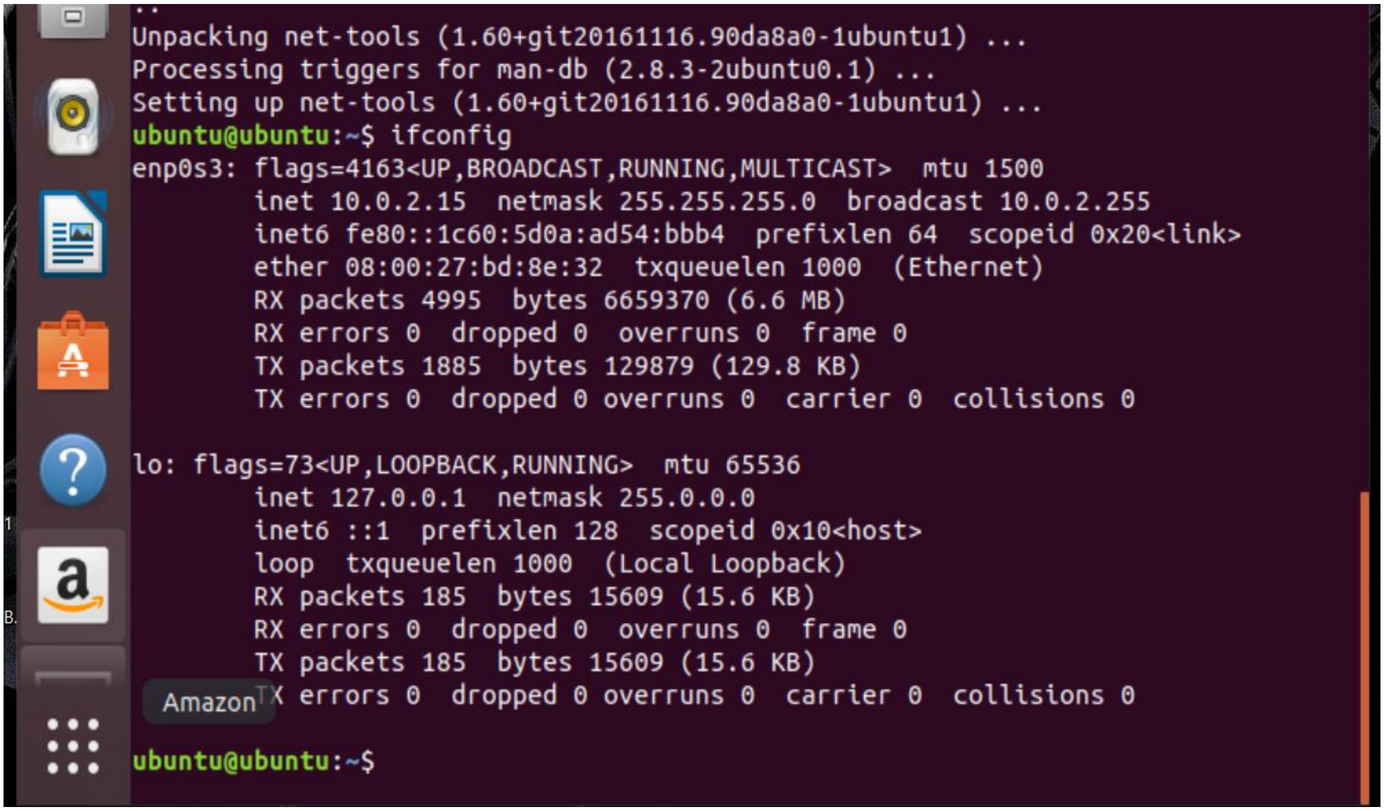
PRATEEK SHETTY

PES1UG19CS345

TASK-1:

Step 1: ifconfig command:

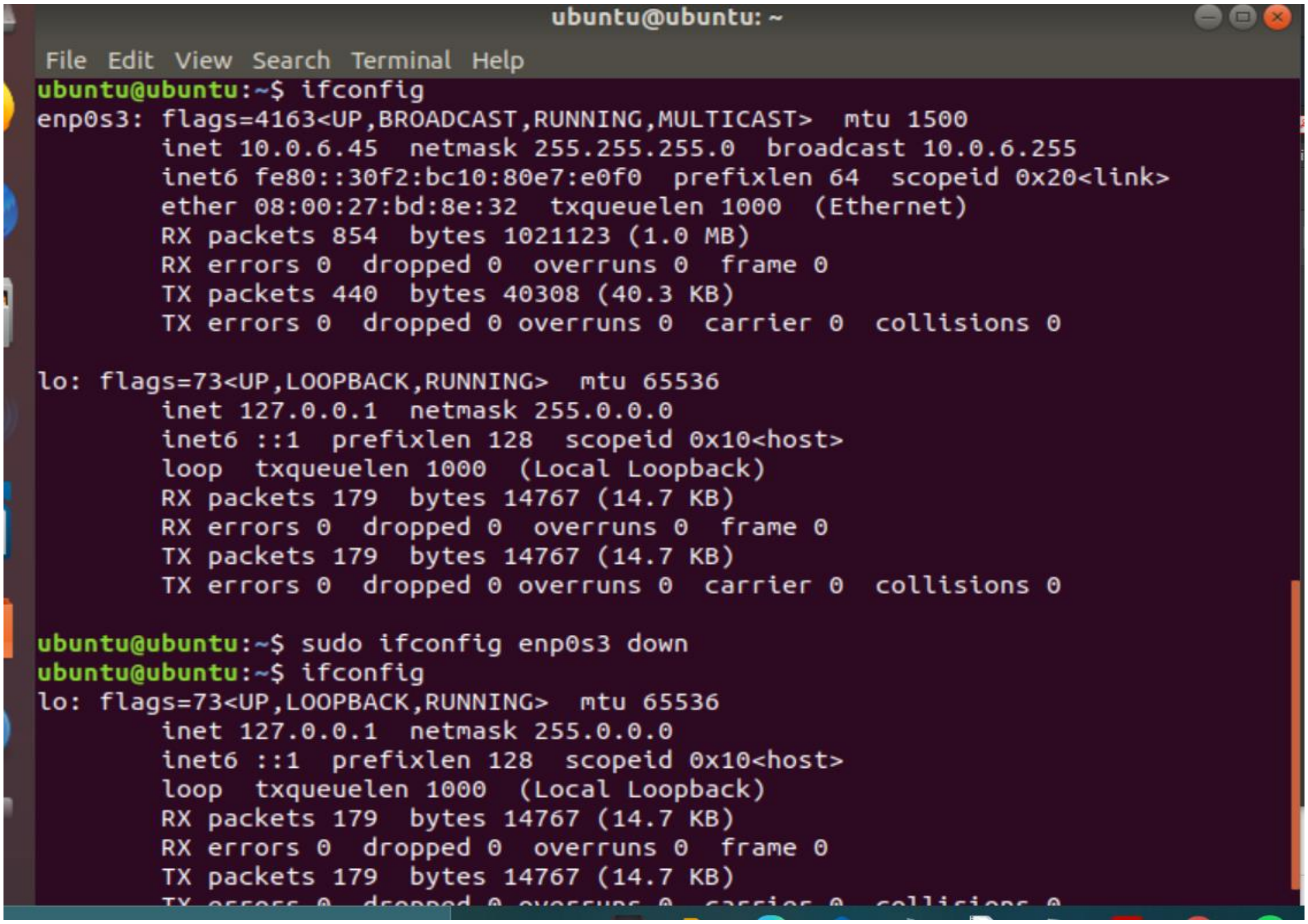


```
..
Unpacking net-tools (1.60+git20161116.90da8a0-1ubuntu1) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
Setting up net-tools (1.60+git20161116.90da8a0-1ubuntu1) ...
ubuntu@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::1c60:5d0a:ad54:bbb4  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bd:8e:32  txqueuelen 1000  (Ethernet)
        RX packets 4995  bytes 6659370 (6.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1885  bytes 129879 (129.8 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 185  bytes 15609 (15.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 185  bytes 15609 (15.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@ubuntu:~$
```

Interface name	**IP address (IPv4 / IPv6)**	**MAC address**
enp0s3	10.0.2.15(before changing)	08:00:27:bd:8e:32
lo	127.0.0.1	**-**

Step 3: Activating/deactivating a network interface:

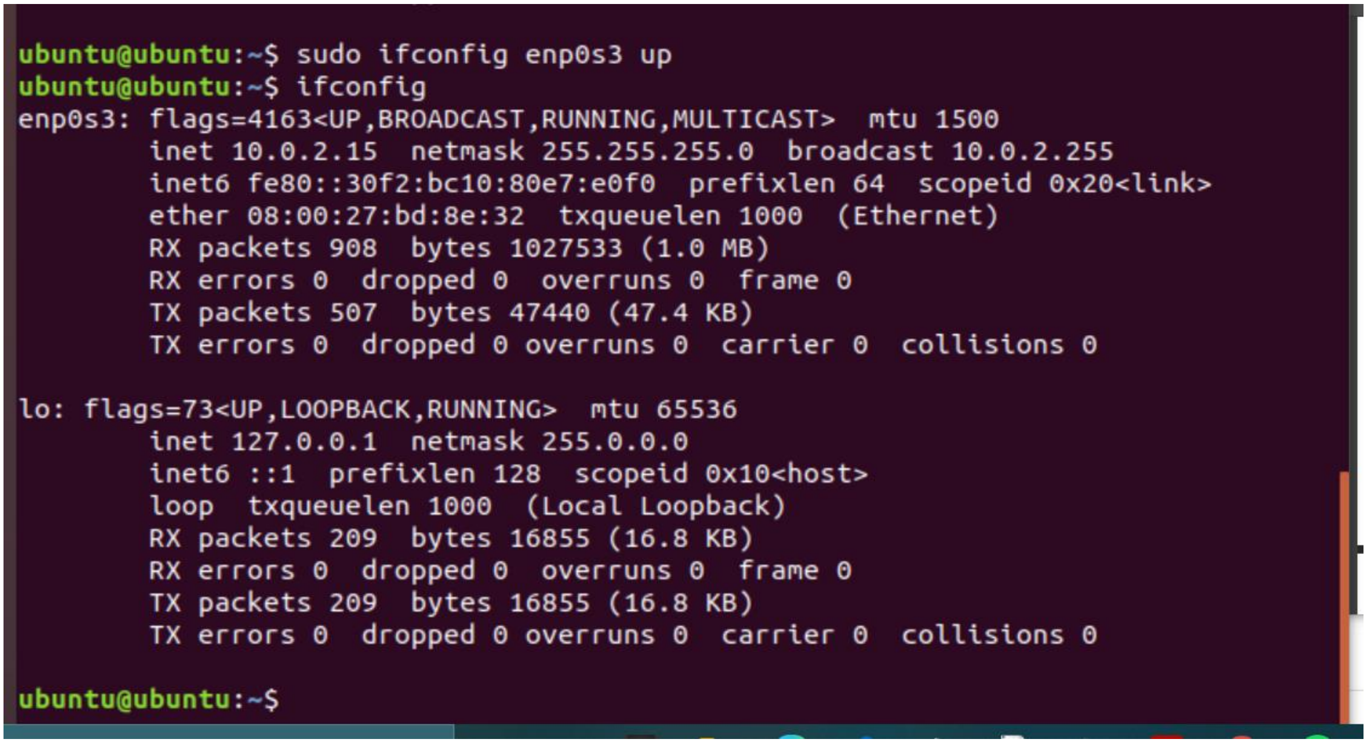
Deactivate:



```
ubuntu@ubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.6.45  netmask 255.255.255.0  broadcast 10.0.6.255
        inet6 fe80::30f2:bc10:80e7:e0f0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bd:8e:32  txqueuelen 1000  (Ethernet)
        RX packets 854  bytes 1021123 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 440  bytes 40308 (40.3 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 179  bytes 14767 (14.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 179  bytes 14767 (14.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@ubuntu:~$ sudo ifconfig enp0s3 down
ubuntu@ubuntu:~$ 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 179  bytes 14767 (14.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 179  bytes 14767 (14.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

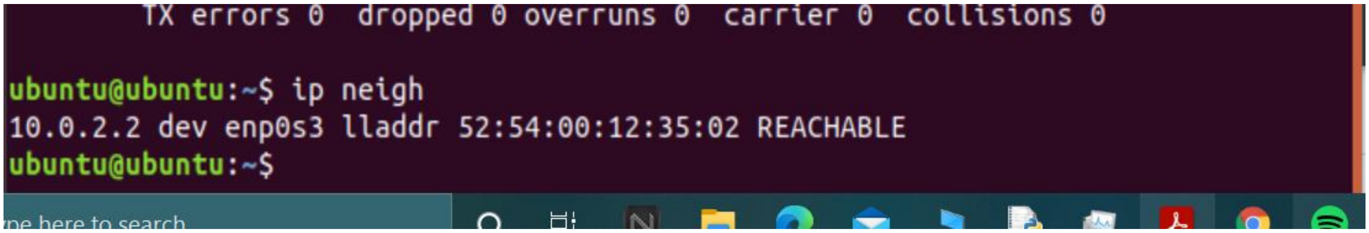
NOTE: Here the IP address has been changed to **10.0.6.45.**

Activate:



```
ubuntu@ubuntu:~$ sudo ifconfig enp0s3 up
ubuntu@ubuntu:~$ 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::30f2:bc10:80e7:e0f0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bd:8e:32  txqueuelen 1000  (Ethernet)
        RX packets 908  bytes 1027533 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 507  bytes 47440 (47.4 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 209  bytes 16855 (16.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 209  bytes 16855 (16.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ubuntu@ubuntu:~$
```

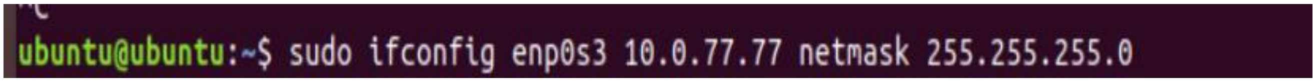
Step 4: Neighbour table:



```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

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

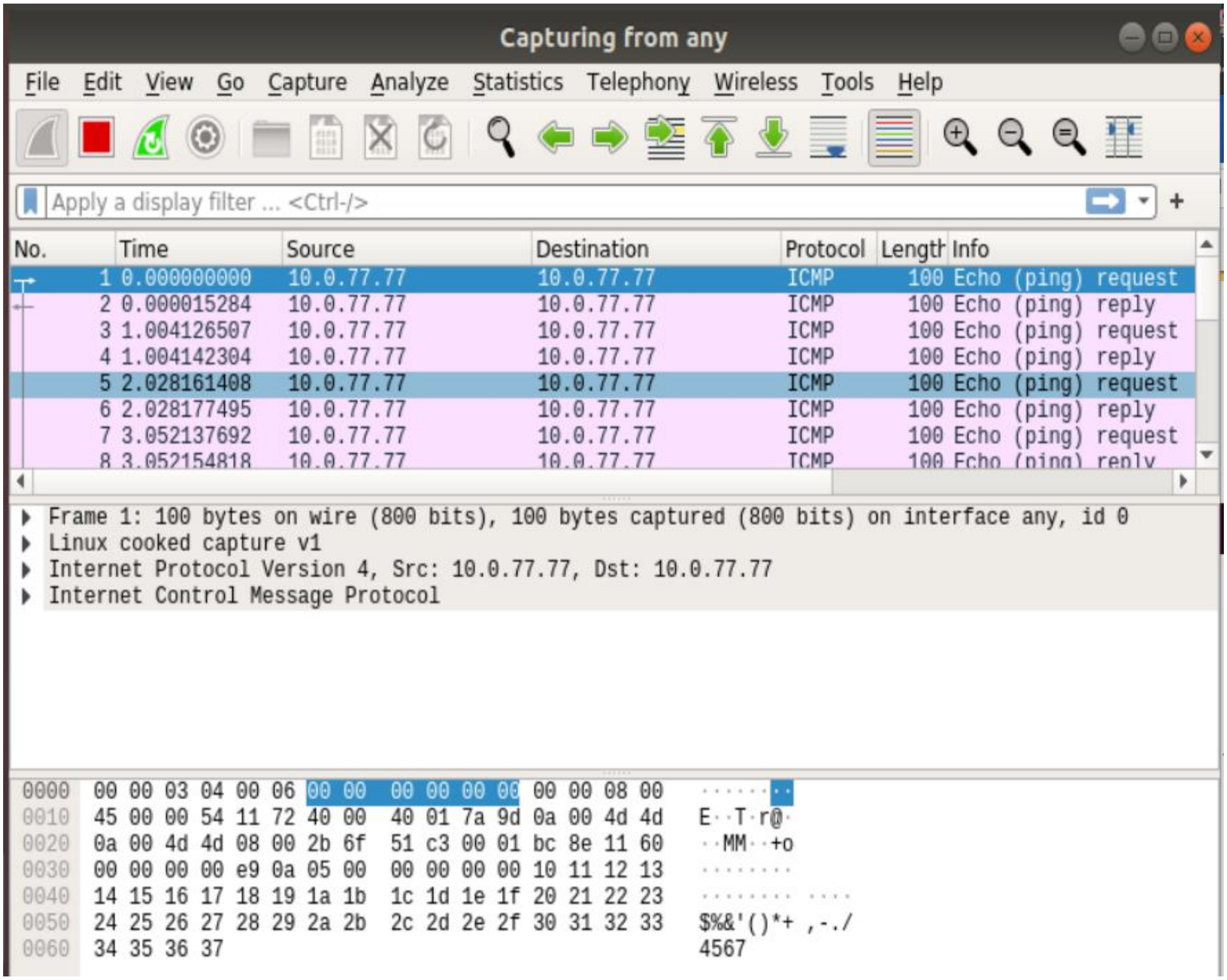
TASK-2:

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



```
ubuntu@ubuntu:~$ sudo ifconfig enp0s3 10.0.77.77 netmask 255.255.255.0
```

Step 2:

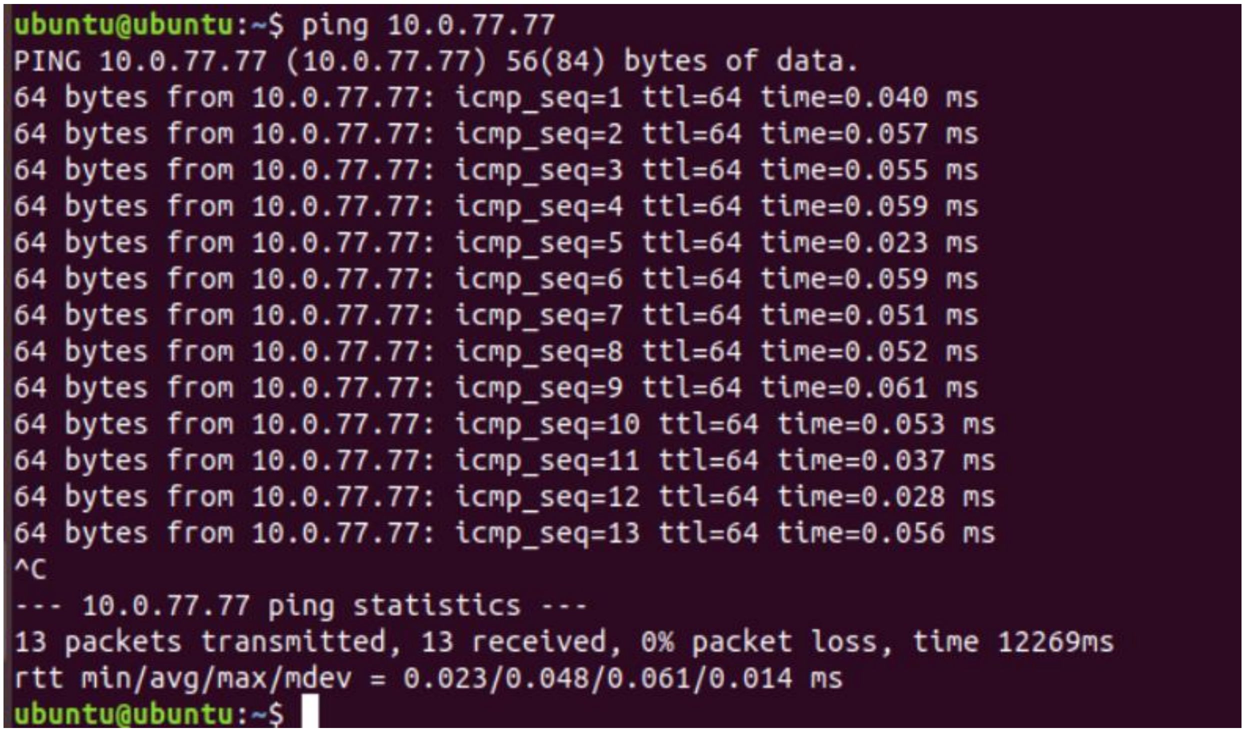

Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source       Destination   Protocol Length Info
    1 0.000000000   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) request
    2 0.000015284   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) reply
    3 1.004126507   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) request
    4 1.004142304   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) reply
    5 2.028161408   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) request
    6 2.028177495   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) reply
    7 3.052137692   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) request
    8 3.052154818   10.0.77.77   10.0.77.77    ICMP        100 Echo (ping) reply
```

```
▸ Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 10.0.77.77, Dst: 10.0.77.77
▸ Internet Control Message Protocol
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········
0010  45 00 00 54 11 72 40 00  40 01 7a 9d 0a 00 4d 4d   E··T·r@·
0020  0a 00 4d 4d 08 00 2b 6f  51 c3 00 01 bc 8e 11 60   ··MM··+o
0030  00 00 00 00 e9 0a 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   $%&'()*+ ,-./
0060  34 35 36 37                                        4567
```

Step 3:



```
ubuntu@ubuntu:~$ ping 10.0.77.77
PING 10.0.77.77 (10.0.77.77) 56(84) bytes of data.
64 bytes from 10.0.77.77: icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from 10.0.77.77: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 10.0.77.77: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 10.0.77.77: icmp_seq=4 ttl=64 time=0.059 ms
64 bytes from 10.0.77.77: icmp_seq=5 ttl=64 time=0.023 ms
64 bytes from 10.0.77.77: icmp_seq=6 ttl=64 time=0.059 ms
64 bytes from 10.0.77.77: icmp_seq=7 ttl=64 time=0.051 ms
64 bytes from 10.0.77.77: icmp_seq=8 ttl=64 time=0.052 ms
64 bytes from 10.0.77.77: icmp_seq=9 ttl=64 time=0.061 ms
64 bytes from 10.0.77.77: icmp_seq=10 ttl=64 time=0.053 ms
64 bytes from 10.0.77.77: icmp_seq=11 ttl=64 time=0.037 ms
64 bytes from 10.0.77.77: icmp_seq=12 ttl=64 time=0.028 ms
64 bytes from 10.0.77.77: icmp_seq=13 ttl=64 time=0.056 ms
^C
--- 10.0.77.77 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12269ms
rtt min/avg/max/mdev = 0.023/0.048/0.061/0.014 ms
ubuntu@ubuntu:~$ 
```

Step 4:From above Screenshot we can see:

TTL=**64**

Protocol used by ping: **ICMP**

Time (Total for all) = **122269ms**

Step 5:

Details	**First Echo Request**	**First Echo Reply**
Frame Number	1	2
Source IP address	10.0.77.77	10.0.77.77
Destination IP address	10.0.77.77	10.0.77.77
ICMP Type Value	8(Echo (ping)request)	0 (Echo (ping)reply)
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00

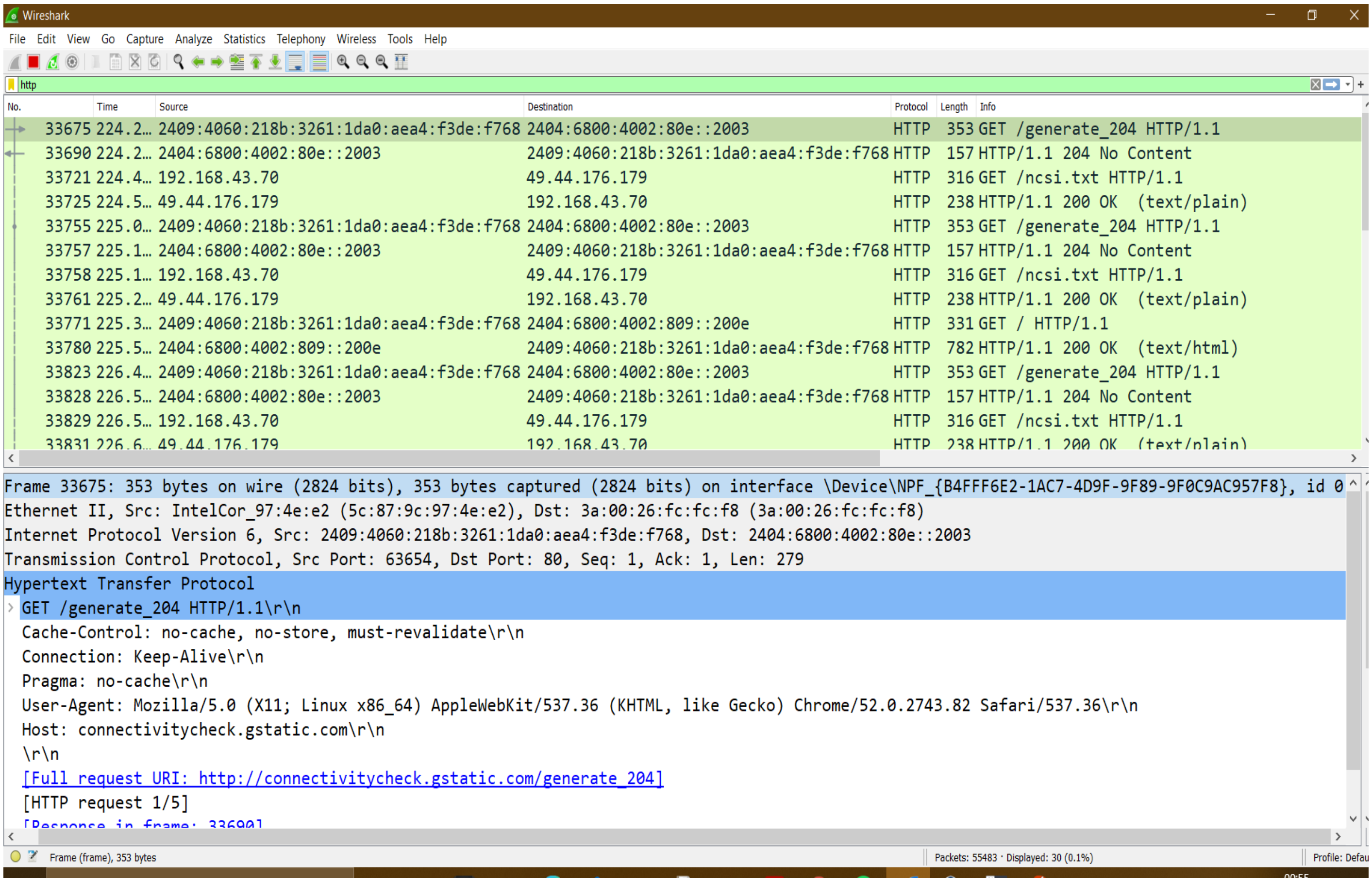
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

Here, I have **pinged from the same system**, and so, *the source IP and Destination IP is same for both echo request and reply*.

TASK-3:

Step 3:

First echo request:



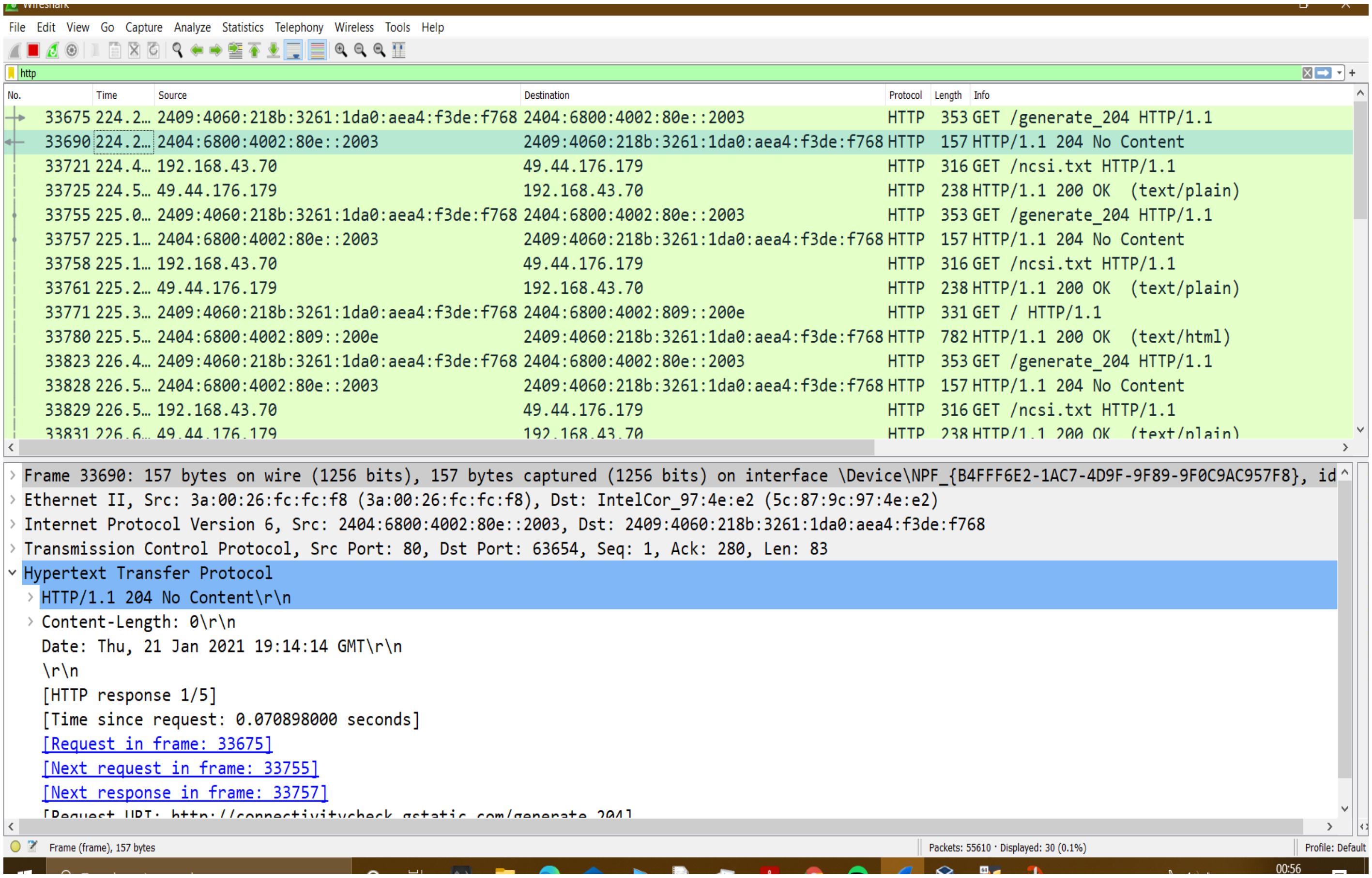
Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time     Source                                  Destination                             Protocol Length Info
33675 224.2… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                HTTP   353 GET /generate_204 HTTP/1.1
33690 224.2… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768 HTTP   157 HTTP/1.1 204 No Content
33721 224.4… 192.168.43.70                           49.44.176.179                           HTTP   316 GET /ncsi.txt HTTP/1.1
33725 224.5… 49.44.176.179                           192.168.43.70                           HTTP   238 HTTP/1.1 200 OK  (text/plain)
33755 225.0… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                HTTP   353 GET /generate_204 HTTP/1.1
33757 225.1… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768 HTTP   157 HTTP/1.1 204 No Content
33758 225.1… 192.168.43.70                           49.44.176.179                           HTTP   316 GET /ncsi.txt HTTP/1.1
33761 225.2… 49.44.176.179                           192.168.43.70                           HTTP   238 HTTP/1.1 200 OK  (text/plain)
33771 225.3… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:809::200e                HTTP   331 GET / HTTP/1.1
33780 225.5… 2404:6800:4002:809::200e                2409:4060:218b:3261:1da0:aea4:f3de:f768 HTTP   782 HTTP/1.1 200 OK  (text/html)
33823 226.4… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                HTTP   353 GET /generate_204 HTTP/1.1
33828 226.5… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768 HTTP   157 HTTP/1.1 204 No Content
33829 226.5… 192.168.43.70                           49.44.176.179                           HTTP   316 GET /ncsi.txt HTTP/1.1
33831 226.6… 49.44.176.179                           192.168.43.70                           HTTP   238 HTTP/1.1 200 OK  (text/plain)
```

```
Frame 33675: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface \Device\NPF_{B4FFF6E2-1AC7-4D9F-9F89-9F0C9AC957F8}, id 0
Ethernet II, Src: IntelCor_97:4e:e2 (5c:87:9c:97:4e:e2), Dst: 3a:00:26:fc:fc:f8 (3a:00:26:fc:fc:f8)
Internet Protocol Version 6, Src: 2409:4060:218b:3261:1da0:aea4:f3de:f768, Dst: 2404:6800:4002:80e::2003
Transmission Control Protocol, Src Port: 63654, Dst Port: 80, Seq: 1, Ack: 1, Len: 279
Hypertext Transfer Protocol
> GET /generate_204 HTTP/1.1\r\n
  Cache-Control: no-cache, no-store, must-revalidate\r\n
  Connection: Keep-Alive\r\n
  Pragma: no-cache\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.82 Safari/537.36\r\n
  Host: connectivitycheck.gstatic.com\r\n
  \r\n
  [Full request URI: http://connectivitycheck.gstatic.com/generate_204]
  [HTTP request 1/5]
  [Response in frame: 33690]
```

```
Frame (frame), 353 bytes          Packets: 55483 · Displayed: 30 (0.1%)          Profile: Defau
```

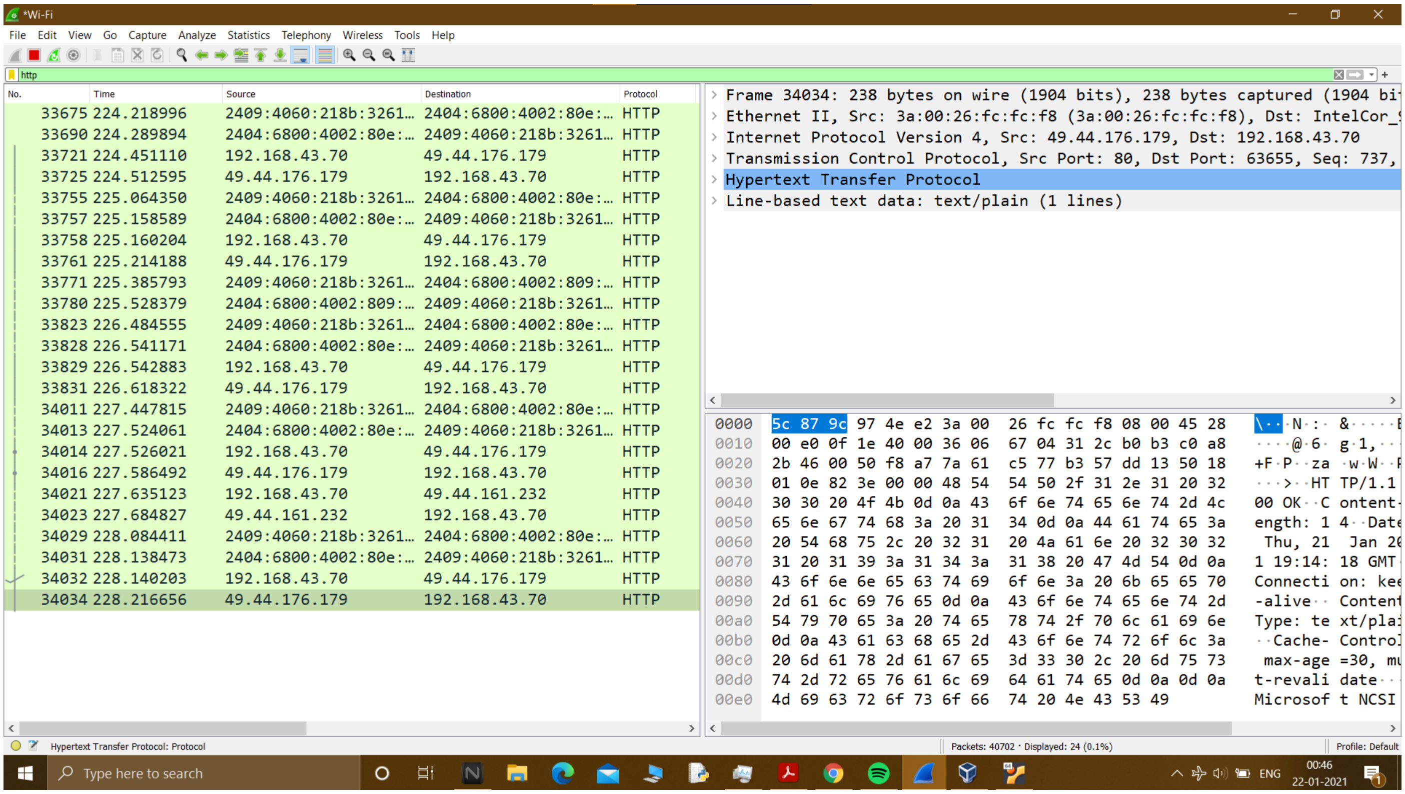
First echo reply:



Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time      Source                                 Destination                            Protocol Length Info
33675 224.2… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                  HTTP  353 GET /generate_204 HTTP/1.1
33690 224.2… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768   HTTP  157 HTTP/1.1 204 No Content
33721 224.4… 192.168.43.70                           49.44.176.179                             HTTP  316 GET /ncsi.txt HTTP/1.1
33725 224.5… 49.44.176.179                           192.168.43.70                             HTTP  238 HTTP/1.1 200 OK  (text/plain)
33755 225.0… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                  HTTP  353 GET /generate_204 HTTP/1.1
33757 225.1… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768   HTTP  157 HTTP/1.1 204 No Content
33758 225.1… 192.168.43.70                           49.44.176.179                             HTTP  316 GET /ncsi.txt HTTP/1.1
33761 225.2… 49.44.176.179                           192.168.43.70                             HTTP  238 HTTP/1.1 200 OK  (text/plain)
33771 225.3… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:809::200e                  HTTP  331 GET / HTTP/1.1
33780 225.5… 2404:6800:4002:809::200e                2409:4060:218b:3261:1da0:aea4:f3de:f768   HTTP  782 HTTP/1.1 200 OK  (text/html)
33823 226.4… 2409:4060:218b:3261:1da0:aea4:f3de:f768 2404:6800:4002:80e::2003                  HTTP  353 GET /generate_204 HTTP/1.1
33828 226.5… 2404:6800:4002:80e::2003                2409:4060:218b:3261:1da0:aea4:f3de:f768   HTTP  157 HTTP/1.1 204 No Content
33829 226.5… 192.168.43.70                           49.44.176.179                             HTTP  316 GET /ncsi.txt HTTP/1.1
33831 226.6… 49.44.176.179                           192.168.43.70                             HTTP  238 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 33690: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{B4FFF6E2-1AC7-4D9F-9F89-9F0C9AC957F8}, id
> Ethernet II, Src: 3a:00:26:fc:fc:f8 (3a:00:26:fc:fc:f8), Dst: IntelCor_97:4e:e2 (5c:87:9c:97:4e:e2)
> Internet Protocol Version 6, Src: 2404:6800:4002:80e::2003, Dst: 2409:4060:218b:3261:1da0:aea4:f3de:f768
> Transmission Control Protocol, Src Port: 80, Dst Port: 63654, Seq: 1, Ack: 280, Len: 83
v Hypertext Transfer Protocol
  > HTTP/1.1 204 No Content\r\n
  > Content-Length: 0\r\n
    Date: Thu, 21 Jan 2021 19:14:14 GMT\r\n
    \r\n
    [HTTP response 1/5]
    [Time since request: 0.070898000 seconds]
    [Request in frame: 33675]
    [Next request in frame: 33755]
    [Next response in frame: 33757]
    [Request URI: http://connectivitycheck.gstatic.com/generate_204]
```


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.    Time        Source                Destination           Protocol
 33675 224.218996  2409:4060:218b:3261…  2404:6800:4002:80e:…  HTTP
 33690 224.289894  2404:6800:4002:80e:…  2409:4060:218b:3261…  HTTP
 33721 224.451110  192.168.43.70         49.44.176.179         HTTP
 33725 224.512595  49.44.176.179         192.168.43.70         HTTP
 33755 225.064350  2409:4060:218b:3261…  2404:6800:4002:80e:…  HTTP
 33757 225.158589  2404:6800:4002:80e:…  2409:4060:218b:3261…  HTTP
 33758 225.160204  192.168.43.70         49.44.176.179         HTTP
 33761 225.214188  49.44.176.179         192.168.43.70         HTTP
 33771 225.385793  2409:4060:218b:3261…  2404:6800:4002:809:…  HTTP
 33780 225.528379  2404:6800:4002:809:…  2409:4060:218b:3261…  HTTP
 33823 226.484555  2409:4060:218b:3261…  2404:6800:4002:80e:…  HTTP
 33828 226.541171  2404:6800:4002:80e:…  2409:4060:218b:3261…  HTTP
 33829 226.542883  192.168.43.70         49.44.176.179         HTTP
 33831 226.618322  49.44.176.179         192.168.43.70         HTTP
 34011 227.447815  2409:4060:218b:3261…  2404:6800:4002:80e:…  HTTP
 34013 227.524061  2404:6800:4002:80e:…  2409:4060:218b:3261…  HTTP
 34014 227.526021  192.168.43.70         49.44.176.179         HTTP
 34016 227.586492  49.44.176.179         192.168.43.70         HTTP
 34021 227.635123  192.168.43.70         49.44.161.232         HTTP
 34023 227.684827  49.44.161.232         192.168.43.70         HTTP
 34029 228.084411  2409:4060:218b:3261…  2404:6800:4002:80e:…  HTTP
 34031 228.138473  2404:6800:4002:80e:…  2409:4060:218b:3261…  HTTP
 34032 228.140203  192.168.43.70         49.44.176.179         HTTP
 34034 228.216656  49.44.176.179         192.168.43.70         HTTP
```

```
> Frame 34034: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bi
> Ethernet II, Src: 3a:00:26:fc:fc:f8 (3a:00:26:fc:fc:f8), Dst: IntelCor_
> Internet Protocol Version 4, Src: 49.44.176.179, Dst: 192.168.43.70
> Transmission Control Protocol, Src Port: 80, Dst Port: 63655, Seq: 737,
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  5c 87 9c 97 4e e2 3a 00  26 fc fc f8 08 00 45 28   \···N·:· &·····E
0010  00 e0 0f 1e 40 00 36 06  67 04 31 2c b0 b3 c0 a8   ····@·6· g·1,···
0020  2b 46 00 50 f8 a7 7a 61  c5 77 b3 57 dd 13 50 18   +F·P··za ·w·W··P
0030  01 0e 82 3e 00 00 48 54  54 50 2f 31 2e 31 20 32   ···>··HT TP/1.1 
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-
0050  65 6e 67 74 68 3a 20 31  34 0d 0a 44 61 74 65 3a   ength: 1 4··Date
0060  20 54 68 75 2c 20 32 31  20 4a 61 6e 20 32 30 32    Thu, 21  Jan 20
0070  31 20 31 39 3a 31 34 3a  31 38 20 47 4d 54 0d 0a   1 19:14: 18 GMT·
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 6b 65 65 70   Connecti on: kee
0090  2d 61 6c 69 76 65 0d 0a  43 6f 6e 74 65 6e 74 2d   -alive·· Content
00a0  54 79 70 65 3a 20 74 65  78 74 2f 70 6c 61 69 6e   Type: te xt/plai
00b0  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control
00c0  20 6d 61 78 2d 61 67 65  3d 33 30 2c 20 6d 75 73    max-age =30, mu
00d0  74 2d 72 65 76 61 6c 69  64 61 74 65 0d 0a 0d 0a   t-revali date···
00e0  4d 69 63 72 6f 73 6f 66  74 20 4e 43 53 49         Microsof t NCSI
```

Hypertext Transfer Protocol: Protocol

Packets: 40702 · Displayed: 24 (0.1%)

Profile: Default

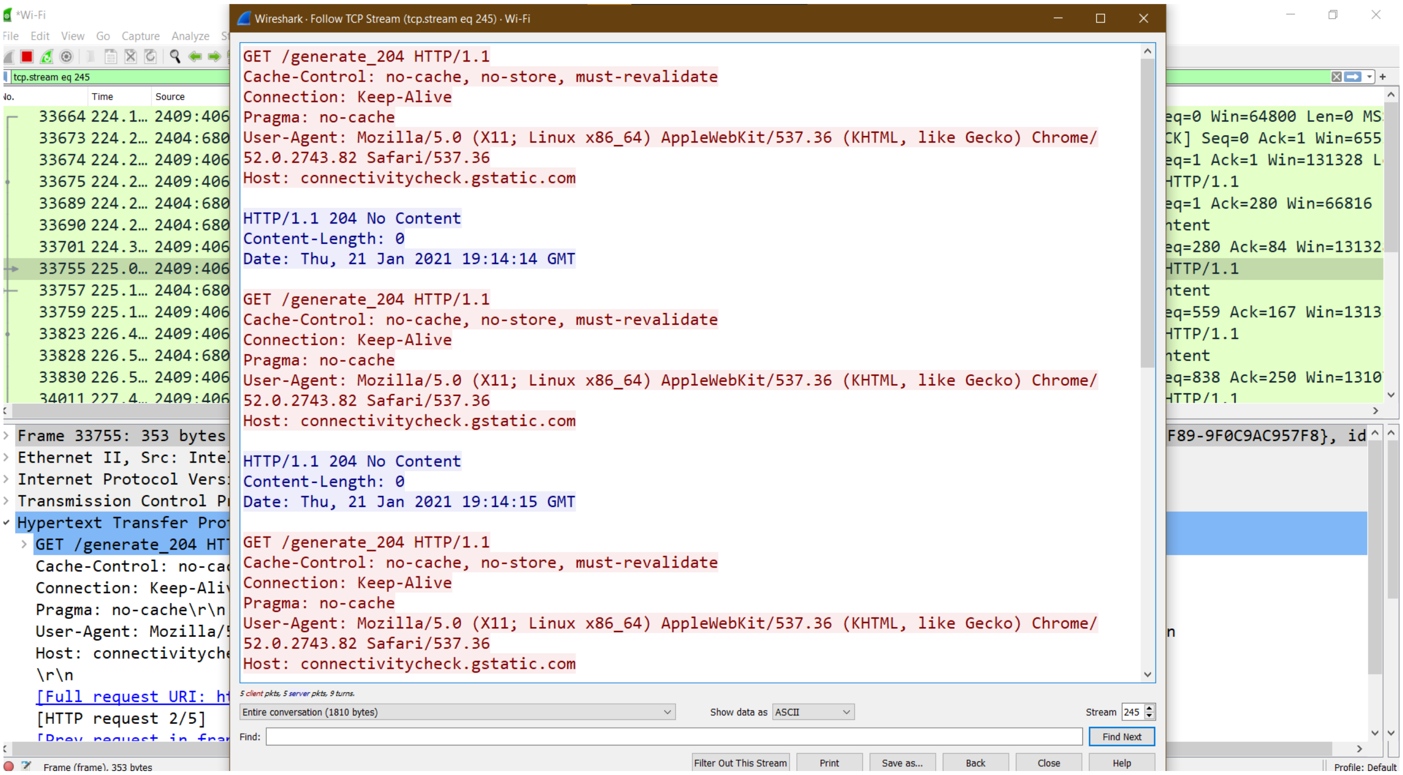
NOTE: I have used Wireshark in windows for this task.

Details	**First Echo Request**	**First Echo Reply**
Frame Number	33675	33690
Source Port	63654	80
Destination Port	80	63654
Source IP address	192.168.43.70	49.44.176.179
Destination IP address	49.44.176.179	192.168.43.70
Source Ethernet Address	5c:87:9c:97:4e:e2	3a:00:26:fc:fc:f8
Destination Ethernet Address	3a:00:26:fc:fc:f8	5c:87:9c:97:4e:e2

Step 4:

HTTP Request		**HTTP Response**	
Get	/ncsi.txt HTTP/1.1\r\n	Server	ngi-nx
Host	www.msfncsi.com\r\n	Content-Type	text/Plain
User-Agent	Mozilla/5.0 (X11;Linux x86_64) AppleWebKit/537.36(KHTML, like Gecko) Chrome/52.0.2743.82 Safari/537.36\r\n	Date	Thu, 21 Jan 2021 19:14:14 GMT\r\n
Accept-Language	en-US,en;q=0.5	Location	-
Accept-Encoding	gzip,deflate	Content-Length	14\r\n
Connection	Keep-Alive\r\n\	Connection	-

Using Wireshark's Follow TCP Stream



```
33664 224.1… 2409:406
33673 224.2… 2404:680
33674 224.2… 2409:406
33675 224.2… 2409:406
33689 224.2… 2404:680
33690 224.2… 2404:680
33701 224.3… 2409:406
33755 225.0… 2409:406
33757 225.1… 2404:680
33759 225.1… 2409:406
33823 226.4… 2409:406
33828 226.5… 2404:680
33830 226.5… 2409:406
34011 227.4… 2409:406
```

```
eq=0 Win=64800 Len=0 MS
CK] Seq=0 Ack=1 Win=655
eq=1 Ack=1 Win=131328 L
HTTP/1.1
eq=1 Ack=280 Win=66816
ntent
eq=280 Ack=84 Win=13132
HTTP/1.1
ntent
eq=559 Ack=167 Win=1313
HTTP/1.1
ntent
eq=838 Ack=250 Win=1310
HTTP/1.1
```

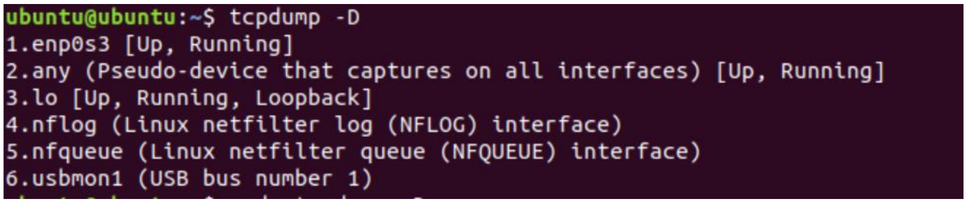
```
> Frame 33755: 353 bytes
> Ethernet II, Src: Inte
> Internet Protocol Vers
> Transmission Control P
v Hypertext Transfer Pro
  > GET /generate_204 HT
    Cache-Control: no-ca
    Connection: Keep-Ali
    Pragma: no-cache\r\n
    User-Agent: Mozilla/
    Host: connectivitych
    \r\n
    [Full request URI: ht
    [HTTP request 2/5]
    [Prev request in fra
```

```
F89-9F0C9AC957F8}, id
n
```

```
GET /generate_204 HTTP/1.1
Cache-Control: no-cache, no-store, must-revalidate
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
52.0.2743.82 Safari/537.36
Host: connectivitycheck.gstatic.com

HTTP/1.1 204 No Content
Content-Length: 0
Date: Thu, 21 Jan 2021 19:14:14 GMT

GET /generate_204 HTTP/1.1
Cache-Control: no-cache, no-store, must-revalidate
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
52.0.2743.82 Safari/537.36
Host: connectivitycheck.gstatic.com

HTTP/1.1 204 No Content
Content-Length: 0
Date: Thu, 21 Jan 2021 19:14:15 GMT

GET /generate_204 HTTP/1.1
Cache-Control: no-cache, no-store, must-revalidate
Connection: Keep-Alive
Pragma: no-cache
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
52.0.2743.82 Safari/537.36
Host: connectivitycheck.gstatic.com
```

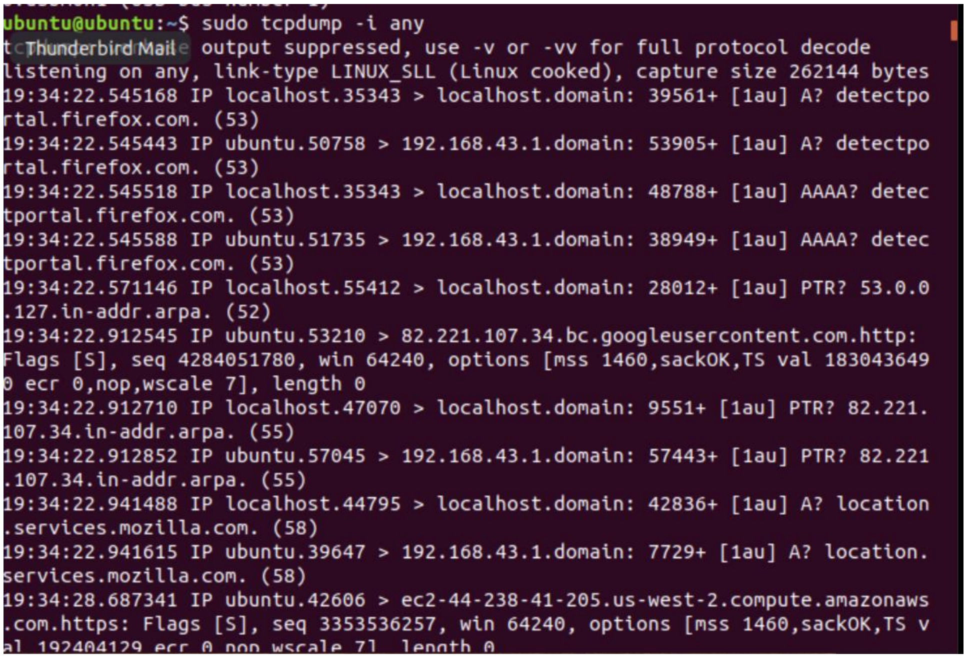
TASK-4:

Step 1:



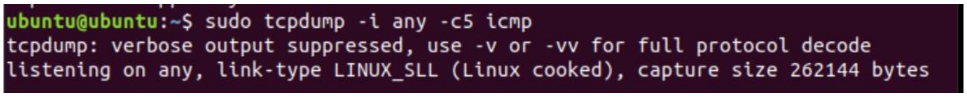
```
ubuntu@ubuntu:~$ tcpdump -D
1.enp0s3 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.nflog (Linux netfilter log (NFLOG) interface)
5.nfqueue (Linux netfilter queue (NFQUEUE) interface)
6.usbmon1 (USB bus number 1)
```

Step 2:



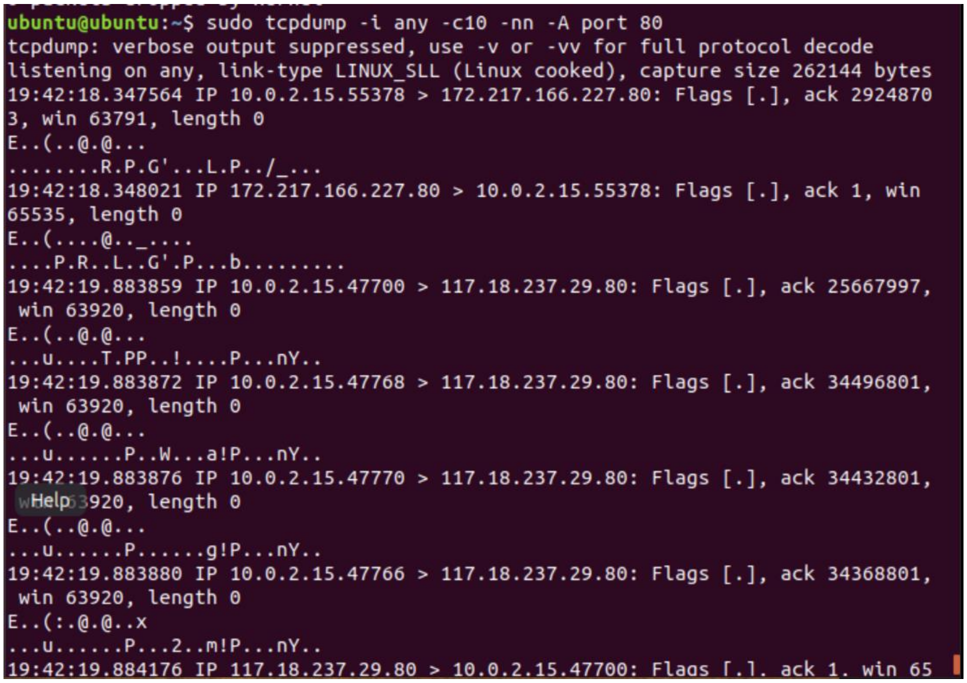
```
ubuntu@ubuntu:~$ sudo tcpdump -i any
tcThunderbird Maile output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
19:34:22.545168 IP localhost.35343 > localhost.domain: 39561+ [1au] A? detectpo
rtal.firefox.com. (53)
19:34:22.545443 IP ubuntu.50758 > 192.168.43.1.domain: 53905+ [1au] A? detectpo
rtal.firefox.com. (53)
19:34:22.545518 IP localhost.35343 > localhost.domain: 48788+ [1au] AAAA? detec
tportal.firefox.com. (53)
19:34:22.545588 IP ubuntu.51735 > 192.168.43.1.domain: 38949+ [1au] AAAA? detec
tportal.firefox.com. (53)
19:34:22.571146 IP localhost.55412 > localhost.domain: 28012+ [1au] PTR? 53.0.0
.127.in-addr.arpa. (52)
19:34:22.912545 IP ubuntu.53210 > 82.221.107.34.bc.googleusercontent.com.http:
Flags [S], seq 4284051780, win 64240, options [mss 1460,sackOK,TS val 183043649
0 ecr 0,nop,wscale 7], length 0
19:34:22.912710 IP localhost.47070 > localhost.domain: 9551+ [1au] PTR? 82.221.
107.34.in-addr.arpa. (55)
19:34:22.912852 IP ubuntu.57045 > 192.168.43.1.domain: 57443+ [1au] PTR? 82.221
.107.34.in-addr.arpa. (55)
19:34:22.941488 IP localhost.44795 > localhost.domain: 42836+ [1au] A? location
.services.mozilla.com. (58)
19:34:22.941615 IP ubuntu.39647 > 192.168.43.1.domain: 7729+ [1au] A? location.
services.mozilla.com. (58)
19:34:28.687341 IP ubuntu.42606 > ec2-44-238-41-205.us-west-2.compute.amazonaws
.com.https: Flags [S], seq 3353536257, win 64240, options [mss 1460,sackOK,TS v
al 192404129 ecr 0,nop,wscale 7], length 0
```

Step 4:



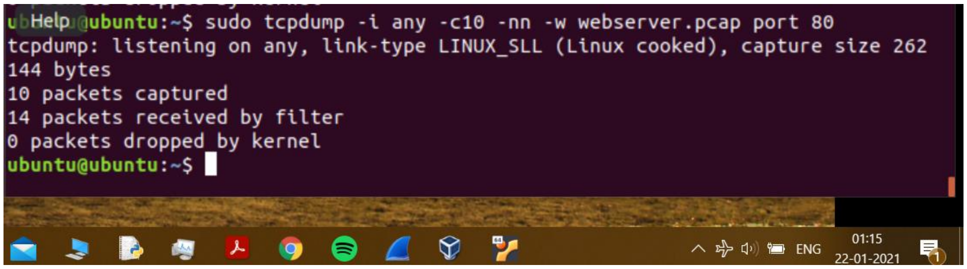
```
ubuntu@ubuntu:~$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
```

Step 5:



```
ubuntu@ubuntu:~$ 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), capture size 262144 bytes
19:42:18.347564 IP 10.0.2.15.55378 > 172.217.166.227.80: Flags [.], ack 2924870
3, win 63791, length 0
E..(..@.@...
........R.P.G'...L.P../_...
19:42:18.348021 IP 172.217.166.227.80 > 10.0.2.15.55378: Flags [.], ack 1, win
65535, length 0
E..(....@.._....
....P.R..L..G'.P...b.........
19:42:19.883859 IP 10.0.2.15.47700 > 117.18.237.29.80: Flags [.], ack 25667997,
 win 63920, length 0
E..(..@.@...
...u....T.PP..!....P...nY..
19:42:19.883872 IP 10.0.2.15.47768 > 117.18.237.29.80: Flags [.], ack 34496801,
 win 63920, length 0
E..(..@.@...
...u......P..W...a!P...nY..
19:42:19.883876 IP 10.0.2.15.47770 > 117.18.237.29.80: Flags [.], ack 34432801,
 wHelp3920, length 0
E..(..@.@...
...u......P......g!P...nY..
19:42:19.883880 IP 10.0.2.15.47766 > 117.18.237.29.80: Flags [.], ack 34368801,
 win 63920, length 0
E..(:.@.@..x
...u......P...2..m!P...nY..
19:42:19.884176 IP 117.18.237.29.80 > 10.0.2.15.47700: Flags [.], ack 1, win 65
```

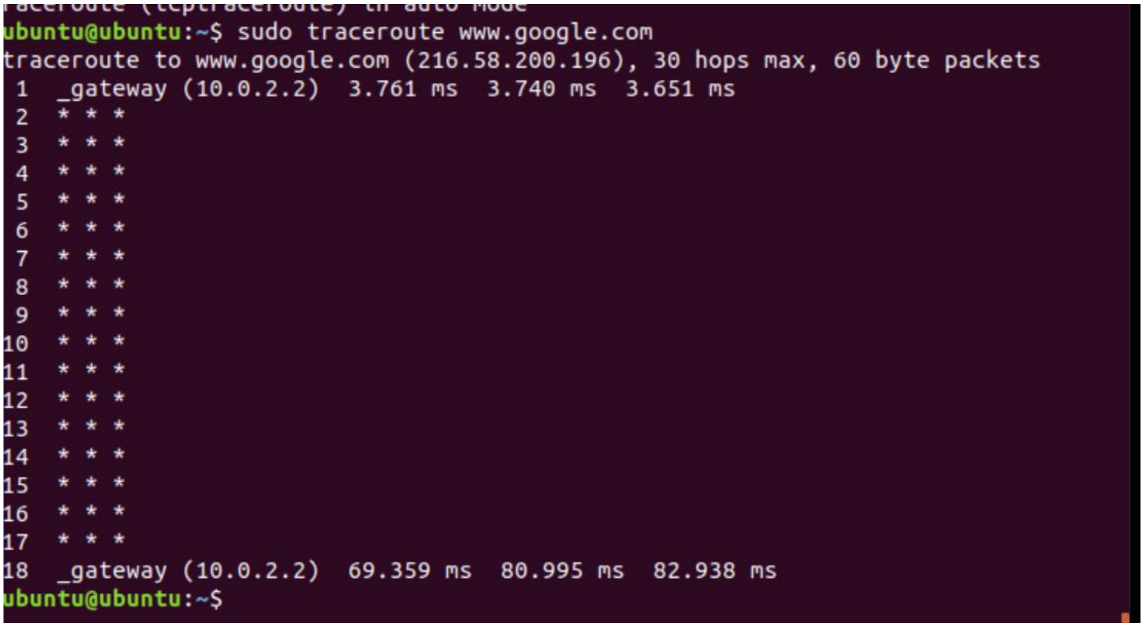
Step 6:



```
ubuntu@ubuntu:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262
144 bytes
10 packets captured
14 packets received by filter
0 packets dropped by kernel
ubuntu@ubuntu:~$
```

TASK-5: Perform Traceroute checks

Step 1: Run the traceroute

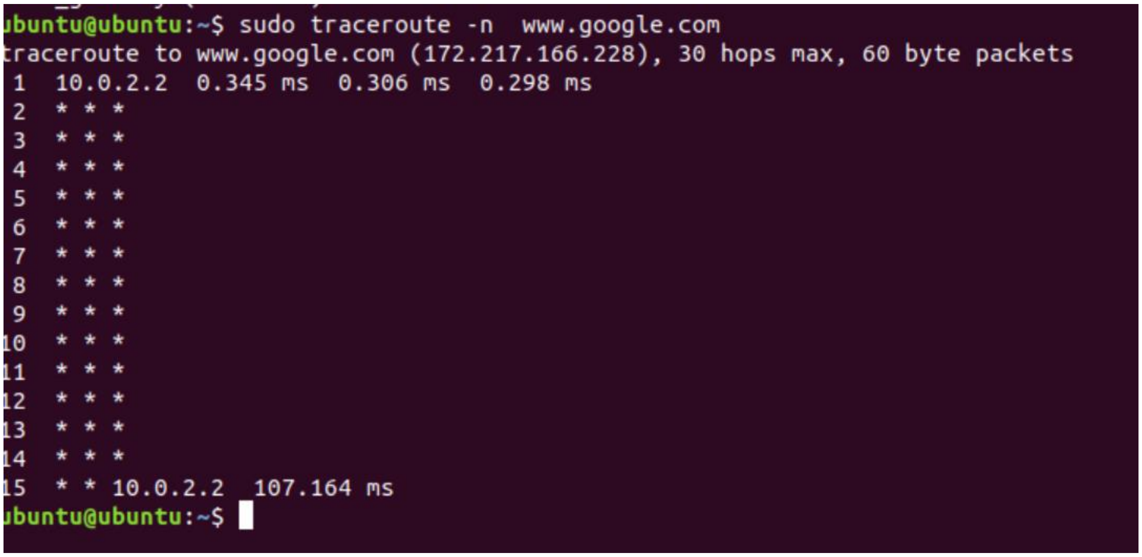


```
ubuntu@ubuntu:~$ sudo traceroute www.google.com
traceroute to www.google.com (216.58.200.196), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  3.761 ms  3.740 ms  3.651 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  _gateway (10.0.2.2)  69.359 ms  80.995 ms  82.938 ms
ubuntu@ubuntu:~$
```

Step 2: Destination address of google.com is **216.58.200.196**

Number of hops required to reach google is **18**.

Step 3: Speeding up the process using –n option:

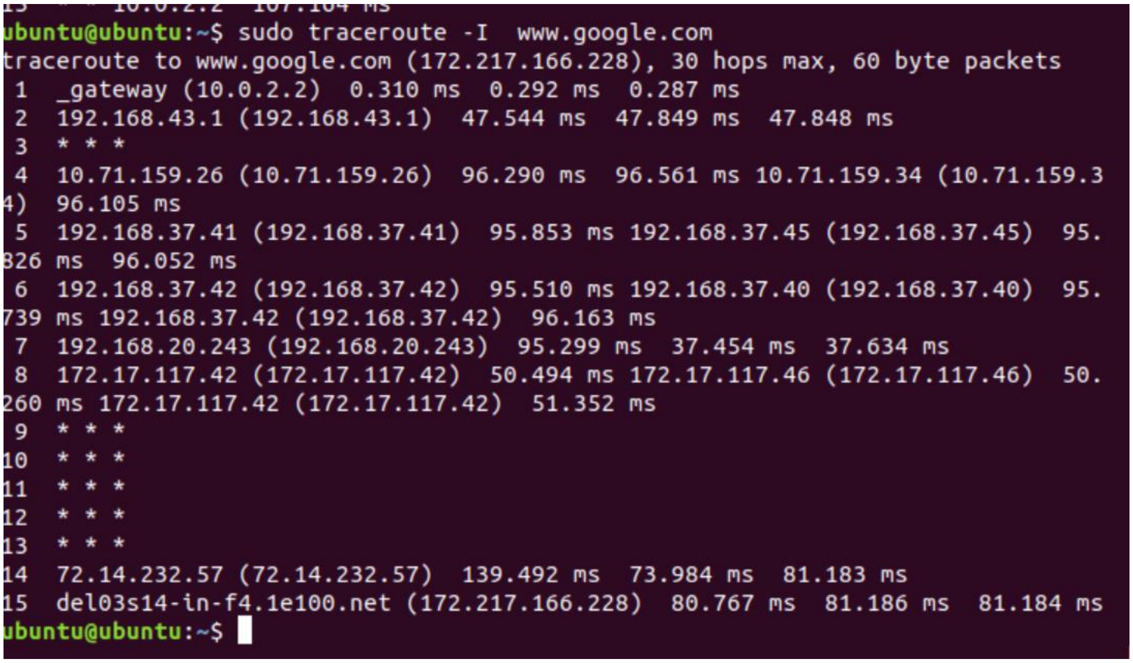


```
ubuntu@ubuntu:~$ sudo traceroute -n  www.google.com
traceroute to www.google.com (172.217.166.228), 30 hops max, 60 byte packets
 1  10.0.2.2  0.345 ms  0.306 ms  0.298 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * 10.0.2.2  107.164 ms
ubuntu@ubuntu:~$ 
```

Number of hops required to reach google has reduced to **15**.

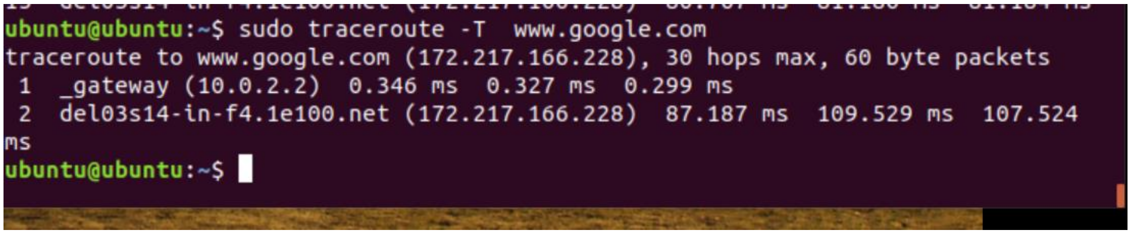
Even the destination address of google changes.

Step 4: Making the traceroute use ICMP using –I option:



```
15  * * 10.0.2.2  107.164 ms
ubuntu@ubuntu:~$ sudo traceroute -I  www.google.com
traceroute to www.google.com (172.217.166.228), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.310 ms  0.292 ms  0.287 ms
 2  192.168.43.1 (192.168.43.1)  47.544 ms  47.849 ms  47.848 ms
 3  * * *
 4  10.71.159.26 (10.71.159.26)  96.290 ms  96.561 ms 10.71.159.34 (10.71.159.3
4)  96.105 ms
 5  192.168.37.41 (192.168.37.41)  95.853 ms 192.168.37.45 (192.168.37.45)  95.
826 ms  96.052 ms
 6  192.168.37.42 (192.168.37.42)  95.510 ms 192.168.37.40 (192.168.37.40)  95.
739 ms 192.168.37.42 (192.168.37.42)  96.163 ms
 7  192.168.20.243 (192.168.20.243)  95.299 ms  37.454 ms  37.634 ms
 8  172.17.117.42 (172.17.117.42)  50.494 ms 172.17.117.46 (172.17.117.46)  50.
260 ms 172.17.117.42 (172.17.117.42)  51.352 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  72.14.232.57 (72.14.232.57)  139.492 ms  73.984 ms  81.183 ms
15  del03s14-in-f4.1e100.net (172.217.166.228)  80.767 ms  81.186 ms  81.184 ms
ubuntu@ubuntu:~$ 
```

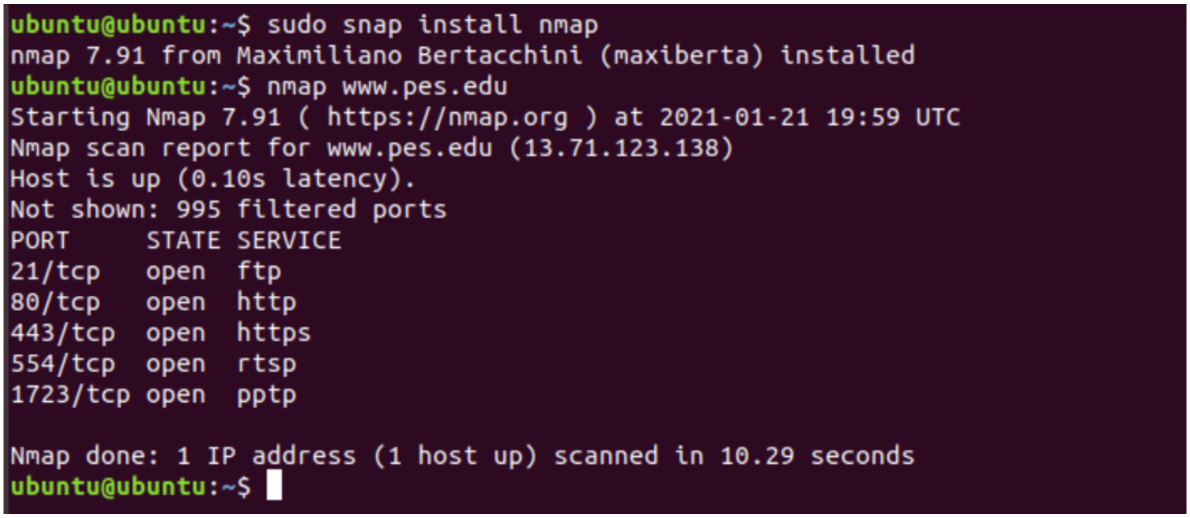
Step 5: Making the traceroute use TCP using –T option:



```
ubuntu@ubuntu:~$ sudo traceroute -T  www.google.com
traceroute to www.google.com (172.217.166.228), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.346 ms  0.327 ms  0.299 ms
 2  del03s14-in-f4.1e100.net (172.217.166.228)  87.187 ms  109.529 ms  107.524
ms
ubuntu@ubuntu:~$ 
```

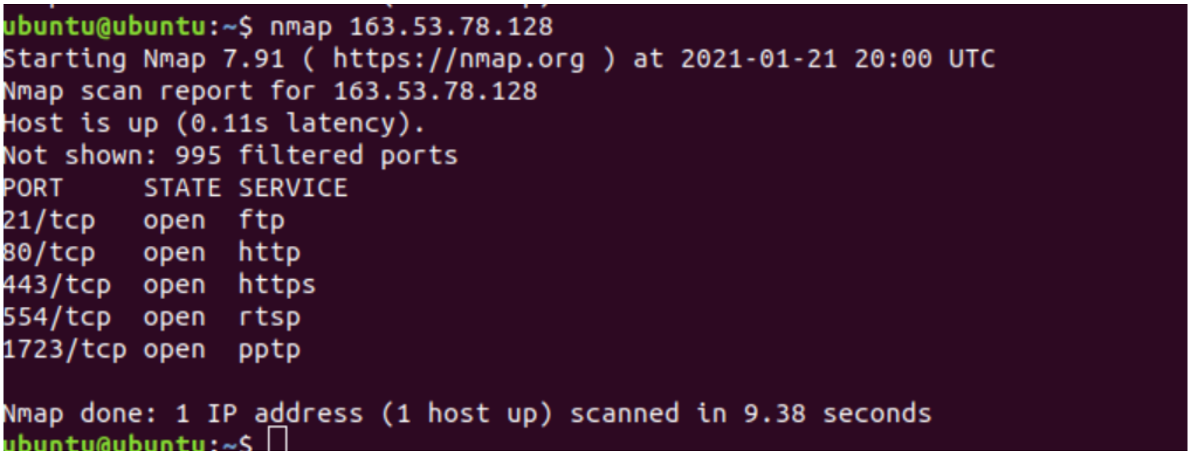
TASK-6: Explore an entire network for information (Nmap)

Step 1: Scan a host using its host name or IP address



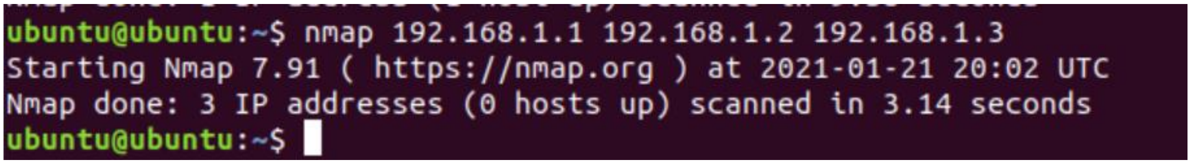
```
ubuntu@ubuntu:~$ sudo snap install nmap
nmap 7.91 from Maximiliano Bertacchini (maxiberta) installed
ubuntu@ubuntu:~$ nmap www.pes.edu
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 19:59 UTC
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.10s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 10.29 seconds
ubuntu@ubuntu:~$ 
```

Step 2: Use an IP address to scan.



```
ubuntu@ubuntu:~$ nmap 163.53.78.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 20:00 UTC
Nmap scan report for 163.53.78.128
Host is up (0.11s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 9.38 seconds
ubuntu@ubuntu:~$ 
```

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



```
ubuntu@ubuntu:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 20:02 UTC
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.14 seconds
ubuntu@ubuntu:~$
```

TASK-7:

a) Intra system communication (Using 2 terminals in the same system)

Step 1: Open a terminal (Ctrl+Alt+T). This will act as a Server.

Step 2: nc -l any_portnum

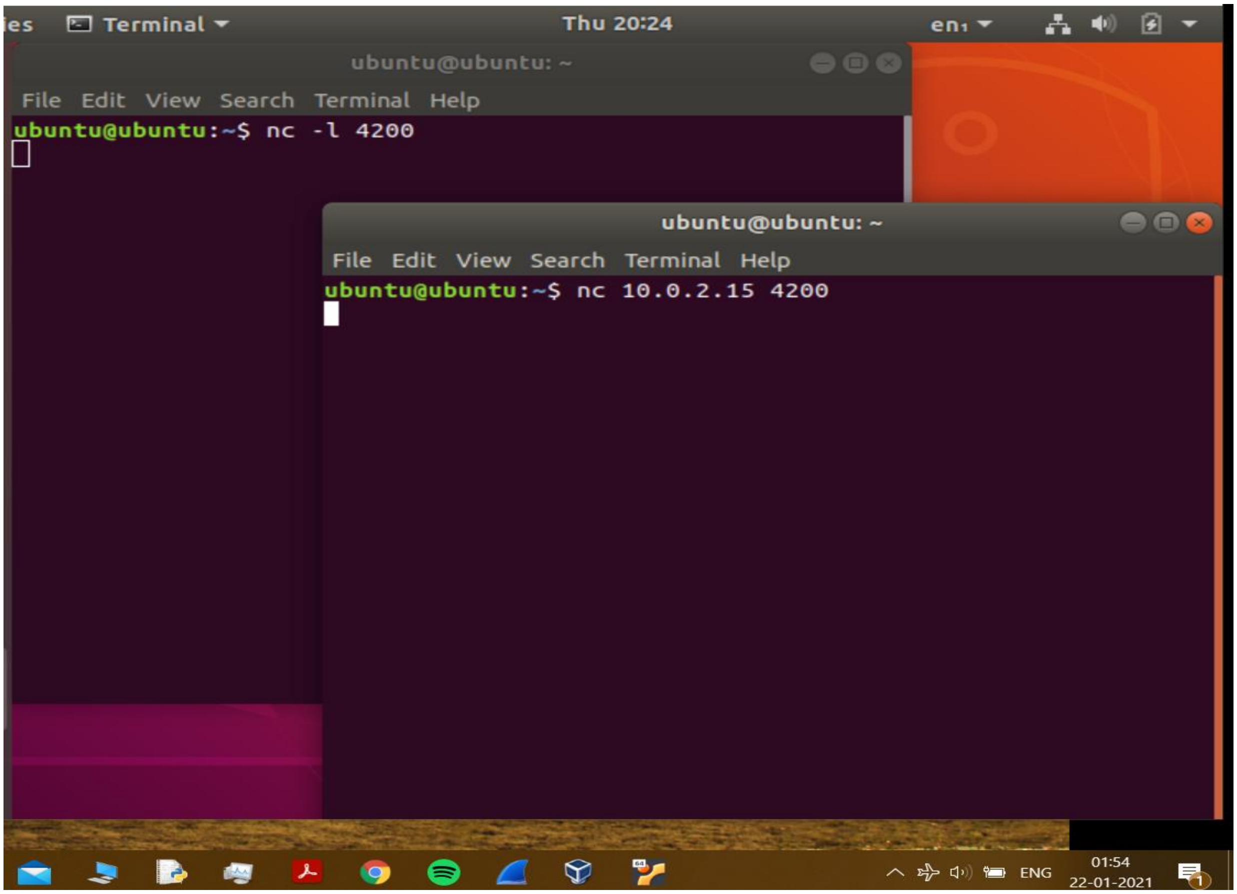
Note: It will go to listening mode

Step 3:

Open another terminal and this will act as a client.

Step 4:Type nc <your-system-ip-address> portnum

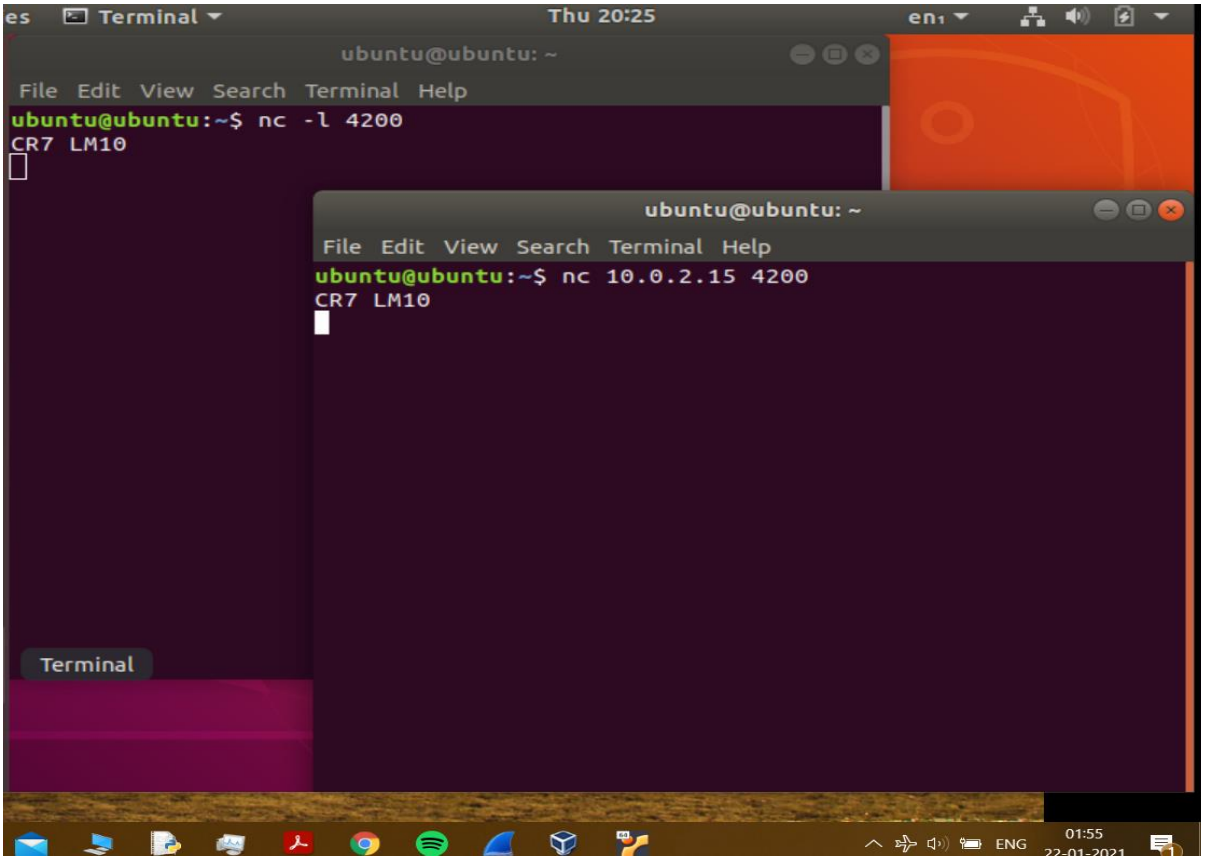
Note: portnum should be common in both the terminals



```
ubuntu@ubuntu:~$ nc -l 4200
```

```
ubuntu@ubuntu:~$ nc 10.0.2.15 4200
```

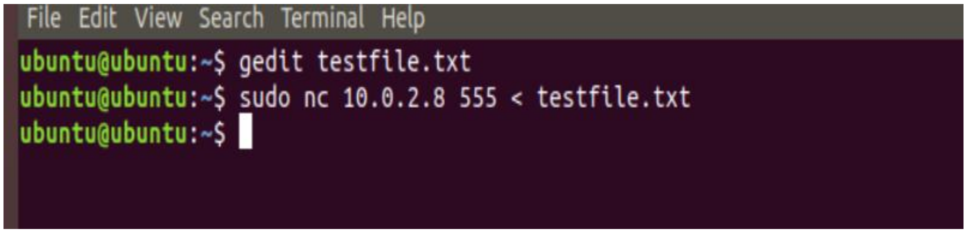
Step 5: Type anything in client will appear in server



```
ubuntu@ubuntu:~$ nc -l 4200
CR7 LM10
```

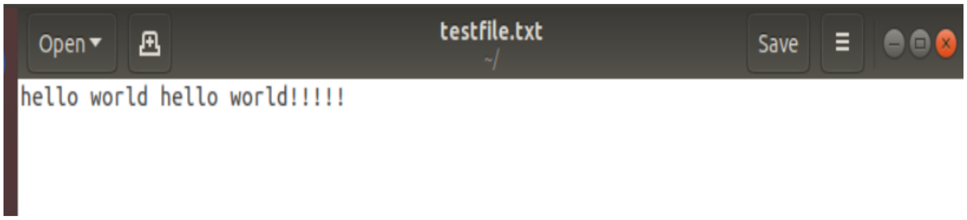
```
ubuntu@ubuntu:~$ nc 10.0.2.15 4200
CR7 LM10
```

b)Client File:



```
ubuntu@ubuntu:~$ gedit testfile.txt
ubuntu@ubuntu:~$ sudo nc 10.0.2.8 555 < testfile.txt
ubuntu@ubuntu:~$
```

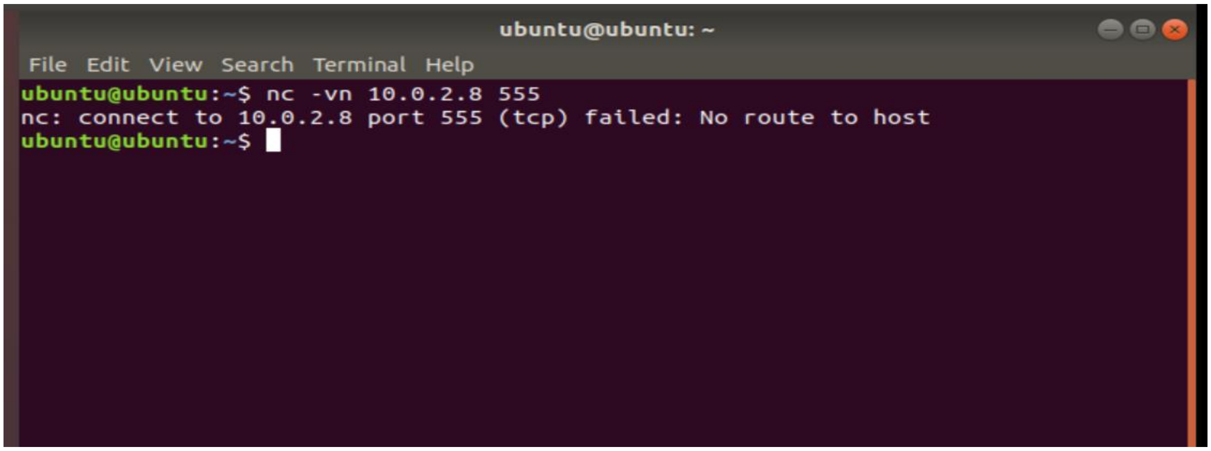
Server file:



```
hello world hello world!!!!!
```

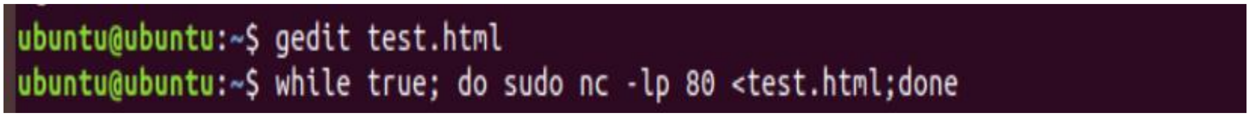
c) Run a web server with a static web page.

1) To test if a particular TCP port of a remote host is open:



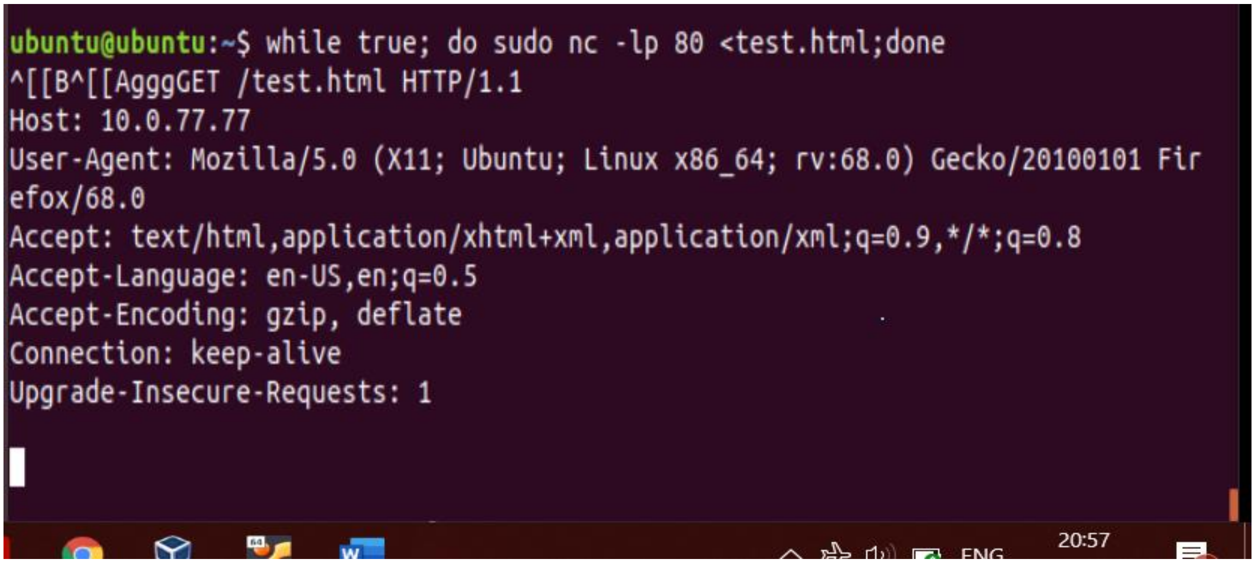
```
ubuntu@ubuntu:~$ nc -vn 10.0.2.8 555
nc: connect to 10.0.2.8 port 555 (tcp) failed: No route to host
ubuntu@ubuntu:~$
```

2)Created a HTML file first



```
ubuntu@ubuntu:~$ gedit test.html
ubuntu@ubuntu:~$ while true; do sudo nc -lp 80 <test.html;done
```

Then opened the webpage from another host



```
ubuntu@ubuntu:~$ while true; do sudo nc -lp 80 <test.html;done
^[[B^[[AgggGET /test.html HTTP/1.1
Host: 10.0.77.77
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:68.0) Gecko/20100101 Fir
efox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

```