Fahmida Alam Anika
Project 4

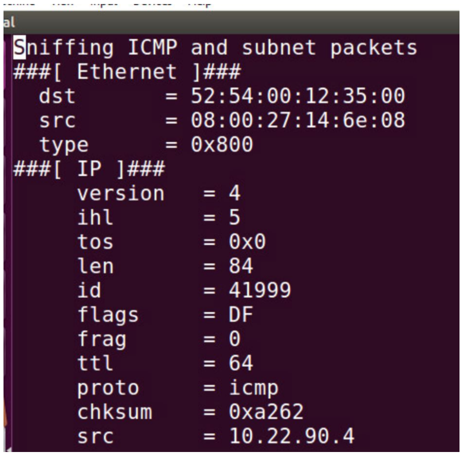
Task 2b. Capture ICMP Packets from/to a particular subnet.

1. Filters used:

- ICMP
  pkt = sniff(filter='icmp', prn=print_pkt)

- subnet 173.194.208.0/24
  pkt = sniff(filter='net 173.194.208.0/24', prn=print_pkt)

2. Python sniffer.py included submission
3. Text dump file sniffer_output.txt also included with submission



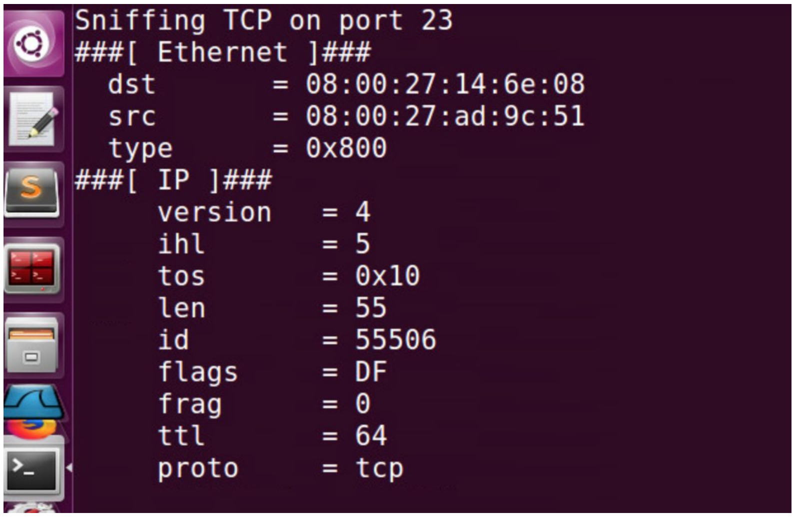
```
Sniffing ICMP and subnet packets
###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:14:6e:08
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 41999
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xa262
     src       = 10.22.90.4
```

Task 2c. Capture TCP packets

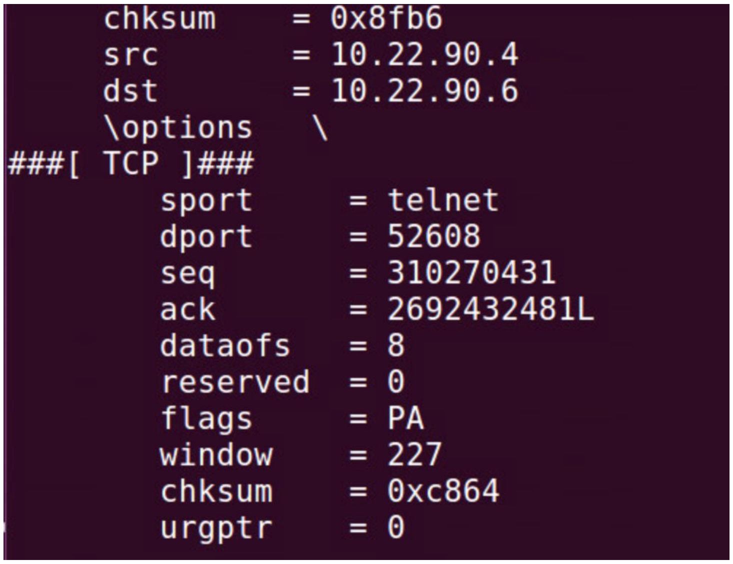
1. Filters used:

- Tcp port 23
  pkt = sniff(filter='tcp port 23', prn=print_pkt)

2. Python snifferTCP.py included submission
3. Text dump file snifferTCP2.txt also included with submission

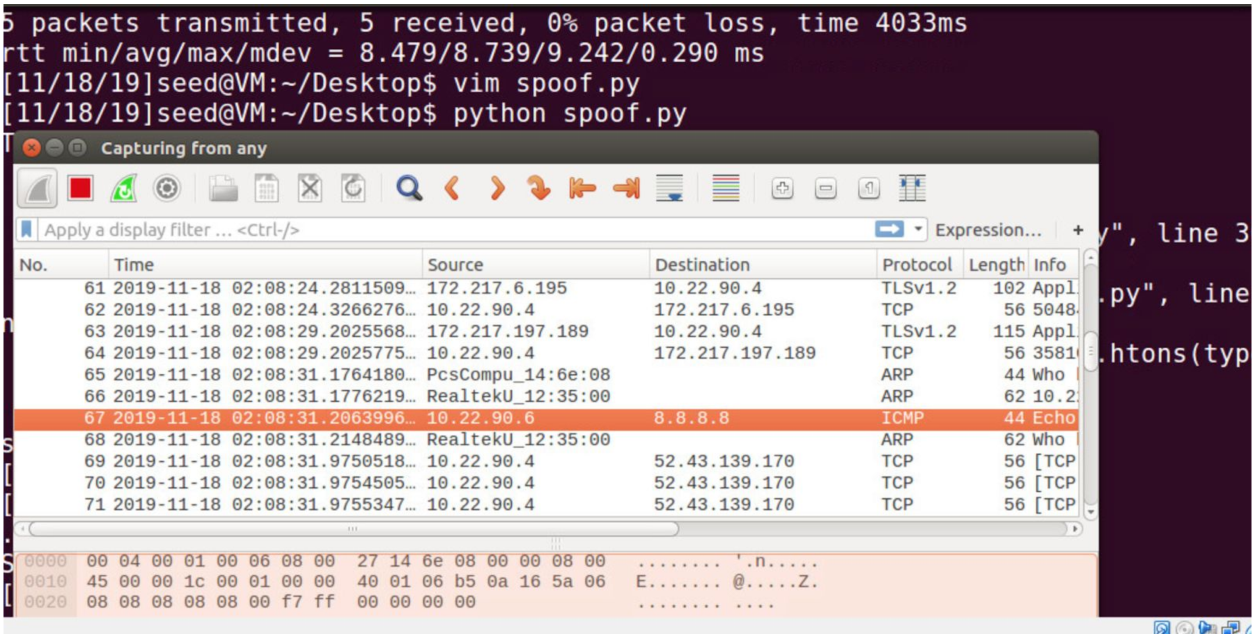


```
Sniffing TCP on port 23
###[ Ethernet ]###
  dst       = 08:00:27:14:6e:08
  src       = 08:00:27:ad:9c:51
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 55
     id        = 55506
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
```



```
     chksum    = 0x8fb6
     src       = 10.22.90.4
     dst       = 10.22.90.6
     \options   \
###[ TCP ]###
        sport     = telnet
        dport     = 52608
        seq       = 310270431
        ack       = 2692432481L
        dataofs   = 8
        reserved  = 0
        flags     = PA
        window    = 227
        chksum    = 0xc864
        urgptr    = 0
```

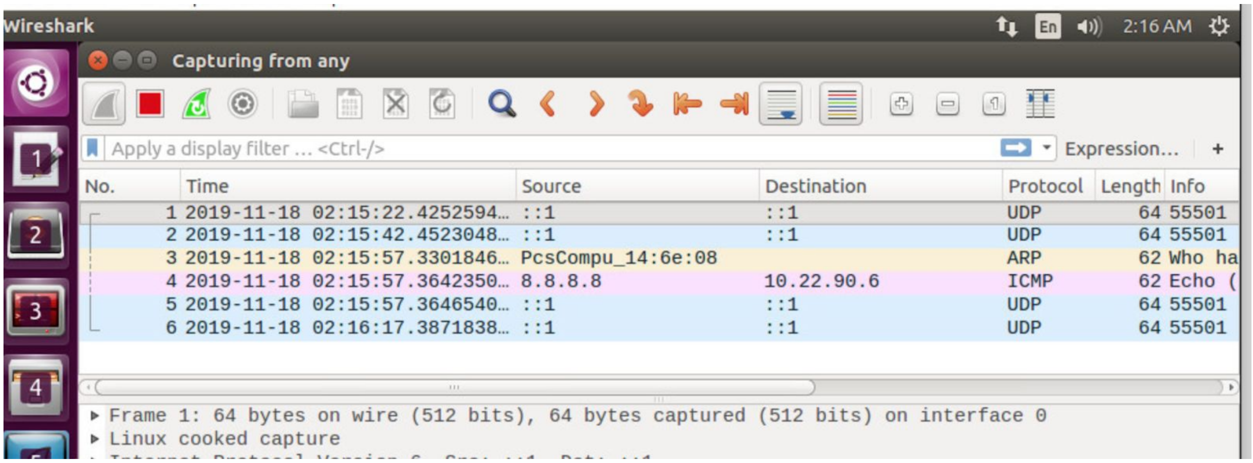
Task 3: spoof an ICMP echo request packet on behalf of another machine (i.e., using another machine's IP address as the packet's source IP address, in your case this will be the victim's VM (VM1: 10.22.90.6)).



```
5 packets transmitted, 5 received, 0% packet loss, time 4033ms
rtt min/avg/max/mdev = 8.479/8.739/9.242/0.290 ms
[11/18/19]seed@VM:~/Desktop$ vim spoof.py
[11/18/19]seed@VM:~/Desktop$ python spoof.py
y", line 3
.py", line
.htons(typ
```

```
No.  Time                          Source               Destination       Protocol  Length Info
  61 2019-11-18 02:08:24.2811509…  172.217.6.195        10.22.90.4        TLSv1.2     102 Appl
  62 2019-11-18 02:08:24.3266276…  10.22.90.4           172.217.6.195     TCP          56 5048
  63 2019-11-18 02:08:29.2025568…  172.217.197.189      10.22.90.4        TLSv1.2     115 Appl
  64 2019-11-18 02:08:29.2025775…  10.22.90.4           172.217.197.189   TCP          56 3581
  65 2019-11-18 02:08:31.1764180…  PcsCompu_14:6e:08                      ARP          44 Who
  66 2019-11-18 02:08:31.1776219…  RealtekU_12:35:00                      ARP          62 10.2
  67 2019-11-18 02:08:31.2063996…  10.22.90.6           8.8.8.8           ICMP         44 Echo
  68 2019-11-18 02:08:31.2148489…  RealtekU_12:35:00                      ARP          62 Who
  69 2019-11-18 02:08:31.9750518…  10.22.90.4           52.43.139.170     TCP          56 [TCP
  70 2019-11-18 02:08:31.9754505…  10.22.90.4           52.43.139.170     TCP          56 [TCP
  71 2019-11-18 02:08:31.9755347…  10.22.90.4           52.43.139.170     TCP          56 [TCP

0000  00 04 00 01 00 06 08 00  27 14 6e 08 00 00 08 00   ........ '.n.....
0010  45 00 00 1c 00 01 00 00  40 01 06 b5 0a 16 5a 06   E....... @.....Z.
0020  08 08 08 08 08 00 f7 ff  00 00 00 00               ........ ....
```

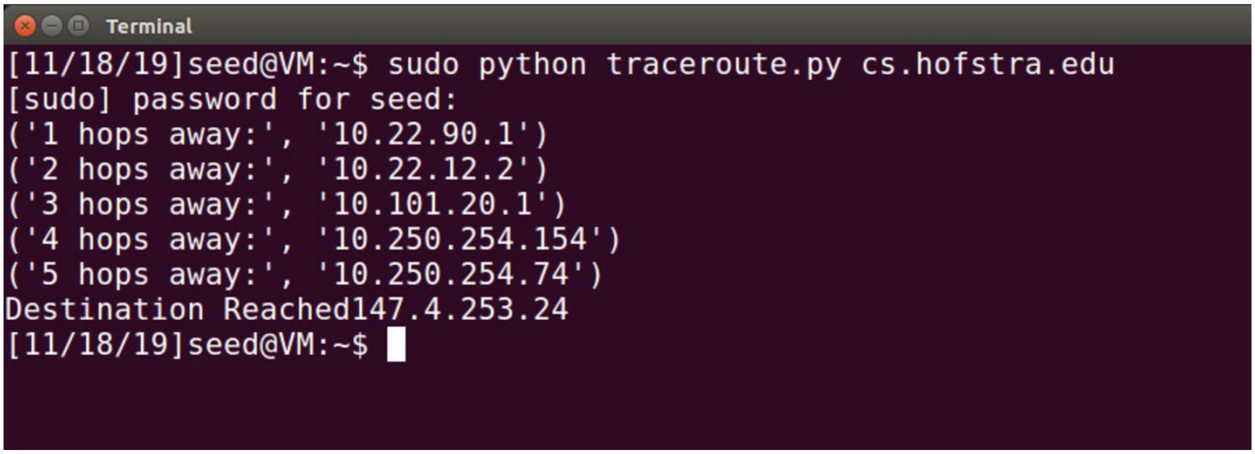


```
No.  Time                          Source              Destination   Protocol  Length Info
   1 2019-11-18 02:15:22.4252594…  ::1                 ::1           UDP           64 55501
   2 2019-11-18 02:15:42.4523048…  ::1                 ::1           UDP           64 55501
   3 2019-11-18 02:15:57.3301846…  PcsCompu_14:6e:08                 ARP           62 Who ha
   4 2019-11-18 02:15:57.3642350…  8.8.8.8             10.22.90.6    ICMP          62 Echo (
   5 2019-11-18 02:15:57.3646540…  ::1                 ::1           UDP           64 55501
   6 2019-11-18 02:16:17.3871838…  ::1                 ::1           UDP           64 55501

▸ Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
▸ Linux cooked capture
```

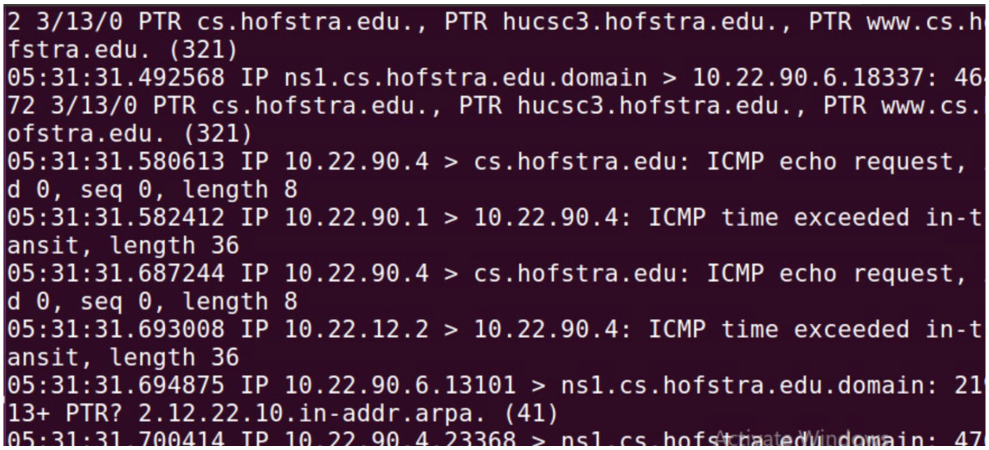
Task 4: Simulate traceroute.

- Traceroute.py included
- Output below:

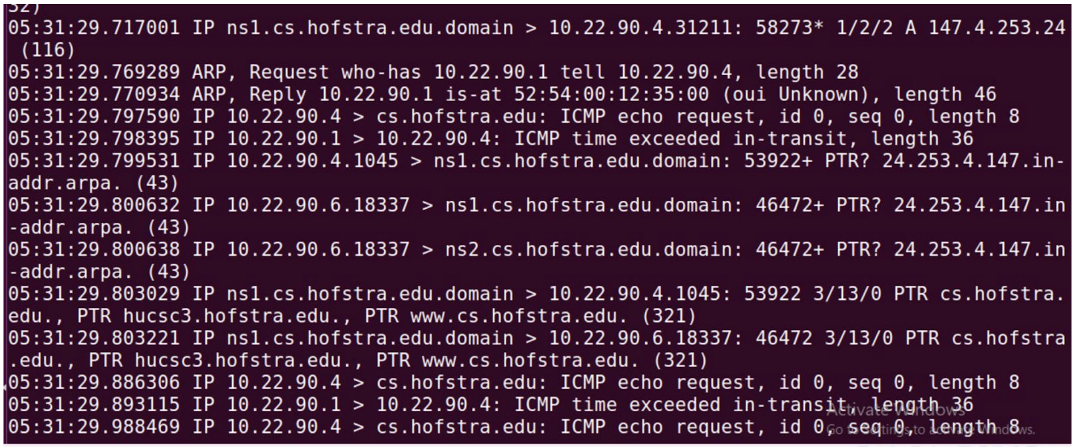


```
[11/18/19]seed@VM:~$ sudo python traceroute.py cs.hofstra.edu
[sudo] password for seed:
('1 hops away:', '10.22.90.1')
('2 hops away:', '10.22.12.2')
('3 hops away:', '10.101.20.1')
('4 hops away:', '10.250.254.154')
('5 hops away:', '10.250.254.74')
Destination Reached147.4.253.24
[11/18/19]seed@VM:~$ 
```

- Wireshark stopped repsonding, hence used pcap to capture packets below:



```
2 3/13/0 PTR cs.hofstra.edu., PTR hucsc3.hofstra.edu., PTR www.cs.h
fstra.edu. (321)
05:31:31.492568 IP ns1.cs.hofstra.edu.domain > 10.22.90.6.18337: 46
72 3/13/0 PTR cs.hofstra.edu., PTR hucsc3.hofstra.edu., PTR www.cs.
ofstra.edu. (321)
05:31:31.580613 IP 10.22.90.4 > cs.hofstra.edu: ICMP echo request, 
d 0, seq 0, length 8
05:31:31.582412 IP 10.22.90.1 > 10.22.90.4: ICMP time exceeded in-t
ansit, length 36
05:31:31.687244 IP 10.22.90.4 > cs.hofstra.edu: ICMP echo request, 
d 0, seq 0, length 8
05:31:31.693008 IP 10.22.12.2 > 10.22.90.4: ICMP time exceeded in-t
ansit, length 36
05:31:31.694875 IP 10.22.90.6.13101 > ns1.cs.hofstra.edu.domain: 21
13+ PTR? 2.12.22.10.in-addr.arpa. (41)
05:31:31.700414 IP 10.22.90.4.23368 > ns1.cs.hofstra.edu.domain: 47
```



```
32)
05:31:29.717001 IP ns1.cs.hofstra.edu.domain > 10.22.90.4.31211: 58273* 1/2/2 A 147.4.253.24
 (116)
05:31:29.769289 ARP, Request who-has 10.22.90.1 tell 10.22.90.4, length 28
05:31:29.770934 ARP, Reply 10.22.90.1 is-at 52:54:00:12:35:00 (oui Unknown), length 46
05:31:29.797590 IP 10.22.90.4 > cs.hofstra.edu: ICMP echo request, id 0, seq 0, length 8
05:31:29.798395 IP 10.22.90.1 > 10.22.90.4: ICMP time exceeded in-transit, length 36
05:31:29.799531 IP 10.22.90.4.1045 > ns1.cs.hofstra.edu.domain: 53922+ PTR? 24.253.4.147.in-
addr.arpa. (43)
05:31:29.800632 IP 10.22.90.6.18337 > ns1.cs.hofstra.edu.domain: 46472+ PTR? 24.253.4.147.in
-addr.arpa. (43)
05:31:29.800638 IP 10.22.90.6.18337 > ns2.cs.hofstra.edu.domain: 46472+ PTR? 24.253.4.147.in
-addr.arpa. (43)
05:31:29.803029 IP ns1.cs.hofstra.edu.domain > 10.22.90.4.1045: 53922 3/13/0 PTR cs.hofstra.
edu., PTR hucsc3.hofstra.edu., PTR www.cs.hofstra.edu. (321)
05:31:29.803221 IP ns1.cs.hofstra.edu.domain > 10.22.90.6.18337: 46472 3/13/0 PTR cs.hofstra
.edu., PTR hucsc3.hofstra.edu., PTR www.cs.hofstra.edu. (321)
05:31:29.886306 IP 10.22.90.4 > cs.hofstra.edu: ICMP echo request, id 0, seq 0, length 8
05:31:29.893115 IP 10.22.90.1 > 10.22.90.4: ICMP time exceeded in-transit, length 36
05:31:29.988469 IP 10.22.90.4 > cs.hofstra.edu: ICMP echo request, id 0, seq 0, length 8
```