

CNS LAB 1

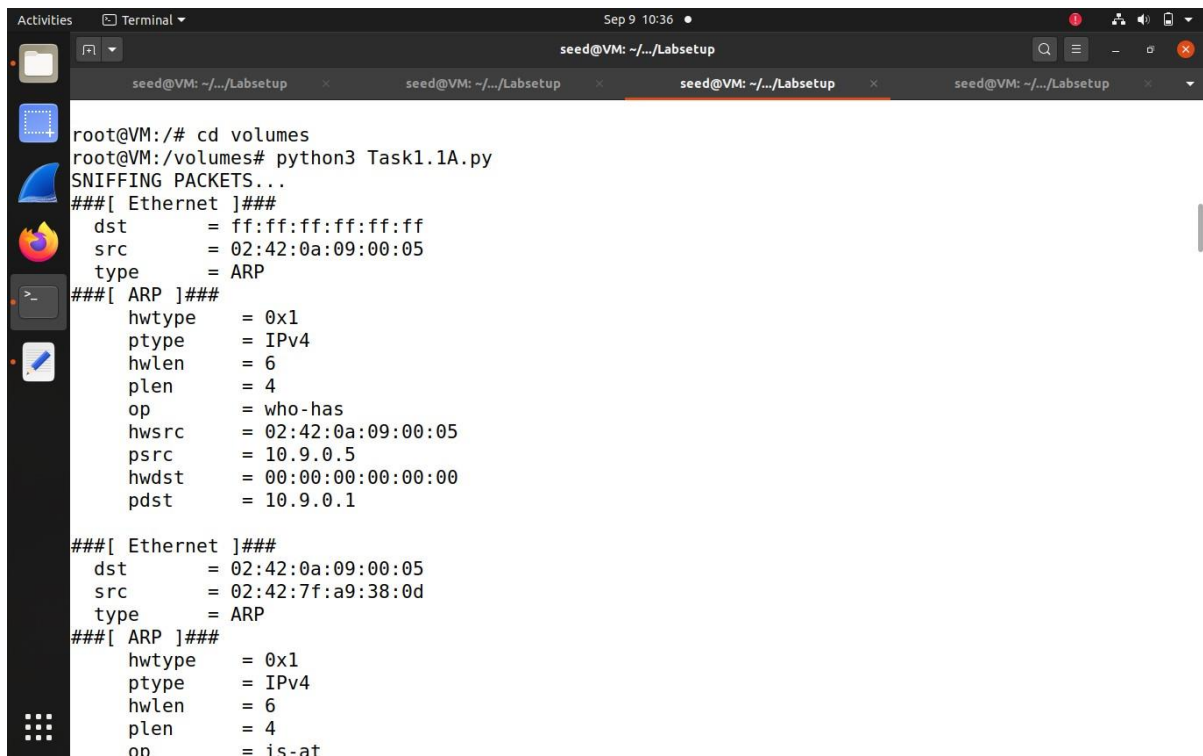
NAME: NAVYA PERAM

SEC: F

SRN: PES1UG21CS924

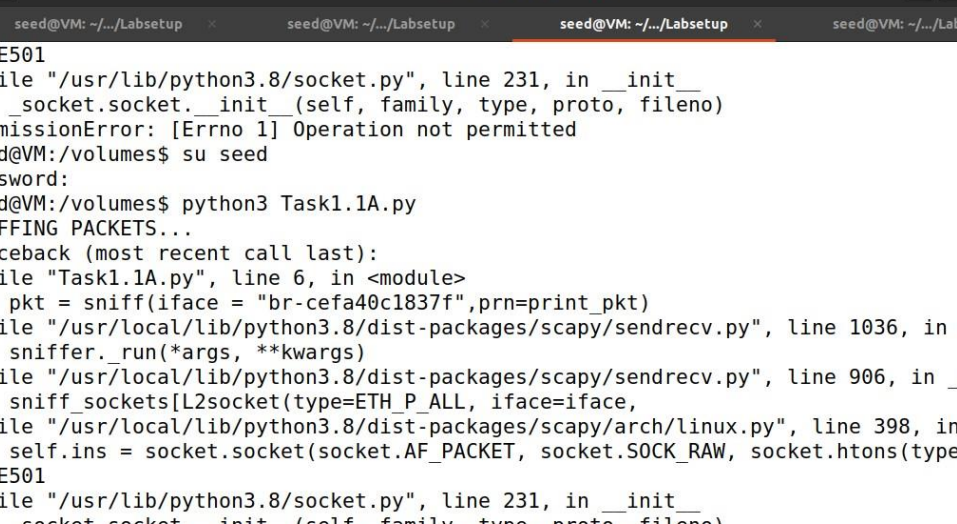
TASK 1.1 A

The host sent and received packets in this process. The attacker system was able to sniff the packets sent and received by the hostA and was able to extract the information. The show() function printed the layers and fields of the packets sent and received. The packets in the br interface were captured and the print_pkt callback function is called.

A screenshot of a terminal window titled 'Terminal' with a date and time of 'Sep 9 10:36'. The terminal shows a series of commands and their outputs. The user is in a VM named 'seed@VM' and has navigated to the '/volumes' directory. They run 'python3 Task1.1A.py', which outputs 'SNIFFING PACKETS...'. The output shows two captured packets. The first packet is an ARP request from 10.9.0.5 to 10.9.0.1. The second packet is an ARP response from 10.9.0.1 to 10.9.0.5. The terminal window has a dark theme and a sidebar with application icons on the left.

```
root@VM:/# cd volumes
root@VM:/volumes# python3 Task1.1A.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst      = ff:ff:ff:ff:ff:ff
  src      = 02:42:0a:09:00:05
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hwlen    = 6
  plen     = 4
  op       = who-has
  hwsrc    = 02:42:0a:09:00:05
  psrc     = 10.9.0.5
  hwdst    = 00:00:00:00:00:00
  pdst     = 10.9.0.1
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:7f:a9:38:0d
  type     = ARP
###[ ARP ]###
  hwtype   = 0x1
  ptype    = IPv4
  hwlen    = 6
  plen     = 4
  op       = is-at
```


In this process, the root privileges were removed. Without root privileges the packets cannot be captured due to the privacy and security risks. To be able to prevent unauthorized users from flooding the network with malicious programs or packets, we need use root privileges. Unless we do so, the program won't be able to access a raw socket or put the interface in a promiscuous mode. Hence in the given process, the operation was not permitted.



The screenshot shows a terminal window with a dark theme. The title bar at the top reads "Activities" on the left and "Terminal" in the center, with a system clock on the right showing "Sep 9 11:37". The terminal window has a tab titled "seed@VM: ~/.../Labsetup". The command prompt is "seed@VM: ~/.../Labsetup". The user has entered the command "python3 Task1.1A.py". The output shows a "PermissionError: [Errno 1] Operation not permitted" message. The user then enters "su seed" and "Password:", but the prompt changes to "seed@VM:/volumes\$". The user then enters "python3 Task1.1A.py" again, and the output shows a "Traceback (most recent call last):" message, followed by the same "PermissionError: [Errno 1] Operation not permitted" message. The user then enters "a: E501" and the output shows a "File \"/usr/lib/python3.8/socket.py\", line 231, in __init__" message, followed by the same "PermissionError: [Errno 1] Operation not permitted" message. The user then enters "a: E501" again and the output shows a "File \"/usr/lib/python3.8/socket.py\", line 231, in __init__" message, followed by the same "PermissionError: [Errno 1] Operation not permitted" message. The user then enters "seed@VM:/volumes\$" and the prompt changes to "seed@VM:/volumes\$".

```

seed@VM: ~/.../Labsetup
a: 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
seed@VM:/volumes$ su seed
Password:
seed@VM:/volumes$ python3 Task1.1A.py
SNIFFING PACKETS...
Traceback (most recent call last):
  File "Task1.1A.py", line 6, in <module>
    pkt = sniff(iface = "br-cefa40c1837f",prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in _run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  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(type)) # noq
a: 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
seed@VM:/volumes$

```

TASK 1.1B

ICMP

We applied an ICMP filter in the given process, only the ICMP packets sent and received were captured. It is completely similar to the first process with the attacker sniffing the packets, but only specified to the ICMP ones.

![Screenshot of a Kali Linux terminal window showing the execution of a task. The terminal displays the output of a Python script that captures and displays ICMP packet details. The output shows the packet type (echo-reply), code (0), checksum (0x9d19), ID (0x1f), and sequence (0x11). It also shows the raw packet data in hexadecimal and ASCII. The terminal window has a title bar with 'Activities', 'Terminal', and 'Sep 9 11:59'. The terminal output is as follows: seed@VM: ~/.._Labsetup seed@VM: ~/.._Labsetup seed@VM: ~/.._Labsetup seed@VM: ~/.._Labsetup ###[ICMP]### type = echo-reply code = 0 chksum = 0x9d19 id = 0x1f seq = 0x11 ###[Raw]### load = '\x84\x92\xfd\x00\x00\x00\x00\xec\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !\](10.9.0.5)

```
Activities Terminal Sep 9 11:59
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
^Cseed-attacker:PE51UG21CS924:Navya:/volumes
$>python3 Task1.1B-ICMP.py
SNIFFING PACKETS...
###[ Ethernet ]###
dst      = 02:42:9f:11:cd:26
src      = 02:42:0a:09:00:05
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 15
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x207d
src      = 10.9.0.5
dst      = 8.8.8.8
\options \
###[ ICMP ]###
type     = echo-request
```

```
Activities Terminal Sep 9 11:59
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
type     = echo-request
code     = 0
chksum   = 0x5e96
id       = 0x20
seq      = 0x1
###[ Raw ]###
load     = '\xe3\x95\xfd\x00\x00\x00\x00\xf9z\x01\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"%$%&'()*+,-./01234567'
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:9f:11:cd:26
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x18
len      = 84
id       = 24552
flags    =
frag     = 0
ttl      = 115
proto    = icmp
chksum   = 0xcd8b
src      = 8.8.8.8
dst      = 10.9.0.5
\options \
###[ ICMP ]###
type     = echo-reply
code     = 0
chksum   = 0x6696
id       = 0x20
```

```

Activities Terminal Sep 9 11:59
seed@VM: ~/.../Labsetup
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=27.7 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=93.0 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=115 time=28.4 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=115 time=27.9 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=115 time=27.4 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=115 time=25.9 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=115 time=28.5 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=115 time=30.2 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=115 time=28.9 ms
^C
--- 8.8.8.8 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16046ms
rtt min/avg/max/mdev = 25.899/32.329/93.047/15.230 ms
hostA: PES1UG21CS924:Navya:/
$>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=115 time=26.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=27.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=26.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=27.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=115 time=26.4 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=43.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=123 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=115 time=59.1 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=115 time=26.6 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=115 time=27.2 ms
^C
--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9037ms
rtt min/avg/max/mdev = 26.007/41.296/122.609/28.975 ms
hostA: PES1UG21CS924:Navya:/
$>

```

TCP

Here, all the packets going from host A to Telnet(the destination port) on the attackers system are captured. Telnet provides remote access, which allows us to access and extract the username and the password used by the host machine in the above process. This can be seen in the load parameter.

```

Activities Terminal Sep 9 12:17
seed@VM: ~/.../Labsetup
options = [('NOP', None), ('NOP', None), ('Timestamp', (1268295056, 2856592998))]

^Cseed-attacker: PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-TCP.py
SNIFFING PACKETS...
###[ Ethernet ]###
dst      = 02:42:9f:11:cd:26
src      = 02:42:0a:09:00:05
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x10
len      = 60
id       = 15511
flags    = DF
frag     = 0
ttl      = 64
proto    = tcp
chksum   = 0xe9fd
src       = 10.9.0.5
dst       = 10.9.0.1
\options \
###[ TCP ]###
sport    = 55518
dport    = telnet
seq      = 3258275258
ack      = 0
dataoffs = 10
reserved = 0
flags    = S
window   = 64240

```



```
Activities Terminal Sep 9 12:17
seed@VM: ~/.../Labsetup

chksum = 0x1446
urgptr = 0
options = [('MSS', 1460), ('SackOK', b''), ('Timestamp', (1268320870, 0)), ('NOP', None), ('WScale', 7)]

###[ Ethernet ]###
dst = 02:42:9f:11:cd:26
src = 02:42:0a:09:00:05
type = IPv4

###[ IP ]###
version = 4
ihl = 5
tos = 0x10
len = 52
id = 15512
flags = DF
frag = 0
ttl = 64
proto = tcp
chksum = 0xea04
src = 10.9.0.5
dst = 10.9.0.1
\options \

###[ TCP ]###
sport = 55518
dport = telnet
seq = 3258275259
ack = 1360779263
dataofs = 8
reserved = 0
flags = A
window = 502
chksum = 0x143e
```

```
Activities Terminal Sep 9 12:17
seed@VM: ~/.../Labsetup

urgptr = 0
options = [('NOP', None), ('NOP', None), ('Timestamp', (1268320870, 2856618812))]

###[ Ethernet ]###
dst = 02:42:9f:11:cd:26
src = 02:42:0a:09:00:05
type = IPv4

###[ IP ]###
version = 4
ihl = 5
tos = 0x10
len = 76
id = 15513
flags = DF
frag = 0
ttl = 64
proto = tcp
chksum = 0xe9eb
src = 10.9.0.5
dst = 10.9.0.1
\options \

###[ TCP ]###
sport = 55518
dport = telnet
seq = 3258275259
ack = 1360779263
dataofs = 8
reserved = 0
flags = PA
window = 502
chksum = 0x1456
urgptr = 0
```

```
Activities Terminal Sep 9 12:17
seed@VM: ~/.../Labsetup

64 bytes from 8.8.8.8: icmp_seq=6 ttl=115 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=115 time=26.6 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 26.326/54.658/116.513/39.046 ms
hostA:PES1UG21CS924:Navya:/
$>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: dees
Password:
^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>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:

Login incorrect
VM login: SEED
Password:

Login incorrect
VM login: ^CConnection closed by foreign host.
hostA:PES1UG21CS924:Navya:/
$>
```

Subnet

The packets with the given source subnet are captured. This refers to the fact that only the response packets are captured, unlike the previous methods where both the response and request are captured. Here, the request packages are not captured as Host A is in a different subnet.

```
Activities Terminal Sep 9 12:58
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
$>cd volumes/
seed-attacker:PES1UG21CS924:Navya:/volumes
$>python3 Task1.1B-Subnet.py
SNIFFING PACKETS...
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:96:c0:28:d2
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 64449
  flags    =
  frag     = 0
  ttl      = 51
  proto    = icmp
  chksum   = 0x71ca
  src      = 8.8.8.8
  dst      = 10.9.0.5
  \options \
###[ ICMP ]###
```

```
Activities Terminal Sep 9 12:59
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
seed@VM: ~/.../Labsetup
  \options \
###[ ICMP ]###
  type     = echo-reply
  code     = 0
  chksum   = 0xca20
  id       = 0x2c
  seq      = 0x1
###[ Raw ]###
  load     = '$\xa4\xfd\x00\x00\x00\x00J\xd6\x0b\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\'()*+,-./01234567'
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:96:c0:28:d2
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 64450
  flags    =
  frag     = 0
```

```

Sep 9 12:59
seed@VM: ~/../Labsetup

###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:96:c0:28:d2
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 64450
flags    =
frag     = 0
ttl      = 51
proto    = icmp
chksum   = 0x71c9
src      = 8.8.8.8
dst      = 10.9.0.5
\options \
###[ ICMP ]###
type     = echo-reply
code     = 0
chksum   = 0x8418
id       = 0x2c
seq      = 0x2
###[ Raw ]###
load     = '\xa4\xcd\x00\x00\x00\x00\x8f\xdd\x0b\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&'()*+,-./01234567'
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:96:c0:28:d2

```

```

Sep 9 12:59
seed@VM: ~/../Labsetup

64 bytes from 8.8.8.8: icmp_seq=8 ttl=51 time=96.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=51 time=122 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=51 time=62.8 ms
^C
--- 8.8.8.8 ping statistics ---
11 packets transmitted, 10 received, 9.09091% packet loss, time 10019ms
rtt min/avg/max/mdev = 62.788/119.445/240.534/57.013 ms
host A: PES1UG21CS924:Navya:/
$> 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=51 time=182 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=59.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=73.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=51 time=191 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=51 time=292 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=51 time=317 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=51 time=43.1 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=51 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=51 time=49.9 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=51 time=74.8 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=51 time=121 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=51 time=238 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=51 time=79.7 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=51 time=488 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=51 time=72.6 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=51 time=331 ms
^C
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15034ms
rtt min/avg/max/mdev = 43.093/167.978/488.431/127.249 ms
host A: PES1UG21CS924:Navya:/
$>

```

TASK 1.2

An ICMP request packet is spoofed with a source IP address of 10.9.0.1 and sent to the Host A machine with the destination IP of 10.9.0.5. The request is then accepted by the host A and a reply is sent to the spoofed IP address.

Activities Wireshark Sep 9 13:04

[SEED Labs] Capturing from br-cefa40c1837f

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
4	2023-09-09 13:0...	02:42:96:c0:28:d2	Broadcast	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
5	2023-09-09 13:0...	02:42:0a:09:00:05	02:42:96:c0:28:d2	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
6	2023-09-09 13:0...	10.9.0.1	10.9.0.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64
7	2023-09-09 13:0...	10.9.0.5	10.9.0.1	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64
8	2023-09-09 13:0...	02:42:0a:09:00:05	02:42:96:c0:28:d2	ARP	42	Who has 10.9.0.1? Tell 10.9.0.5
9	2023-09-09 13:0...	02:42:96:c0:28:d2	02:42:0a:09:00:05	ARP	42	10.9.0.1 is at 02:42:96:c0:28:d2

Frame 1: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface br-cefa40c1837f, id 0

- Ethernet II, Src: 02:42:96:c0:28:d2 (02:42:96:c0:28:d2), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
- Internet Protocol Version 6, Src: fe80::42:96ff:fec0:28d2, Dst: ff02::fb
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)

0000 33 33 00 00 00 fb 02 42 96 c0 28 d2 86 dd 60 00 33B ..(...
0010 d0 43 00 7e 11 ff fe 80 00 00 00 00 00 00 00 42 -C-.....B
0020 96 ff fe c0 28 d2 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 5f 74 63 70 85 c6 6f 63 61 6c 00 00 0c 00 01 04 _tcp_loc al.....

br-cefa40c1837f: <live capture in progress> Packets: 9 · Displayed: 9 (100.0%) Profile: Default

Activities Terminal Sep 9 13:05

seed@VM: ~/LabSetup

```

seed-attacker: PES1UG21CS924:Navya:/volumes
$>cd volumes
bash: cd: volumes: No such file or directory
seed-attacker: PES1UG21CS924:Navya:/volumes
$>python Task1.2A.py
bash: python: command not found
seed-attacker: PES1UG21CS924:Navya:/volumes
$>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

```

seed-attacker: PES1UG21CS924:Navya:/volumes
\$>

Activities Wireshark Sep 9 13:05

[SEED Labs] Capturing from br-cefa40c1837f

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-09-09 13:0...	fe80::42:96ff:fec0:28d2	ff02::fb	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
2	2023-09-09 13:0...	10.9.0.1	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
3	2023-09-09 13:0...	10.9.0.1	224.0.0.251	MDNS	87	Standard query 0x0000 PTR _lpps._tcp.local, "QM" question PTR
4	2023-09-09 13:0...	02:42:96:c0:28:d2	Broadcast	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
5	2023-09-09 13:0...	02:42:0a:09:00:05	02:42:96:c0:28:d2	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
6	2023-09-09 13:0...	10.9.0.1	10.9.0.5	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (reply in 7)
7	2023-09-09 13:0...	10.9.0.5	10.9.0.1	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 6)
8	2023-09-09 13:0...	02:42:0a:09:00:05	02:42:96:c0:28:d2	ARP	42	Who has 10.9.0.1? Tell 10.9.0.5
9	2023-09-09 13:0...	02:42:96:c0:28:d2	02:42:0a:09:00:05	ARP	42	10.9.0.1 is at 02:42:96:c0:28:d2
10	2023-09-09 13:0...	fe80::42:96ff:fec0:28d2	ff02::fb	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR
11	2023-09-09 13:0...	10.9.0.1	224.0.0.251	MDNS	160	Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR

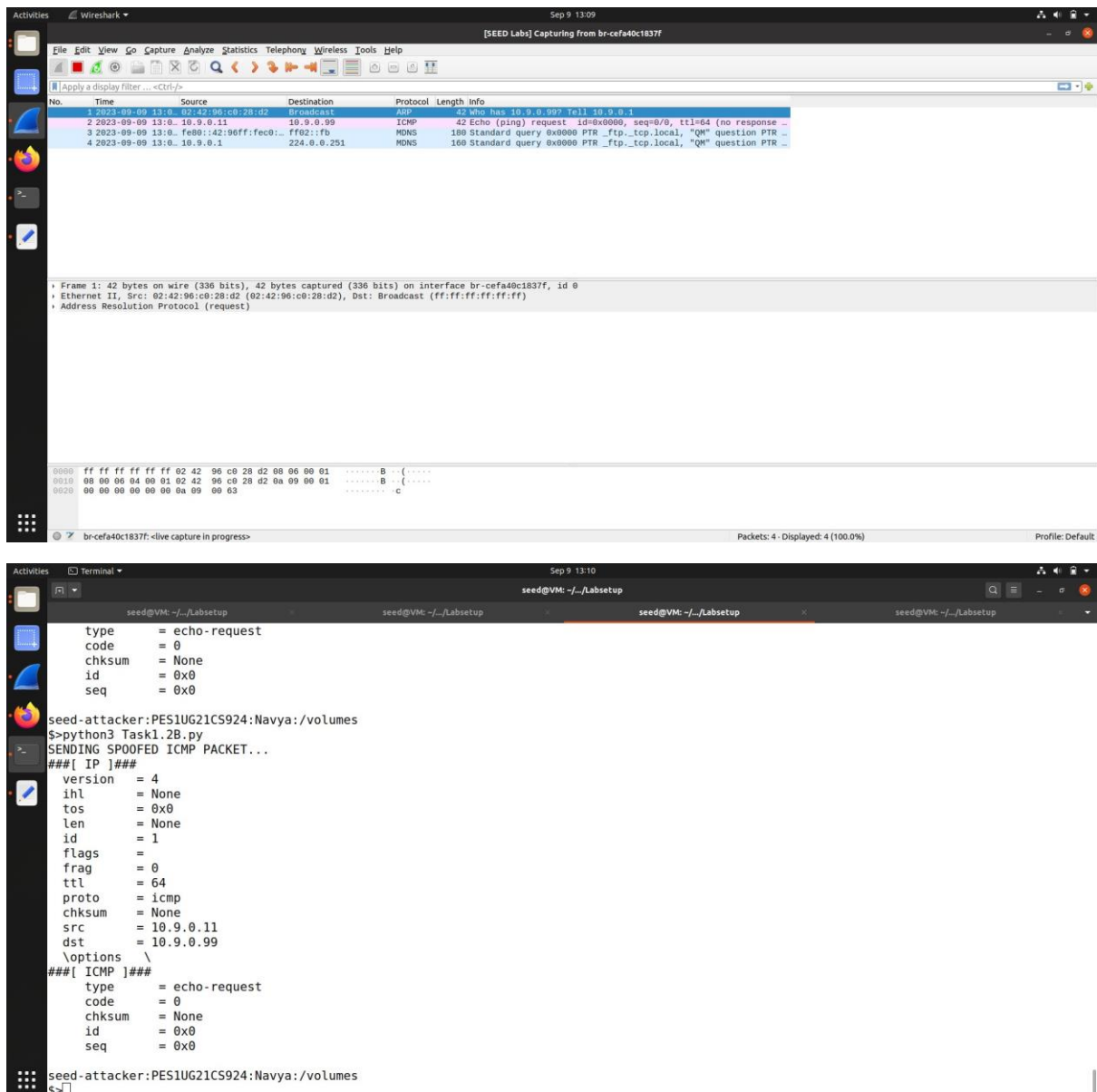
Frame 1: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface br-cefa40c1837f, id 0

- Ethernet II, Src: 02:42:96:c0:28:d2 (02:42:96:c0:28:d2), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
- Internet Protocol Version 6, Src: fe80::42:96ff:fec0:28d2, Dst: ff02::fb
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
- Multicast Domain Name System (query)

0000 33 33 00 00 00 fb 02 42 96 c0 28 d2 86 dd 60 00 33B ..(...
0010 d0 43 00 7e 11 ff fe 80 00 00 00 00 00 00 00 42 -C-.....B
0020 96 ff fe c0 28 d2 ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050 5f 74 63 70 85 c6 6f 63 61 6c 00 00 0c 00 01 04 _tcp_loc al.....

br-cefa40c1837f: <live capture in progress> Packets: 11 · Displayed: 11 (100.0%) Profile: Default

If the destination IP doesn't exist then no reply is sent to the request.



The top screenshot shows a Wireshark capture from interface br-cefa40c1837f. The packet list shows four packets: 1. ICMP Echo (ping) request from 10.9.0.11 to 10.9.0.99, 2. ICMP Echo (ping) request from 10.9.0.11 to 10.9.0.99, 3. MDNS Standard query from fe80::42:96ff:fec0::2 to ff02::fb, and 4. MDNS Standard query from 10.9.0.1 to 224.0.0.251. The packet details pane shows the first packet as an ICMP Echo (ping) request with id=0x0000, seq=0/0, ttl=64, and no response. The packet bytes pane shows the raw data of the first packet.

The bottom screenshot shows a terminal window with the following output:

```
seed@VM: ~/Labsetup
type      = echo-request
code      = 0
chksum    = None
id        = 0x0
seq       = 0x0

seed-attacker: PES1UG21CS924: Navya: /volumes
$>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: PES1UG21CS924: Navya: /volumes
$>
```

Task 1.3

The given process captures the number of hops that occur between the host machine and the destination IP given by the user, along with source IP of the captured packet. In the given code the time to live is given as 1. The ttl is however exceeded as seen in the wireshark.

Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	10.0.2.4	216.58.196.161	TLSv1.2	95 Application Data
2	0.000869787	10.0.2.4	216.58.196.161	TLSv1.2	80 Application Data
3	0.001091107	10.0.2.4	216.58.196.161	TCP	56 44854 → 443 [FIN, ACK] Seq=64 Ack=1 Win=62780 Len=0
4	0.001700067	216.58.196.161	10.0.2.4	TCP	62 443 → 44854 [ACK] Seq=1 Ack=64 Win=32344 Len=0
5	0.001700449	216.58.196.161	10.0.2.4	TCP	62 443 → 44854 [ACK] Seq=1 Ack=65 Win=32343 Len=0
6	0.043553710	216.58.196.161	10.0.2.4	TCP	62 443 → 44854 [FIN, ACK] Seq=1 Ack=65 Win=32343 Len=0
7	0.043735936	10.0.2.4	216.58.196.161	TCP	56 44854 → 443 [ACK] Seq=65 Ack=2 Win=62780 Len=0
8	1.895021237	10.0.2.4	142.250.183.238	TLSv1.2	95 Application Data
9	1.902265941	142.250.183.238	10.0.2.4	TCP	62 443 → 41210 [ACK] Seq=1 Ack=40 Win=32690 Len=0
10	2.199768202	142.250.183.238	10.0.2.4	TLSv1.2	95 Application Data
11	2.199843920	10.0.2.4	142.250.183.238	TCP	56 41210 → 443 [ACK] Seq=40 Ack=40 Win=63714 Len=0
12	2.896691156	127.0.0.1	127.0.0.53	DNS	77 Standard query 0xfcd8 A ssl.gstatic.com
13	2.896743887	127.0.0.1	127.0.0.53	DNS	77 Standard query 0x3fd7 AAAA ssl.gstatic.com
14	2.899831409	10.0.2.4	8.8.8.8	DNS	88 Standard query 0x6252 A ssl.gstatic.com OPT
15	2.900266696	10.0.2.4	8.8.8.8	DNS	88 Standard query 0x287e AAAA ssl.gstatic.com OPT
16	2.905347042	10.0.2.4	142.250.193.99	TLSv1.2	146 Application Data
17	2.909580726	142.250.193.99	10.0.2.4	TCP	62 443 → 57976 [ACK] Seq=1 Ack=91 Win=31588 Len=0
18	3.153705697	142.250.193.99	10.0.2.4	TLSv1.2	264 Application Data, Application Data
19	3.153706252	8.8.8.8	10.0.2.4	DNS	104 Standard query response 0x6252 A ssl.gstatic.com A 142.250.19...
20	3.153706388	8.8.8.8	10.0.2.4	DNS	116 Standard query response 0x287e AAAA ssl.gstatic.com AAAA 2404...
21	3.155110371	10.0.2.4	142.250.193.99	TLSv1.2	95 Application Data
22	3.159812580	127.0.0.53	127.0.0.1	DNS	93 Standard query response 0xfcd8 A ssl.gstatic.com A 142.250.19...
23	3.160164036	127.0.0.53	127.0.0.1	DNS	105 Standard query response 0x3fd7 AAAA ssl.gstatic.com AAAA 2404...
24	3.162110209	142.250.193.99	10.0.2.4	TCP	62 443 → 57976 [ACK] Seq=209 Ack=130 Win=31549 Len=0
25	4.585643876	PcsCompu_ff:ba:5e		ARP	44 Who has 10.0.2.1? Tell 10.0.2.4
26	4.586143403	RealtekU_12:35:00		ARP	62 10.0.2.1 is at 52:54:00:12:35:00
27	4.612521324	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response f...
28	4.613025972	10.0.2.1	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
29	4.661895325	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response f...
30	4.688729348	10.30.200.1	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
31	4.737477501	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=3 (no response f...
32	4.768521728	192.168.4.1	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
33	4.826583840	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response f...
34	4.874277165	192.168.254.1	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
35	4.918148267	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response f...
36	5.117920308	14.143.35.157	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
37	5.179185499	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=6 (no response f...
38	5.221075183	172.29.251.33	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
39	5.285823623	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=7 (no response f...
40	5.366536398	180.87.36.9	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
41	5.422433490	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response f...
42	5.461821292	180.87.36.95	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
43	5.509134213	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=9 (no response f...
44	5.556890119	129.134.34.179	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
45	5.594523739	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=10 (no response ...
46	5.621116412	157.240.38.179	10.0.2.4	ICMP	72 Time-to-live exceeded (Time to live exceeded in transit)
47	5.695507177	10.0.2.4	157.240.23.35	ICMP	44 Echo (ping) request id=0x0000, seq=0/0, ttl=11 (reply in 48)
48	5.740327650	157.240.23.35	10.0.2.4	ICMP	62 Echo (ping) reply id=0x0000, seq=0/0, ttl=54 (request in 4...
49	10.001715178	10.0.2.4	142.250.195.78	TLSv1.2	95 Application Data
50	10.002611607	10.0.2.4	142.250.195.78	TLSv1.2	80 Application Data
51	10.002692309	10.0.2.4	142.250.195.78	TCP	56 49146 → 443 [FIN, ACK] Seq=64 Ack=1 Win=63714 Len=0
52	10.003462336	142.250.195.78	10.0.2.4	TCP	62 443 → 49146 [ACK] Seq=1 Ack=64 Win=32588 Len=0
53	10.003462710	142.250.195.78	10.0.2.4	TCP	62 443 → 49146 [ACK] Seq=1 Ack=65 Win=32587 Len=0
54	10.055156575	142.250.195.78	10.0.2.4	TCP	62 443 → 49146 [FIN, ACK] Seq=1 Ack=65 Win=32587 Len=0
55	10.055326226	10.0.2.4	142.250.195.78	TCP	56 49146 → 443 [ACK] Seq=65 Ack=2 Win=63714 Len=0

```

Activities  Terminal  Sep 9 13:10
seed@VM: ~/./Labsetup
seed-attacker: PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
 1 hops away: 10.0.2.1
 2 hops away: 172.16.20.1
 3 hops away: 119.226.103.130
 4 hops away: 100.70.137.135
 5 hops away: 100.70.137.119
 6 hops away: 172.31.180.57
 7 hops away: 180.87.36.9
 8 hops away: 180.87.36.95
 9 hops away: 129.134.34.175
10 hops away: 173.252.67.19
11 hops away: 157.240.23.35
Done 157.240.23.35
seed-attacker: PES1UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
 1 hops away: 10.0.2.1
 2 hops away: 172.16.20.1
 3 hops away: 119.226.103.130
 4 hops away: 100.70.137.135
 5 hops away: 100.70.137.119
 6 hops away: 172.31.180.57
 7 hops away: 180.87.36.9
 8 hops away: 180.87.36.95
 9 hops away: 129.134.34.175
10 hops away: 173.252.67.19
11 hops away: 157.240.23.35
Done 157.240.23.35
seed-attacker: PES1UG21CS924:Navya:/volumes
$>

```

Task 1.4

In the given process, the Host A pings a non-existent IP address and since the attacker is also present on the same network, it is able to sniff the packets. However, the specifications applied are that only the ICMP packets with the source IP of 10.9.0.5 are to be captured. The reply is then spoofed by the attacker based on the information gathered from the sniffed packets. This in turn makes the host machine assume that the replies were sent by the IP it pinged.

```
Activities Terminal Sep 9 13:23
seed@VM: ~/Labsetup
~C
--- 8.8.8.8 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15034ms
rtt min/avg/max/mdev = 43.093/167.978/488.431/127.249 ms
host A: PES1UG21CS924:Navya:/
$> 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=53.4 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=15.7 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=17.4 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=28.3 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=24.2 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=64 time=18.9 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=64 time=19.7 ms
64 bytes from 1.2.3.4: icmp_seq=8 ttl=64 time=20.0 ms
64 bytes from 1.2.3.4: icmp_seq=9 ttl=64 time=19.8 ms
64 bytes from 1.2.3.4: icmp_seq=10 ttl=64 time=18.8 ms
64 bytes from 1.2.3.4: icmp_seq=11 ttl=64 time=24.8 ms
64 bytes from 1.2.3.4: icmp_seq=12 ttl=64 time=19.9 ms
64 bytes from 1.2.3.4: icmp_seq=13 ttl=64 time=17.6 ms
64 bytes from 1.2.3.4: icmp_seq=14 ttl=64 time=15.0 ms
64 bytes from 1.2.3.4: icmp_seq=15 ttl=64 time=25.6 ms
64 bytes from 1.2.3.4: icmp_seq=16 ttl=64 time=20.3 ms
64 bytes from 1.2.3.4: icmp_seq=17 ttl=64 time=21.4 ms
64 bytes from 1.2.3.4: icmp_seq=18 ttl=64 time=23.7 ms
64 bytes from 1.2.3.4: icmp_seq=19 ttl=64 time=21.1 ms
~C
--- 1.2.3.4 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18057ms
rtt min/avg/max/mdev = 14.973/22.399/53.381/8.019 ms
host A: PES1UG21CS924:Navya:/
$>
```

```
Activities Wireshark Sep 9 13:22
Capturing from br-cefa40c1837f

No. Time Source Destination Protocol Length Info
1 0.000000 10.9.0.5 10.9.0.5 Broadcast ARP 42 Who has 10.9.0.5? (11:11:11)
2 0.000000 02:42:96:c0:28:d2 02:42:96:c0:28:d2 ARP 42 10.9.0.5 is at 02:42:96:c0:28:d2
3 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=1/254, ttl=64 (request in 4)
4 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=2/512, ttl=64 (reply in 6)
5 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=3/768, ttl=64 (request in 8)
6 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=4/1024, ttl=64 (reply in 10)
7 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=5/1280, ttl=64 (request in 12)
8 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=6/1536, ttl=64 (reply in 14)
9 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=7/1792, ttl=64 (request in 16)
10 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=8/2048, ttl=64 (reply in 18)
11 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=9/2304, ttl=64 (request in 20)
12 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=10/2560, ttl=64 (reply in 22)
13 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=11/2816, ttl=64 (request in 24)
14 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=12/3072, ttl=64 (reply in 26)
15 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=13/3328, ttl=64 (request in 28)
16 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=14/3584, ttl=64 (reply in 30)
17 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=15/3840, ttl=64 (request in 32)
18 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=16/4096, ttl=64 (reply in 34)
19 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=17/4352, ttl=64 (request in 36)
20 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=18/4608, ttl=64 (reply in 38)
21 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=19/4864, ttl=64 (request in 40)
22 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=20/5120, ttl=64 (reply in 42)
23 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=21/5376, ttl=64 (request in 44)
24 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=22/5632, ttl=64 (reply in 46)
25 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=23/5888, ttl=64 (request in 48)
26 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=24/6144, ttl=64 (reply in 50)
27 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=25/6400, ttl=64 (request in 52)
28 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=26/6656, ttl=64 (reply in 54)
29 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=27/6912, ttl=64 (request in 56)
30 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=28/7168, ttl=64 (reply in 58)
31 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=29/7424, ttl=64 (request in 60)
32 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=30/7680, ttl=64 (reply in 62)
33 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=31/7936, ttl=64 (request in 64)
34 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=32/8192, ttl=64 (reply in 66)
35 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=33/8448, ttl=64 (request in 68)
36 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=34/8704, ttl=64 (reply in 70)
37 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=35/8960, ttl=64 (request in 72)
38 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=36/9216, ttl=64 (reply in 74)
39 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=37/9472, ttl=64 (request in 76)
40 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=38/9728, ttl=64 (reply in 78)
41 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=39/9984, ttl=64 (request in 80)
42 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=40/10240, ttl=64 (reply in 82)
43 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=41/10496, ttl=64 (request in 84)
44 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=42/10752, ttl=64 (reply in 86)
45 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=43/11008, ttl=64 (request in 88)
46 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=44/11264, ttl=64 (reply in 90)
47 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=45/11520, ttl=64 (request in 92)
48 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=46/11776, ttl=64 (reply in 94)
49 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=47/12032, ttl=64 (request in 96)
50 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=48/12288, ttl=64 (reply in 98)
51 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=49/12544, ttl=64 (request in 100)
52 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=50/12800, ttl=64 (reply in 102)
53 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=51/13056, ttl=64 (request in 104)
54 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=52/13312, ttl=64 (reply in 106)
55 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=53/13568, ttl=64 (request in 108)
56 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=54/13824, ttl=64 (reply in 110)
57 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=55/14080, ttl=64 (request in 112)
58 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=56/14336, ttl=64 (reply in 114)
59 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=57/14592, ttl=64 (request in 116)
60 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=58/14848, ttl=64 (reply in 118)
61 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=59/15104, ttl=64 (request in 120)
62 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=60/15360, ttl=64 (reply in 122)
63 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=61/15616, ttl=64 (request in 124)
64 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=62/15872, ttl=64 (reply in 126)
65 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=63/16128, ttl=64 (request in 128)
66 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=64/16384, ttl=64 (reply in 130)
67 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=65/16640, ttl=64 (request in 132)
68 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=66/16896, ttl=64 (reply in 134)
69 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=67/17152, ttl=64 (request in 136)
70 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=68/17408, ttl=64 (reply in 138)
71 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=69/17664, ttl=64 (request in 140)
72 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=70/17920, ttl=64 (reply in 142)
73 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=71/18176, ttl=64 (request in 144)
74 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=72/18432, ttl=64 (reply in 146)
75 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=73/18688, ttl=64 (request in 148)
76 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=74/18944, ttl=64 (reply in 150)
77 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=75/19200, ttl=64 (request in 152)
78 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=76/19456, ttl=64 (reply in 154)
79 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=77/19712, ttl=64 (request in 156)
80 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=78/19968, ttl=64 (reply in 158)
81 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=79/20224, ttl=64 (request in 160)
82 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=80/20480, ttl=64 (reply in 162)
83 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=81/20736, ttl=64 (request in 164)
84 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=82/21088, ttl=64 (reply in 166)
85 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=83/21344, ttl=64 (request in 168)
86 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=84/21600, ttl=64 (reply in 170)
87 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=85/21856, ttl=64 (request in 172)
88 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=86/22112, ttl=64 (reply in 174)
89 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=87/22368, ttl=64 (request in 176)
90 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=88/22624, ttl=64 (reply in 178)
91 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=89/22880, ttl=64 (request in 180)
92 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=90/23136, ttl=64 (reply in 182)
93 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=91/23392, ttl=64 (request in 184)
94 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=92/23648, ttl=64 (reply in 186)
95 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=93/23904, ttl=64 (request in 188)
96 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=94/24160, ttl=64 (reply in 190)
97 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=95/24416, ttl=64 (request in 192)
98 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=96/24672, ttl=64 (reply in 194)
99 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=97/24928, ttl=64 (request in 196)
100 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=98/25184, ttl=64 (reply in 198)
101 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=99/25440, ttl=64 (request in 200)
102 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=100/25696, ttl=64 (reply in 202)
103 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=101/25952, ttl=64 (request in 204)
104 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=102/26208, ttl=64 (reply in 206)
105 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=103/26464, ttl=64 (request in 208)
106 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=104/26720, ttl=64 (reply in 210)
107 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=105/26976, ttl=64 (request in 212)
108 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=106/27232, ttl=64 (reply in 214)
109 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=107/27488, ttl=64 (request in 216)
110 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=108/27744, ttl=64 (reply in 218)
111 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=109/28000, ttl=64 (request in 220)
112 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=110/28256, ttl=64 (reply in 222)
113 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=111/28512, ttl=64 (request in 224)
114 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=112/28768, ttl=64 (reply in 226)
115 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=113/29024, ttl=64 (request in 228)
116 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=114/29280, ttl=64 (reply in 230)
117 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=115/29536, ttl=64 (request in 232)
118 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=116/29792, ttl=64 (reply in 234)
119 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=117/30048, ttl=64 (request in 236)
120 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=118/30304, ttl=64 (reply in 238)
121 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=119/30560, ttl=64 (request in 240)
122 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=120/30816, ttl=64 (reply in 242)
123 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=121/31072, ttl=64 (request in 244)
124 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=122/31328, ttl=64 (reply in 246)
125 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=123/31584, ttl=64 (request in 248)
126 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=124/31840, ttl=64 (reply in 250)
127 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=125/32096, ttl=64 (request in 252)
128 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=126/32352, ttl=64 (reply in 254)
129 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=127/32608, ttl=64 (request in 256)
130 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=128/32864, ttl=64 (reply in 258)
131 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=129/33120, ttl=64 (request in 260)
132 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=130/33376, ttl=64 (reply in 262)
133 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=131/33632, ttl=64 (request in 264)
134 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=132/33888, ttl=64 (reply in 266)
135 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=133/34144, ttl=64 (request in 268)
136 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=134/34400, ttl=64 (reply in 270)
137 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=135/34656, ttl=64 (request in 272)
138 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=136/34912, ttl=64 (reply in 274)
139 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=137/35168, ttl=64 (request in 276)
140 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=138/35424, ttl=64 (reply in 278)
141 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=139/35680, ttl=64 (request in 280)
142 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=140/35936, ttl=64 (reply in 282)
143 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=141/36192, ttl=64 (request in 284)
144 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=142/36448, ttl=64 (reply in 286)
145 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=143/36704, ttl=64 (request in 288)
146 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=144/36960, ttl=64 (reply in 290)
147 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=145/37216, ttl=64 (request in 292)
148 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=146/37472, ttl=64 (reply in 294)
149 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=147/37728, ttl=64 (request in 296)
150 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=148/37984, ttl=64 (reply in 298)
151 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=149/38240, ttl=64 (request in 300)
152 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=150/38496, ttl=64 (reply in 302)
153 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=151/38752, ttl=64 (request in 304)
154 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) reply 10-0x0020, seq=152/39008, ttl=64 (reply in 306)
155 0.000000 10.9.0.5 10.9.0.5 ICMP 64 Echo (ping) request 10-0x0020, seq=153/39264, ttl=64 (request in 308)
156 0.000000 10.9.0.5 
```

```
Activities Terminal Sep 9 13:22
seed@VM: ~/.../Labsetup
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

seed-attacker:PE51UG21CS924:Navya:/volumes
$>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.....
```

```
Activities Terminal Sep 9 13:16
seed@VM: ~/.../Labsetup
seed-attacker:PE51UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away: 10.0.2.1
2 hops away: 172.16.20.1
3 hops away: 119.226.103.130
4 hops away: 100.70.137.135
5 hops away: 100.70.137.119
6 hops away: 172.31.180.57
7 hops away: 180.87.36.9
8 hops away: 180.87.36.95
9 hops away: 129.134.34.175
10 hops away: 173.252.67.19
11 hops away: 157.240.23.35
Done 157.240.23.35
seed-attacker:PE51UG21CS924:Navya:/volumes
$>python3 Task1.3.py 157.240.23.35
Traceroute 157.240.23.35
1 hops away: 10.0.2.1
2 hops away: 172.16.20.1
3 hops away: 119.226.103.130
4 hops away: 100.70.137.135
5 hops away: 100.70.137.119
6 hops away: 172.31.180.57
7 hops away: 180.87.36.9
8 hops away: 180.87.36.95
9 hops away: 129.134.34.175
10 hops away: 173.252.67.19
11 hops away: 157.240.23.35
Done 157.240.23.35
seed-attacker:PE51UG21CS924:Navya:/volumes
$>
```