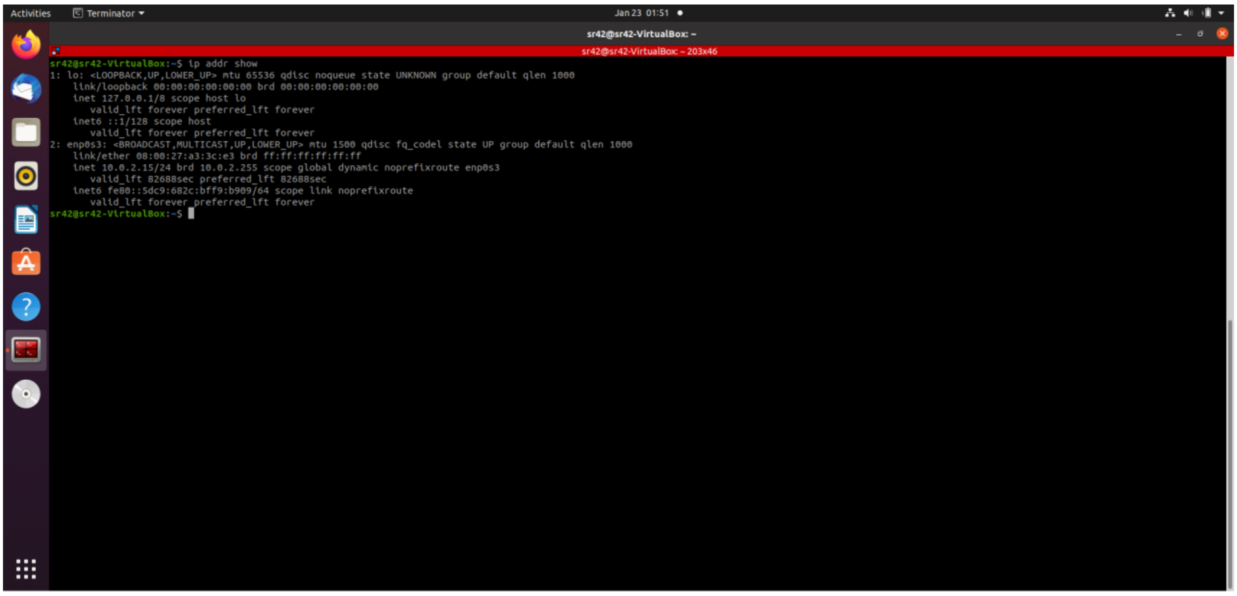
Sriram R – PES1UG20CS435

Week #1

Task 1: Linux Interface Configuration (ifconfig / IP command)

Step 1: To display status of all active network interfaces.

ifconfig (or) **ip addr show**



```
sr42@sr42-VirtualBox:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:a3:3c:e3 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 82688sec preferred_lft 82688sec
    inet6 fe80::5dc9:682c:bff9:b909/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
sr42@sr42-VirtualBox:~$
```

Analyze and fill the following table:

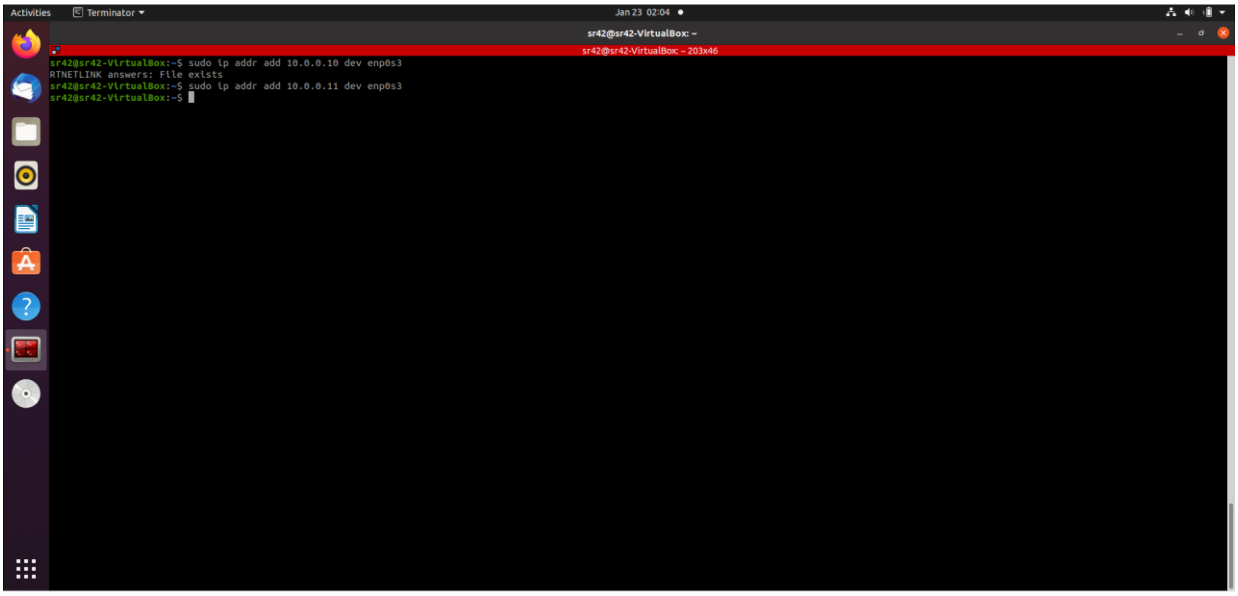
ip address table:

Interface name	**IP address (IPv4 / IPv6)**	**MAC address**
lo	125.0.0.1	<loopback>
enp0s3	10.0.2.15	08:00:27:a3:3c:e3

Step 2: To assign an IP address to an interface, use the following command.

sudo ifconfig interface_name 10.0.your_section.your_sno netmask 255.255.255.0 (or)

sudo ip addr add 10.0.your_section.your_sno /24 dev interface_name

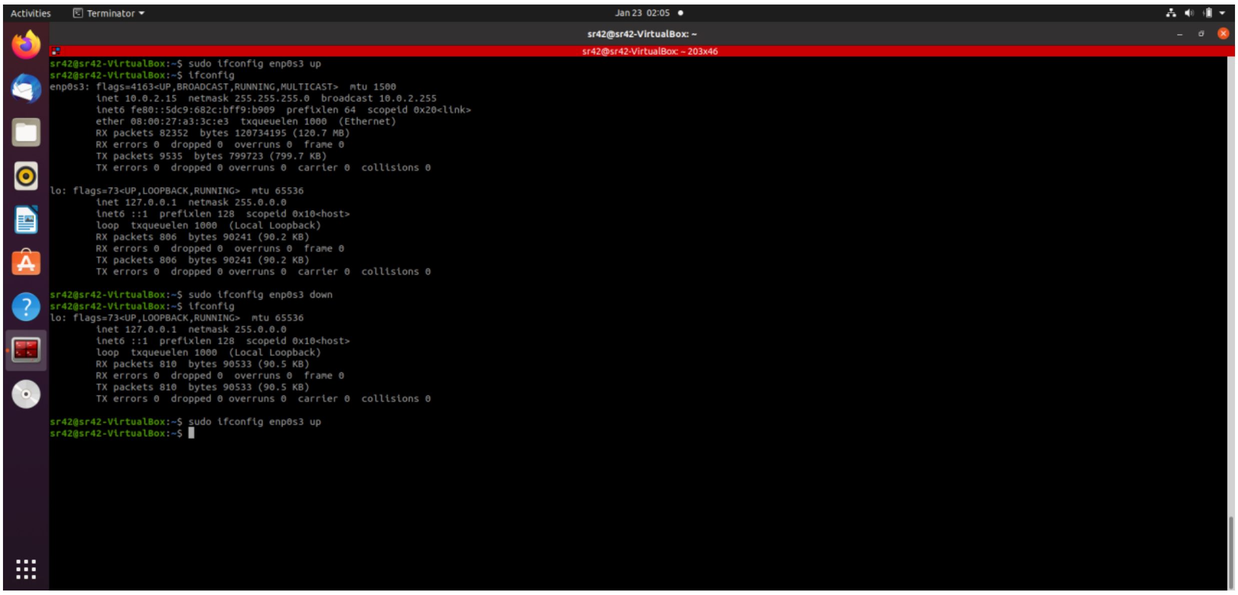


```
sr42@sr42-VirtualBox:~$ sudo ip addr add 10.0.0.10 dev enp0s3
RTNETLINK answers: File exists
sr42@sr42-VirtualBox:~$ sudo ip addr add 10.0.0.11 dev enp0s3
sr42@sr42-VirtualBox:~$
```

Step 3: To activate / deactivate a network interface, type.

sudo ifconfig interface_name down

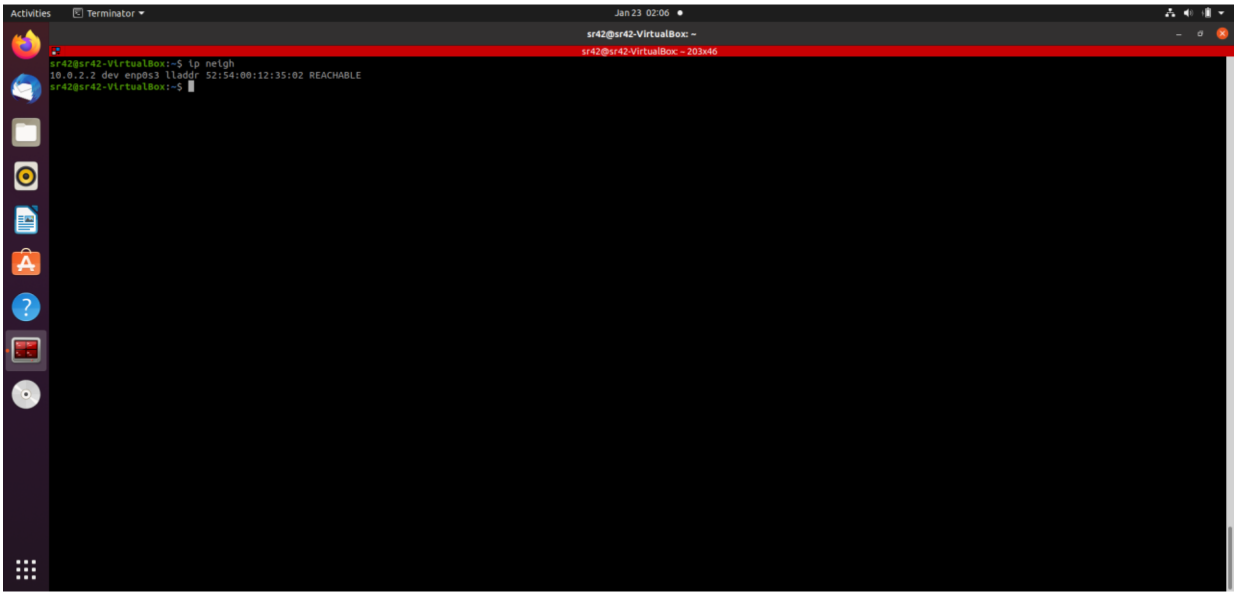
sudo ifconfig interface_name up



```
sr42@sr42-VirtualBox:~$ sudo ifconfig enp0s3 up
sr42@sr42-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5dc9:682c:bff9:b909  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a3:3c:e3  txqueuelen 1000  (Ethernet)
        RX packets 82352  bytes 120734195 (120.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9535  bytes 799723 (799.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 806  bytes 90241 (90.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 806  bytes 90241 (90.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sr42@sr42-VirtualBox:~$ sudo ifconfig enp0s3 down
sr42@sr42-VirtualBox:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 810  bytes 90533 (90.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 810  bytes 90533 (90.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sr42@sr42-VirtualBox:~$ sudo ifconfig enp0s3 up
sr42@sr42-VirtualBox:~$ 
```

Step 4: To show the current neighbor table in kernel, type

ip neigh



```
sr42@sr42-VirtualBox:~$ ip neigh
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
sr42@sr42-VirtualBox:~$ 
```

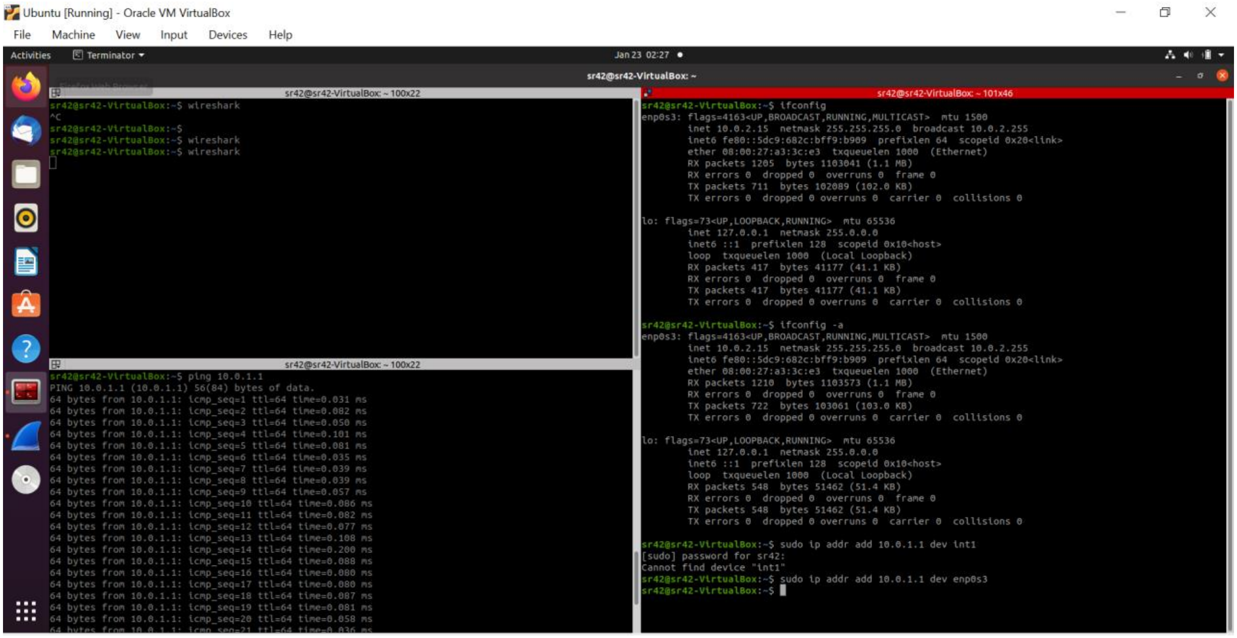
Task 2: Ping PDU (Packet Data Units or Packets) Capture

Step 1: Assign an IP address to the system (Host).

Note: IP address of your system should be 10.0.your_section.your_sno.

Step 2: Launch Wireshark and select ‘any’ interface

Step 3: In terminal, type **ping 10.0.your_section.your_sno**


Ubuntu [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminator
Jan 23 02:27
sr42@sr42-VirtualBox: ~
sr42@sr42-VirtualBox: ~ 100x22
sr42@sr42-VirtualBox: ~ 101x46

```
sr42@sr42-VirtualBox:~$ wireshark
^C
sr42@sr42-VirtualBox:~$
sr42@sr42-VirtualBox:~$ wireshark
sr42@sr42-VirtualBox:~$ wireshark
```

```
sr42@sr42-VirtualBox:~$ ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from 10.0.1.1: icmp_seq=4 ttl=64 time=0.101 ms
64 bytes from 10.0.1.1: icmp_seq=5 ttl=64 time=0.081 ms
64 bytes from 10.0.1.1: icmp_seq=6 ttl=64 time=0.035 ms
64 bytes from 10.0.1.1: icmp_seq=7 ttl=64 time=0.039 ms
64 bytes from 10.0.1.1: icmp_seq=8 ttl=64 time=0.039 ms
64 bytes from 10.0.1.1: icmp_seq=9 ttl=64 time=0.057 ms
64 bytes from 10.0.1.1: icmp_seq=10 ttl=64 time=0.086 ms
64 bytes from 10.0.1.1: icmp_seq=11 ttl=64 time=0.082 ms
64 bytes from 10.0.1.1: icmp_seq=12 ttl=64 time=0.077 ms
64 bytes from 10.0.1.1: icmp_seq=13 ttl=64 time=0.108 ms
64 bytes from 10.0.1.1: icmp_seq=14 ttl=64 time=0.200 ms
64 bytes from 10.0.1.1: icmp_seq=15 ttl=64 time=0.088 ms
64 bytes from 10.0.1.1: icmp_seq=16 ttl=64 time=0.080 ms
64 bytes from 10.0.1.1: icmp_seq=17 ttl=64 time=0.080 ms
64 bytes from 10.0.1.1: icmp_seq=18 ttl=64 time=0.087 ms
64 bytes from 10.0.1.1: icmp_seq=19 ttl=64 time=0.081 ms
64 bytes from 10.0.1.1: icmp_seq=20 ttl=64 time=0.058 ms
64 bytes from 10.0.1.1: icmp_seq=21 ttl=64 time=0.036 ms
```

```
sr42@sr42-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5dc9:682c:bff9:b909  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a3:3c:e3  txqueuelen 1000  (Ethernet)
        RX packets 1205  bytes 1103041 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 711  bytes 102089 (102.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 417  bytes 41177 (41.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 417  bytes 41177 (41.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sr42@sr42-VirtualBox:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::5dc9:682c:bff9:b909  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:a3:3c:e3  txqueuelen 1000  (Ethernet)
        RX packets 1210  bytes 1103573 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 722  bytes 103061 (103.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 548  bytes 51462 (51.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 548  bytes 51462 (51.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sr42@sr42-VirtualBox:~$ sudo ip addr add 10.0.1.1 dev int1
[sudo] password for sr42:
Cannot find device "int1"
sr42@sr42-VirtualBox:~$ sudo ip addr add 10.0.1.1 dev enp0s3
sr42@sr42-VirtualBox:~$
```

Observations to be made

Step 4: Analyze the following in Terminal

- TTL
- Protocol used by ping
- Time

Step 5: Analyze the following in Wireshark

On Packet List Pane, select the first echo packet on the list. On Packet Details Pane, click on each of the four “+” to expand the information. Analyze the frames with the first echo request and echo reply and complete the table below.

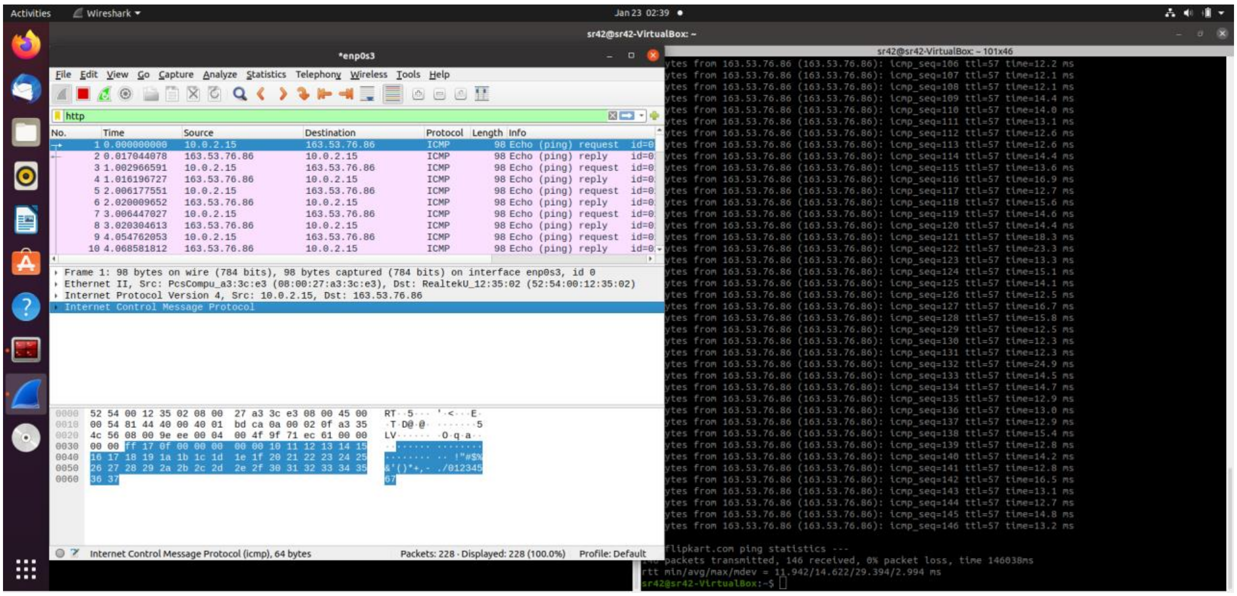
Details	**First Echo Request**	**First Echo Reply**
Frame Number	1	2
Source IP address	10.0.1.1	10.0.1.1
Destination IP address	10.0.1.1	10.0.1.1
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

Task 3: HTTP PDU Capture

Using Wireshark’s Filter feature

Step 1: Launch Wireshark and select ‘any’ interface. On the Filter toolbar, type-in ‘http’ and press enter

Step 2: Open Firefox browser, and browse info.cern.ch



Activities
Wireshark
Jan 23 02:39
sr42@sr42-VirtualBox: ~
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sr42@sr42-VirtualBox: ~ 101x46

http

```
No.   Time         Source          Destination     Protocol  Length Info
    1 0.000000000  10.0.2.15       163.53.76.86    ICMP       98 Echo (ping) request  id=0
    2 0.017044078  163.53.76.86    10.0.2.15       ICMP       98 Echo (ping) reply    id=0
    3 1.002966591  10.0.2.15       163.53.76.86    ICMP       98 Echo (ping) request  id=0
    4 1.016196727  163.53.76.86    10.0.2.15       ICMP       98 Echo (ping) reply    id=0
    5 2.006177551  10.0.2.15       163.53.76.86    ICMP       98 Echo (ping) request  id=0
    6 2.020009652  163.53.76.86    10.0.2.15       ICMP       98 Echo (ping) reply    id=0
    7 3.006447027  10.0.2.15       163.53.76.86    ICMP       98 Echo (ping) request  id=0
    8 3.020304613  163.53.76.86    10.0.2.15       ICMP       98 Echo (ping) reply    id=0
    9 4.054762053  10.0.2.15       163.53.76.86    ICMP       98 Echo (ping) request  id=0
   10 4.068581812  163.53.76.86    10.0.2.15       ICMP       98 Echo (ping) reply    id=0
```

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_a3:3c:e3 (08:00:27:a3:3c:e3), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 163.53.76.86
Internet Control Message Protocol
```

```
0000  52 54 00 12 35 02 08 00  27 a3 3c e3 08 00 45 00   RT··5···'·<···E·
0010  00 54 81 44 40 00 40 01  bd ca 0a 00 02 0f a3 35   ·T·D@·@·  ······5
0020  4c 56 08 00 9e ee 00 04  00 4f 9f 71 ec 61 00 00   LV······ ·O·q·a··
0030  00 00 ff 17 0f 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Internet Control Message Protocol (icmp), 64 bytes   Packets: 228 · Displayed: 228 (100.0%)   Profile: Default

```
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=106 ttl=57 time=12.2 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=107 ttl=57 time=12.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=108 ttl=57 time=12.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=109 ttl=57 time=14.4 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=110 ttl=57 time=14.0 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=111 ttl=57 time=13.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=112 ttl=57 time=12.6 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=113 ttl=57 time=12.6 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=114 ttl=57 time=14.4 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=115 ttl=57 time=13.6 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=116 ttl=57 time=16.9 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=117 ttl=57 time=12.7 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=118 ttl=57 time=15.6 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=119 ttl=57 time=14.6 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=120 ttl=57 time=14.4 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=121 ttl=57 time=18.3 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=122 ttl=57 time=23.3 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=123 ttl=57 time=13.3 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=124 ttl=57 time=15.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=125 ttl=57 time=14.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=126 ttl=57 time=12.5 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=127 ttl=57 time=16.7 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=128 ttl=57 time=15.8 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=129 ttl=57 time=12.5 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=130 ttl=57 time=12.3 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=131 ttl=57 time=12.3 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=132 ttl=57 time=24.9 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=133 ttl=57 time=14.5 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=134 ttl=57 time=14.7 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=135 ttl=57 time=12.9 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=136 ttl=57 time=13.0 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=137 ttl=57 time=12.9 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=138 ttl=57 time=15.4 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=139 ttl=57 time=12.8 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=140 ttl=57 time=14.2 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=141 ttl=57 time=12.8 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=142 ttl=57 time=16.5 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=143 ttl=57 time=13.1 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=144 ttl=57 time=12.7 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=145 ttl=57 time=14.8 ms
ytes from 163.53.76.86 (163.53.76.86): icmp_seq=146 ttl=57 time=13.2 ms

flipkart.com ping statistics ---
packets transmitted, 146 received, 0% packet loss, time 146038ms
rtt min/avg/max/mdev = 11.942/14.622/29.394/2.994 ms
sr42@sr42-VirtualBox:~$ 
```

Observations to be made

Step 3: Analyze the first (interaction of host to the web server) and second frame (response of server to the client). By analyzing the filtered frames, complete the table below:

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source Port	33799	80
Destination Port	80	33799
Source IP address	10.0.2.15	163.53.76.86
Destination IP address	163.53.76.86	10.0.2.15
Source Ethernet Address	08:00:27:a3:3c:e3	08:00:27:a3:3c:e3
Destination Ethernet Address	52:54:00:12:35:02	52:54:00:12:35:02

Step 4: Analyze the HTTP request and response and complete the table below.

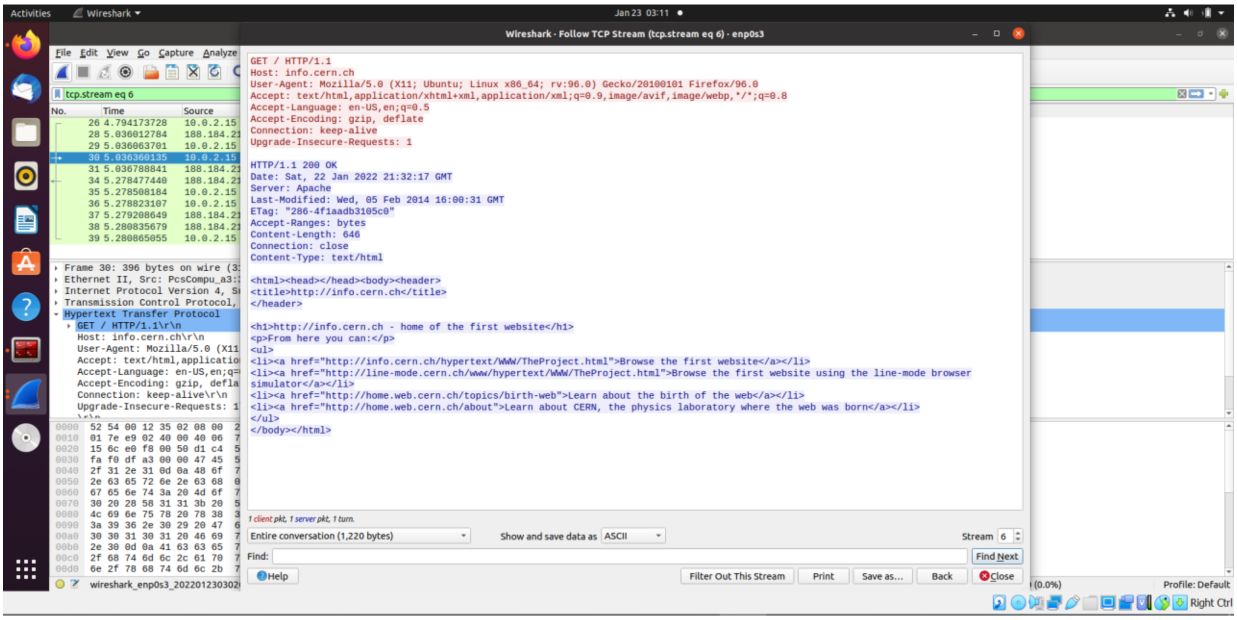
HTTP Request		HTTP Response	
Get	GET / HTTP/1.1\r\n	Server	HTTP/1.1 200 OK\r\n

Host	info.cern.ch\r\n	Content-Type	text/html
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0	Date	Sat, 22 Jan 2022 21:32:17 GMT
Accept-Language	en-US,en;q=0.5	Location	n/a
Accept-Encoding	gzip, deflate	Content-Length	646
Connection	keep-alive	Connection	close

Using Wireshark's Follow TCP Stream

Step 1: Make sure the filter is blank. Right-click any packet inside the Packet List Pane, then select 'Follow TCP Stream'. For demo purpose, a packet containing the HTTP GET request "GET / HTTP / 1.1" can be selected.

Step 2: Upon following a TCP stream, screenshot the whole window.



Wireshark · Follow TCP Stream (tcp.stream eq 6) · enp0s3

```
GET / HTTP/1.1
Host: info.cern.ch
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Date: Sat, 22 Jan 2022 21:32:17 GMT
Server: Apache
Last-Modified: Wed, 05 Feb 2014 16:00:31 GMT
ETag: "286-4f1aadb3105c0"
Accept-Ranges: bytes
Content-Length: 646
Connection: close
Content-Type: text/html

<html><head></head><body><header>
<title>http://info.cern.ch</title>
</header>

<h1>http://info.cern.ch - home of the first website</h1>
<p>From here you can:</p>
<ul>
<li><a href="http://info.cern.ch/hypertext/WWW/TheProject.html">Browse the first website</a></li>
<li><a href="http://line-mode.cern.ch/www/hypertext/WWW/TheProject.html">Browse the first website using the line-mode browser
simulator</a></li>
<li><a href="http://home.web.cern.ch/topics/birth-web">Learn about the birth of the web</a></li>
<li><a href="http://home.web.cern.ch/about">Learn about CERN, the physics laboratory where the web was born</a></li>
</ul>
</body></html>
```

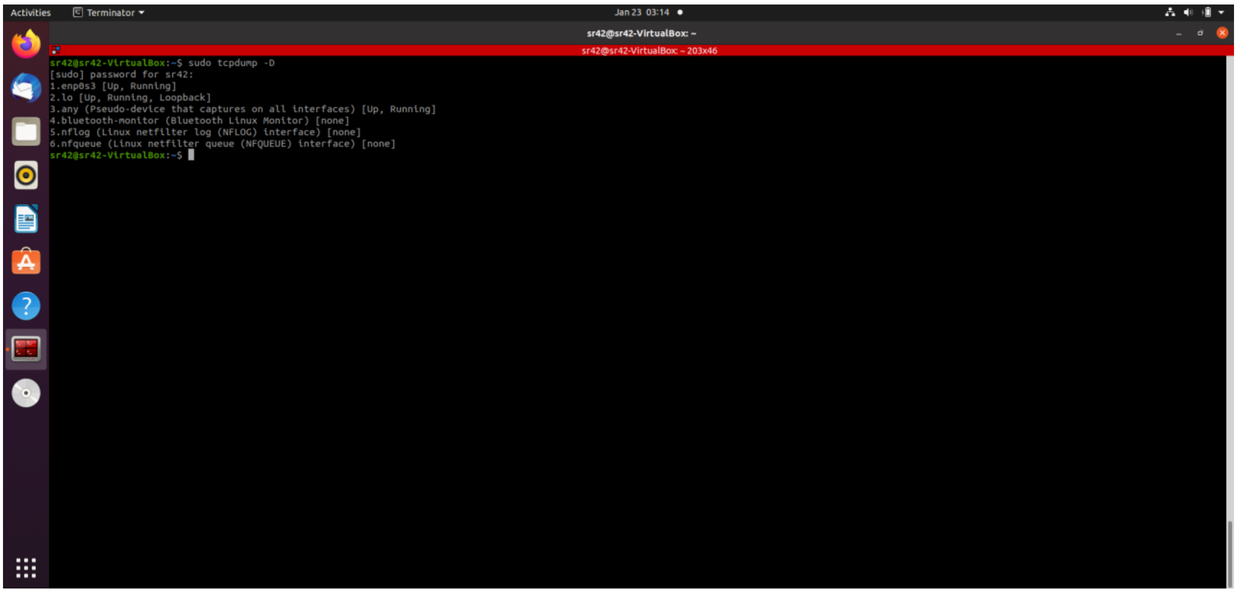
1 client pkt, 1 server pkt, 1 turn.

Entire conversation (1,220 bytes) — Show and save data as: ASCII — Stream: 6

Task 4: Capturing packets with tcpdump

Step 1: Use the command **tcpdump -D** to see which interfaces are available for capture.

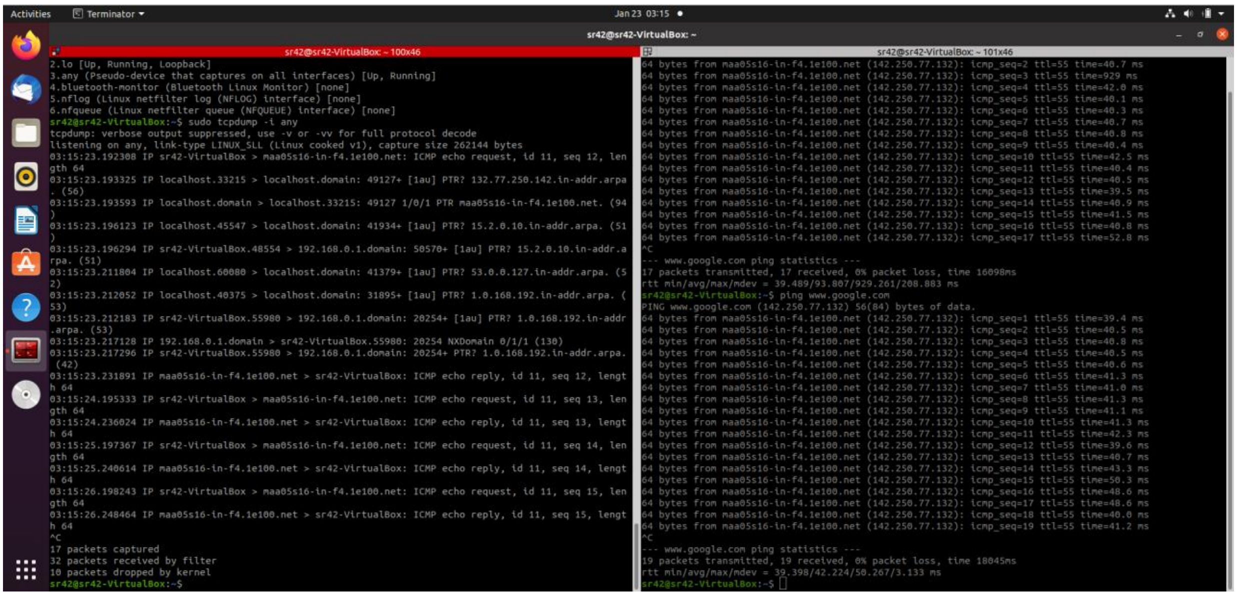
sudo tcpdump –D



```
sr42@sr42-VirtualBox:~$ sudo tcpdump -D
[sudo] password for sr42:
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
sr42@sr42-VirtualBox:~$ 
```

Step 2: Capture all packets in any interface by running this command:

sudo tcpdump -i any


Activities
Terminator
Jan 23 03:15
sr42@sr42-VirtualBox: ~
sr42@sr42-VirtualBox: ~ 100x46
sr42@sr42-VirtualBox: ~ 101x46

```
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
sr42@sr42-VirtualBox:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
03:15:23.192308 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 12, len
gth 64
03:15:23.193325 IP localhost.33215 > localhost.domain: 49127+ [1au] PTR? 132.77.250.142.in-addr.arpa
. (56)
03:15:23.193593 IP localhost.domain > localhost.33215: 49127 1/0/1 PTR maa05s16-in-f4.1e100.net. (94
)
03:15:23.196123 IP localhost.45547 > localhost.domain: 41934+ [1au] PTR? 15.2.0.10.in-addr.arpa. (51
)
03:15:23.196294 IP sr42-VirtualBox.48554 > 192.168.0.1.domain: 50570+ [1au] PTR? 15.2.0.10.in-addr.a
rpa. (51)
03:15:23.211804 IP localhost.60080 > localhost.domain: 41379+ [1au] PTR? 53.0.0.127.in-addr.arpa. (5
2)
03:15:23.212052 IP localhost.40375 > localhost.domain: 31895+ [1au] PTR? 1.0.168.192.in-addr.arpa. (
53)
03:15:23.212183 IP sr42-VirtualBox.55980 > 192.168.0.1.domain: 20254+ [1au] PTR? 1.0.168.192.in-addr
.arpa. (53)
03:15:23.217128 IP 192.168.0.1.domain > sr42-VirtualBox.55980: 20254 NXDomain 0/1/1 (130)
03:15:23.217296 IP sr42-VirtualBox.55980 > 192.168.0.1.domain: 20254+ PTR? 1.0.168.192.in-addr.arpa.
 (42)
03:15:23.231891 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 12, lengt
h 64
03:15:24.195333 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 13, len
gth 64
03:15:24.236024 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 13, lengt
h 64
03:15:25.197367 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 14, len
gth 64
03:15:25.240614 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 14, lengt
h 64
03:15:26.198243 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 15, len
gth 64
03:15:26.248464 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 15, lengt
h 64
^C
17 packets captured
32 packets received by filter
10 packets dropped by kernel
sr42@sr42-VirtualBox:~$
```

```
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=2 ttl=55 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=3 ttl=55 time=929 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=4 ttl=55 time=42.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=5 ttl=55 time=40.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=6 ttl=55 time=40.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=7 ttl=55 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=8 ttl=55 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=9 ttl=55 time=40.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=10 ttl=55 time=42.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=11 ttl=55 time=40.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=12 ttl=55 time=40.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=13 ttl=55 time=39.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=14 ttl=55 time=40.9 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=15 ttl=55 time=41.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=16 ttl=55 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=17 ttl=55 time=52.8 ms
^C
--- www.google.com ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16098ms
rtt min/avg/max/mdev = 39.489/93.807/929.261/208.883 ms
sr42@sr42-VirtualBox:~$ ping www.google.com
PING www.google.com (142.250.77.132) 56(84) bytes of data.
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=1 ttl=55 time=39.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=2 ttl=55 time=40.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=3 ttl=55 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=4 ttl=55 time=40.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=5 ttl=55 time=40.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=6 ttl=55 time=41.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=7 ttl=55 time=41.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=8 ttl=55 time=41.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=9 ttl=55 time=41.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=10 ttl=55 time=41.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=11 ttl=55 time=42.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=12 ttl=55 time=39.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=13 ttl=55 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=14 ttl=55 time=43.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=15 ttl=55 time=50.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=16 ttl=55 time=48.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=17 ttl=55 time=48.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=18 ttl=55 time=40.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=19 ttl=55 time=41.2 ms
^C
--- www.google.com ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18045ms
rtt min/avg/max/mdev = 39.398/42.224/50.267/3.133 ms
sr42@sr42-VirtualBox:~$ 
```

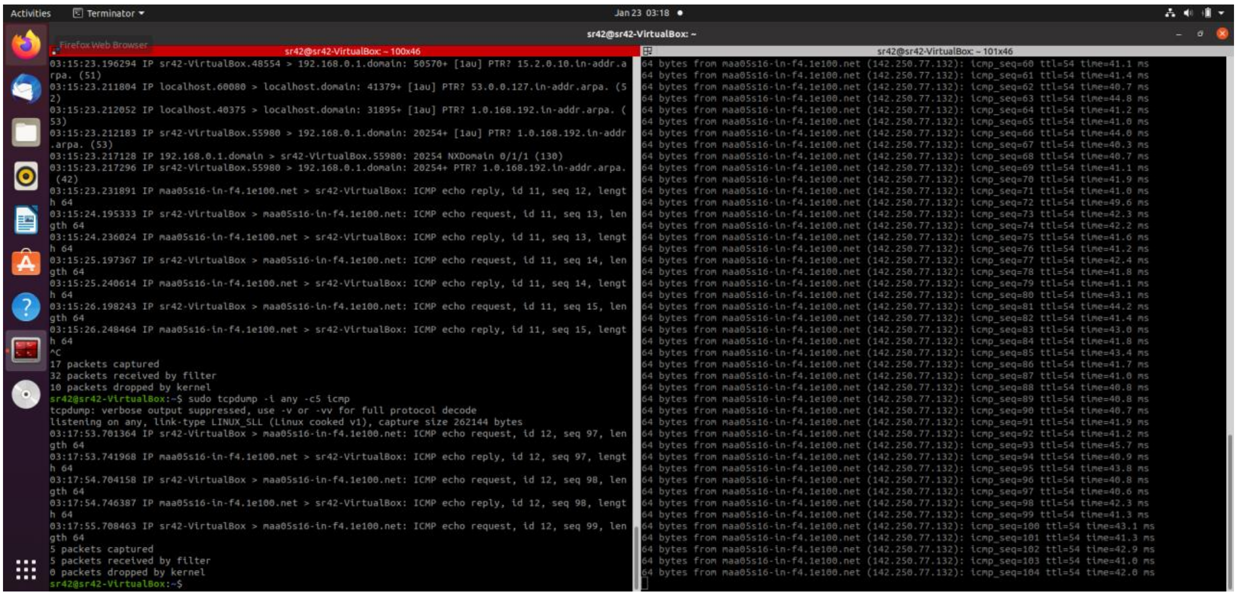
Note: Perform some pinging operation while giving above command. Also type www.google.com in browser.

Observation

Step 3: Understand the output format.

Step 4: To filter packets based on protocol, specifying the protocol in the command line. For example, capture ICMP packets only by using this command:

sudo tcpdump -i any -c5 icmp

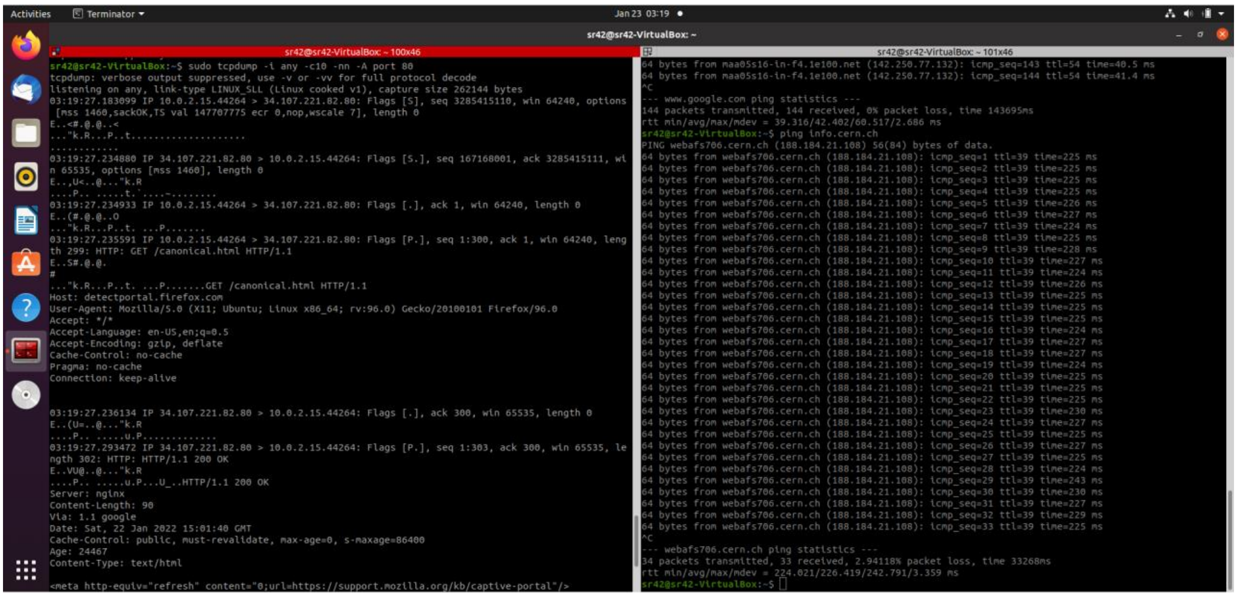


```
03:15:23.196294 IP sr42-VirtualBox.48554 > 192.168.0.1.domain: 50570+ [1au] PTR? 15.2.0.10.in-addr.a
rpa. (51)
03:15:23.211804 IP localhost.60080 > localhost.domain: 41379+ [1au] PTR? 53.0.0.127.in-addr.arpa. (5
2)
03:15:23.212052 IP localhost.40375 > localhost.domain: 31895+ [1au] PTR? 1.0.168.192.in-addr.arpa. (
53)
03:15:23.212183 IP sr42-VirtualBox.55980 > 192.168.0.1.domain: 20254+ [1au] PTR? 1.0.168.192.in-addr
.arpa. (53)
03:15:23.217128 IP 192.168.0.1.domain > sr42-VirtualBox.55980: 20254 NXDomain 0/1/1 (130)
03:15:23.217296 IP sr42-VirtualBox.55980 > 192.168.0.1.domain: 20254+ PTR? 1.0.168.192.in-addr.arpa.
 (42)
03:15:23.231891 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 12, lengt
h 64
03:15:24.195333 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 13, len
gth 64
03:15:24.236024 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 13, lengt
h 64
03:15:25.197367 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 14, len
gth 64
03:15:25.240614 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 14, lengt
h 64
03:15:26.198243 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 11, seq 15, len
gth 64
03:15:26.248464 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 11, seq 15, lengt
h 64
^C
17 packets captured
32 packets received by filter
10 packets dropped by kernel
sr42@sr42-VirtualBox:~$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
03:17:53.701364 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 12, seq 97, len
gth 64
03:17:53.741968 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 12, seq 97, lengt
h 64
03:17:54.704158 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 12, seq 98, len
gth 64
03:17:54.746387 IP maa05s16-in-f4.1e100.net > sr42-VirtualBox: ICMP echo reply, id 12, seq 98, lengt
h 64
03:17:55.708463 IP sr42-VirtualBox > maa05s16-in-f4.1e100.net: ICMP echo request, id 12, seq 99, len
gth 64
5 packets captured
5 packets received by filter
0 packets dropped by kernel
sr42@sr42-VirtualBox:~$
```

```
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=60 ttl=54 time=41.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=61 ttl=54 time=41.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=62 ttl=54 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=63 ttl=54 time=44.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=64 ttl=54 time=41.2 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=65 ttl=54 time=41.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=66 ttl=54 time=44.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=67 ttl=54 time=40.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=68 ttl=54 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=69 ttl=54 time=41.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=70 ttl=54 time=41.9 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=71 ttl=54 time=41.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=72 ttl=54 time=49.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=73 ttl=54 time=42.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=74 ttl=54 time=42.2 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=75 ttl=54 time=41.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=76 ttl=54 time=41.2 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=77 ttl=54 time=42.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=78 ttl=54 time=41.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=79 ttl=54 time=41.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=80 ttl=54 time=43.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=81 ttl=54 time=44.2 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=82 ttl=54 time=41.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=83 ttl=54 time=43.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=84 ttl=54 time=41.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=85 ttl=54 time=43.4 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=86 ttl=54 time=41.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=87 ttl=54 time=41.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=88 ttl=54 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=89 ttl=54 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=90 ttl=54 time=40.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=91 ttl=54 time=41.9 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=92 ttl=54 time=41.2 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=93 ttl=54 time=45.7 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=94 ttl=54 time=40.9 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=95 ttl=54 time=43.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=96 ttl=54 time=40.8 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=97 ttl=54 time=40.6 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=98 ttl=54 time=42.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=99 ttl=54 time=41.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=100 ttl=54 time=43.1 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=101 ttl=54 time=41.3 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=102 ttl=54 time=42.9 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=103 ttl=54 time=41.0 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=104 ttl=54 time=42.0 ms
```

Step 5: Check the packet content. For example, inspect the HTTP content of a web request like this:

sudo tcpdump -i any -c10 -nn -A port 80


Activities
Terminator
Jan 23 03:19
sr42@sr42-VirtualBox: ~
sr42@sr42-VirtualBox: ~ 100x46
sr42@sr42-VirtualBox: ~ 101x46

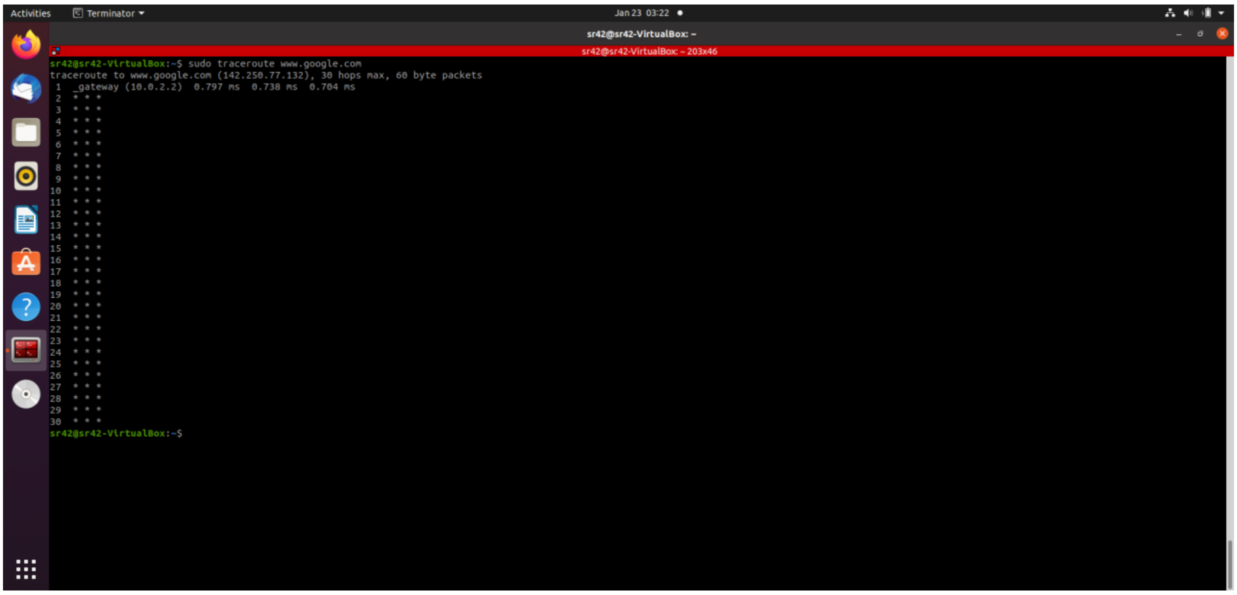
```
sr42@sr42-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
03:19:27.183099 IP 10.0.2.15.44264 > 34.107.221.82.80: Flags [S], seq 3285415110, win 64240, options
 [mss 1460,sackOK,TS val 147707775 ecr 0,nop,wscale 7], length 0
E..<#.@.@..<
..."k.R...P..t....................
............
03:19:27.234880 IP 34.107.221.82.80 > 10.0.2.15.44264: Flags [S.], seq 167168001, ack 3285415111, wi
n 65535, options [mss 1460], length 0
E..,U<..@..."k.R
....P.. .....t.`....-........
03:19:27.234933 IP 10.0.2.15.44264 > 34.107.221.82.80: Flags [.], ack 1, win 64240, length 0
E..(#.@.@..O
..."k.R...P..t. ...P.......
03:19:27.235591 IP 10.0.2.15.44264 > 34.107.221.82.80: Flags [P.], seq 1:300, ack 1, win 64240, leng
th 299: HTTP: GET /canonical.html HTTP/1.1
E..S#.@.@.
#
..."k.R...P..t. ...P.......GET /canonical.html HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive


03:19:27.236134 IP 34.107.221.82.80 > 10.0.2.15.44264: Flags [.], ack 300, win 65535, length 0
E..(U=..@..."k.R
....P.. .....u.P.............
03:19:27.293472 IP 34.107.221.82.80 > 10.0.2.15.44264: Flags [P.], seq 1:303, ack 300, win 65535, le
ngth 302: HTTP: HTTP/1.1 200 OK
E..VU@..@..."k.R
....P.. .....u.P...U_..HTTP/1.1 200 OK
Server: nginx
Content-Length: 90
Via: 1.1 google
Date: Sat, 22 Jan 2022 15:01:40 GMT
Cache-Control: public, must-revalidate, max-age=0, s-maxage=86400
Age: 24467
Content-Type: text/html

<meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal"/>
```

```
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=143 ttl=54 time=40.5 ms
64 bytes from maa05s16-in-f4.1e100.net (142.250.77.132): icmp_seq=144 ttl=54 time=41.4 ms
^C
--- www.google.com ping statistics ---
144 packets transmitted, 144 received, 0% packet loss, time 143695ms
rtt min/avg/max/mdev = 39.316/42.402/60.517/2.686 ms
sr42@sr42-VirtualBox:~$ ping info.cern.ch
PING webafs706.cern.ch (188.184.21.108) 56(84) bytes of data.
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=1 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=2 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=3 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=4 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=5 ttl=39 time=226 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=6 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=7 ttl=39 time=224 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=8 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=9 ttl=39 time=228 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=10 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=11 ttl=39 time=224 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=12 ttl=39 time=226 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=13 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=14 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=15 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=16 ttl=39 time=224 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=17 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=18 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=19 ttl=39 time=224 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=20 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=21 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=22 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=23 ttl=39 time=230 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=24 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=25 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=26 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=27 ttl=39 time=225 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=28 ttl=39 time=224 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=29 ttl=39 time=243 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=30 ttl=39 time=230 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=31 ttl=39 time=227 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=32 ttl=39 time=229 ms
64 bytes from webafs706.cern.ch (188.184.21.108): icmp_seq=33 ttl=39 time=225 ms
^C
--- webafs706.cern.ch ping statistics ---
34 packets transmitted, 33 received, 2.94118% packet loss, time 33268ms
rtt min/avg/max/mdev = 224.021/226.419/242.791/3.359 ms
sr42@sr42-VirtualBox:~$ 
```

Task 5: Perform Traceroute checks

Step 1: Run the traceroute using the following command.

sudo traceroute www.google.com

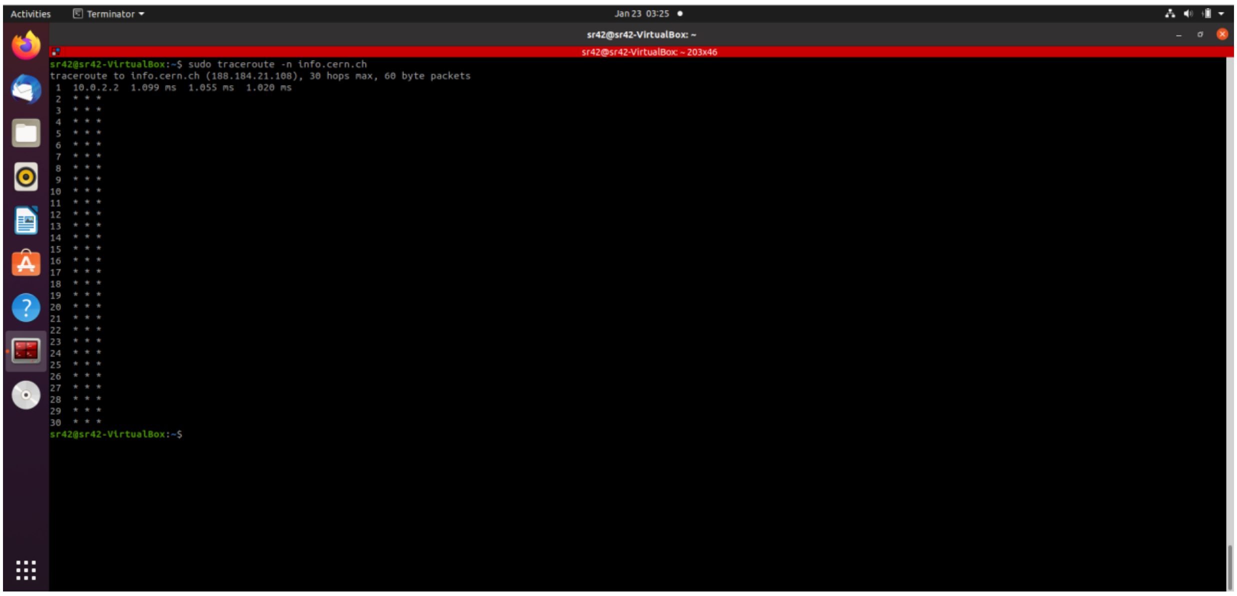


```
sr42@sr42-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.77.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.797 ms  0.738 ms  0.704 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
sr42@sr42-VirtualBox:~$
```

Step 2: Analyze destination address of google.com and no. of hops

Step 3: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the *-n* option

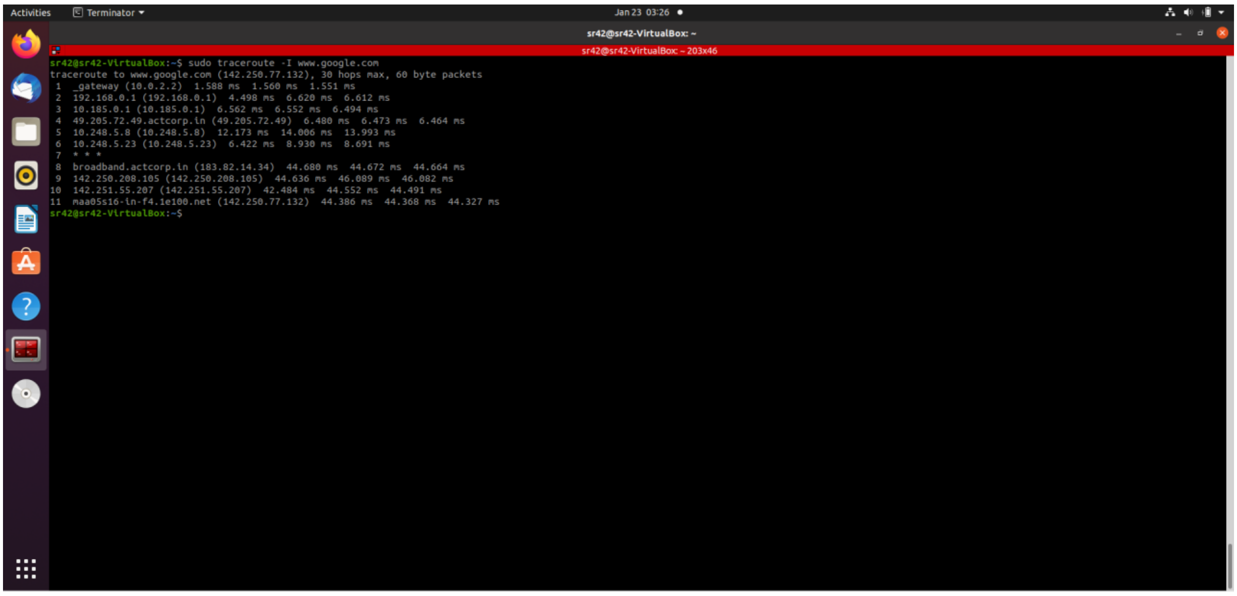
sudo traceroute -n info.cern.ch



```
sr42@sr42-VirtualBox:~$ sudo traceroute -n info.cern.ch
traceroute to info.cern.ch (188.184.21.108), 30 hops max, 60 byte packets
 1  10.0.2.2  1.099 ms  1.055 ms  1.020 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
sr42@sr42-VirtualBox:~$
```

Step 4: The -I option is necessary so that the traceroute uses ICMP.

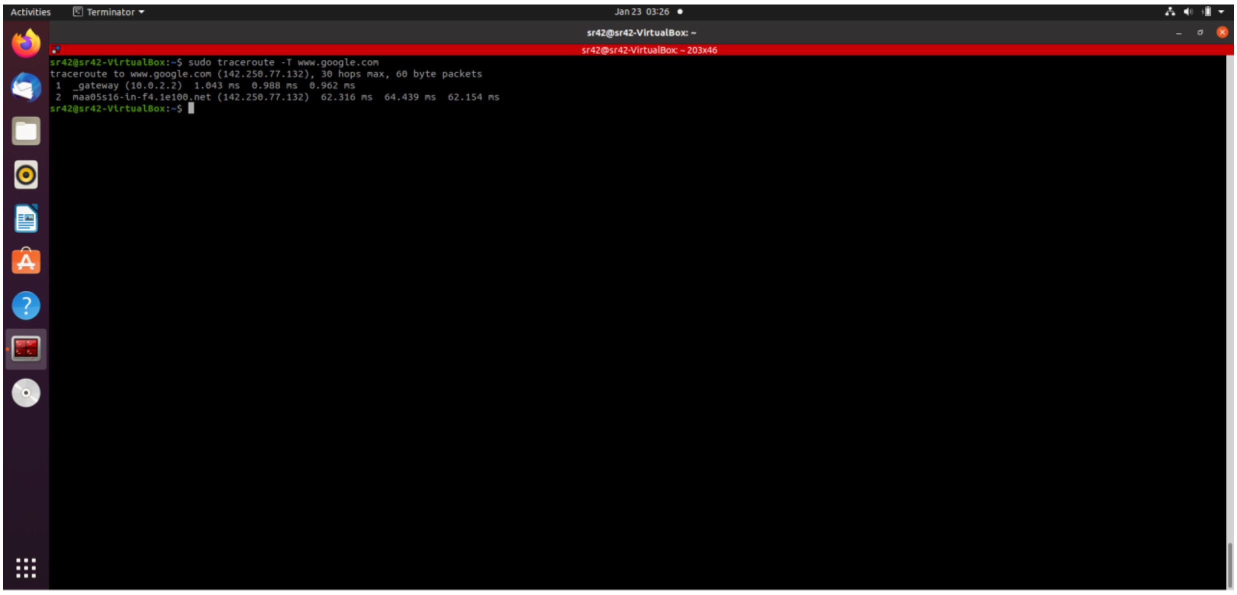
sudo traceroute -I www.google.com



```
sr42@sr42-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.77.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  1.588 ms  1.560 ms  1.551 ms
 2  192.168.0.1 (192.168.0.1)  4.498 ms  6.620 ms  6.612 ms
 3  10.185.0.1 (10.185.0.1)  6.562 ms  6.552 ms  6.494 ms
 4  49.205.72.49.actcorp.in (49.205.72.49)  6.480 ms  6.473 ms  6.464 ms
 5  10.248.5.8 (10.248.5.8)  12.173 ms  14.006 ms  13.993 ms
 6  10.248.5.23 (10.248.5.23)  6.422 ms  8.930 ms  8.691 ms
 7  * * *
 8  broadband.actcorp.in (183.82.14.34)  44.680 ms  44.672 ms  44.664 ms
 9  142.250.208.105 (142.250.208.105)  44.636 ms  46.089 ms  46.082 ms
10  142.251.55.207 (142.251.55.207)  42.484 ms  44.552 ms  44.491 ms
11  maa05s16-in-f4.1e100.net (142.250.77.132)  44.386 ms  44.368 ms  44.327 ms
sr42@sr42-VirtualBox:~$
```

Step 5: By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag.

sudo traceroute -T www.google.com

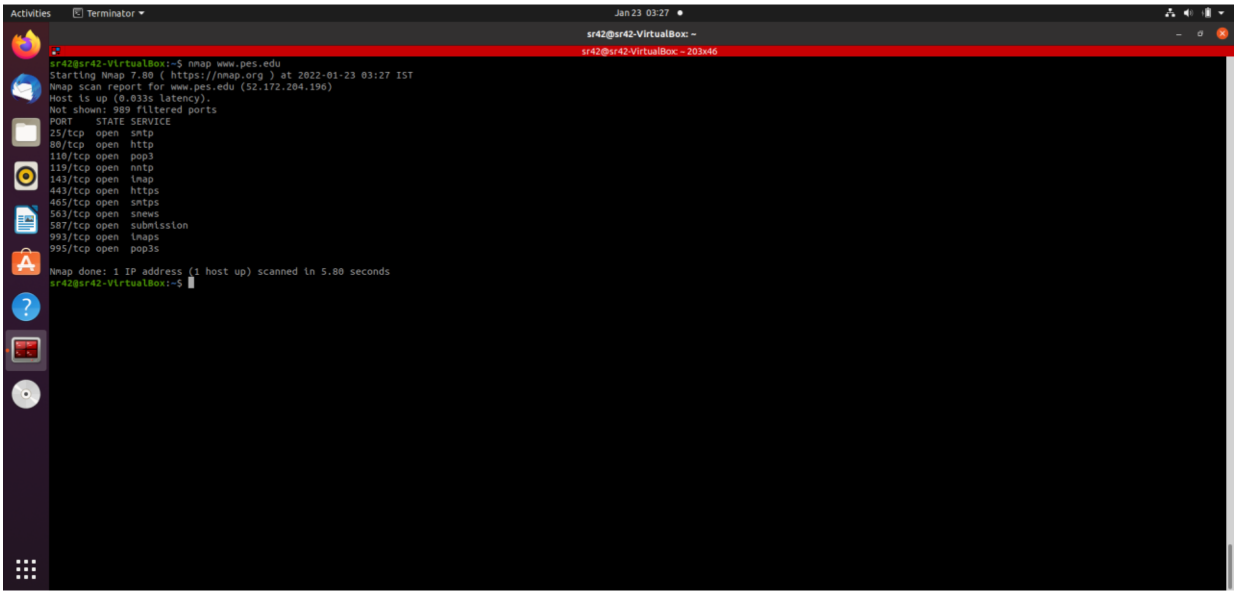


```
sr42@sr42-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.77.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  1.043 ms  0.988 ms  0.962 ms
 2  maa05s16-in-f4.1e100.net (142.250.77.132)  62.316 ms  64.439 ms  62.154 ms
sr42@sr42-VirtualBox:~$ 
```

Task 6: Explore an entire network for information (Nmap)

Step 1: You can scan a host using its host name or IP address, for instance.

nmap www.pes.edu



```
sr42@sr42-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-23 03:27 IST
Nmap scan report for www.pes.edu (52.172.204.196)
Host is up (0.033s latency).
Not shown: 989 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
119/tcp open  nntp
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
563/tcp open  snews
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 5.80 seconds
sr42@sr42-VirtualBox:~$
```

Step 2: Alternatively, use an IP address to scan.

nmap 163.53.78.128

Step 3: Scan multiple IP address or subnet (IPv4)

nmap 192.168.1.1 192.168.1.2 192.168.1.3

Questions on above observations:

1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server?

   – Ans. : Both the browser & the server run HTTP 1.1

2) When was the HTML file that you are retrieving last modified at the server?
   – Ans. : Sat, 22 Jan 2022 21:32:17 GMT

3) How to tell ping to exit after a specified number of ECHO_REQUEST packets?
   – Ans.: ping -c <insert number of packets here>

4) How will you identify remote host apps and OS?
   – Ans.: nmap –O –v <server IP address>