PES UNIVERSITY

COMPUTER NETWORKS LAB

WEEK 1

PES2201800211

TASK 1:

1.1

```
[01/25/21]seed@PES2201800211-Attacker:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:2b:58:8a
          inet addr:10.0.2.8  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::b037:2b59:69f7:aef0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:364 errors:0 dropped:0 overruns:0 frame:0
          TX packets:257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:279171 (279.1 KB)  TX bytes:22563 (22.5 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:200 errors:0 dropped:0 overruns:0 frame:0
          TX packets:200 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:41259 (41.2 KB)  TX bytes:41259 (41.2 KB)

[01/25/21]seed@PES2201800211-Attacker:~$
```

```
[01/25/21]seed@PES2201800211-Victim:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e3:1a:87
          inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::c30f:38ac:cddc:6045/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266979 (266.9 KB)  TX bytes:20151 (20.1 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:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:39906 (39.9 KB)  TX bytes:39906 (39.9 KB)

[01/25/21]seed@PES2201800211-Victim:~$
```

The code is executed on attacker system as the attacker has to get the victim's packet and the data.

```
[01/25/21]seed@PES2201800211-Attacker:~$ sudo python sample.py
sudo: unable to resolve host PES2201800211-Attacker
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:e3:1a:87
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 22340
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xc74c
     src       = 10.0.2.9
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0xe2b5
        id        = 0x1031
        seq       = 0x1
###[ Raw ]###
           load      = '\x14\xe8\x0e`\xf3\xcc\x03\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 08:00:27:e3:1a:87
  src       = 52:54:00:12:35:00
  type      = 0x800
```

```
           load      = '\x14\xe8\x0e`\xf3\xcc\x03\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 08:00:27:e3:1a:87
  src       = 52:54:00:12:35:00
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 518
     flags     =
     frag      = 0
     ttl       = 119
     proto     = icmp
     chksum    = 0x258b
     src       = 8.8.8.8
     dst       = 10.0.2.9
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0xeab5
        id        = 0x1031
        seq       = 0x1
###[ Raw ]###
           load      = '\x14\xe8\x0e`\xf3\xcc\x03\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\x11\x1
2\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'

###[ Ethernet ]###
  dst       = 52:54:00:12:35:00
  src       = 08:00:27:e3:1a:87
  type      = 0x800
```

```
[01/25/21]seed@PES2201800211-Victim:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e3:1a:87
          inet addr:10.0.2.9  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::c30f:38ac:cddc:6045/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266979 (266.9 KB)  TX bytes:20151 (20.1 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:182 errors:0 dropped:0 overruns:0 frame:0
          TX packets:182 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:39906 (39.9 KB)  TX bytes:39906 (39.9 KB)

[01/25/21]seed@PES2201800211-Victim:~$
```

```
[01/25/21]seed@PES2201800211-Victim:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=58.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=10.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=94.5 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=54.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=53.0 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 10.994/54.376/94.515/26.513 ms
[01/25/21]seed@PES2201800211-Victim:~$
```

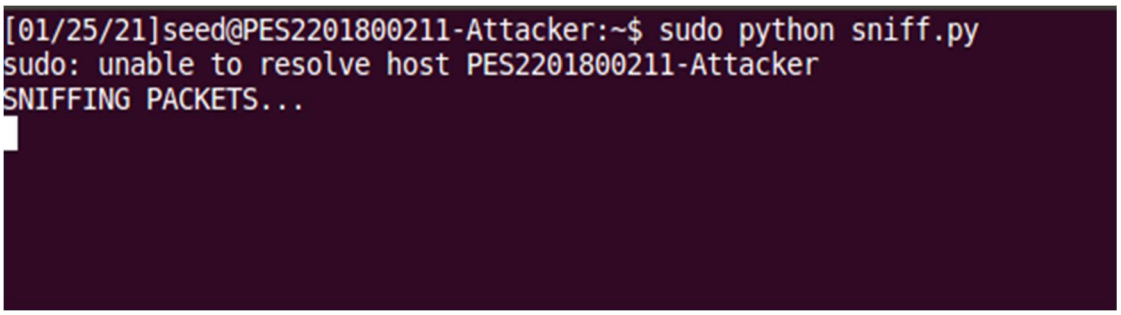
When the code is executed without root privilege it gives error message as seen below.

```
[01/25/21]seed@PES2201800211-Attacker:~$ python sample.py
SNIFFING PACKETS...
Traceback (most recent call last):
  File "sample.py", line 8, in <module>
    pkt = sniff(filter='icmp', prn = print_pkt)
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/sendrecv.py", line 731, in sni
ff
    *arg, **karg)] = iface
  File "/home/seed/.local/lib/python2.7/site-packages/scapy/arch/linux.py", line 567, in _
_init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type))
  File "/usr/lib/python2.7/socket.py", line 191, in __init__
    _sock = _realsocket(family, type, proto)
socket.error: [Errno 1] Operation not permitted
[01/25/21]seed@PES2201800211-Attacker:~$
```

1.2

```
[01/25/21]seed@PES2201800211-Attacker:~$ nano sniff.py
[01/25/21]seed@PES2201800211-Attacker:~$ cat sniff.py
#!/usr/bin/python

from scapy.all import *

print("SNIFFING PACKETS...");

def print_pkt(pkt):
        pkt.show()

pkt = sniff(filter='tcp  and (src host 10.0.2.9 and dst port 23)', prn = print_pkt)

[01/25/21]seed@PES2201800211-Attacker:~$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
PES2201800211-Victim login:
```

```
[01/25/21]seed@PES2201800211-Attacker:~$ nano sniff.py
[01/25/21]seed@PES2201800211-Attacker:~$ cat sniff.py
#!/usr/bin/python

from scapy.all import *

print("SNIFFING PACKETS...");

def print_pkt(pkt):
        pkt.show()

pkt = sniff(filter='tcp  and (src host 10.0.2.9 and dst port 23)', prn = print_pkt)

[01/25/21]seed@PES2201800211-Attacker:~$ telnet 10.0.2.9
Trying 10.0.2.9...
Connected to 10.0.2.9.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
PES2201800211-Victim login: seed
Password:
Last login: Mon Jan 25 10:55:50 EST 2021 from 10.0.2.8 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

1 package can be updated.
0 updates are security updates.

PS1: command not found
[01/25/21]seed@PES2201800211-Victim:~$
```



The telnet is run by attacker to get remote access of the victim's machine.

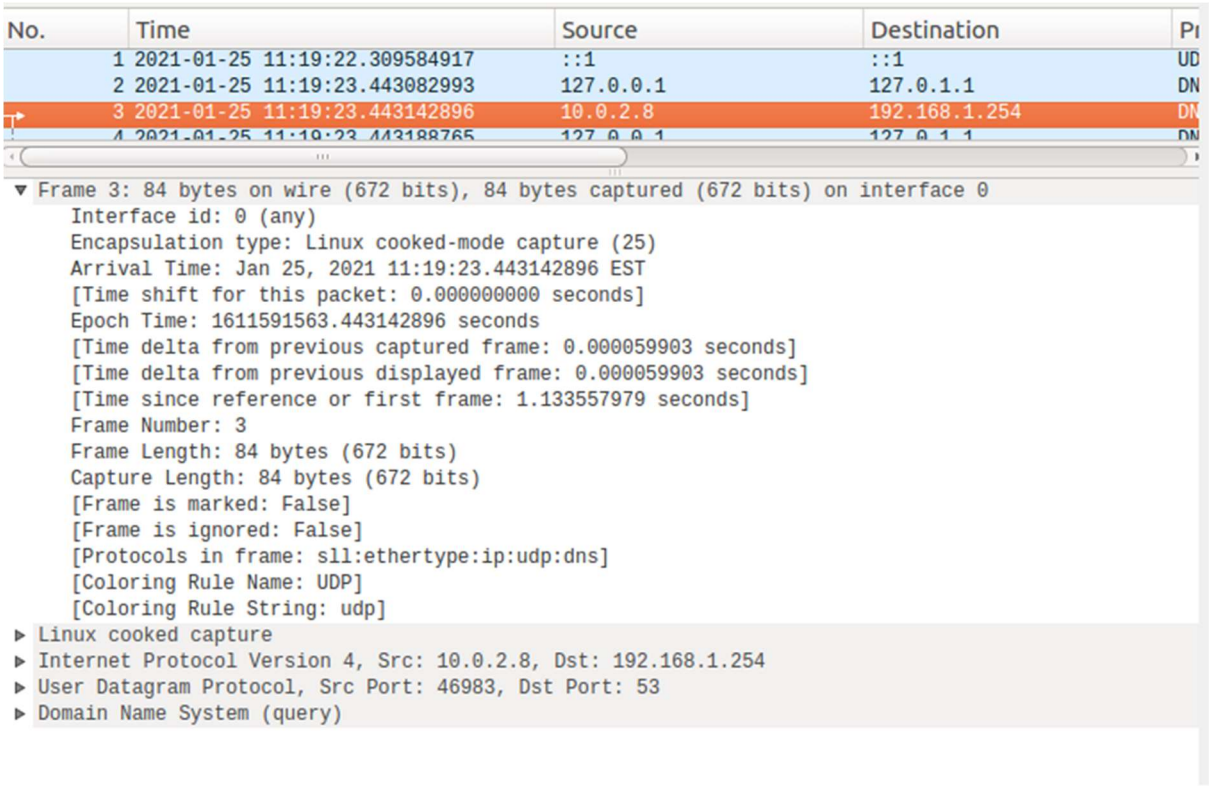
1.3

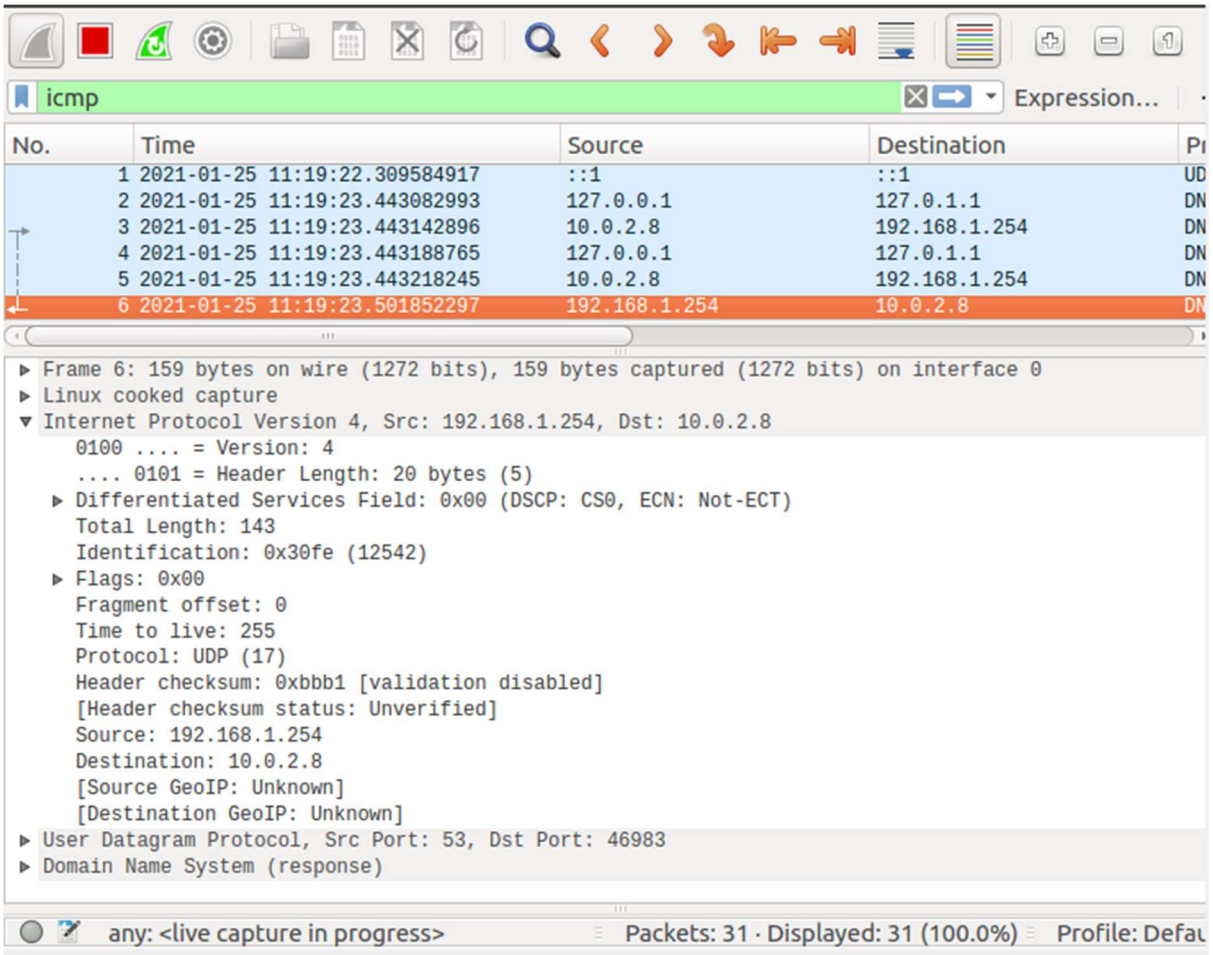
```
[01/25/21]seed@PES2201800211-Attacker:~$ nano sniff1.py
[01/25/21]seed@PES2201800211-Attacker:~$ cat sniff1.py
#!/usr/bin/python

from scapy.all import *

print("SNIFFING PACKETS...");

def print_pkt(pkt):
        pkt.show()

pkt = sniff(filter='src net 192.168.1.0/24', prn = print_pkt)

[01/25/21]seed@PES2201800211-Attacker:~$ sudo python sniff1.py
sudo: unable to resolve host PES2201800211-Attacker
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 08:00:27:2b:58:8a
  src       = 52:54:00:12:35:00
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 56
     id        = 12514
     flags     =
     frag      = 0
     ttl       = 127
     proto     = icmp
     chksum    = 0x3d21
     src       = 192.168.1.18
     dst       = 10.0.2.8
     \options   \
###[ ICMP ]###
```

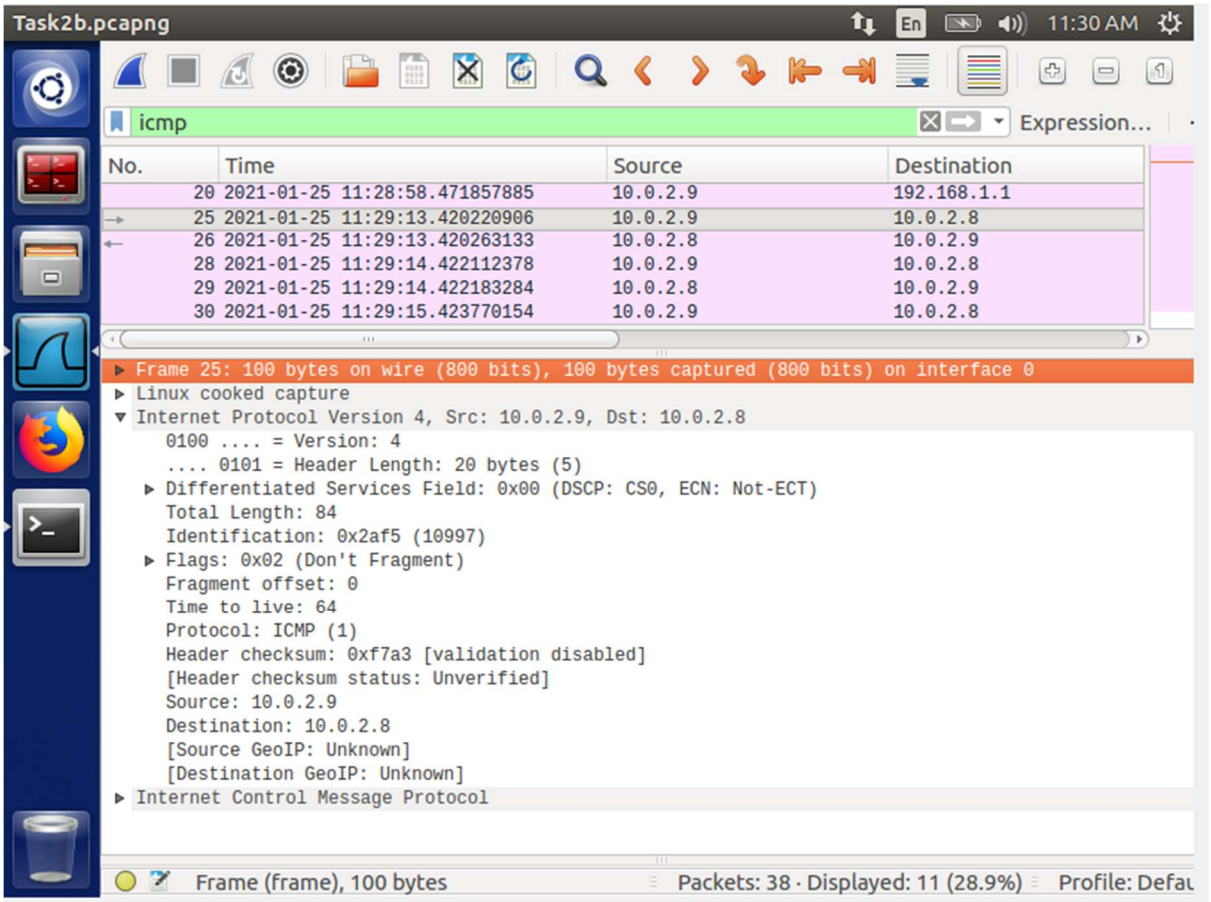
```
###[ ICMP ]###
        type      = dest-unreach
        code      = host-unreachable
        chksum    = 0x9a7e
        reserved  = 0
        length    = 0
        nexthopmtu= 0
###[ IP in ICMP ]###
           version   = 4
           ihl       = 5
           tos       = 0x0
           len       = 84
           id        = 54960
           flags     = DF
           frag      = 0
           ttl       = 64
           proto     = icmp
           chksum    = 0x9647
           src       = 10.0.2.8
           dst       = 192.168.1.1
           \options   \
###[ ICMP in ICMP ]###
              type      = echo-request
              code      = 0
              chksum    = 0x3f35
              id        = 0x1b42
              seq       = 0x9

###[ Ethernet ]###
  dst       = 08:00:27:2b:58:8a
  src       = 52:54:00:12:35:00
  type      = 0x800
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 56
     id        = 12517
     flags     =
     frag      = 0
     ttl       = 127
```

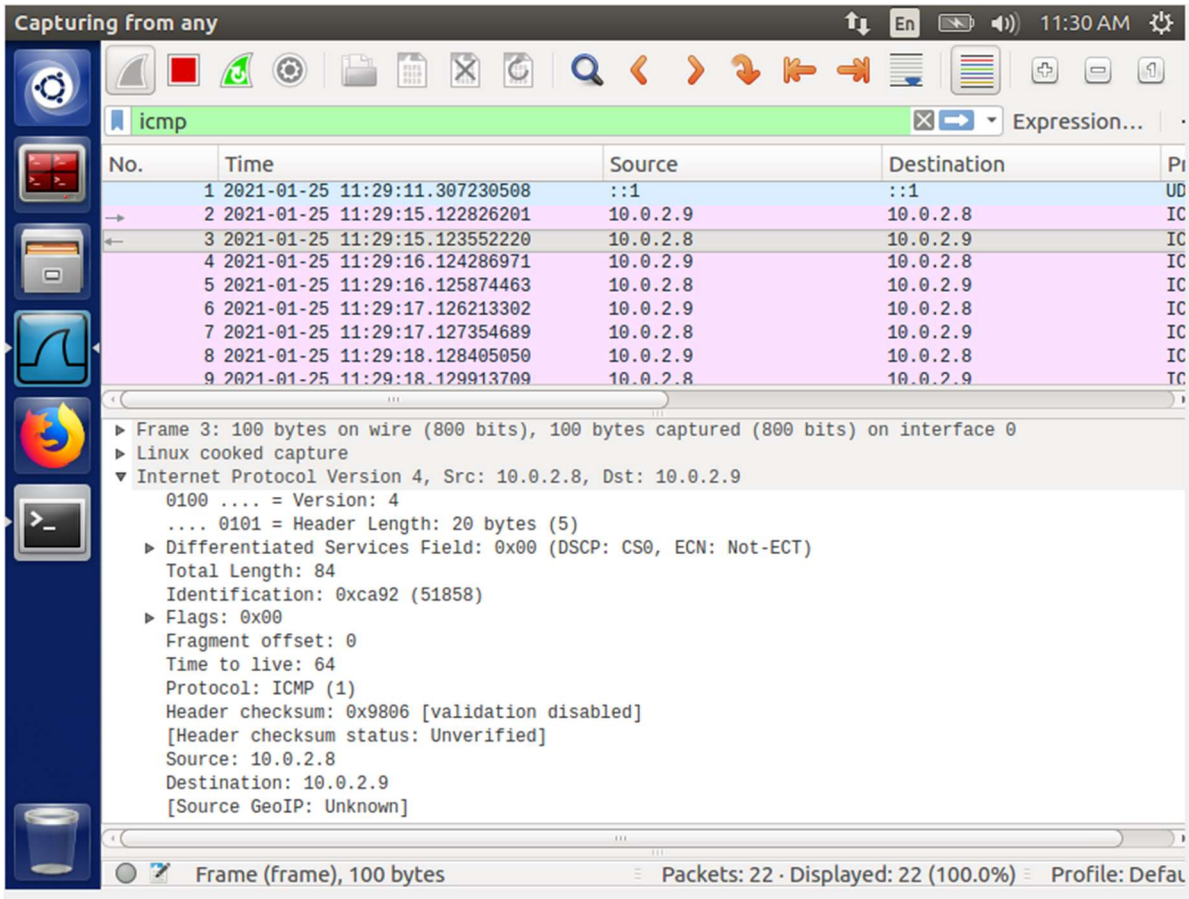
```
[01/25/21]seed@PES2201800211-Attacker:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.18 icmp_seq=3 Destination Host Unreachable
From 192.168.1.18 icmp_seq=6 Destination Host Unreachable
From 192.168.1.18 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.1.1 ping statistics ---
10 packets transmitted, 0 received, +3 errors, 100% packet loss, time 9109ms

[01/25/21]seed@PES2201800211-Attacker:~$
```

TASK 2:


No. Time Source Destination Pr
1 2021-01-25 11:19:22.309584917 ::1 ::1 UD
2 2021-01-25 11:19:23.443082993 127.0.0.1 127.0.1.1 DN
3 2021-01-25 11:19:23.443142896 10.0.2.8 192.168.1.254 DN
Frame 3: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface 0
Interface id: 0 (any)
Encapsulation type: Linux cooked-mode capture (25)
Arrival Time: Jan 25, 2021 11:19:23.443142896 EST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1611591563.443142896 seconds
[Time delta from previous captured frame: 0.000059903 seconds]
[Time delta from previous displayed frame: 0.000059903 seconds]
[Time since reference or first frame: 1.133557979 seconds]
Frame Number: 3
Frame Length: 84 bytes (672 bits)
Capture Length: 84 bytes (672 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: sll:ethertype:ip:udp:dns]
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.8, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 46983, Dst Port: 53
Domain Name System (query)


icmp
Expression...
No. Time Source Destination Pr
1 2021-01-25 11:19:22.309584917 ::1 ::1 UD
2 2021-01-25 11:19:23.443082993 127.0.0.1 127.0.1.1 DN
3 2021-01-25 11:19:23.443142896 10.0.2.8 192.168.1.254 DN
4 2021-01-25 11:19:23.443188765 127.0.0.1 127.0.1.1 DN
5 2021-01-25 11:19:23.443218245 10.0.2.8 192.168.1.254 DN
6 2021-01-25 11:19:23.501852297 192.168.1.254 10.0.2.8 DN
Frame 6: 159 bytes on wire (1272 bits), 159 bytes captured (1272 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 10.0.2.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 143
Identification: 0x30fe (12542)
Flags: 0x00
Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0xbbb1 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.1.254
Destination: 10.0.2.8
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 53, Dst Port: 46983
Domain Name System (response)
any: <live capture in progress>
Packets: 31 · Displayed: 31 (100.0%)
Profile: Defau

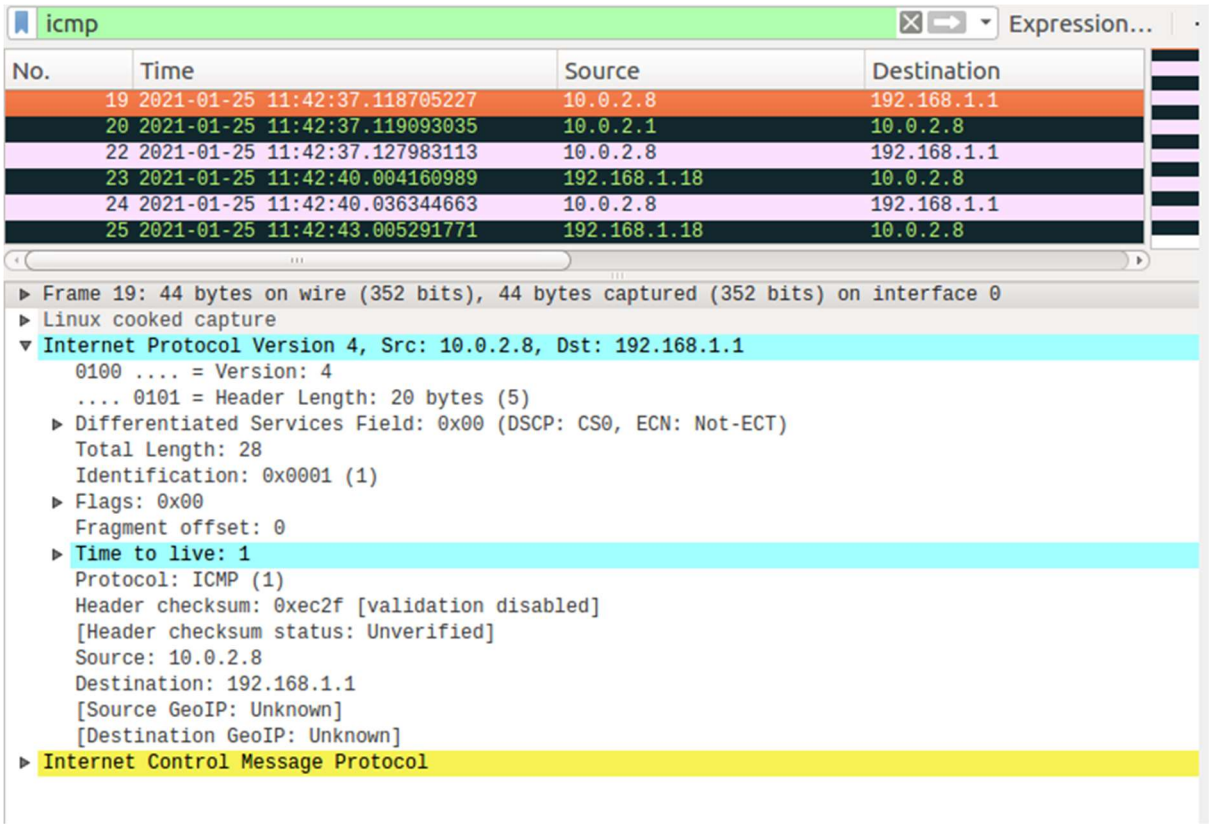

Task2b.pcapng
11:30 AM
icmp
Expression…
No. Time Source Destination
20 2021-01-25 11:28:58.471857885 10.0.2.9 192.168.1.1
25 2021-01-25 11:29:13.420220906 10.0.2.9 10.0.2.8
26 2021-01-25 11:29:13.420263133 10.0.2.8 10.0.2.9
28 2021-01-25 11:29:14.422112378 10.0.2.9 10.0.2.8
29 2021-01-25 11:29:14.422183284 10.0.2.8 10.0.2.9
30 2021-01-25 11:29:15.423770154 10.0.2.9 10.0.2.8
Frame 25: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.9, Dst: 10.0.2.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x2af5 (10997)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xf7a3 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.9
Destination: 10.0.2.8
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol
Frame (frame), 100 bytes
Packets: 38 · Displayed: 11 (28.9%)
Profile: Defau


Capturing from any
11:30 AM
icmp
Expression…
No. Time Source Destination
1 2021-01-25 11:29:11.307230508 ::1 ::1
2 2021-01-25 11:29:15.122826201 10.0.2.9 10.0.2.8
3 2021-01-25 11:29:15.123552220 10.0.2.8 10.0.2.9
4 2021-01-25 11:29:16.124286971 10.0.2.9 10.0.2.8
5 2021-01-25 11:29:16.125874463 10.0.2.8 10.0.2.9
6 2021-01-25 11:29:17.126213302 10.0.2.9 10.0.2.8
7 2021-01-25 11:29:17.127354689 10.0.2.8 10.0.2.9
8 2021-01-25 11:29:18.128405050 10.0.2.9 10.0.2.8
Frame 3: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.8, Dst: 10.0.2.9
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0xca92 (51858)
Flags: 0x00
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0x9806 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.8
Destination: 10.0.2.9
[Source GeoIP: Unknown]
Frame (frame), 100 bytes
Packets: 22 · Displayed: 22 (100.0%)
Profile: Defau

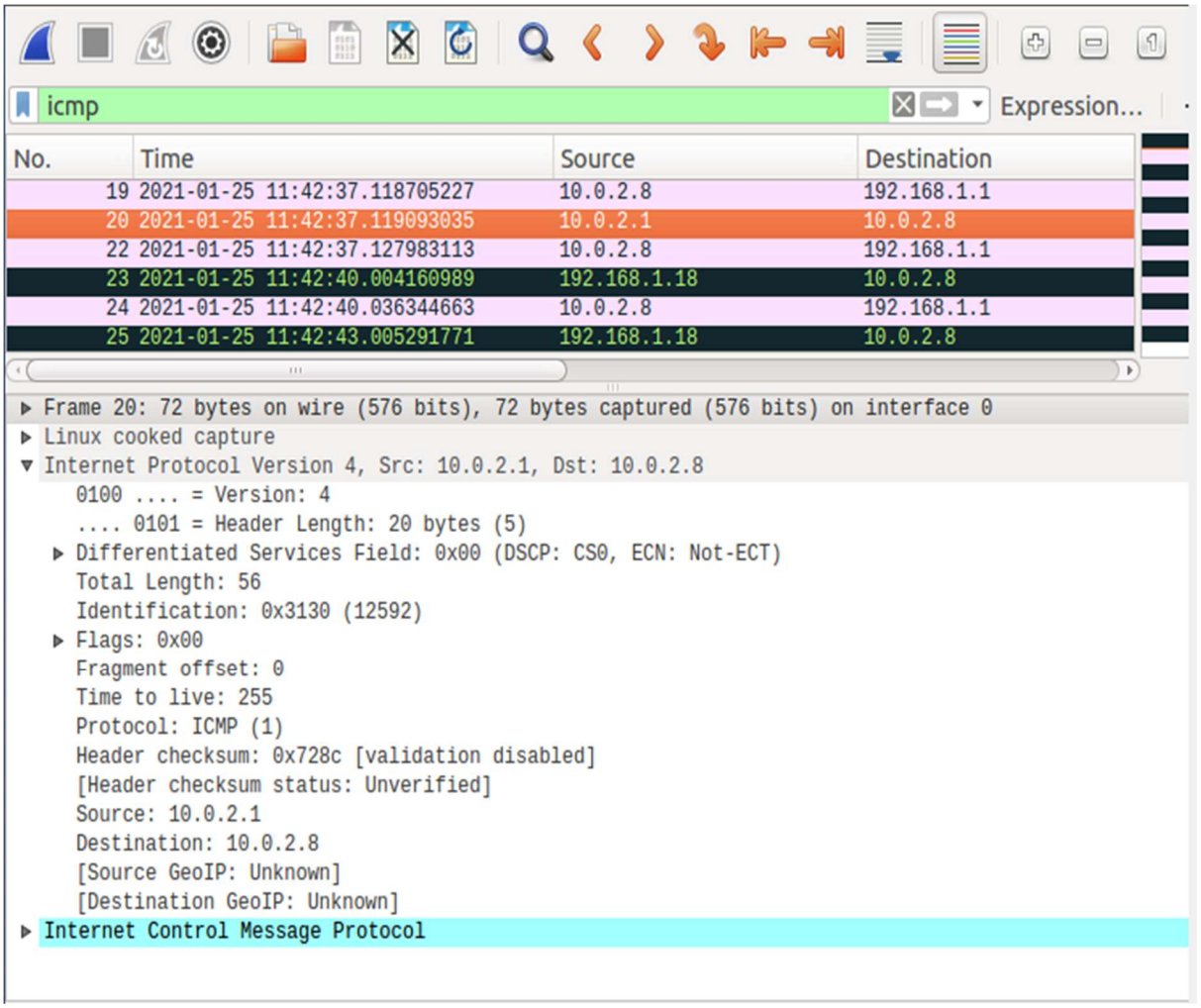
TASK 3:

```
from scapy.all import *
'''Usage: ./traceroute.py "hostname or ip address"'''
host = sys.argv[1]
print("Traceroute " + host)
ttl = 1

while 1:
        IPLayer = IP()
        IPLayer.dst = host
        IPLayer.ttl = ttl
        ICMPpkt = ICMP()
        pkt = IPLayer/ICMPpkt
        replypkt = sr1(pkt, verbose=0)

        if replypkt is None:
                break;

        elif replypkt [ICMP].type == 0:
                print("%d hops away: " %tt, replypkt [IP].src)
                print("Done", replypkt [IP].src)
                break;

        else:
                print("%d hops away: "%ttl, replypkt [IP].src)
                ttl += 1
```

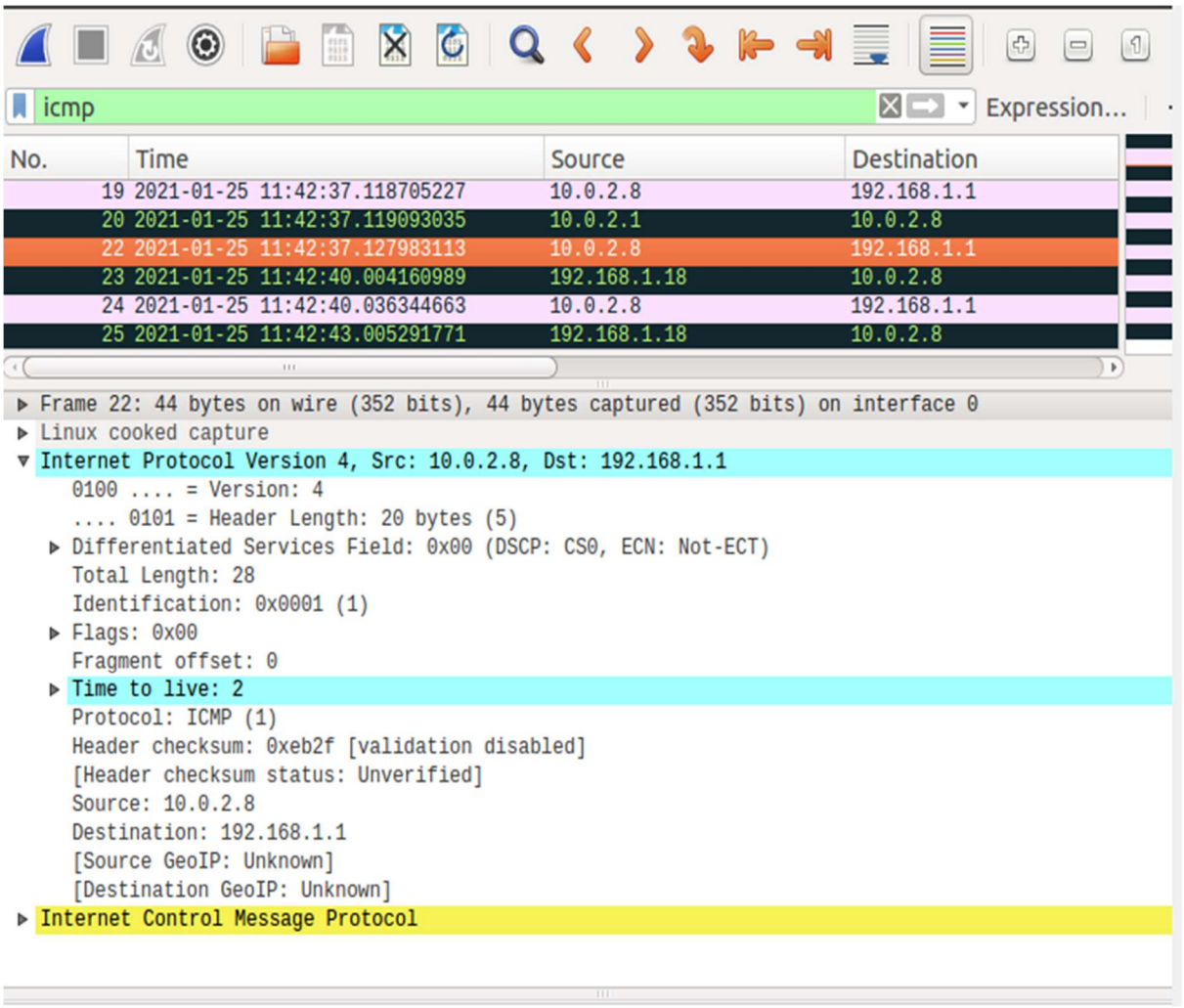
```
[01/25/21]seed@PES2201800211-Attacker:~$ sudo python traceroute.py 192.168.1.1
sudo: unable to resolve host PES2201800211-Attacker
Traceroute 192.168.1.1
('1 hops away: ', '10.0.2.1')
('2 hops away: ', '192.168.1.18')
('3 hops away: ', '192.168.1.18')
('4 hops away: ', '192.168.1.18')
('5 hops away: ', '192.168.1.18')
('6 hops away: ', '192.168.1.18')
```



Above the Time to live is 1 for No. 19.



For No. 20, Time to live is 255 or exceeded



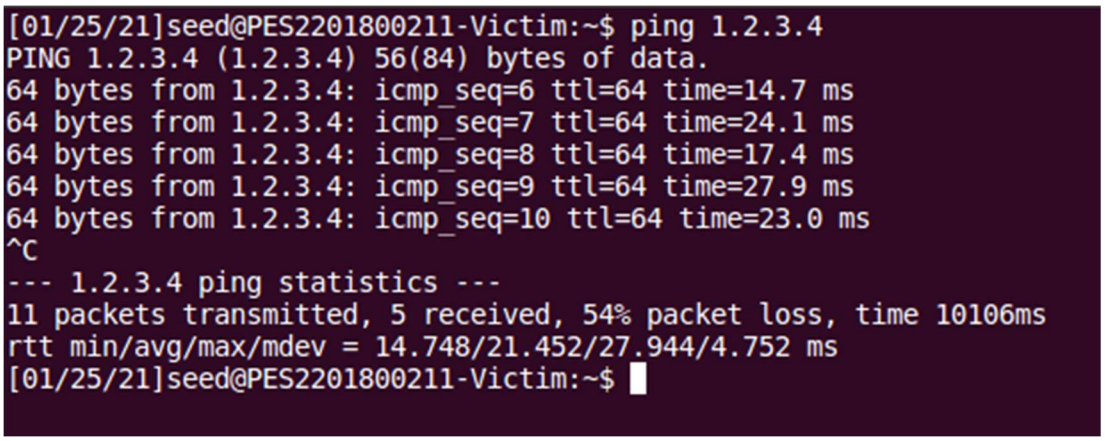
Time to live is 2 again for No.22

TASK 4:

```
[01/25/21]seed@PES2201800211-Attacker:~$ sudo python sniiffspoof.py
sudo: unable to resolve host PES2201800211-Attacker
Original packet ......
('Source IP: ', '10.0.2.9')
('Destination IP: ', '1.2.3.4')
Spoofed packet.....
('Source IP: ', '1.2.3.4')
('Destination IP: ', '10.0.2.9')
Original packet ......
('Source IP: ', '10.0.2.9')
('Destination IP: ', '1.2.3.4')
Spoofed packet.....
('Source IP: ', '1.2.3.4')
('Destination IP: ', '10.0.2.9')
Original packet ......
('Source IP: ', '10.0.2.9')
('Destination IP: ', '1.2.3.4')
Spoofed packet.....
('Source IP: ', '1.2.3.4')
('Destination IP: ', '10.0.2.9')
Original packet ......
('Source IP: ', '10.0.2.9')
('Destination IP: ', '1.2.3.4')
Spoofed packet.....
('Source IP: ', '1.2.3.4')
('Destination IP: ', '10.0.2.9')
Original packet ......
('Source IP: ', '10.0.2.9')
('Destination IP: ', '1.2.3.4')
Spoofed packet.....
('Source IP: ', '1.2.3.4')
('Destination IP: ', '10.0.2.9')
^C[01/25/21]seed@PES2201800211-Attacker:~$
```

```
[01/25/21]seed@PES2201800211-Victim:~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
```

Victim's machine before executing code on attacker machine, below is after the python code is executed.


[01/25/21]seed@PES2201800211-Victim:~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=14.7 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=64 time=24.1 ms
64 bytes from 1.2.3.4: icmp_seq=8 ttl=64 time=17.4 ms
64 bytes from 1.2.3.4: icmp_seq=9 ttl=64 time=27.9 ms
64 bytes from 1.2.3.4: icmp_seq=10 ttl=64 time=23.0 ms
^C
--- 1.2.3.4 ping statistics ---
11 packets transmitted, 5 received, 54% packet loss, time 10106ms
rtt min/avg/max/mdev = 14.748/21.452/27.944/4.752 ms
[01/25/21]seed@PES2201800211-Victim:~$