| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No:01 |
|---|---|---|
| | Section: B | Date: 27/08/2022 |

| Task 1.1 A | Sniff IP packets using Scapy. |
|---|---|
| Output Screenshot | From Host-A: |

```
root@015dd2950967:/# export PS1="hostA:PES1UG20CS016:Name:AdarshKumar$>"
hostA:PES1UG20CS016:Name:AdarshKumar$>ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11254ms

hostA:PES1UG20CS016:Name:AdarshKumar$>
```

Pinging from Host-A to 8.8.8.8 (www.google.com) 12 packets transmitted.

On Attacker Terminal:

```
seed-attacker:PES1UG20CS016:Name:AdarshKumar$>python3 Task1.1A.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:88:a6:c7:6a
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 45937
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x6d1a
     src       = 10.9.0.5
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0x2ad7
        id        = 0x1c
        seq       = 0x1
###[ Raw ]###
           load      = '\xcf\xb1\x08c\x00\x00\x00\x00-$\t\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1
e\x1f !"#$%&\'()*+,-./01234567'
```

## Observation:

A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.
ICMP packets received on attacker's terminal after Pinging from host-A IP:10.9.0.5
Type of IP address is IPv4 and checksum of IP header is also calculated as 0x6dla
ICMP packet checksum is 0x2ad7, Raw packet load is present in some encrypted format.

| Task 1.1 B | Capture only the ICMP packet |
|---|---|
| Output Screenshot | From Host A: |

```
hostA:PES1UG20CS016:Name:AdarshKumar$>ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4084ms

hostA:PES1UG20CS016:Name:AdarshKumar$>
```

Pinging from Host-A to 8.8.8.8 (www.google.com) 5 packets transmitted.

On Attacker Terminal:

```
seed-attacker:PES1UG20CS016:Name:AdarshKumar$>python3 Task1.1B-I
CMP.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:88:a6:c7:6a
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 56357
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0x4466
     src       = 10.9.0.5
     dst       = 8.8.8.8
     \options   \
###[ ICMP ]###
        type      = echo-request
        code      = 0
        chksum    = 0x98dc
        id        = 0x1e
        seq       = 0x1
###[ Raw ]###
           load      = '@\xb4\x08c\x00\x00\x00\x00P\x1a\x07\x00\
x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\
x1c\x1d\x1e\x1f !"#$%&\'()*+,-./01234567'
```

Observation:

A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.
Only ICMP packet received on attacker's terminal after pinging from host-A IP:10.9.0.5 by using filter
Type of IP address is IPv4 and checksum of IP header is calculated as 0x4466
ICMP packet echo-request checksum is 0x98dc, sequence no 1.
Raw packet load is present in some encrypted format

| | |
|---|---|
| Q) | Capture any TCP packet that comes from a particular IP and with a destination port number 23 |
| Output Screenshot | From Host A:<br>Connecting with telnet from IP address 10.9.0.1.<br>Got login portal sign in successfully and got connected to successfully.<br>Now terminating the telnet connection. |

```
hostA:PES1UG20CS016:Name:AdarshKumar$>telnet 10.9.0.1
Trying 10.9.0.1...
Connected to 10.9.0.1.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

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

0 updates can be installed immediately.
0 of these updates are security updates.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

[08/26/22]seed@VM:~$
```

On Attacker Terminal:

```
seed-attacker:PES1UG20CS016:Name:AdarshKumar$>python3 Task1.1B-TCP.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:88:a6:c7:6a
  src       = 02:42:0a:09:00:05
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x10
     len       = 60
     id        = 47846
     flags     = DF
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x6bae
     src       = 10.9.0.5
     dst       = 10.9.0.1
     \options   \
###[ TCP ]###
        sport     = 35764
        dport     = telnet
        seq       = 1763214429
        ack       = 0
        dataofs   = 10
        reserved  = 0
        flags     = S
        window    = 64240
        chksum    = 0x1446
        urgptr    = 0
        options   = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (1163230244, 0)), ('NOP', None), ('WScale', 7)]

###[ Ethernet ]###
  dst       = 02:42:88:a6:c7:6a
```

## Observation:

When host-A was trying to connect with talent service then TCP packet received.
Here packet received which has only 4 headers like Ethernet, IP, TCP.
Only TCP packet received on attacker's terminal after establishing connection from host-A IP:10.9.0.5 by using filter.
Type of IP address is IPv4 and checksum of IP header is calculated as 0x6bae
TCP packet dport is telnet and checksum is ox1446, ack is 0, Note here RAW packet is not Present

| Q) | Capture packets that come from or go to a particular subnet |
|---|---|
| Output Screenshot | From Host A |

```
hostA:PES1UG20CS016:Name:AdarshKumar$>ping 172.17.0.1
PING 172.17.0.1 (172.17.0.1) 56(84) bytes of data.
64 bytes from 172.17.0.1: icmp_seq=1 ttl=64 time=0.057 ms
64 bytes from 172.17.0.1: icmp_seq=2 ttl=64 time=0.155 ms
64 bytes from 172.17.0.1: icmp_seq=3 ttl=64 time=0.085 ms
64 bytes from 172.17.0.1: icmp_seq=4 ttl=64 time=0.150 ms
64 bytes from 172.17.0.1: icmp_seq=5 ttl=64 time=0.159 ms
64 bytes from 172.17.0.1: icmp_seq=6 ttl=64 time=0.096 ms
64 bytes from 172.17.0.1: icmp_seq=7 ttl=64 time=0.153 ms
64 bytes from 172.17.0.1: icmp_seq=8 ttl=64 time=0.152 ms
^C
--- 172.17.0.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7152ms
rtt min/avg/max/mdev = 0.057/0.125/0.159/0.037 ms
hostA:PES1UG20CS016:Name:AdarshKumar$>
```

Pinging from Host-A to IP 172.17.0.1 which is in same subnet, ping successful sending a sequence of ICMP Packet.

8 packet successfully transmitted in time 7152ms.

On Attacker Terminal:

```
seed-attacker:PES1UG20CS016:Name:AdarshKumar$>python3 Task1.1B-Subnet.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:05
  src       = 02:42:88:a6:c7:6a
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 84
     id        = 3238
     flags     =
     frag      = 0
     ttl       = 64
     proto     = icmp
     chksum    = 0xb7e3
     src       = 172.17.0.1
     dst       = 10.9.0.5
     \options   \
###[ ICMP ]###
        type      = echo-reply
        code      = 0
        chksum    = 0x84ad
        id        = 0x27
        seq       = 0x1
###[ Raw ]###
           load      = 'S\xb9\x08c\x00\x00\x00\x00W;\t\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x
1f !"#$%&\'()*+,-./01234567'
```

Observation:

A packet received which has 4 headers like Ethernet, IP, ICMP, Raw.

Type of IP address is IPv4 and checksum of IP header is calculated as 0xb7e3, in same subnet

ICMP packet echo-request checksum is 0x84ad, sequence no 0x1.

Raw packet load is present in some encrypted format.

| Task 1.2 | spoofing ICMP echo request packets |
|---|---|
| Output Screenshot | On Attacker Terminal: |

```
Seed-attacker:PES2UG20CS016:AdarshKumar$>python3 Task1.2A.py
SENDING SPOOFED ICMP PACKET...
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = None
  src       = 10.9.0.1
  dst       = 10.9.0.5
  \options   \
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = None
     id        = 0x0
     seq       = 0x0
```

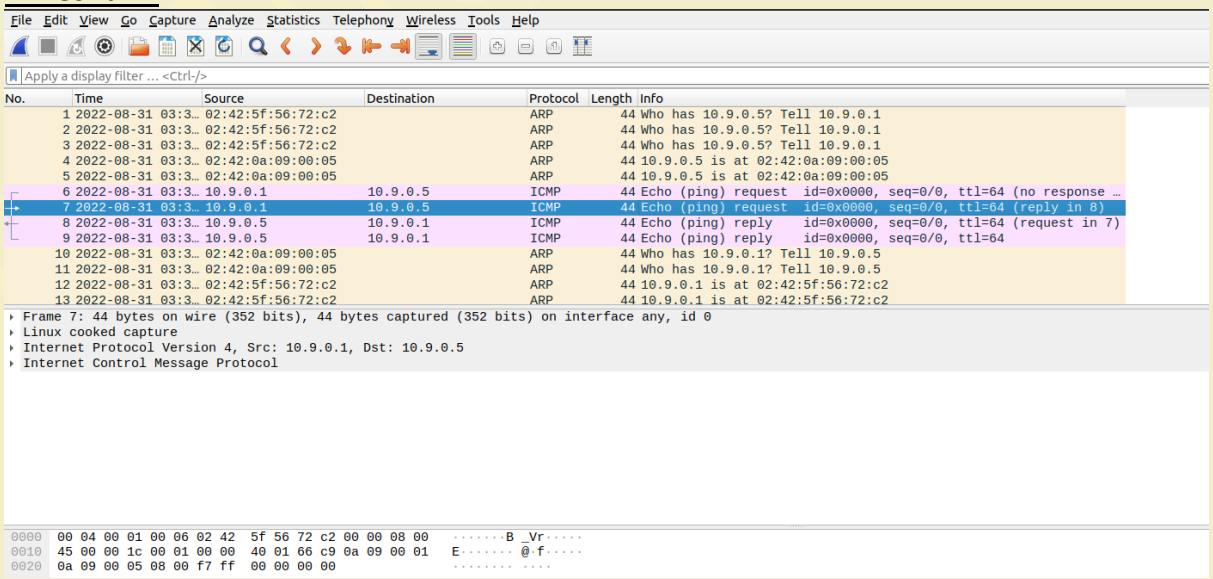
Observation:

Sending a spoofed packet from source=10.9.0.1 to destination=10.9.1.5

Photocall type ICMP, IP address is type is IPv4

NOTE: checksum is None it will be considered as missing checksum but will be allowed and flags field is also empty length of packet is not defined. And tos is 0x0.

Wireshark:




For ICMP Echo request from 10.9.0.1 we got an ICMP Echo reply from 10.9.0.5

| | |
|---|---|
| Q.) | spoofing ICMP echo request packets arbitrary source IP address |
| Output Screenshot | On Attacker Terminal: |

```
Seed-attacker:PES2UG20CS016:AdarshKumar$>python3 Task1.2B.py
SENDING SPOOFED ICMP PACKET...
###[ IP ]###
  version   = 4
  ihl       = None
  tos       = 0x0
  len       = None
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = icmp
  chksum    = None
  src       = 10.9.0.11
  dst       = 10.9.0.99
  \options   \
###[ ICMP ]###
     type      = echo-request
     code      = 0
     chksum    = None
     id        = 0x0
     seq       = 0x0

Seed-attacker:PES2UG20CS016:AdarshKumar$>
```

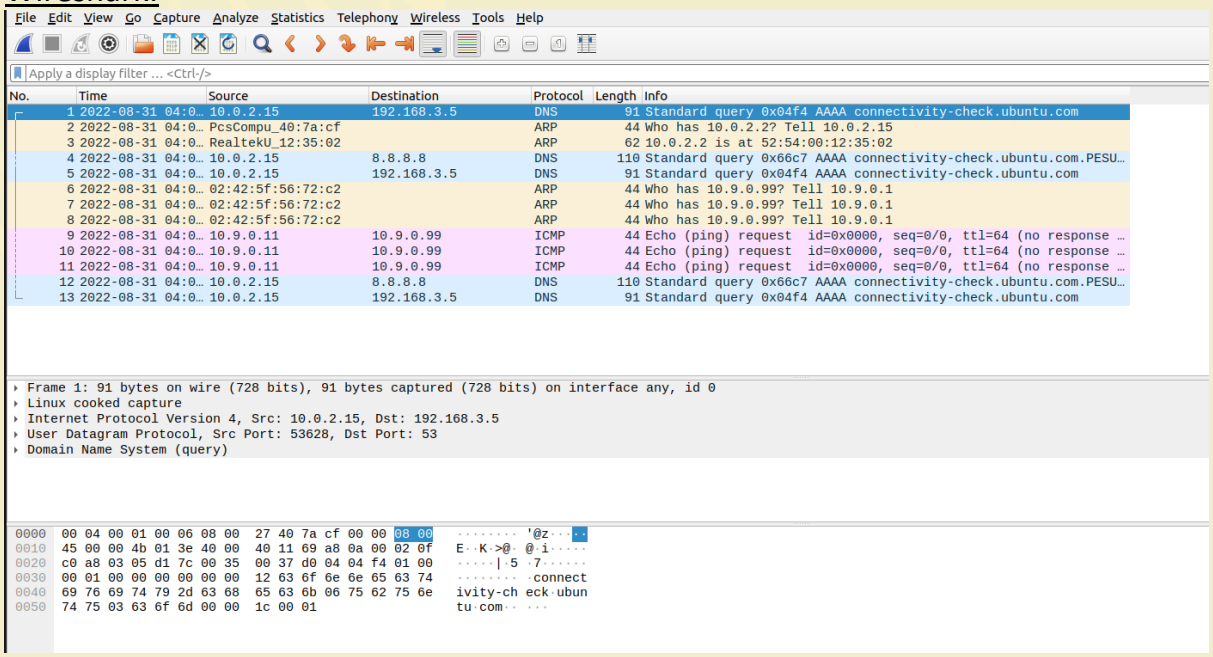
## Observation:

Similar to above here we are spoofing to arbitrator IP address as you can see that in ICPM header code, checksum, id, sequence everything is 0.

We send only IP, ICMP header part rest all is set to default value by scapy module.

ttl value is 64 so packet was not able to reach to destination and IP version is IPv4, flags are not set

## Wireshark:




As you can that see sending packet to arbitrary address is we are unable to receive Echo reply packet. While we tried to send ICMP packet 3 times but no rely was found.

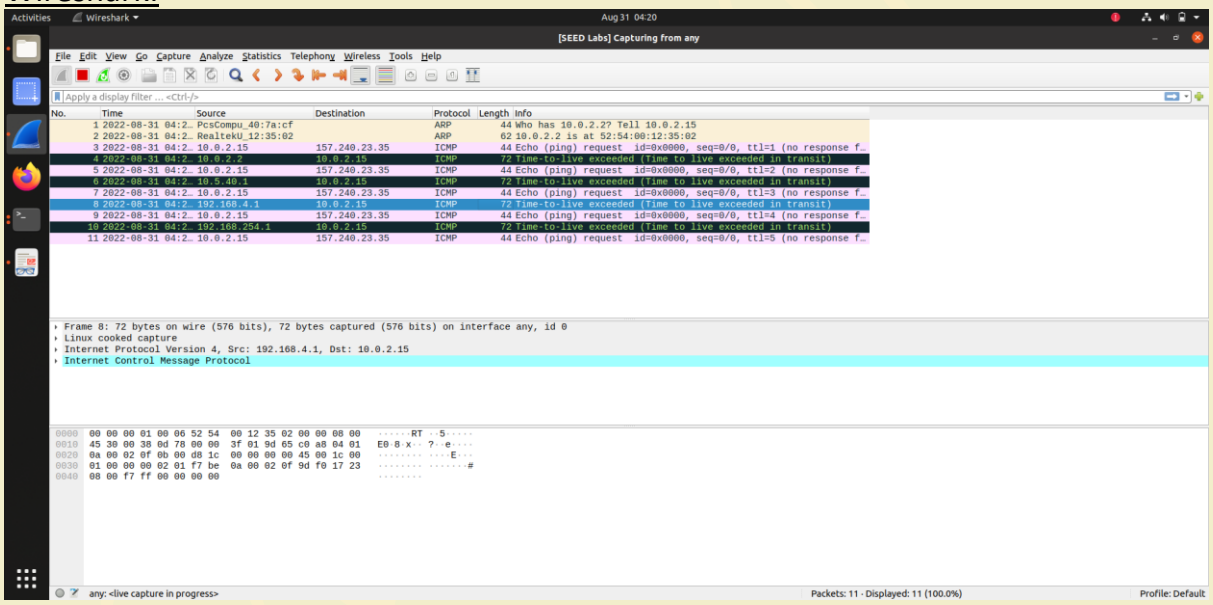
| Task 1.3: | Traceroute |
|---|---|
| Output Screenshot | On Attacker Terminal |

```
seed@VM: ~/.../volumes        seed@VM: ~/.../volumes
Seed-attacker:PES2UG20CS016:AdarshKumar$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away:  10.0.2.2
2 hops away:  10.5.40.1
3 hops away:  192.168.4.1
4 hops away:  192.168.254.1
Seed-attacker:PES2UG20CS016:AdarshKumar$>
```

## Observation:

As you can see that when we try to trace the packet of IP 157.240.23.35 it went to 4 hops and then connection closed, possible cause might be that IP doesn't exist.

## Wireshark:



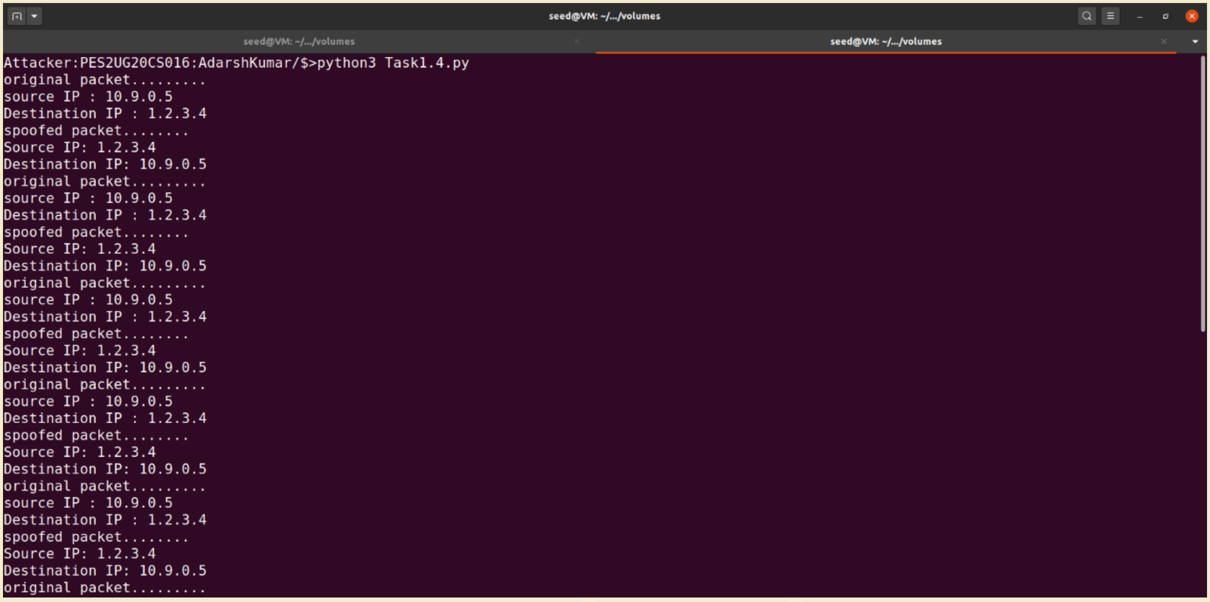

When we try to ping the destination of packet length 72 byes time to live was exceeded that indicates that IP is currently not reachable.

| Task 1.4 | Sniffing and-then Spoofing |
|---|---|
| Output Screenshot | From Host A: |

```
HostA:PES2UG20CS016:AdarshKumar/$>ls
bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
HostA:PES2UG20CS016:AdarshKumar/$>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=1 ttl=64 time=58.5 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=25.4 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=18.5 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=16.5 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=15.5 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=19.6 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=64 time=13.3 ms
64 bytes from 1.2.3.4: icmp_seq=8 ttl=64 time=23.3 ms
64 bytes from 1.2.3.4: icmp_seq=9 ttl=64 time=24.3 ms
64 bytes from 1.2.3.4: icmp_seq=10 ttl=64 time=16.5 ms
^C
--- 1.2.3.4 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9020ms
rtt min/avg/max/mdev = 13.326/23.155/58.509/12.381 ms
HostA:PES2UG20CS016:AdarshKumar/$>
```

Host-A trying to ping a non-existing IP address 1.2.3.4 and still getting response message.
10 packets transmitted and 10 packet received.

## On Attacker Terminal:

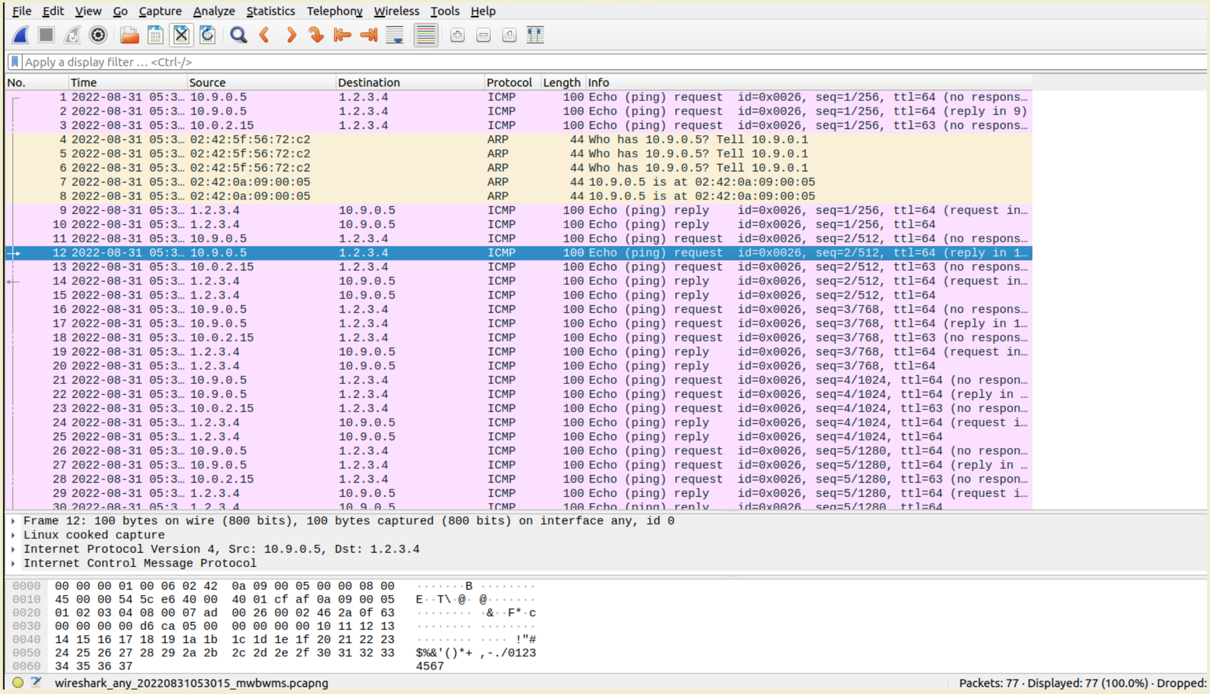


```
Attacker:PES2UG20CS016:AdarshKumar/$>python3 Task1.4.py
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
source IP : 10.9.0.5
Destination IP : 1.2.3.4
spoofed packet........
Source IP: 1.2.3.4
Destination IP: 10.9.0.5
original packet.........
```

## Observation:

When the Host-A try to ping some imaginary IP address our program sniff that packet and create an Echo-reply packet with the source address of that imaginary IP address and send back to host-A.

## Wireshark:



```
No.  Time                Source              Destination  Protocol Length Info
   1 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=1/256, ttl=64 (no respons…
   2 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=1/256, ttl=64 (reply in 9)
   3 2022-08-31 05:3… 10.0.2.15           1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=1/256, ttl=63 (no respons…
   4 2022-08-31 05:3… 02:42:5f:56:72:c2                ARP       44 Who has 10.9.0.5? Tell 10.9.0.1
   5 2022-08-31 05:3… 02:42:5f:56:72:c2                ARP       44 Who has 10.9.0.5? Tell 10.9.0.1
   6 2022-08-31 05:3… 02:42:5f:56:72:c2                ARP       44 Who has 10.9.0.5? Tell 10.9.0.1
   7 2022-08-31 05:3… 02:42:0a:09:00:05                ARP       44 10.9.0.5 is at 02:42:0a:09:00:05
   8 2022-08-31 05:3… 02:42:0a:09:00:05                ARP       44 10.9.0.5 is at 02:42:0a:09:00:05
   9 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=1/256, ttl=64 (request in…
  10 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=1/256, ttl=64
  11 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=2/512, ttl=64 (no respons…
  12 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=2/512, ttl=64 (reply in 1…
  13 2022-08-31 05:3… 10.0.2.15           1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=2/512, ttl=63 (no respons…
  14 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=2/512, ttl=64 (request in…
  15 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=2/512, ttl=64
  16 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=3/768, ttl=64 (no respons…
  17 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=3/768, ttl=64 (reply in 1…
  18 2022-08-31 05:3… 10.0.2.15           1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=3/768, ttl=63 (no respons…
  19 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=3/768, ttl=64 (request in…
  20 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=3/768, ttl=64
  21 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=4/1024, ttl=64 (no respon…
  22 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=4/1024, ttl=64 (reply in …
  23 2022-08-31 05:3… 10.0.2.15           1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=4/1024, ttl=63 (no respon…
  24 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=4/1024, ttl=64 (request i…
  25 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=4/1024, ttl=64
  26 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=5/1280, ttl=64 (no respon…
  27 2022-08-31 05:3… 10.9.0.5            1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=5/1280, ttl=64 (reply in …
  28 2022-08-31 05:3… 10.0.2.15           1.2.3.4      ICMP     100 Echo (ping) request  id=0x0026, seq=5/1280, ttl=63 (no respon…
  29 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=5/1280, ttl=64 (request i…
  30 2022-08-31 05:3… 1.2.3.4             10.9.0.5     ICMP     100 Echo (ping) reply    id=0x0026, seq=5/1280, ttl=64

› Frame 12: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 10.9.0.5, Dst: 1.2.3.4
› Internet Control Message Protocol

0000  00 00 00 01 00 06 02 42  0a 09 00 05 00 00 08 00   ·······B ········
0010  45 00 00 54 5c e6 40 00  40 01 cf af 0a 09 00 05   E··T\·@· @·······
0020  01 02 03 04 08 00 07 ad  00 26 00 02 46 2a 0f 63   ········ ·&··F*·c
0030  00 00 00 00 d6 ca 05 00  00 00 00 00 10 11 12 13   ········ ········
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ········ ···· !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
0060  34 35 36 37                                        4567

wireshark_any_20220831053015_mwbwms.pcapng          Packets: 77 · Displayed: 77 (100.0%) · Dropped:
```

ICMP Echo request message was sent by the Source 10.9.0.5 to destination 1.2.3.4 even the destination doesn’t exist but we can see that ICMP ECHO reply message is send from 1.2.3.4 to host-A which is clearly a spoofed packet.

THANKING YOU