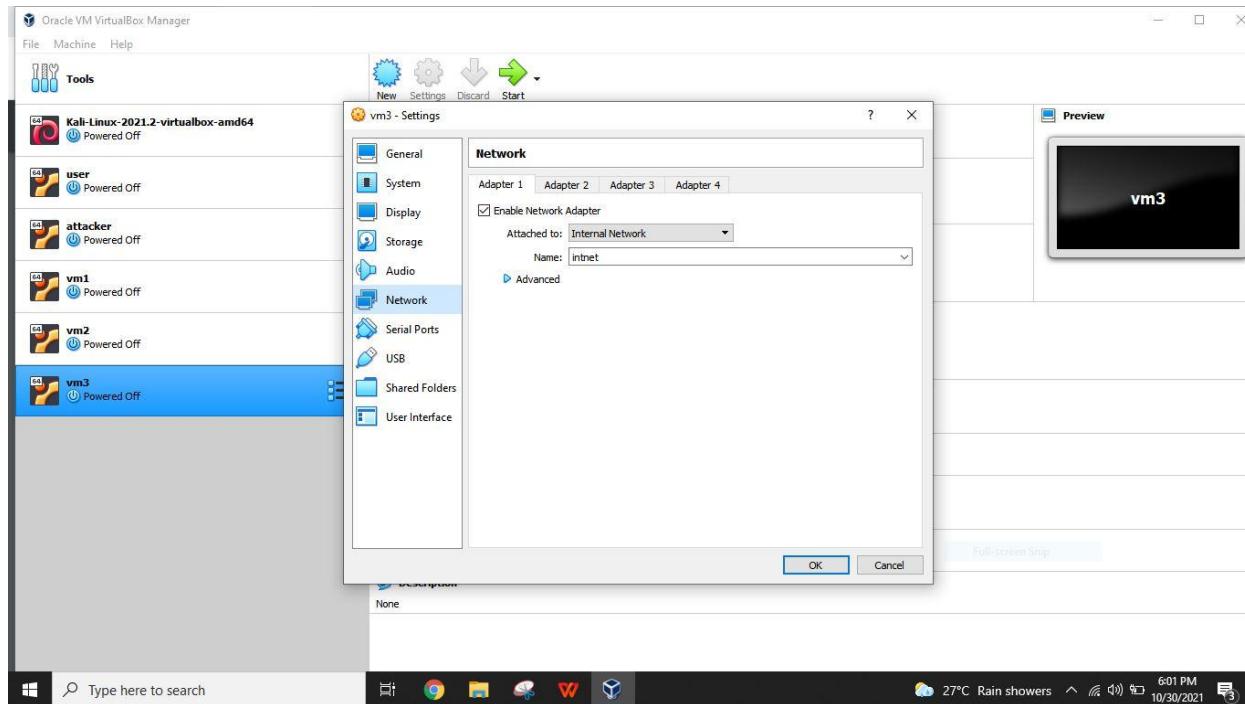
i) internal network



ii) NAT network

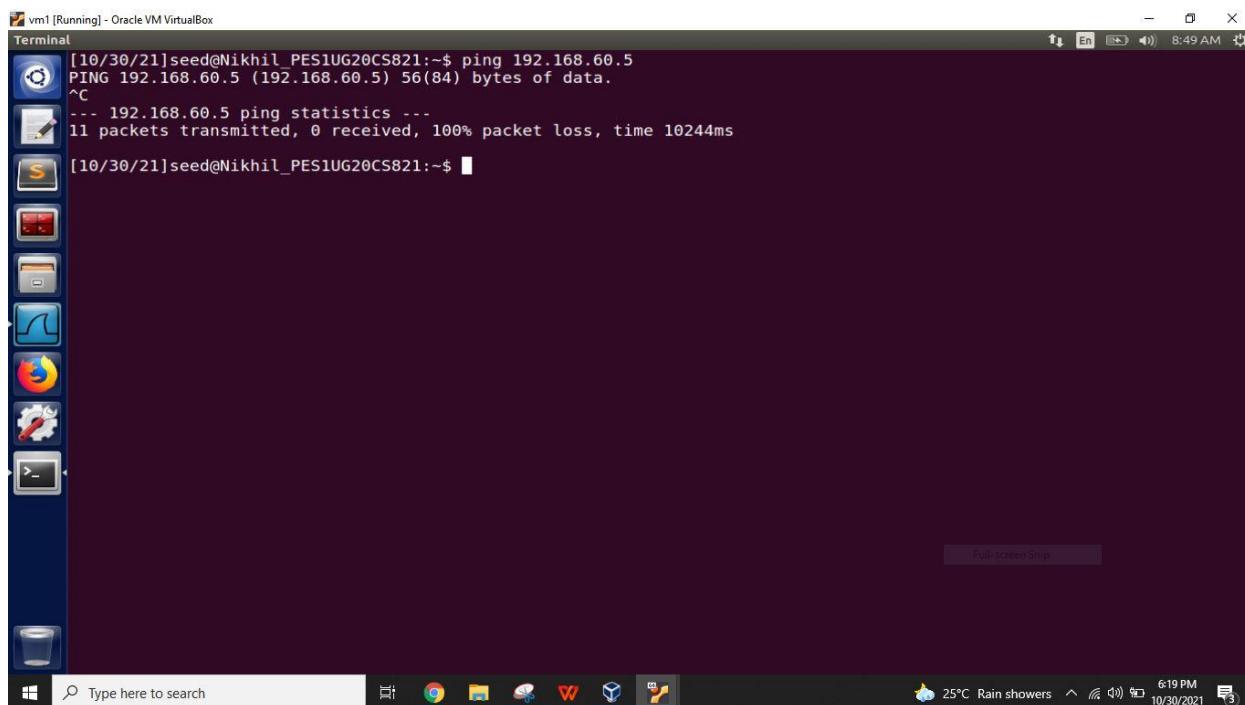


Only internal network interface is set on vm3

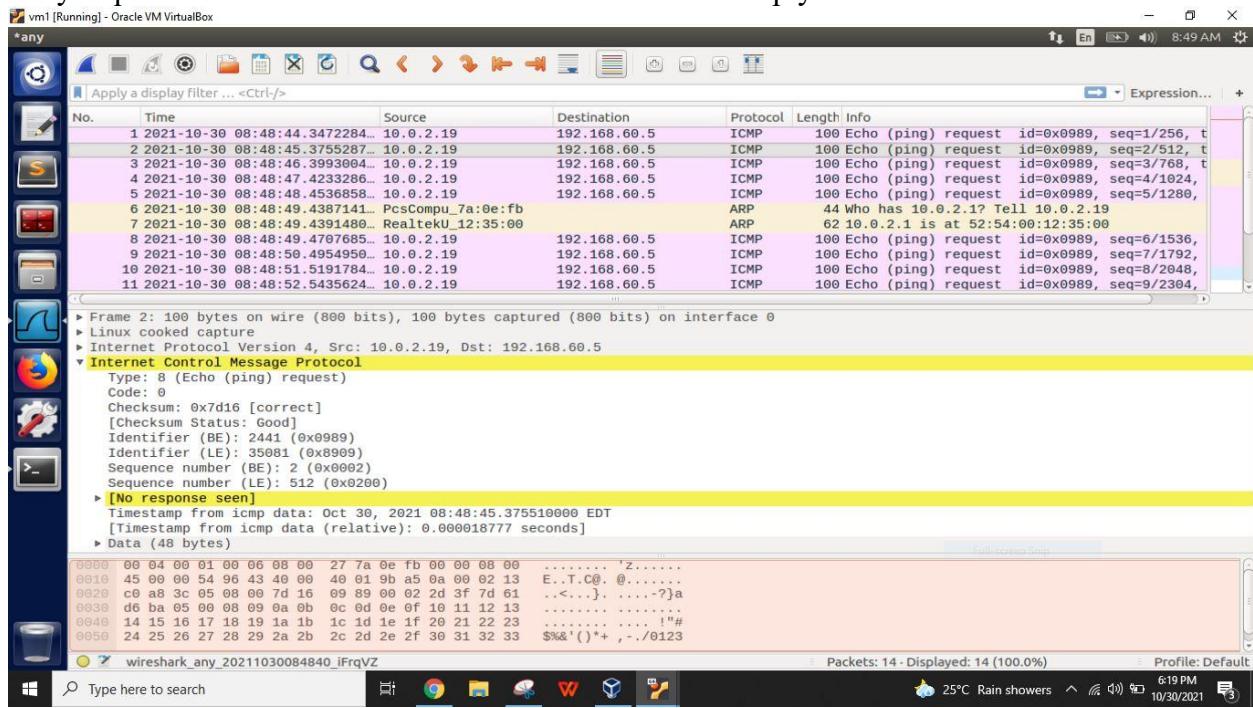


Task 3B: Routing setup

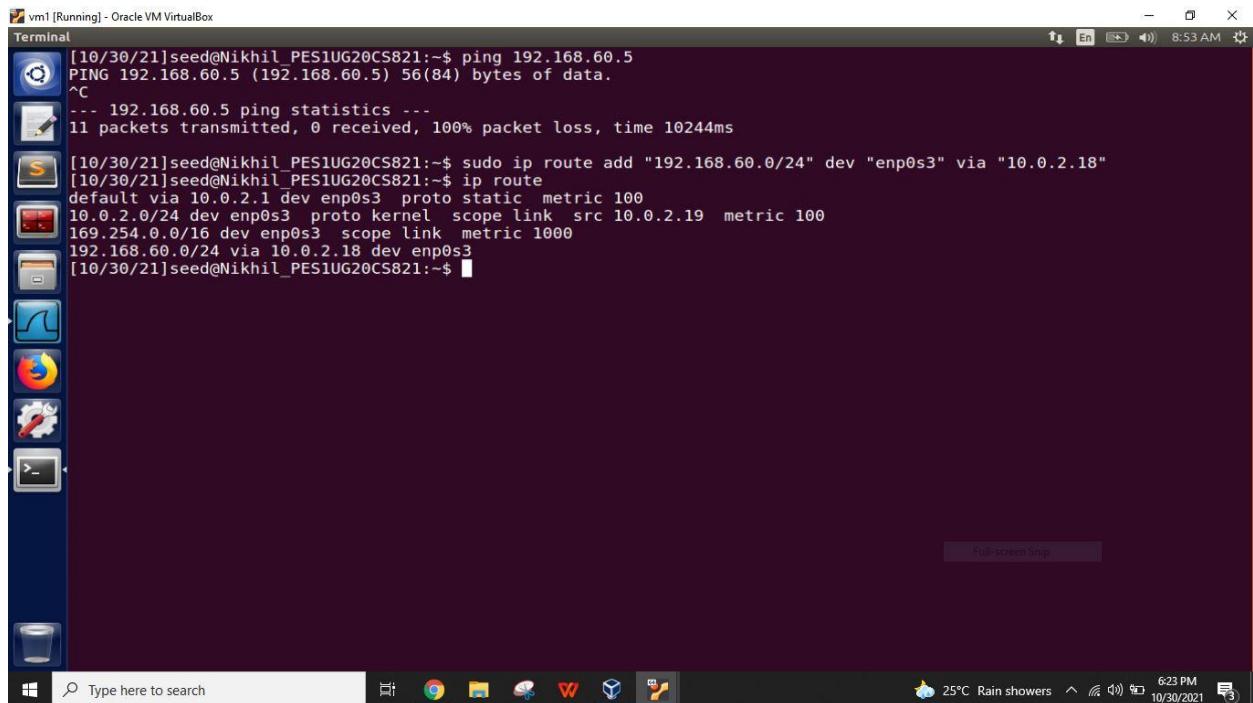
Vm1 cannot communicate with the vm3 direct as we haven't done any routing setup



Only request can be seen in the wireshark observation no reply from the vm3



Now we set the routing path from vm1 to vm2



We set path from vm2 to vm3

```
vm2 [Running] - Oracle VM VirtualBox
Terminal
RTNETLINK answers: Network is unreachable
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ip route
default via 10.0.2.1 dev enp0s3 proto static metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.18 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=61 time=5.72 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=61 time=8.69 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=61 time=5.56 ms
^Z
[1]+ Stopped ping 192.168.60.1
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
^Z
[2]+ Stopped ping 192.168.60.5
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=64 time=1.15 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=64 time=1.10 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=64 time=0.760 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 192.168.60.5: icmp_seq=5 ttl=64 time=0.882 ms
^C
--- 192.168.60.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4036ms
rtt min/avg/max/mdev = 0.760/0.989/1.158/0.148 ms
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ sudo ip route add "192.168.60.0/24" dev "enp0s8" via "192.168.60.1"
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ip route
default via 10.0.2.1 dev enp0s3 proto static metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.18 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.60.0/24 via 192.168.60.1 dev enp0s8
192.168.60.0/24 dev enp0s8 proto kernel scope link src 192.168.60.1 metric 100
[10/30/21]seed@Nikhil_PESIUG20CS821:~$
```

Same is done for vm3 also

```
vm3 [Running] - Oracle VM VirtualBox
Terminal
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ sudo ip route add "10.0.2.0/24" dev "enp0s3" via "192.168.60.1"
[10/30/21]seed@Nikhil_PESIUG20CS821:~$ ip route
10.0.2.0/24 via 192.168.60.1 dev enp0s3
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.60.0/24 dev enp0s3 proto kernel scope link src 192.168.60.5 metric 100
[10/30/21]seed@Nikhil_PESIUG20CS821:~$
```

After setting the patch we are going to ping again from vm1 to vm3

A screenshot of a Windows desktop environment. At the top is a terminal window titled "vm1 [Running] - Oracle VM VirtualBox" with the command "ping 192.168.60.5" and its output. Below the terminal is a standard Windows taskbar with icons for File Explorer, Edge, and other applications. The system tray shows the date and time as 10/30/2021 6:41 PM.

```
[10/30/21]seed@Nikhil_PES1UG20CS821:~$ ping 192.168.60.5
PING 192.168.60.5 (192.168.60.5) 56(84) bytes of data.
64 bytes from 192.168.60.5: icmp_seq=1 ttl=63 time=1.54 ms
64 bytes from 192.168.60.5: icmp_seq=2 ttl=63 time=2.89 ms
64 bytes from 192.168.60.5: icmp_seq=3 ttl=63 time=1.76 ms
64 bytes from 192.168.60.5: icmp_seq=4 ttl=63 time=5.73 ms
^C
--- 192.168.60.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.540/2.984/5.733/1.668 ms
[10/30/21]seed@Nikhil_PES1UG20CS821:~$
```

We can see both request and reply as the ip routing patch is set successfully

A screenshot of the Wireshark network traffic analyzer. The main pane displays a list of captured frames, with frame 7 highlighted. The details and bytes panes provide a detailed view of the selected ICMP echo request and response frames. The bottom status bar shows the number of packets displayed.

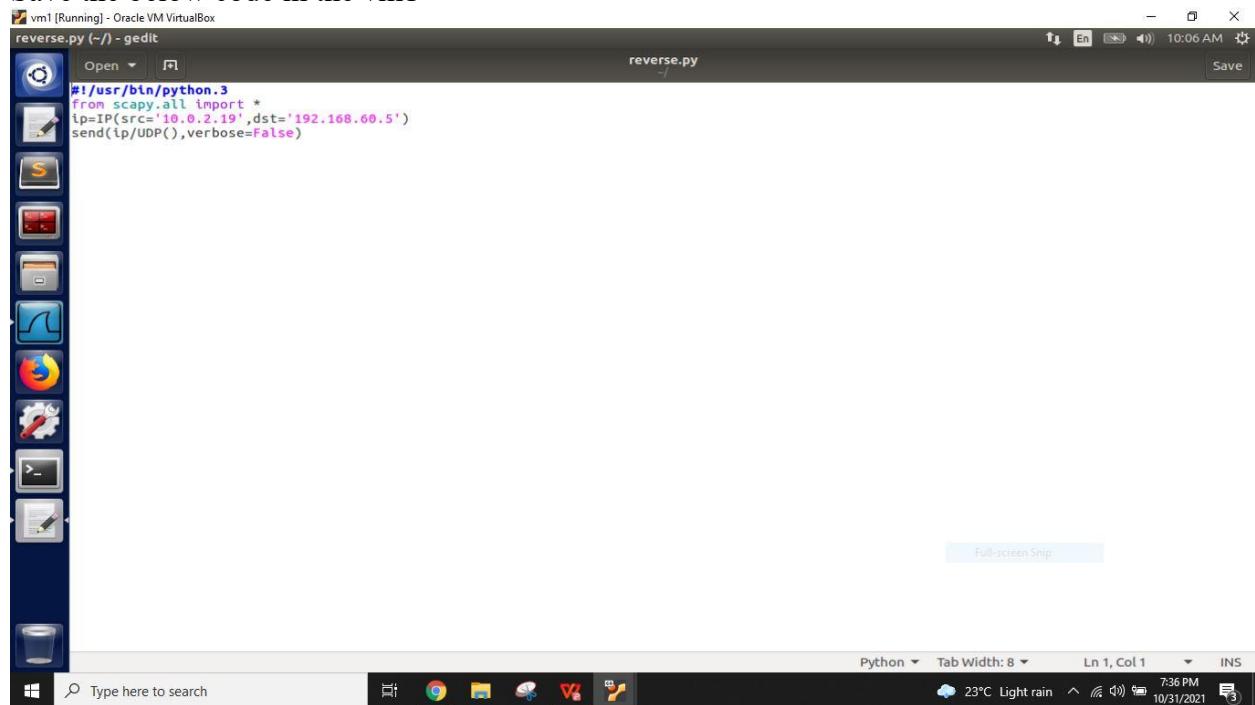
Frame 7: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0

Internet Control Message Protocol

No.	Time	Source	Destination	Protocol	Length	Info
1	2021-10-30 09:10:49.6318898...	::1	::1	UDP	64	54847 → 53244 Len=0
2	2021-10-30 09:10:55.0162298...	10.0.2.19	192.168.60.5	ICMP	100	Echo (ping) request id=0x0c3d, seq=1/256,...
3	2021-10-30 09:10:55.0177572...	192.168.60.5	10.0.2.19	ICMP	100	Echo (ping) reply id=0x0c3d, seq=1/256,...
4	2021-10-30 09:10:56.0175477...	10.0.2.19	192.168.60.5	ICMP	100	Echo (ping) request id=0x0c3d, seq=2/512,...
5	2021-10-30 09:10:56.0204146...	192.168.60.5	10.0.2.19	ICMP	100	Echo (ping) reply id=0x0c3d, seq=2/512,...
6	2021-10-30 09:10:57.0191457...	10.0.2.19	192.168.60.5	ICMP	100	Echo (ping) request id=0x0c3d, seq=3/768,...
7	2021-10-30 09:10:57.0288035...	192.168.60.5	10.0.2.19	ICMP	100	Echo (ping) reply id=0x0c3d, seq=3/768,...
8	2021-10-30 09:10:58.0284060...	10.0.2.19	192.168.60.5	ICMP	100	Echo (ping) request id=0x0c3d, seq=4/1024,...

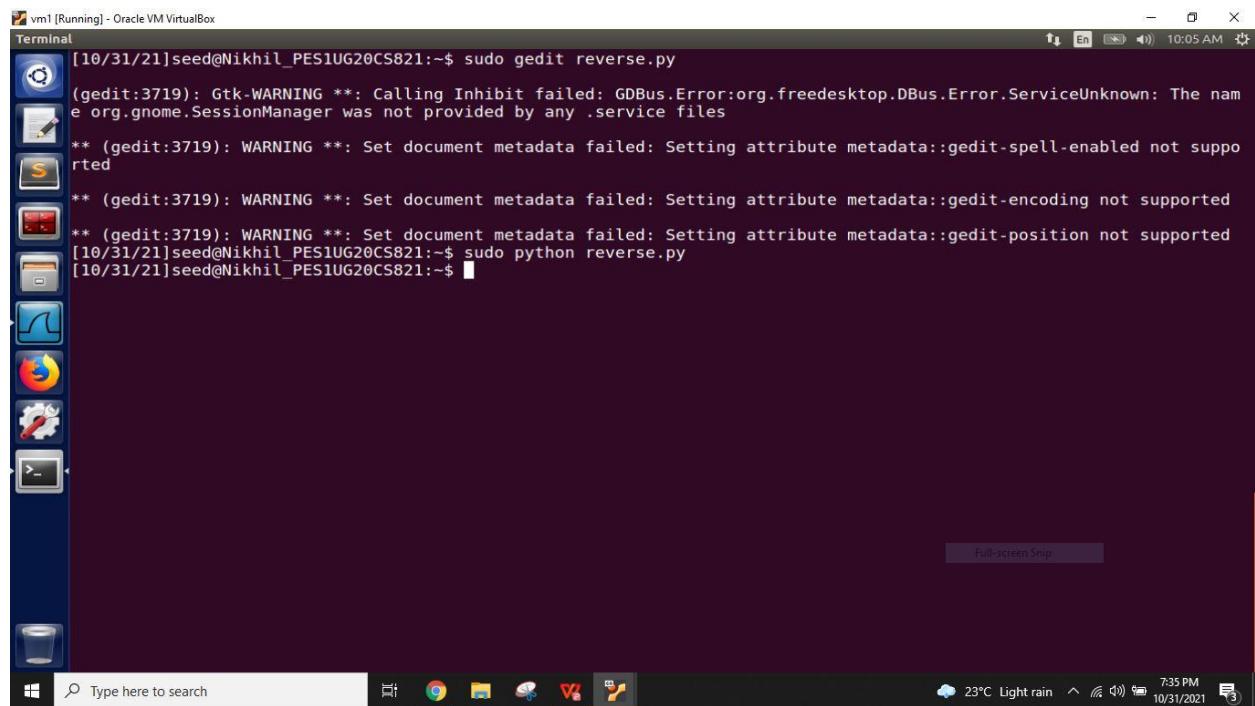
Task 3c: reverse path filtering

Save the below code in the vm1



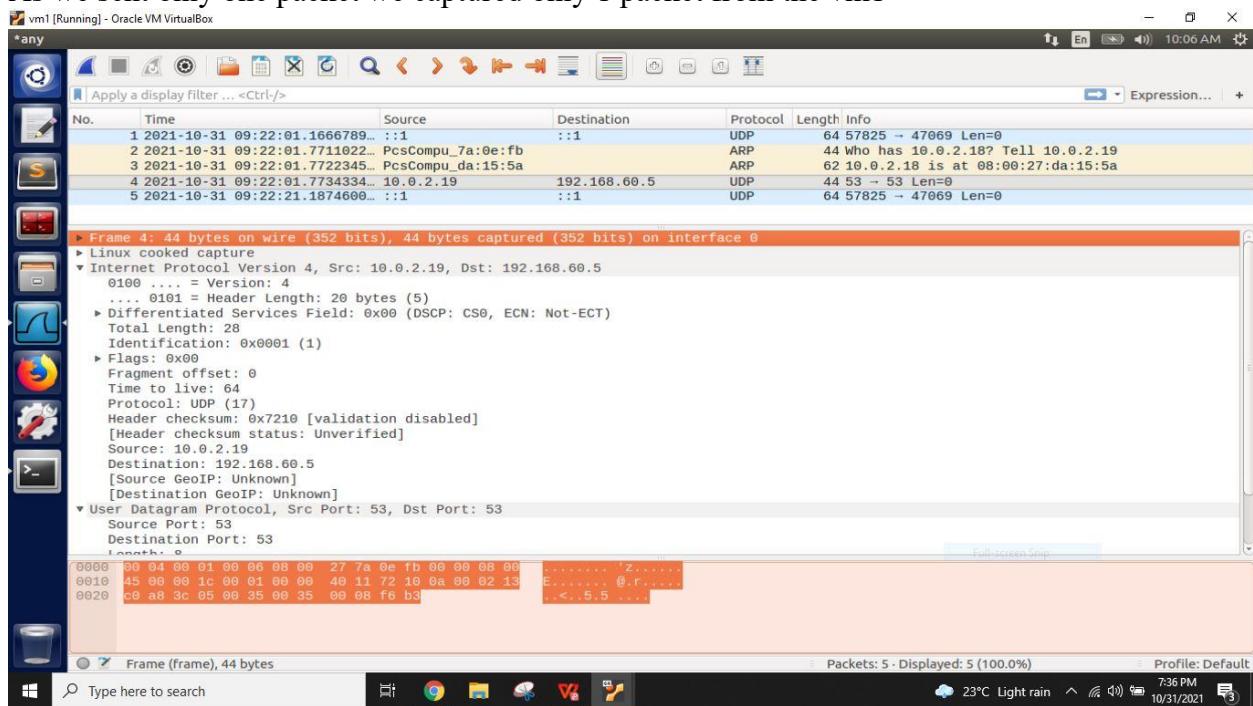
```
#!/usr/bin/python3
from scapy.all import *
ip=IP(src='10.0.2.19',dst='192.168.60.5')
send(ip/UDP(),verbose=False)
```

Save and run the above code in the vm1

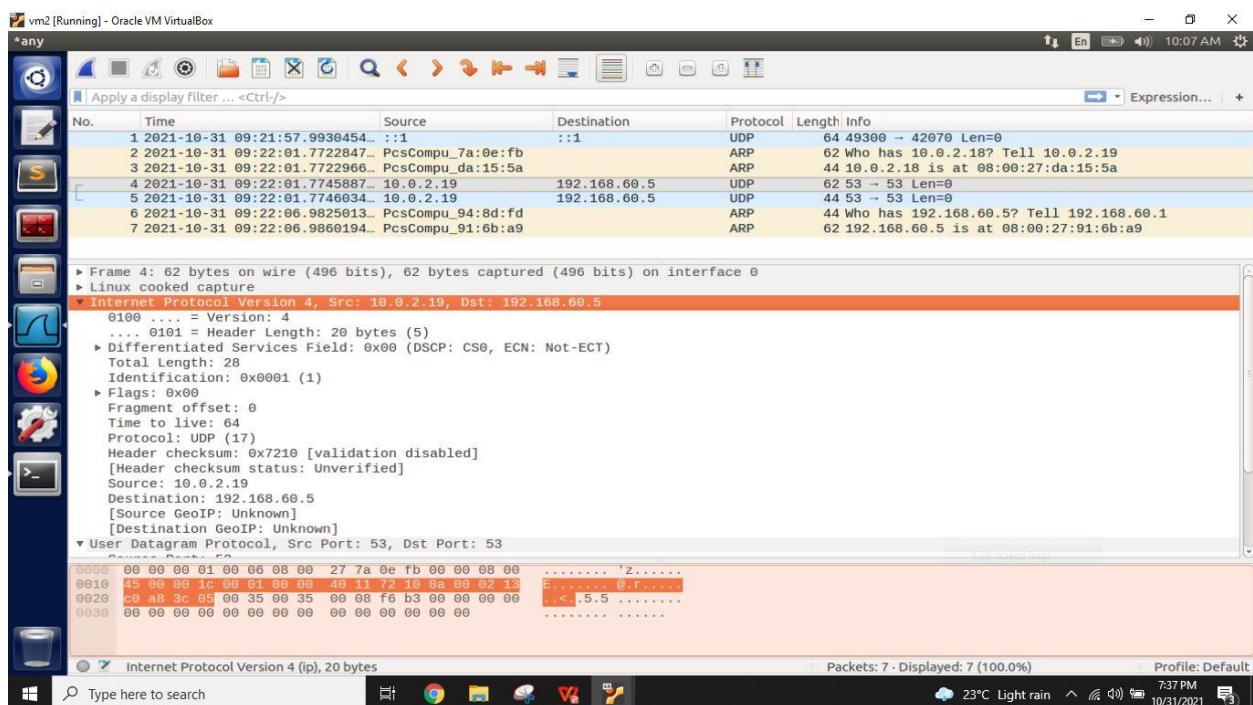


```
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit reverse.py
(gedit:3719): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:3719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:3719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:3719): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reverse.py
[10/31/21]seed@Nikhil_PES1UG20CS821:~$
```

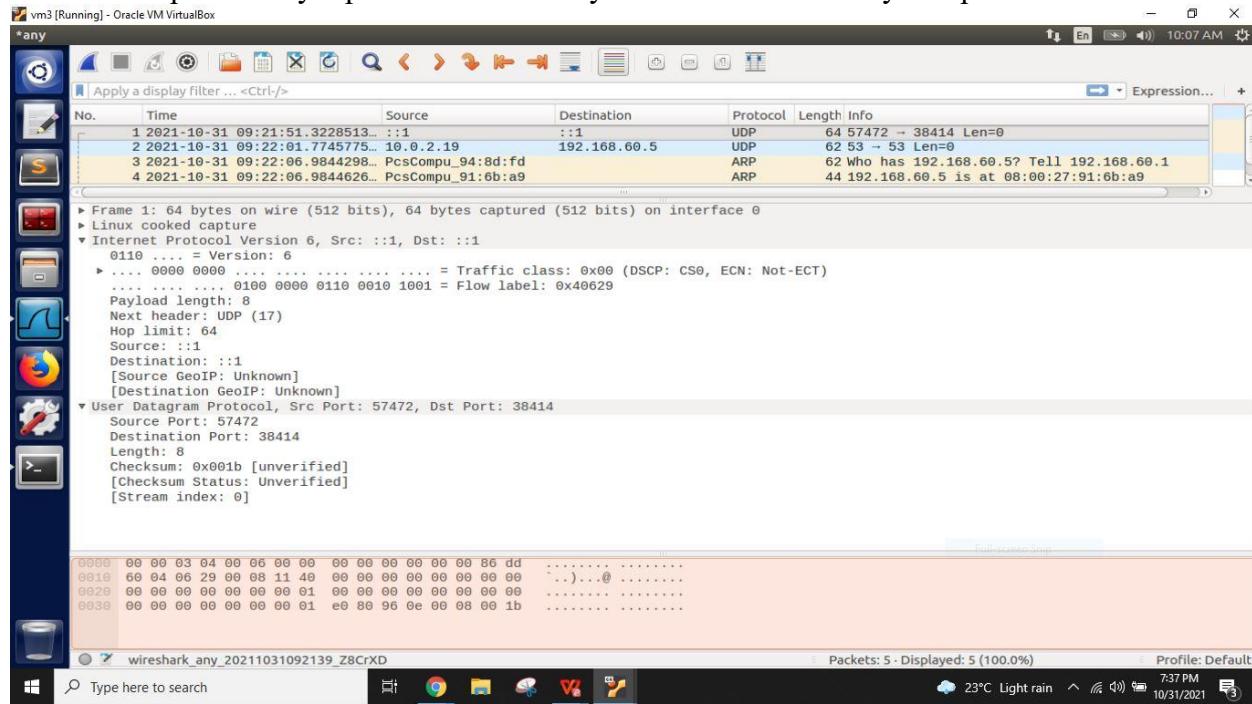
As we sent only one packet we captured only 1 packet from the vm1



Vm2 captures 2 consecutive packets but from different interface

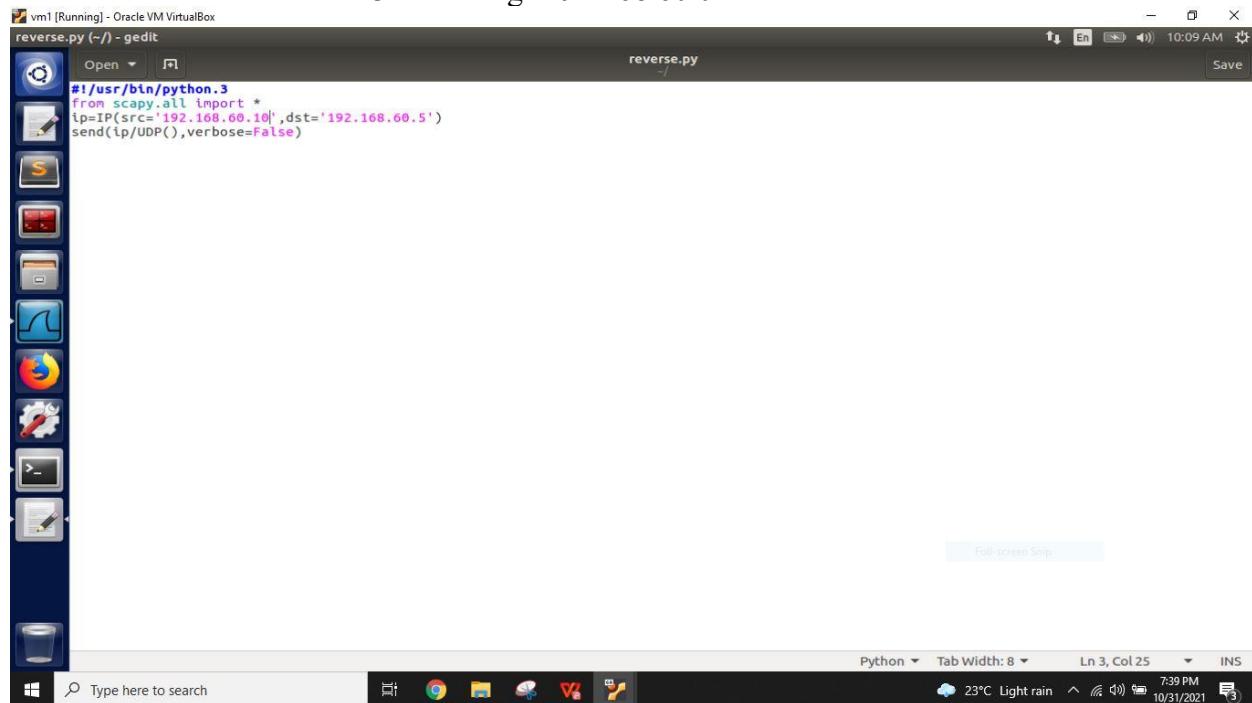


Vm3 also captures only 1 packet as it has only one interface and only one packet is sent



An IP address belonging to the network 10.0.2.0/24

Packet sent from vm1 to vm3 from range 192.168.60.0/24



Save and run the above code in the vm1

```
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit reverse.py
** (gedit:7193): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reverse.py
[10/31/21]seed@Nikhil_PES1UG20CS821:~$
```

Capture those packets at all the 3 vm's

At vm1 we can see one packet

Frame 4: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface 0

Internet Protocol Version 4, Src: 192.168.60.10, Dst: 192.168.60.5

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSFP: CS0, ECN: Not-ECT)

Total Length: 28

Identification: 0x0001 (1)

Flags: 0x00

Fragment offset: 0

Time to live: 64

Protocol: UDP (17)

Header checksum: 0x8170 [validation disabled]

[Header checksum status: Unverified]

Source: 192.168.60.10

Destination: 192.168.60.5

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

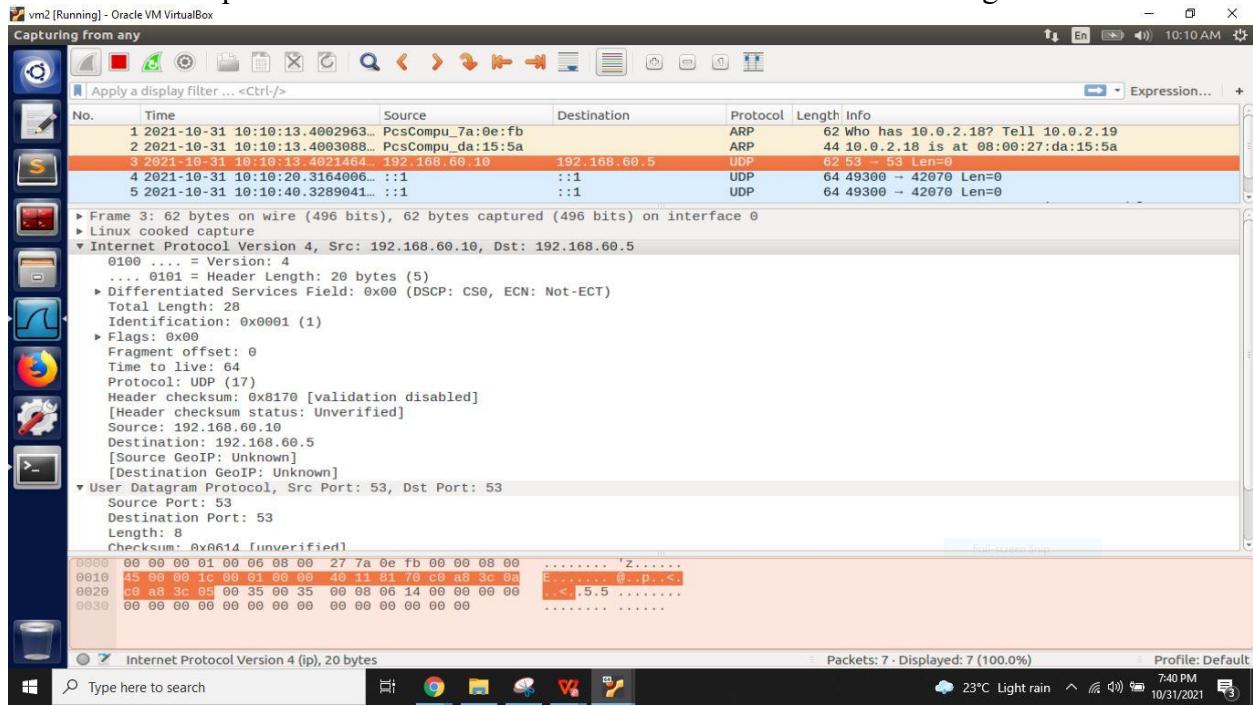
User Datagram Protocol, Src Port: 53, Dst Port: 53

Source Port: 53

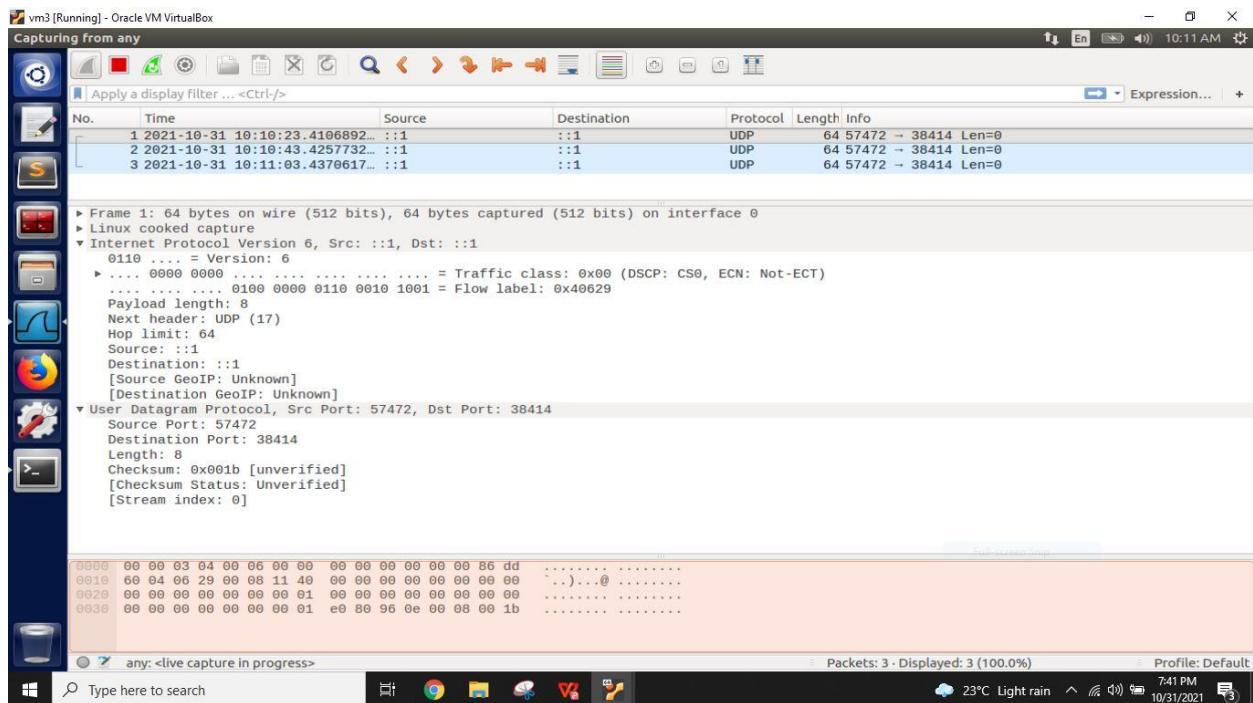
Destination Port: 53

0000: 00 04 00 01 00 00 00 00 27 7a 0e 1b 00 00 00 00 |.....'z.....|
0010: 45 00 00 1c 00 01 00 00 40 11 81 70 c0 a8 3c 0a |E.....@..p..<.
0020: c0 a8 3c 05 00 35 00 35 00 08 06 14 |...<.5.5|

In vm2 also one packet is seen even it has 2 interface because we set the range

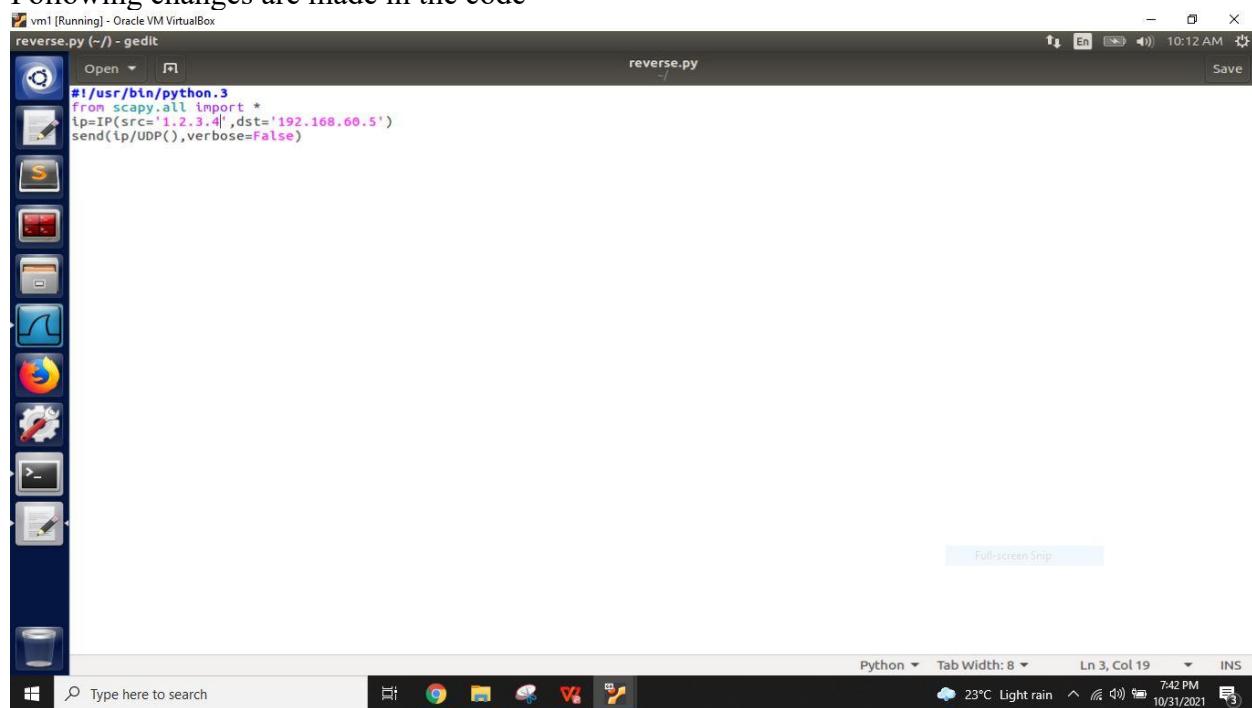


As expected we cannot see any packet in the vm3 as it has ip address out of range



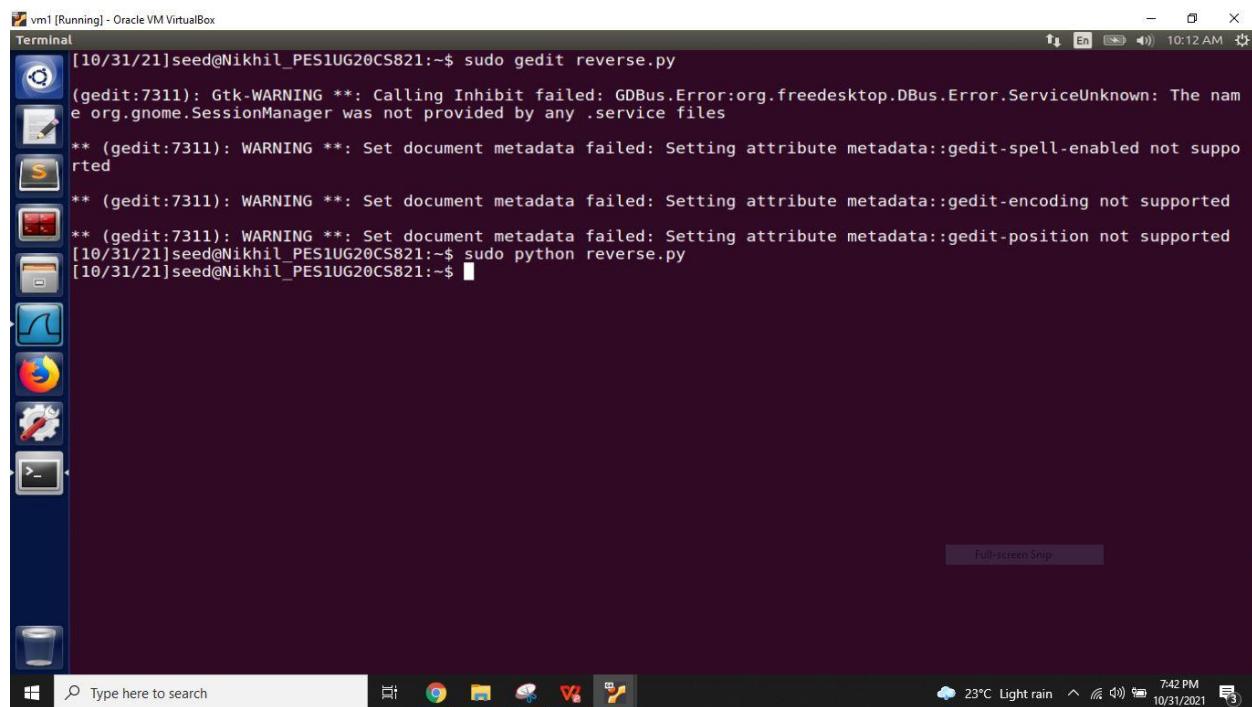
An IP address belonging to the Internet, such as 1.2.3.4.

Following changes are made in the code



```
#!/usr/bin/python3
from scapy.all import *
ip=IP(src='1.2.3.4',dst='192.168.60.5')
send(ip/UDP(),verbose=False)
```

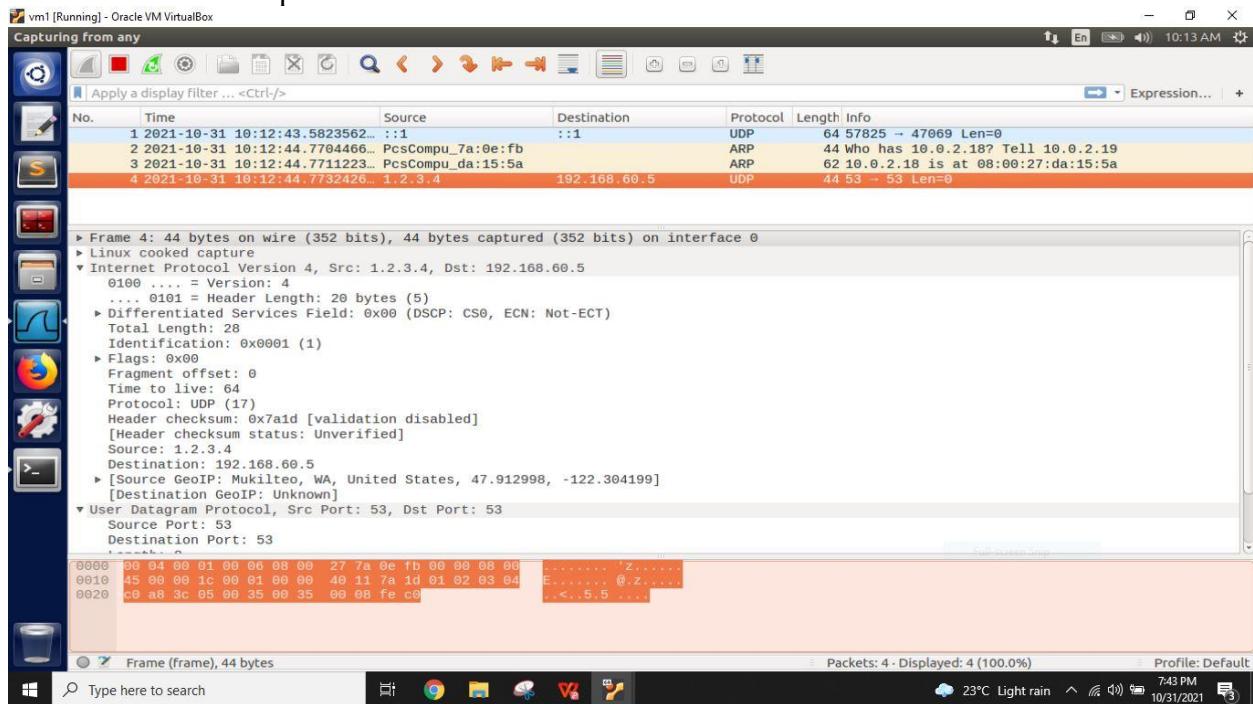
Save and run the above code in the vm1



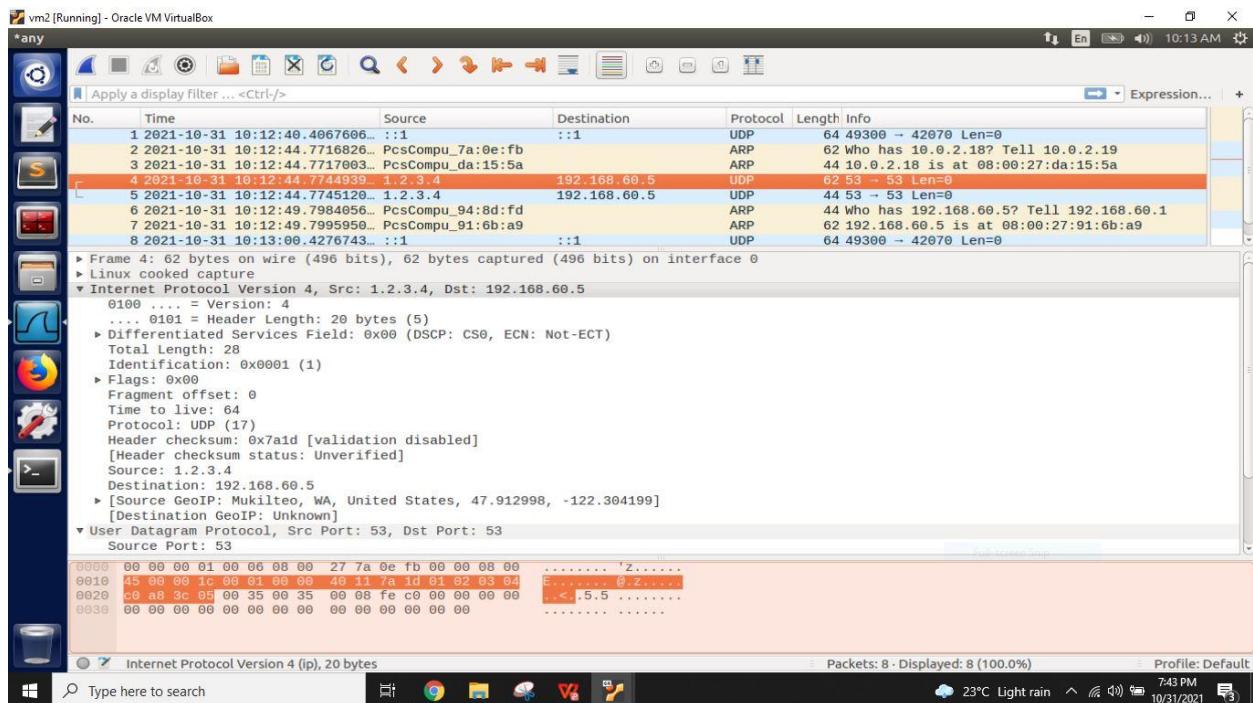
```
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo gedit reverse.py
(gedit:7311): Gtk-WARNING **: Calling Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.ServiceUnknown: The name org.gnome.SessionManager was not provided by any .service files
** (gedit:7311): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-spell-enabled not supported
** (gedit:7311): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:7311): WARNING **: Set document metadata failed: Setting attribute metadata::gedit-position not supported
[10/31/21]seed@Nikhil_PES1UG20CS821:~$ sudo python reverse.py
[10/31/21]seed@Nikhil_PES1UG20CS821:~$
```

Capture the packets in all the 3 vm's

In vm1 we can see 1 packet in the wireshark observation



In vm2 we can see 2 consecutive packets of both the interfaces



Only one packet is seen in the vm3

