COMPUTER NETWORKS LABORATORY

By:
Nitish S
PES2201800368
5 ‘A’

WEEK – 1 – Learn and Understand Network Tools
Date: 31/08/2020

Study and understand the basic networking tools - Wireshark, Tcpdump, Ping, Traceroute and Netcat.

Learn and Understand Network Tools

1. Wireshark

- □ Perform and analyze Ping PDU capture
- □ Examine HTTP packet capture
- □ Analyze HTTP packet capture using filter

2. Netcat

- □ Establish communication between client and server
- □ Transfer files

3. Tcpdump

- Capture packets

4. Ping

- Test the connectivity between 2 systems

5. Traceroute

- Perform traceroute checks

6. Nmap

- Explore an entire network

TASK 1: LINUX INTERFACE CONFIGURATION (IFCONFIG / IP COMMAND)

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

ifconfig (or) **ip addr show**

ip address table:

Interface name	IP address (IPv4 / IPv6)	MAC address	
enp0s3	10.0.2.15	08:00:27:89:68:38	
lo	127.0.0.1	00:00:00:00:00:00	

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

sudo ifconfig enp0s3 10.0.1.32

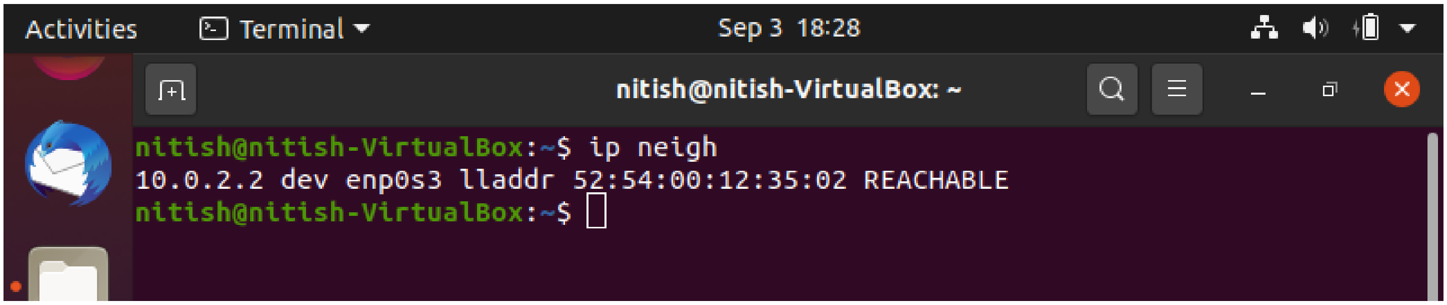
Step 3: To activate / deactivate a network interface, type.

Command given: sudo ifconfig 10.0.1.32 down

sudo ifconfig 10.0.1.32 up

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

ip neigh



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

TASK 2: PING PDU (PACKET DATA UNITS OR PACKETS) CAPTURE

In terminal: **ping 10.0.1.32**

TTL: **64**

Protocol Used By Ping: **ICMP**

Time: **Two packets are arriving per second**

Observations made in Wireshark:

Details	First Echo Request	First Echo Reply
Frame Number	1	2
Source IP address	10.0.1.32	10.0.1.32
Destination IP address	10.0.1.32	10.0.1.32
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	PcsCompu_89:68:38 (08:00:27:89:68:38)	RealtekU_12:35:02 52:54:00:12:35:02)
Destination Ethernet Address	RealtekU_12:35:02 52:54:00:12:35:02)	PcsCompu_89:68:38 (08:00:27:89:68:38)
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	112

TASK 3: HTTP PDU CAPTURE

Using Wireshark's Filter feature

Step 1: Launch Wireshark and select 'enp0s3' interface. On the Filter toolbar, type-in 'http' and press enter

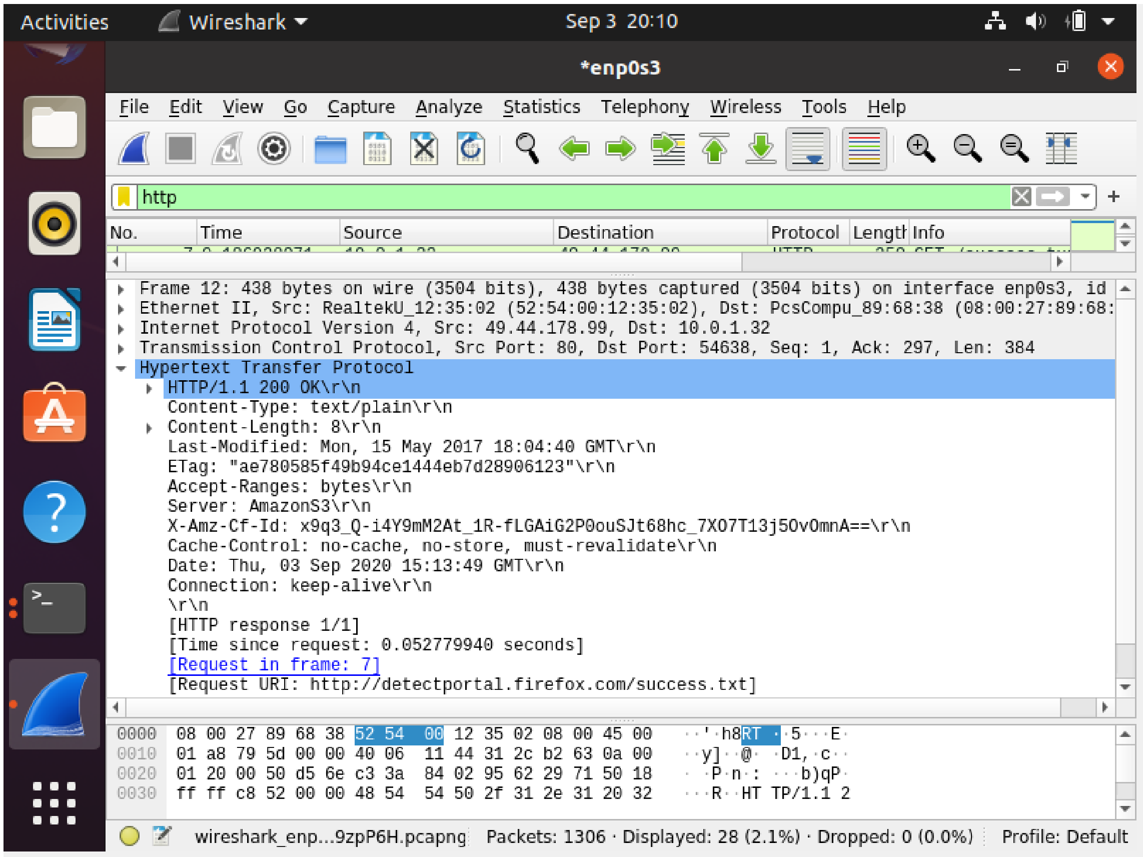
Step 2: Open Firefox browser, and browse www.flipkart.com

Observations made:

Details	First Echo Request	First Echo Reply
Frame Number	6	16
Source Port	48608	80
Destination Port	80	48608
Source IP address	10.0.1.32	49.44.112.206
Destination IP address	49.44.112.206	10.0.1.32
Source Ethernet Address	PcsCompu_89:68:38 (08:00:27:89:68:38)	RealtekU_12:35:02 52:54:00:12:35:02)
Destination Ethernet Address	RealtekU_12:35:02 52:54:00:12:35:02)	PcsCompu_89:68:38 (08:00:27:89:68:38)

Analyzing the HTTP request and response:

HTTP Request		HTTP Response	
Get	GET /success.txt HTTP/1.1\r\n	Server	AmazonS3\r\n
Host	detectportal.firefox.com\r\n	Content-Type	text/plain\r\n
User-Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n	Date	Wed, 02 Sep 2020 13:48:48 GMT\r\n
Accept-Language	en-US,en;q=0.5\r\n	Location	
Accept-Encoding	gzip, deflate\r\n	Content-Length	8\r\n
Connection	keep-alive\r\n	Connection	keep-alive\r\n



Activities
Wireshark
Sep 3 20:10
*enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info

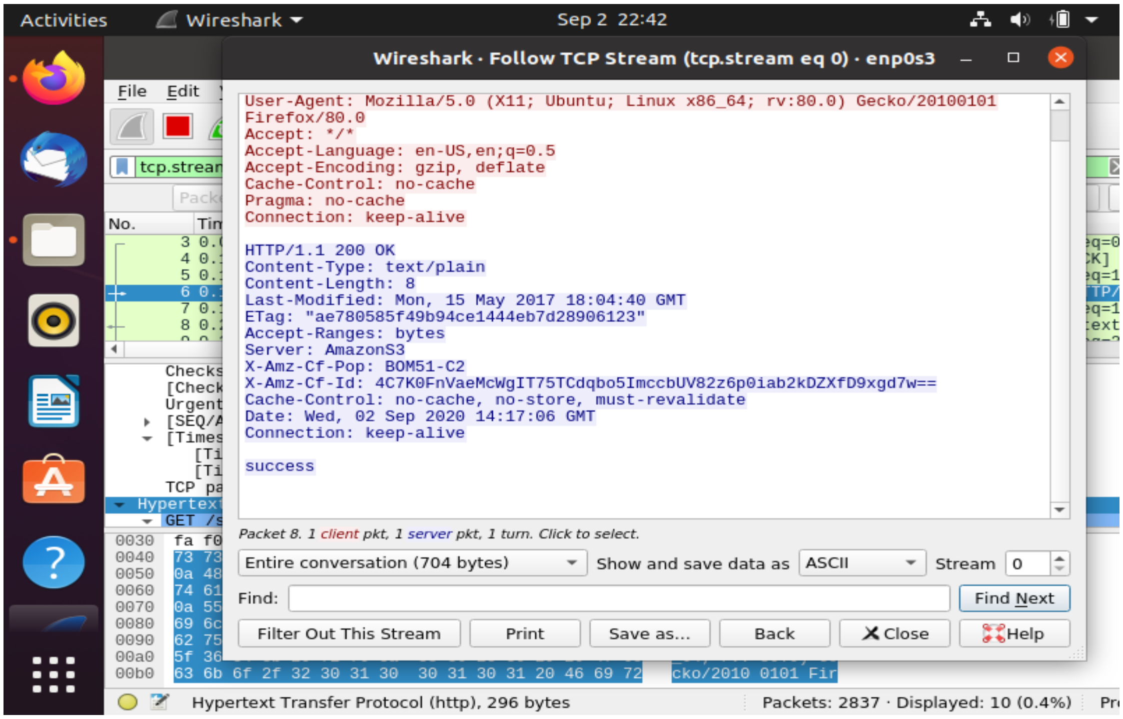
```
Frame 12: 438 bytes on wire (3504 bits), 438 bytes captured (3504 bits) on interface enp0s3, id
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_89:68:38 (08:00:27:89:68:
Internet Protocol Version 4, Src: 49.44.178.99, Dst: 10.0.1.32
Transmission Control Protocol, Src Port: 80, Dst Port: 54638, Seq: 1, Ack: 297, Len: 384
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Content-Type: text/plain\r\n
  Content-Length: 8\r\n
  Last-Modified: Mon, 15 May 2017 18:04:40 GMT\r\n
  ETag: "ae780585f49b94ce1444eb7d28906123"\r\n
  Accept-Ranges: bytes\r\n
  Server: AmazonS3\r\n
  X-Amz-Cf-Id: x9q3_Q-i4Y9mM2At_1R-fLGAiG2P0ouSJt68hc_7XO7T13j5OvOmnA==\r\n
  Cache-Control: no-cache, no-store, must-revalidate\r\n
  Date: Thu, 03 Sep 2020 15:13:49 GMT\r\n
  Connection: keep-alive\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.052779940 seconds]
  [Request in frame: 7]
  [Request URI: http://detectportal.firefox.com/success.txt]
```

```
0000  08 00 27 89 68 38 52 54  00 12 35 02 08 00 45 00   ··'·h8RT ··5···E·
0010  01 a8 79 5d 00 00 40 06  11 44 31 2c b2 63 0a 00   ··y]··@·  ·D1,·c··
0020  01 20 00 50 d5 6e c3 3a  84 02 95 62 29 71 50 18   · ·P·n·:  ···b)qP·
0030  ff ff c8 52 00 00 48 54  54 50 2f 31 2e 31 20 32   ···R··HT TP/1.1 2
```

wireshark_enp...9zpP6H.pcapng Packets: 1306 · Displayed: 28 (2.1%) · Dropped: 0 (0.0%) Profile: Default

LOCATION FIELD NOT SHOWN

Using Wireshark’s Follow TCP Stream



```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101
Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 8
Last-Modified: Mon, 15 May 2017 18:04:40 GMT
ETag: "ae780585f49b94ce1444eb7d28906123"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Pop: BOM51-C2
X-Amz-Cf-Id: 4C7K0FnVaeMcWgIT75TCdqbo5ImccbUV82z6p0iab2kDZXfD9xgd7w==
Cache-Control: no-cache, no-store, must-revalidate
Date: Wed, 02 Sep 2020 14:17:06 GMT
Connection: keep-alive

success
```

Packet 8. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (704 bytes) Show and save data as ASCII Stream 0

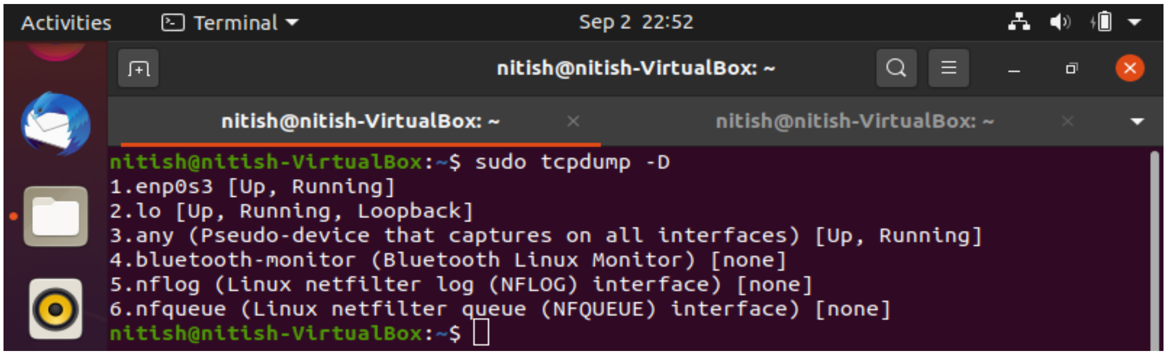
Find:

Hypertext Transfer Protocol (http), 296 bytes Packets: 2837 · Displayed: 10 (0.4%)

TASK 4: CAPTURING PACKETS WITH TCPDUMP

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

sudo tcpdump -D



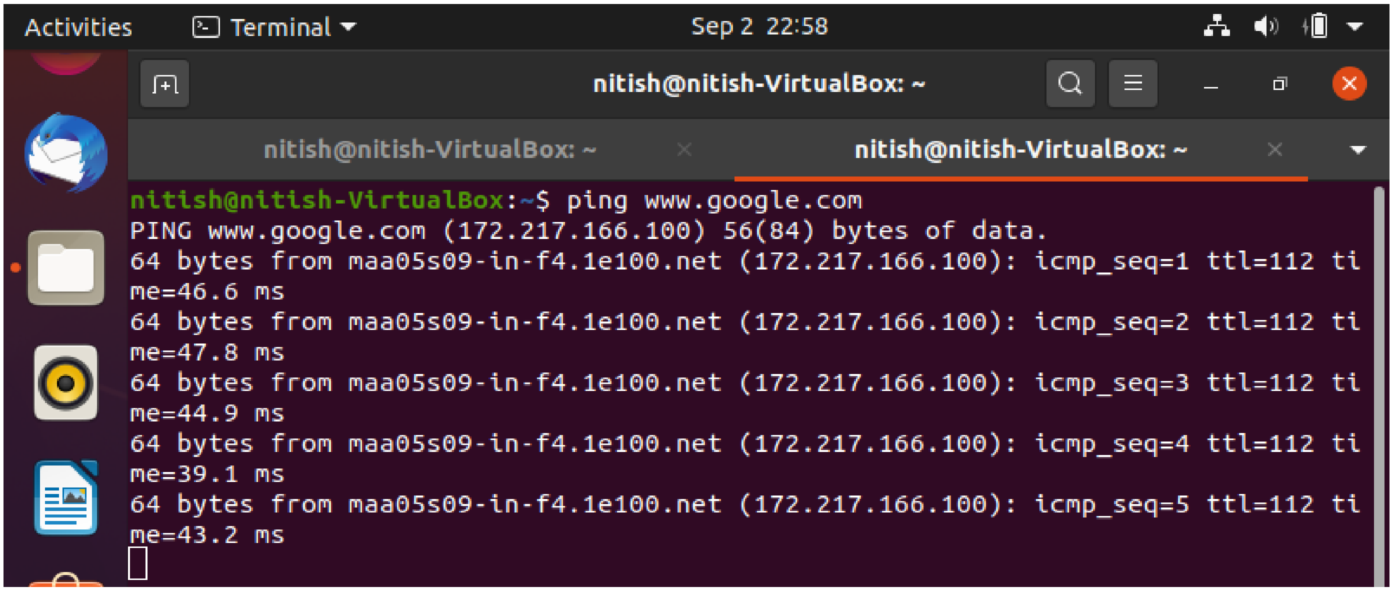
Activities
Terminal
Sep 2 22:52
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ sudo tcpdump -D
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]
nitish@nitish-VirtualBox:~$
```

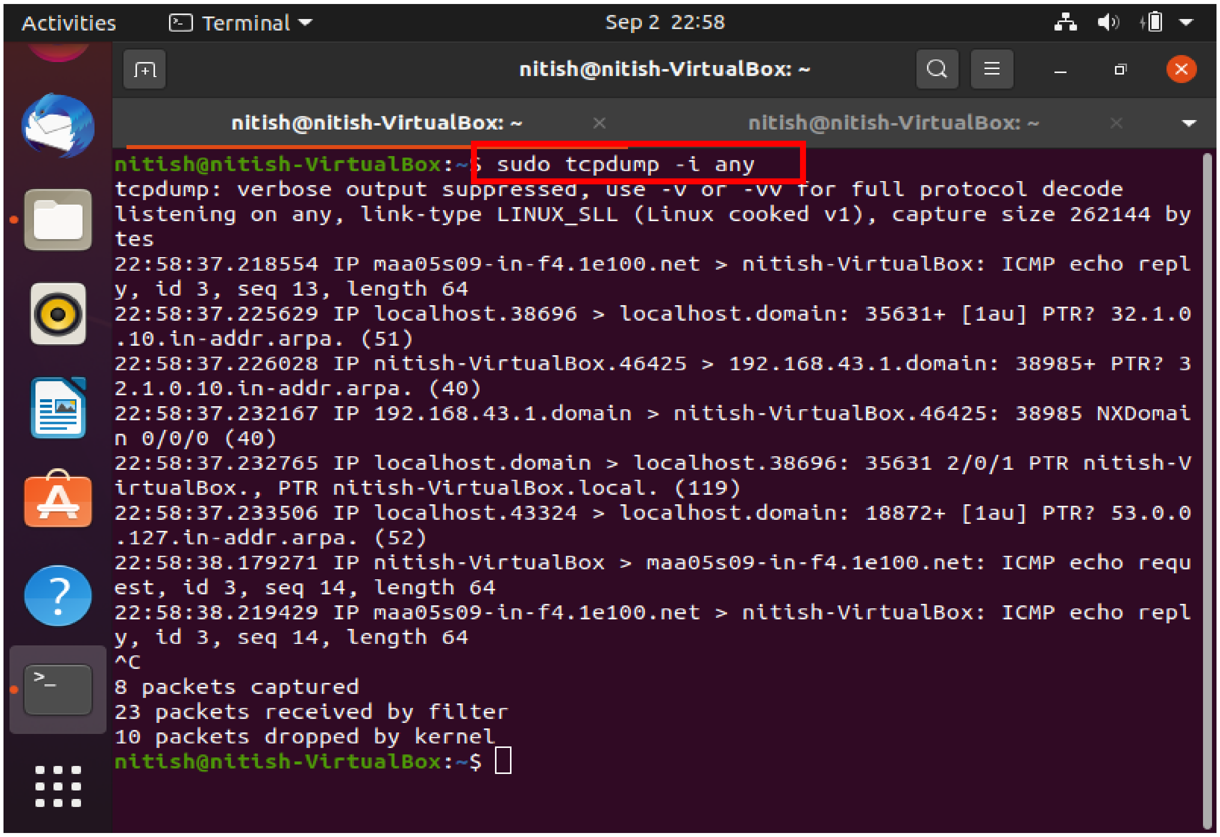
Step 2: Capture all packets in any interface by running this command:

sudo tcpdump -i any

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


Activities
Terminal
Sep 2 22:58
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ ping www.google.com
PING www.google.com (172.217.166.100) 56(84) bytes of data.
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100): icmp_seq=1 ttl=112 ti
me=46.6 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100): icmp_seq=2 ttl=112 ti
me=47.8 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100): icmp_seq=3 ttl=112 ti
me=44.9 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100): icmp_seq=4 ttl=112 ti
me=39.1 ms
64 bytes from maa05s09-in-f4.1e100.net (172.217.166.100): icmp_seq=5 ttl=112 ti
me=43.2 ms
```

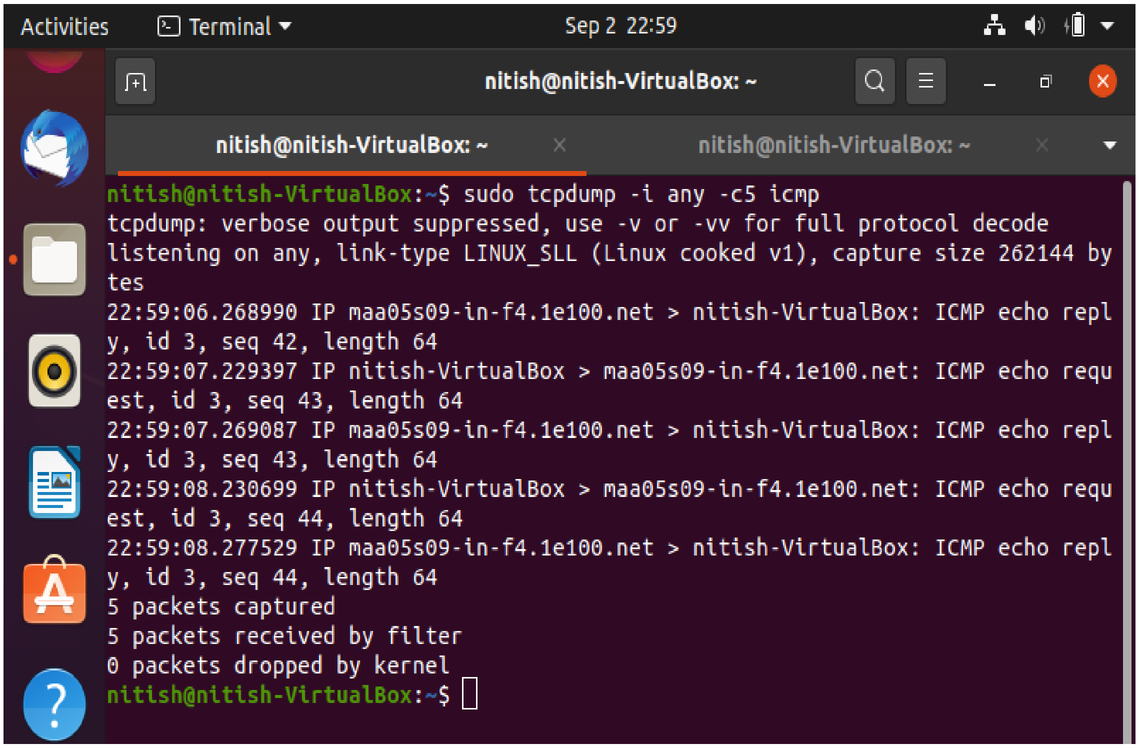

Activities
Terminal
Sep 2 22:58
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-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 by
tes
22:58:37.218554 IP maa05s09-in-f4.1e100.net > nitish-VirtualBox: ICMP echo repl
y, id 3, seq 13, length 64
22:58:37.225629 IP localhost.38696 > localhost.domain: 35631+ [1au] PTR? 32.1.0
.10.in-addr.arpa. (51)
22:58:37.226028 IP nitish-VirtualBox.46425 > 192.168.43.1.domain: 38985+ PTR? 3
2.1.0.10.in-addr.arpa. (40)
22:58:37.232167 IP 192.168.43.1.domain > nitish-VirtualBox.46425: 38985 NXDomai
n 0/0/0 (40)
22:58:37.232765 IP localhost.domain > localhost.38696: 35631 2/0/1 PTR nitish-V
irtualBox., PTR nitish-VirtualBox.local. (119)
22:58:37.233506 IP localhost.43324 > localhost.domain: 18872+ [1au] PTR? 53.0.0
.127.in-addr.arpa. (52)
22:58:38.179271 IP nitish-VirtualBox > maa05s09-in-f4.1e100.net: ICMP echo requ
est, id 3, seq 14, length 64
22:58:38.219429 IP maa05s09-in-f4.1e100.net > nitish-VirtualBox: ICMP echo repl
y, id 3, seq 14, length 64
^C
8 packets captured
23 packets received by filter
10 packets dropped by kernel
nitish@nitish-VirtualBox:~$
```

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

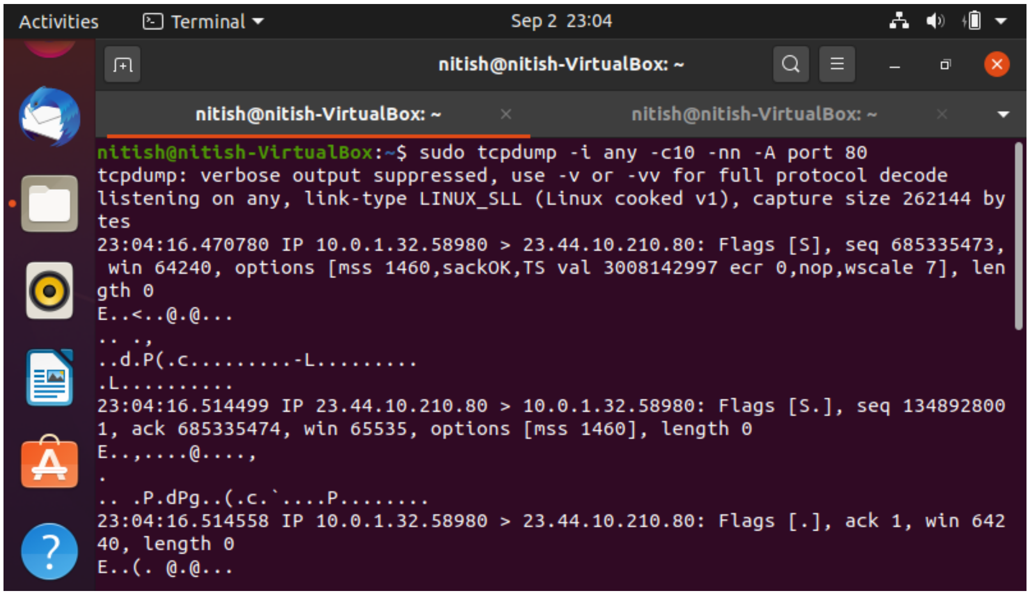


Activities
Terminal
Sep 2 22:59
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-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 by
tes
22:59:06.268990 IP maa05s09-in-f4.1e100.net > nitish-VirtualBox: ICMP echo repl
y, id 3, seq 42, length 64
22:59:07.229397 IP nitish-VirtualBox > maa05s09-in-f4.1e100.net: ICMP echo requ
est, id 3, seq 43, length 64
22:59:07.269087 IP maa05s09-in-f4.1e100.net > nitish-VirtualBox: ICMP echo repl
y, id 3, seq 43, length 64
22:59:08.230699 IP nitish-VirtualBox > maa05s09-in-f4.1e100.net: ICMP echo requ
est, id 3, seq 44, length 64
22:59:08.277529 IP maa05s09-in-f4.1e100.net > nitish-VirtualBox: ICMP echo repl
y, id 3, seq 44, length 64
5 packets captured
5 packets received by filter
0 packets dropped by kernel
nitish@nitish-VirtualBox:~$ 
```

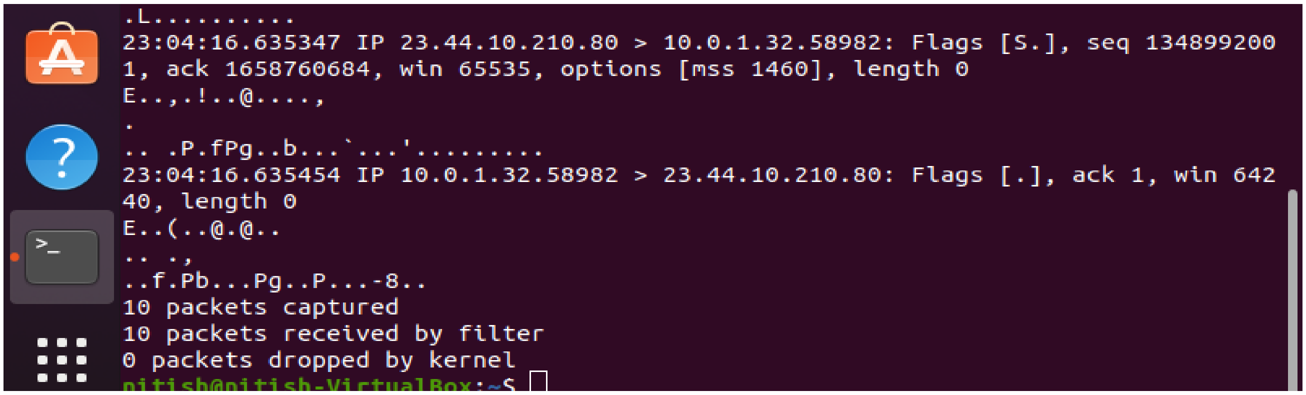
Step 5: Check the packet content. For example, inspect the HTTP content of a web request like this:

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



Activities
Terminal
Sep 2 23:04
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

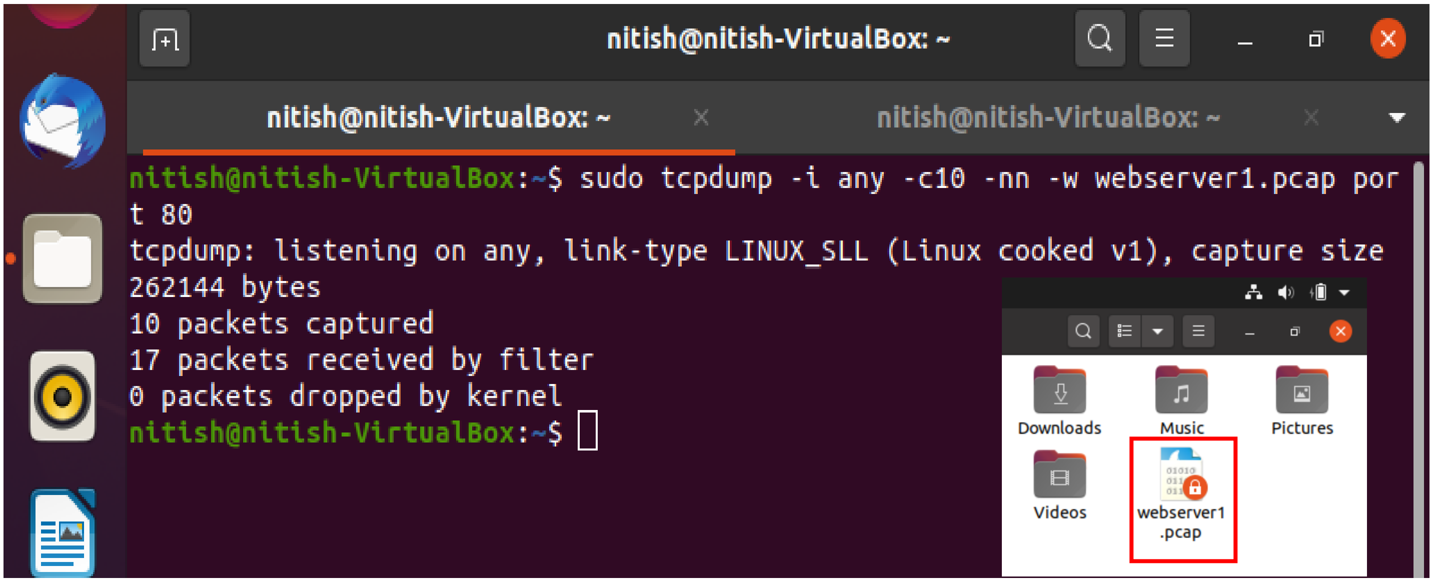
```
nitish@nitish-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 by
tes
23:04:16.470780 IP 10.0.1.32.58980 > 23.44.10.210.80: Flags [S], seq 685335473,
 win 64240, options [mss 1460,sackOK,TS val 3008142997 ecr 0,nop,wscale 7], len
gth 0
E..<..@.@...
.. .,
..d.P(.c.........-L.........
.L..........
23:04:16.514499 IP 23.44.10.210.80 > 10.0.1.32.58980: Flags [S.], seq 134892800
1, ack 685335474, win 65535, options [mss 1460], length 0
E..,....@....,
.
.. .P.dPg..(.c.`....P........
23:04:16.514558 IP 10.0.1.32.58980 > 23.44.10.210.80: Flags [.], ack 1, win 642
40, length 0
E..(. @.@...
```



```
.L..........
23:04:16.635347 IP 23.44.10.210.80 > 10.0.1.32.58982: Flags [S.], seq 134899200
1, ack 1658760684, win 65535, options [mss 1460], length 0
E..,.!..@....,
.
.. .P.fPg..b...`...'.........
23:04:16.635454 IP 10.0.1.32.58982 > 23.44.10.210.80: Flags [.], ack 1, win 642
40, length 0
E..(..@.@..
.. .,
..f.Pb...Pg..P...-8..
10 packets captured
10 packets received by filter
0 packets dropped by kernel
nitish@nitish-VirtualBox:~$
```

Step 6: To save packets to a file instead of displaying them on screen, use the option -w:

sudo tcpdump -i any -c10 -nn -w webserver1.pcap port 80

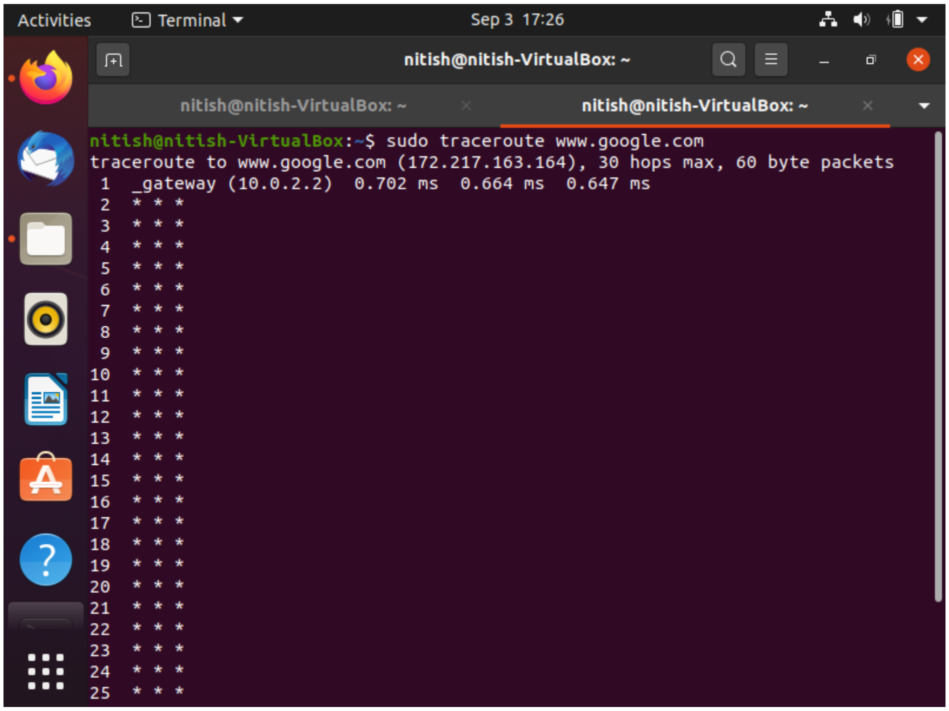


nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
Downloads
Music
Pictures
Videos
webserver1.pcap

```
nitish@nitish-VirtualBox:~$ sudo tcpdump -i any -c10 -nn -w webserver1.pcap por
t 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size
262144 bytes
10 packets captured
17 packets received by filter
0 packets dropped by kernel
nitish@nitish-VirtualBox:~$
```

TASK 5: PERFORM TRACEROUTE CHECKS

Step 1: sudo traceroute www.google.com


Activities
Terminal
Sep 3 17:26
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

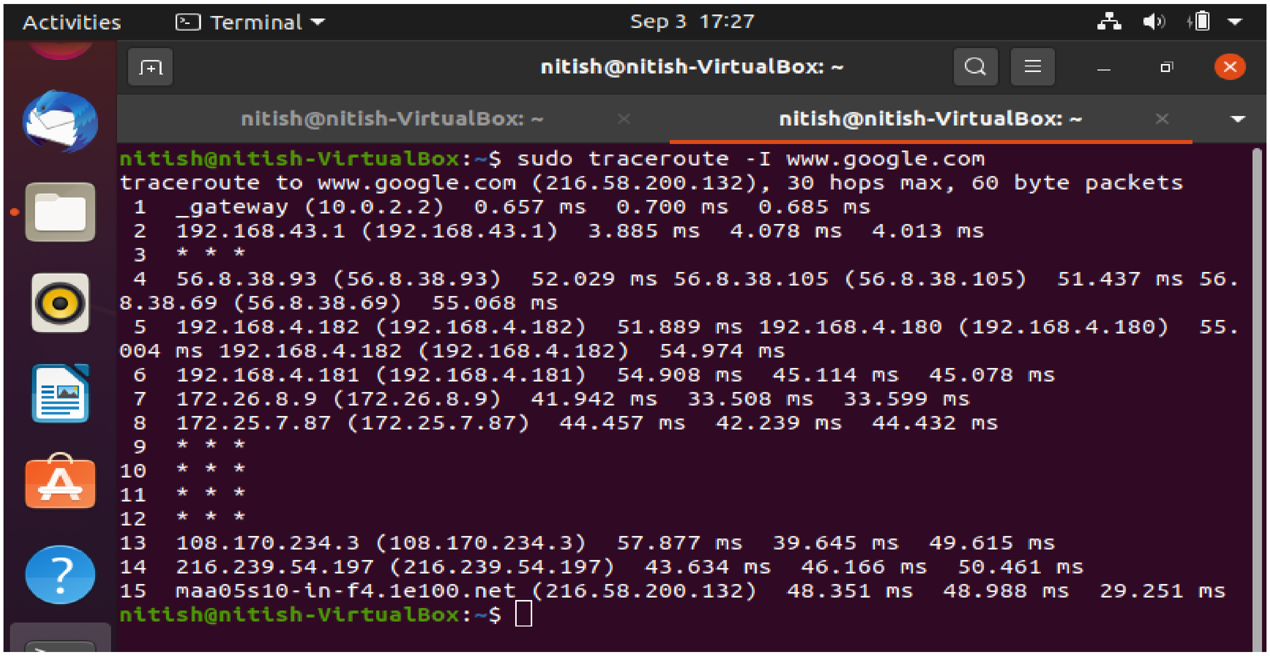
```
nitish@nitish-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.702 ms  0.664 ms  0.647 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
```

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

Destination Address of google.com = 172.217.163.164 and no of hops : 30

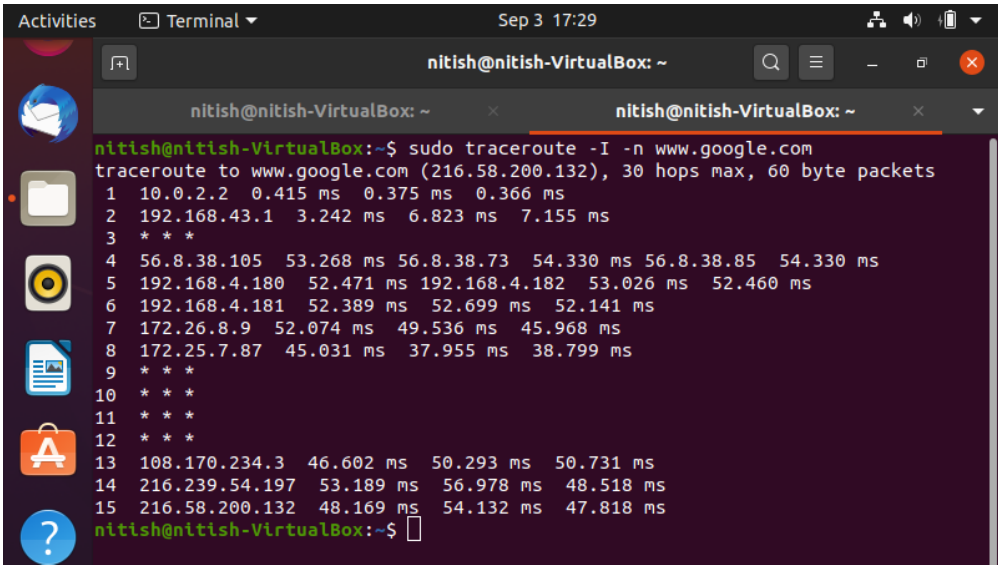
Step 3: The -I option is necessary so that the traceroute uses ICMP.

sudo traceroute -I www.google.com


Activities
Terminal
Sep 3 17:27
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (216.58.200.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.657 ms  0.700 ms  0.685 ms
 2  192.168.43.1 (192.168.43.1)  3.885 ms  4.078 ms  4.013 ms
 3  * * *
 4  56.8.38.93 (56.8.38.93)  52.029 ms 56.8.38.105 (56.8.38.105)  51.437 ms 56.
8.38.69 (56.8.38.69)  55.068 ms
 5  192.168.4.182 (192.168.4.182)  51.889 ms 192.168.4.180 (192.168.4.180)  55.
004 ms 192.168.4.182 (192.168.4.182)  54.974 ms
 6  192.168.4.181 (192.168.4.181)  54.908 ms  45.114 ms  45.078 ms
 7  172.26.8.9 (172.26.8.9)  41.942 ms  33.508 ms  33.599 ms
 8  172.25.7.87 (172.25.7.87)  44.457 ms  42.239 ms  44.432 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  108.170.234.3 (108.170.234.3)  57.877 ms  39.645 ms  49.615 ms
14  216.239.54.197 (216.239.54.197)  43.634 ms  46.166 ms  50.461 ms
15  maa05s10-in-f4.1e100.net (216.58.200.132)  48.351 ms  48.988 ms  29.251 ms
nitish@nitish-VirtualBox:~$
```

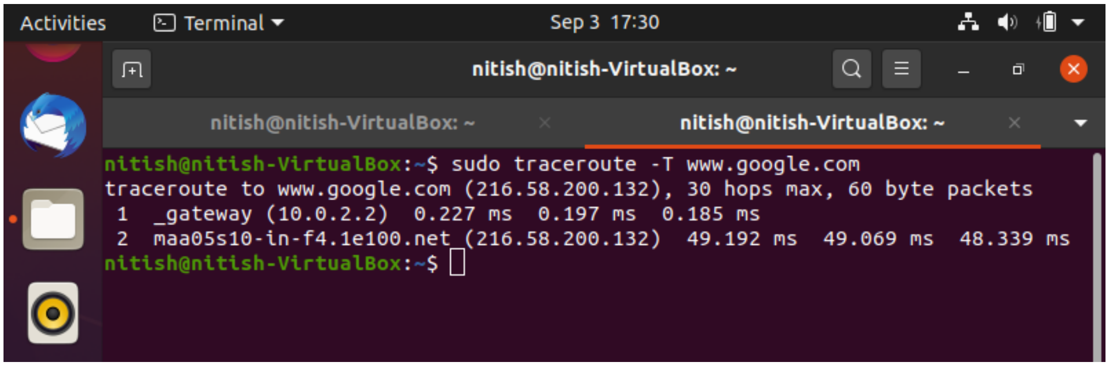
Step 4: To speed up the process, you can disable the mapping of IP addresses with hostnames by using the *-n* option : **sudo traceroute -I -n** www.google.com


Activities
Terminal
Sep 3 17:29
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ sudo traceroute -I -n www.google.com
traceroute to www.google.com (216.58.200.132), 30 hops max, 60 byte packets
 1  10.0.2.2  0.415 ms  0.375 ms  0.366 ms
 2  192.168.43.1  3.242 ms  6.823 ms  7.155 ms
 3  * * *
 4  56.8.38.105  53.268 ms 56.8.38.73  54.330 ms 56.8.38.85  54.330 ms
 5  192.168.4.180  52.471 ms 192.168.4.182  53.026 ms  52.460 ms
 6  192.168.4.181  52.389 ms  52.699 ms  52.141 ms
 7  172.26.8.9  52.074 ms  49.536 ms  45.968 ms
 8  172.25.7.87  45.031 ms  37.955 ms  38.799 ms
 9  * * *
10  * * *
11  * * *
12  * * *
13  108.170.234.3  46.602 ms  50.293 ms  50.731 ms
14  216.239.54.197  53.189 ms  56.978 ms  48.518 ms
15  216.58.200.132  48.169 ms  54.132 ms  47.818 ms
nitish@nitish-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

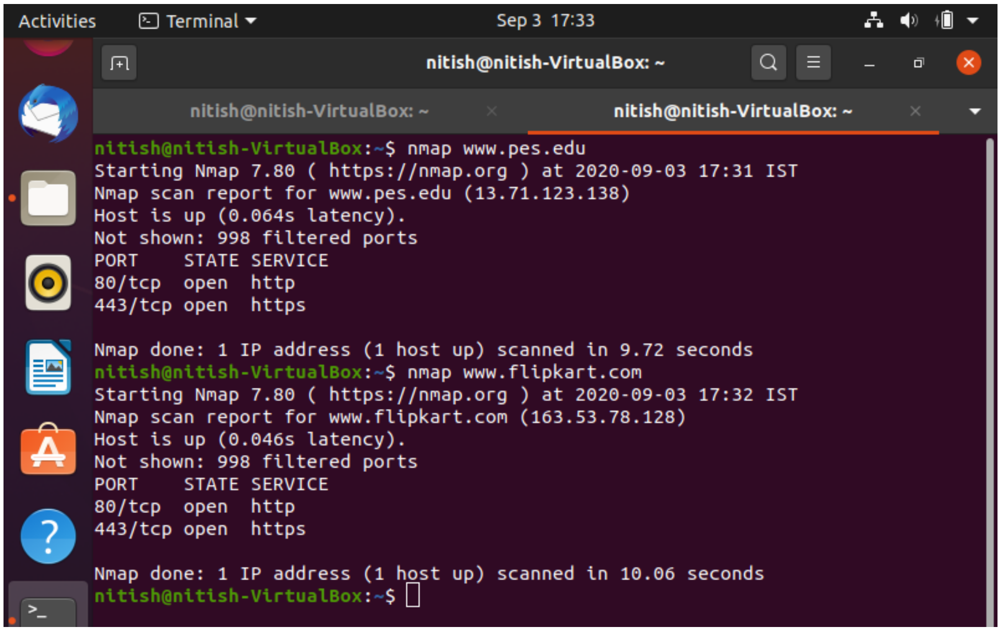

Activities
Terminal
Sep 3 17:30
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (216.58.200.132), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  0.227 ms  0.197 ms  0.185 ms
 2  maa05s10-in-f4.1e100.net (216.58.200.132)  49.192 ms  49.069 ms  48.339 ms
nitish@nitish-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.

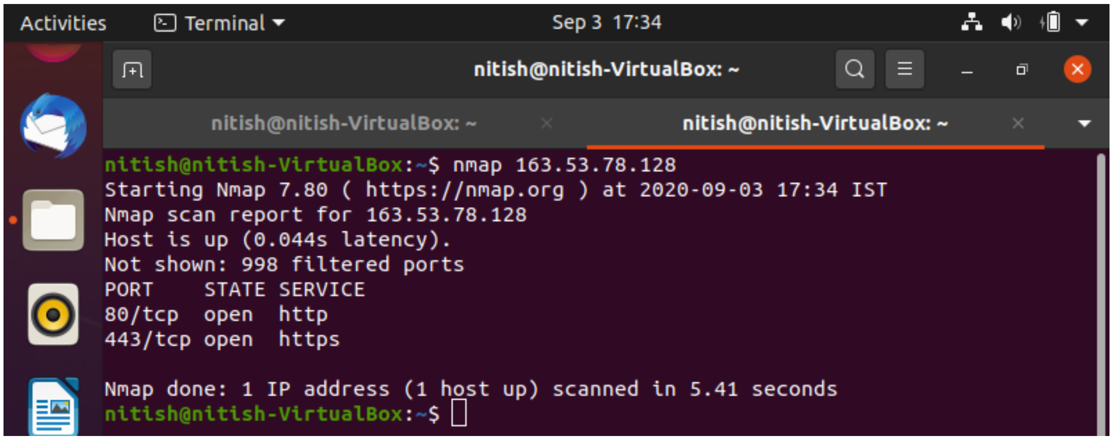
nmap www.pes.edu



Activities
Terminal
Sep 3 17:33
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:31 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.064s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
nitish@nitish-VirtualBox:~$ nmap www.flipkart.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:32 IST
Nmap scan report for www.flipkart.com (163.53.78.128)
Host is up (0.046s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.06 seconds
nitish@nitish-VirtualBox:~$ 
```

Step 2: Alternatively, use an IP address to scan. **nmap 163.53.78.128**

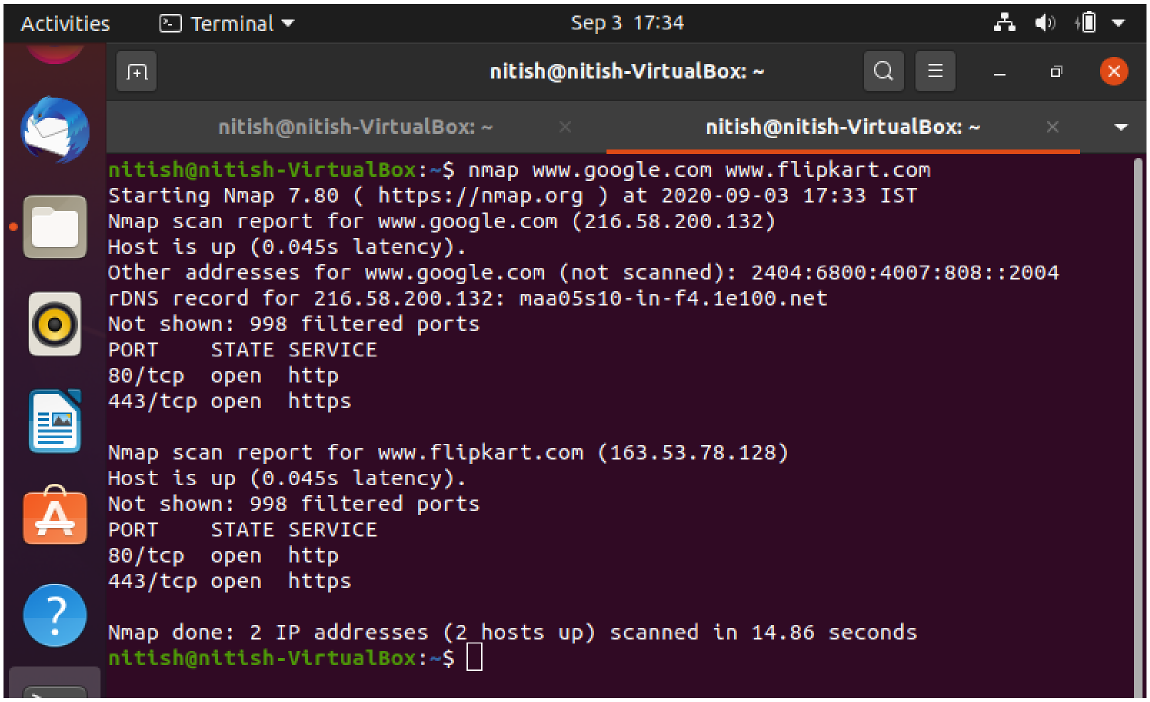


Activities
Terminal
Sep 3 17:34
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:34 IST
Nmap scan report for 163.53.78.128
Host is up (0.044s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds
nitish@nitish-VirtualBox:~$ 
```

Step 3: Scan multiple websites or ip addresses

nmap www.google.com www.flipkart.com

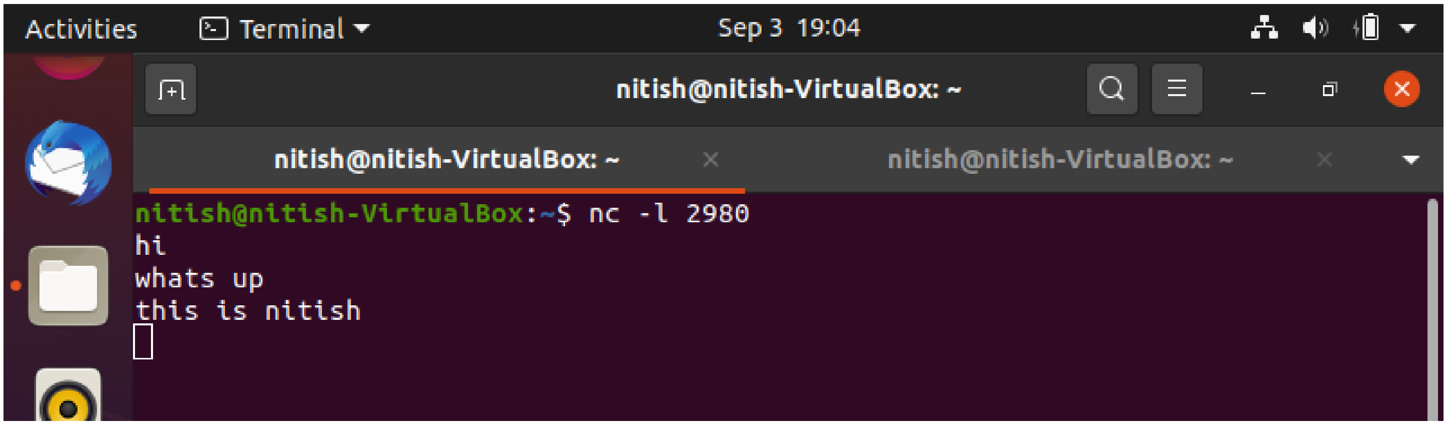

Activities
Terminal
Sep 3 17:34
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ nmap www.google.com www.flipkart.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-03 17:33 IST
Nmap scan report for www.google.com (216.58.200.132)
Host is up (0.045s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:808::2004
rDNS record for 216.58.200.132: maa05s10-in-f4.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap scan report for www.flipkart.com (163.53.78.128)
Host is up (0.045s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 2 IP addresses (2 hosts up) scanned in 14.86 seconds
nitish@nitish-VirtualBox:~$ 
```

TASK 7 A): NETCAT AS CHAT TOOL

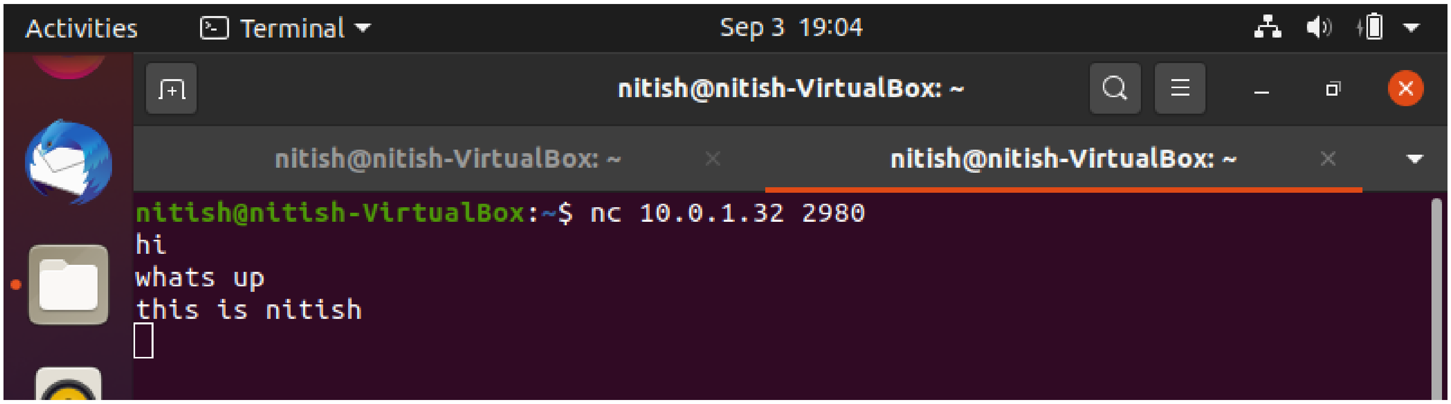
a) Intra system communication (Using 2 terminals in the same system)

SERVER TERMINAL:


Activities
Terminal
Sep 3 19:04
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

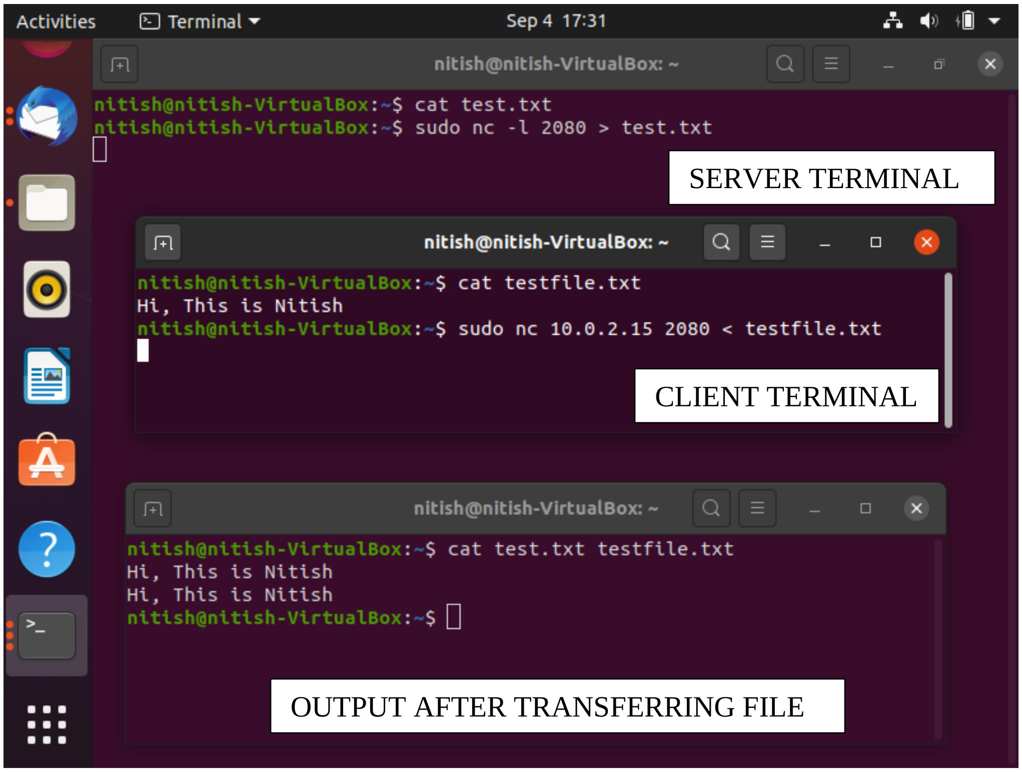
```
nitish@nitish-VirtualBox:~$ nc -l 2980
hi
whats up
this is nitish
```

CLIENT TERMINAL:


Activities
Terminal
Sep 3 19:04
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ nc 10.0.1.32 2980
hi
whats up
this is nitish
```

TASK 7 B): USE NETCAT TO TRANSFER FILES



SERVER TERMINAL

```
nitish@nitish-VirtualBox:~$ cat test.txt
nitish@nitish-VirtualBox:~$ sudo nc -l 2080 > test.txt
```

CLIENT TERMINAL

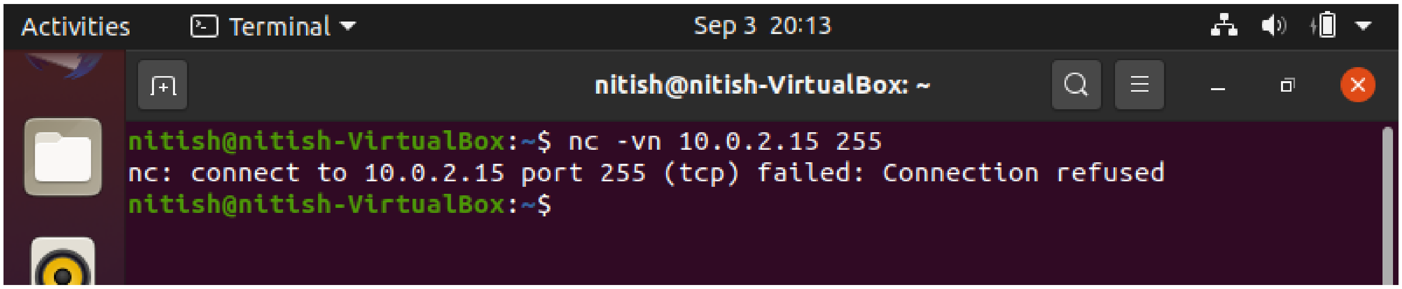
```
nitish@nitish-VirtualBox:~$ cat testfile.txt
Hi, This is Nitish
nitish@nitish-VirtualBox:~$ sudo nc 10.0.2.15 2080 < testfile.txt
```

OUTPUT AFTER TRANSFERRING FILE

```
nitish@nitish-VirtualBox:~$ cat test.txt testfile.txt
Hi, This is Nitish
Hi, This is Nitish
nitish@nitish-VirtualBox:~$
```

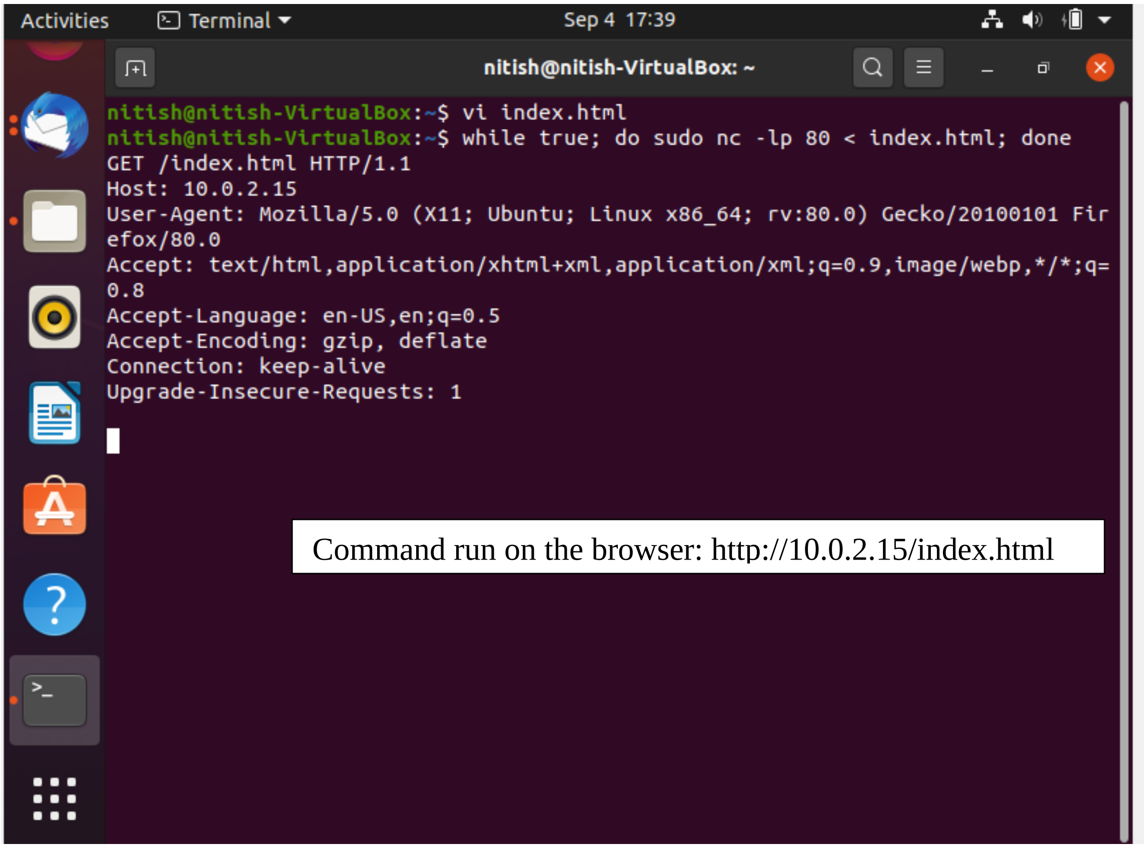
7 C) OTHER COMMANDS:-

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



```
nitish@nitish-VirtualBox:~$ nc -vn 10.0.2.15 255
nc: connect to 10.0.2.15 port 255 (tcp) failed: Connection refused
nitish@nitish-VirtualBox:~$
```

2) Netcat exchanging file via Terminal:



```
nitish@nitish-VirtualBox:~$ vi index.html
nitish@nitish-VirtualBox:~$ while true; do sudo nc -lp 80 < index.html; done
GET /index.html HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Fir
efox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Command run on the browser: http://10.0.2.15/index.html

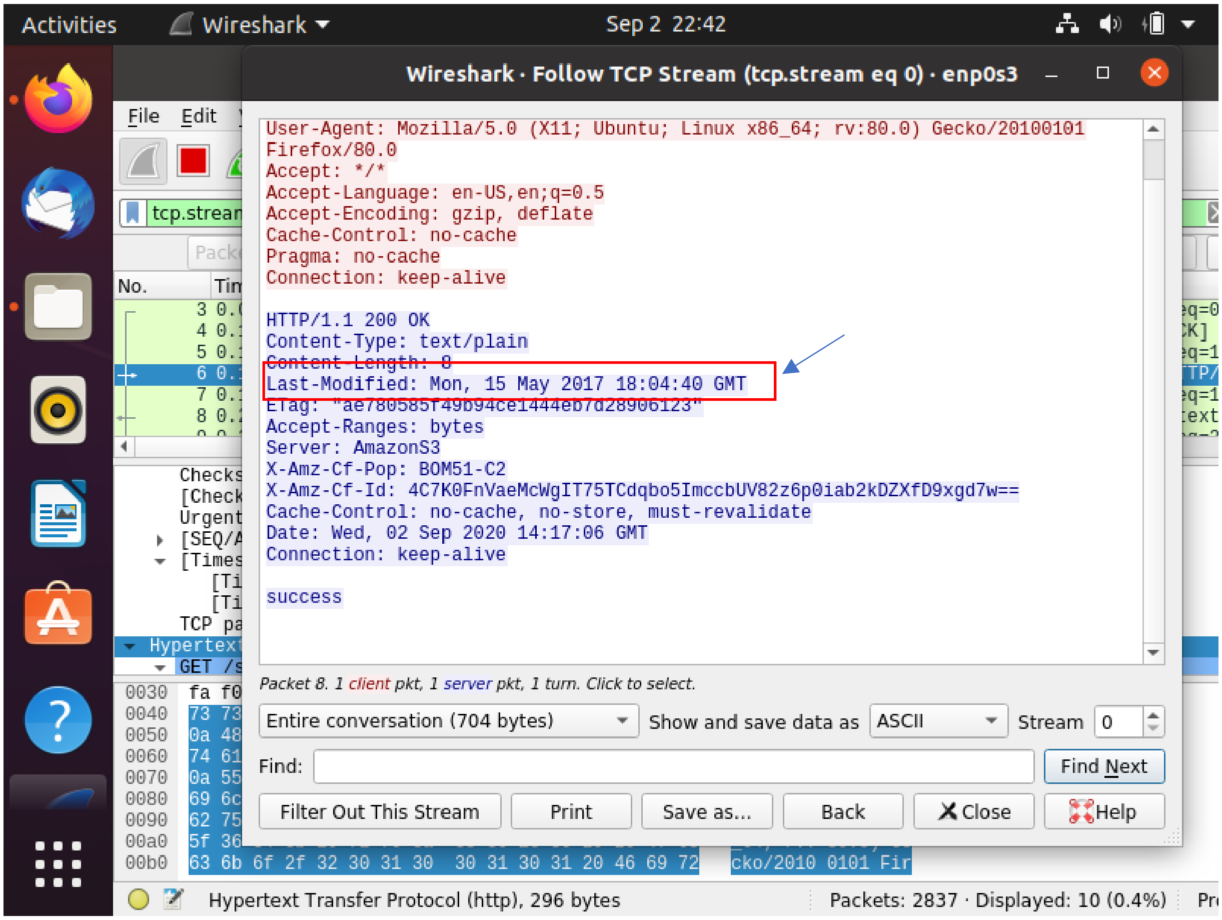
QUESTIONS ON THE ABOVE OBSERVATIONS:-

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

Ans:- Both the browser and server are running HTTP version 1.1

2) When was the HTML file that you are retrieving last modified at the server?

Ans:- Using Wireshark, we can check the Packet TCP Stream Request and then we can see the timestamp values in the Stream.
The below screenshot shows the last modified date:



Wireshark · Follow TCP Stream (tcp.stream eq 0) · enp0s3

```
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101
Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 8
Last-Modified: Mon, 15 May 2017 18:04:40 GMT
ETag: "ae780585f49b94ce1444eb7d28906123"
Accept-Ranges: bytes
Server: AmazonS3
X-Amz-Cf-Pop: BOM51-C2
X-Amz-Cf-Id: 4C7K0FnVaeMcWgIT75TCdqbo5ImccbUV82z6p0iab2kDZXfD9xgd7w==
Cache-Control: no-cache, no-store, must-revalidate
Date: Wed, 02 Sep 2020 14:17:06 GMT
Connection: keep-alive

success
```

Packet 8. 1 client pkt, 1 server pkt, 1 turn. Click to select.

Entire conversation (704 bytes) Show and save data as ASCII Stream 0

Find:

Hypertext Transfer Protocol (http), 296 bytes Packets: 2837 · Displayed: 10 (0.4%)

3) How to tell ping to exit after a specified number of ECHO_REQUEST packets?

Ans:- The below command pings 5 Packets and displays the route the packet traverses and then stops.
Ping -R -c 5 www.google.com

4) How will you identify remote host apps and OS?
Ans:-

- **nmap -O -v IPADDRESS :-** Gives the Remote Host Os That it is currently running on'
- **nmap -sV IPADDRESS :-** Get the Service/Deamons that are running in the remote Host IP.

EXERCISES:

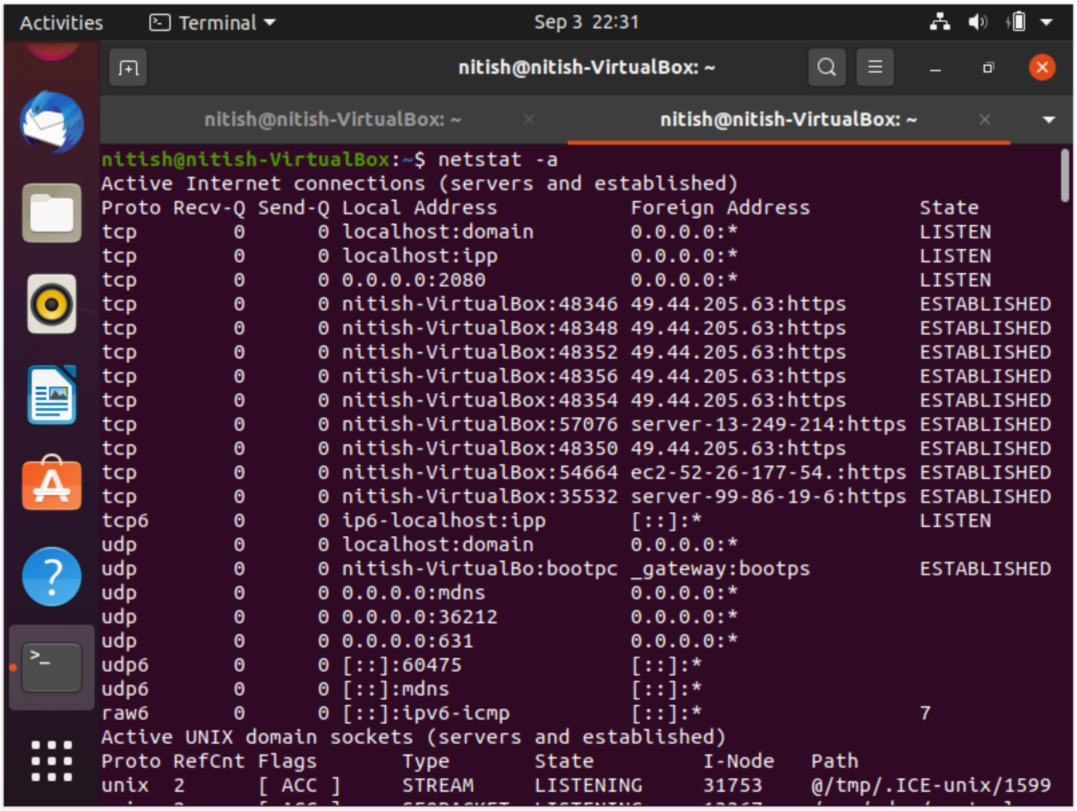
1) Capture and Analyze IPv4 / IPv6 packets .

GET	GET /success.txt HTTP/1.1\r\n
HOST	detectportal.firefox.com\r\n
USER-AGENT	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0\r\n
ACCEPT-LANGUAGE	en-US,en;q=0.5\r\n
CACHE-CONTROL	no-cache\r\n
PRAGMA	no-cache\r\n
CONNECTION	keep-alive\r\n

2) Explore various other network configuration, troubleshooting and debugging tools such as Route, Netstat, etc.
Ans:-

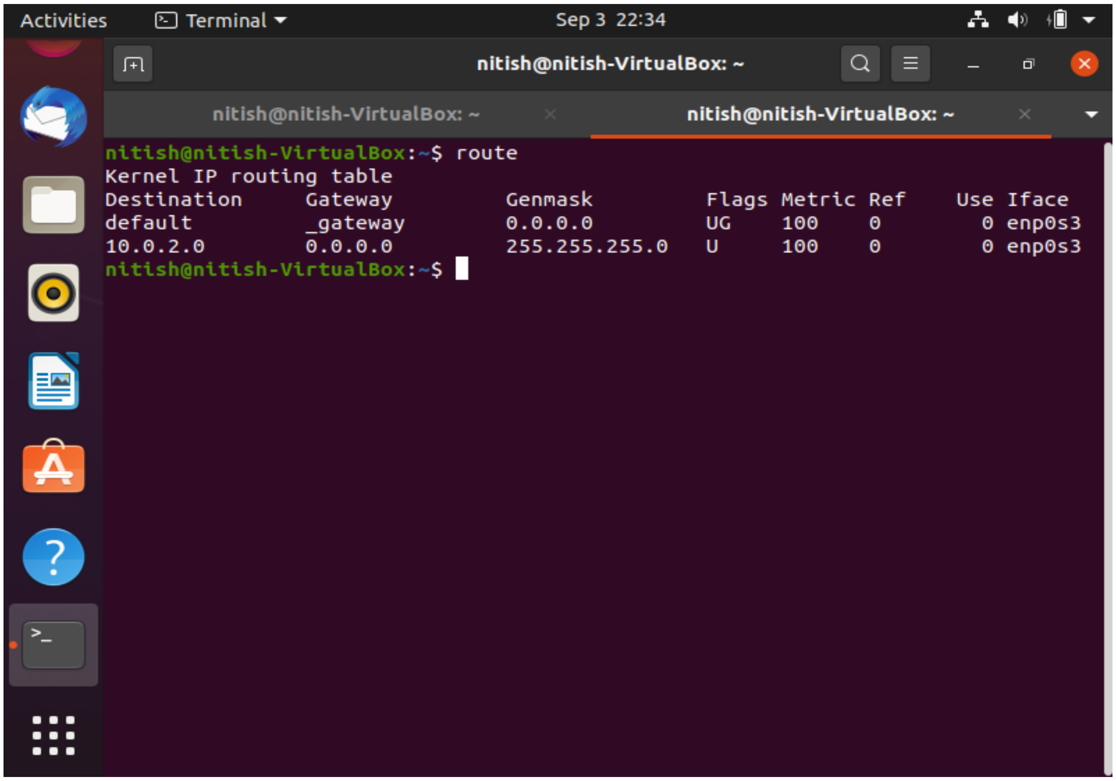
1) NETSTAT:- The **netstat** command generates displays that show **network** status and protocol statistics. You can display the status of TCP and UDP endpoints in table format, routing table information, and interface information. **netstat** displays various types of **network** data depending on the command line option selected.

Eg: netstat -a
Displays all active connections and the TCP and UDP ports on which the computer is listening.


Activities
Terminal
Sep 3 22:31
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2080            0.0.0.0:*               LISTEN
tcp        0      0 nitish-VirtualBox:48346 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:48348 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:48352 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:48356 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:48354 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:57076 server-13-249-214:https ESTABLISHED
tcp        0      0 nitish-VirtualBox:48350 49.44.205.63:https      ESTABLISHED
tcp        0      0 nitish-VirtualBox:54664 ec2-52-26-177-54.:https ESTABLISHED
tcp        0      0 nitish-VirtualBox:35532 server-99-86-19-6:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 nitish-VirtualBo:bootpc _gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 0.0.0.0:36212           0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 [::]:60475              [::]:*
udp6       0      0 [::]:mdns               [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     31753    @/tmp/.ICE-unix/1599
```

2) ROUTE :- This utility is used to display the current status of the routing table on a host.


Activities
Terminal
Sep 3 22:34
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~
nitish@nitish-VirtualBox: ~

```
nitish@nitish-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
nitish@nitish-VirtualBox:~$
```