



COMPUTER NETWORKS LAB

COURSE CODE:UE19CS255

NAME : PRIYA MOHATA
SRN : PES2UG19CS301
SECTION:E
DATE : 24/01/2021

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

a) Display status of network interfaces

Command Used : ip addr show

SCREENSHOT

```
Ubuntu-20.10 [Running]
Activities Terminal Jan 24 13:47 priya@priya-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:a0:2c:49 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 86160sec preferred_lft 86160sec
    inet6 fe80::8182:ddc:713:8f31/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
priya@priya-VirtualBox: $
```

a.Two interfaces are seen in the screenshot

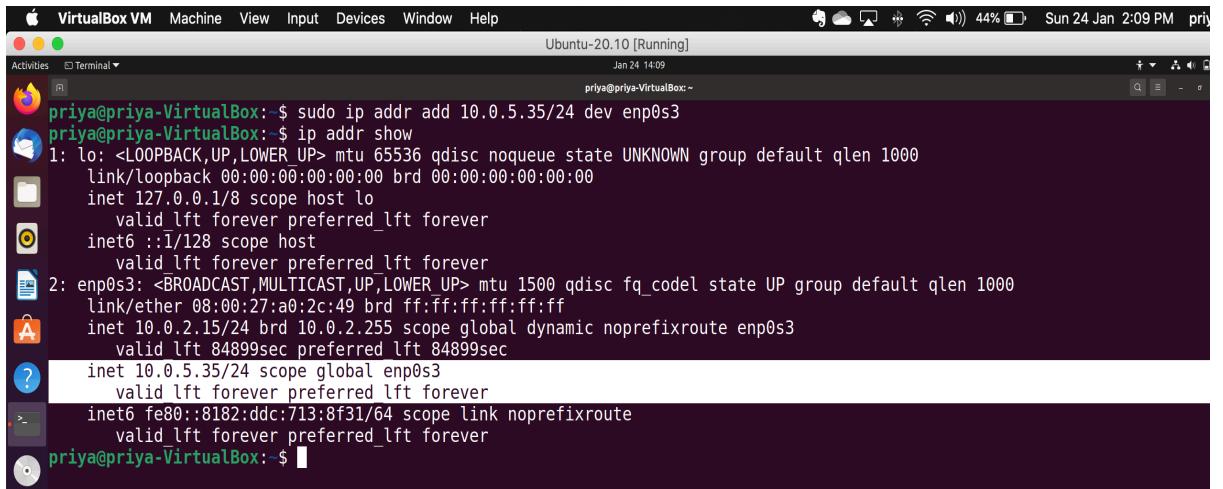
TABLE

Interface Name	IP address (IPv4 / IPv6)	MAC address
lo	IPv4 - 127.0.0.1/8 IPv6 - ::1/128	00:00:00:00:00:00
enp0s3	IPv4- 10.0.2.15/24 IPv6- fe80::8182:ddc:713:8f31/64	08:00:27:a0:2c:49

b) Assigning the IP

Command used : `sudo ip addr add 10.0.5.35/24 dev enp0s3`

SCREENSHOT



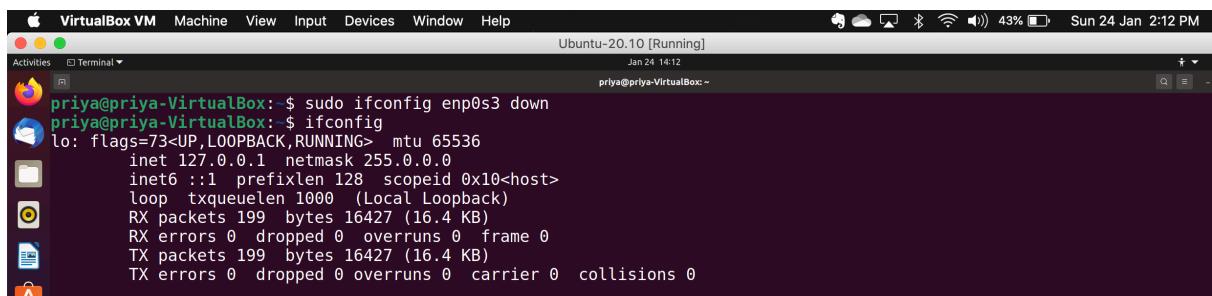
```
priya@priya-VirtualBox: $ sudo ip addr add 10.0.5.35/24 dev enp0s3
priya@priya-VirtualBox: $ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            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:a0:2c:49 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 84899sec preferred_lft 84899sec
        inet 10.0.5.35/24 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::8182:ddc:713:8f31/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
priya@priya-VirtualBox: $
```

inet 10.0.5.35/24 scope global enp0s3

c) Activating & Deactivating Network Interfaces

Command used to deactivate: `sudo ifconfig enp0s3 down`

SCREENSHOT

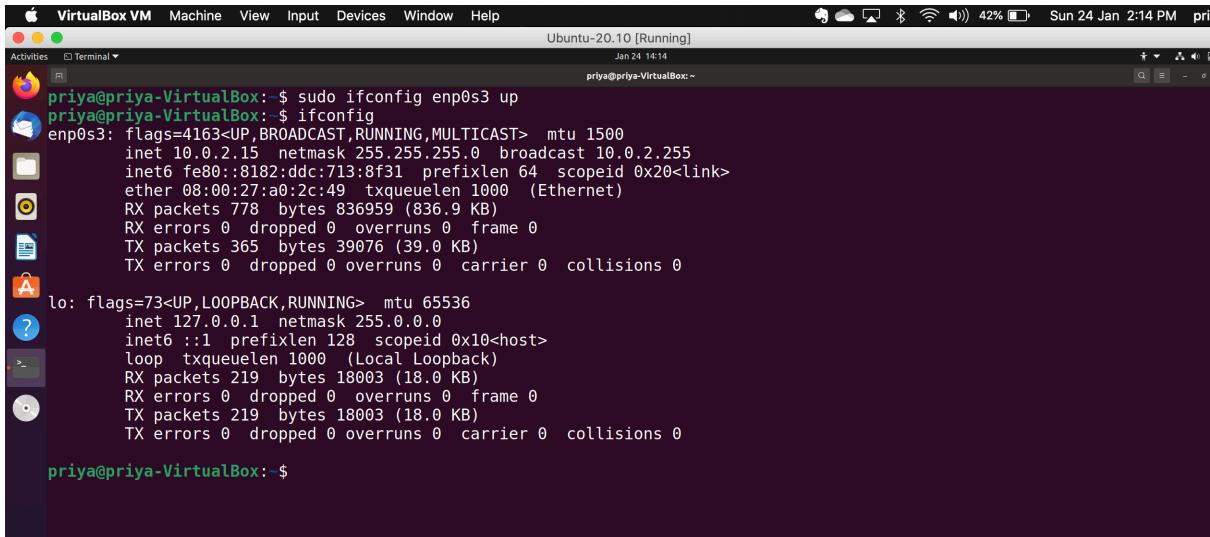


```
priya@priya-VirtualBox:~$ sudo ifconfig enp0s3 down
priya@priya-VirtualBox:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    netmask 255.0.0.0
    inet 127.0.0.1 netmask 255.0.0.0
        broadcast 127.255.255.255
        scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
            RX packets 199 bytes 16427 (16.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 199 bytes 16427 (16.4 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

enp0s3 is not seen

Command used to activate: `sudo ifconfig enp0s3 up`

SCREENSHOT



```
priya@priya-VirtualBox: $ sudo ifconfig enp0s3 up
priya@priya-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::8f31:713ff:fe00:2a9 brd fe80::ff02:713ff:fe00:2a9 scopeid 0x20<link>
                      ether 08:00:27:a0:2c:49 txqueuelen 1000 (Ethernet)
                        RX packets 778 bytes 836959 (836.9 KB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 365 bytes 39076 (39.0 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 219 bytes 18003 (18.0 KB)
                        RX errors 0 dropped 0 overruns 0 frame 0
                        TX packets 219 bytes 18003 (18.0 KB)
                        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
priya@priya-VirtualBox: $
```

enp0s3 is seen

d) Command Used : ip neigh

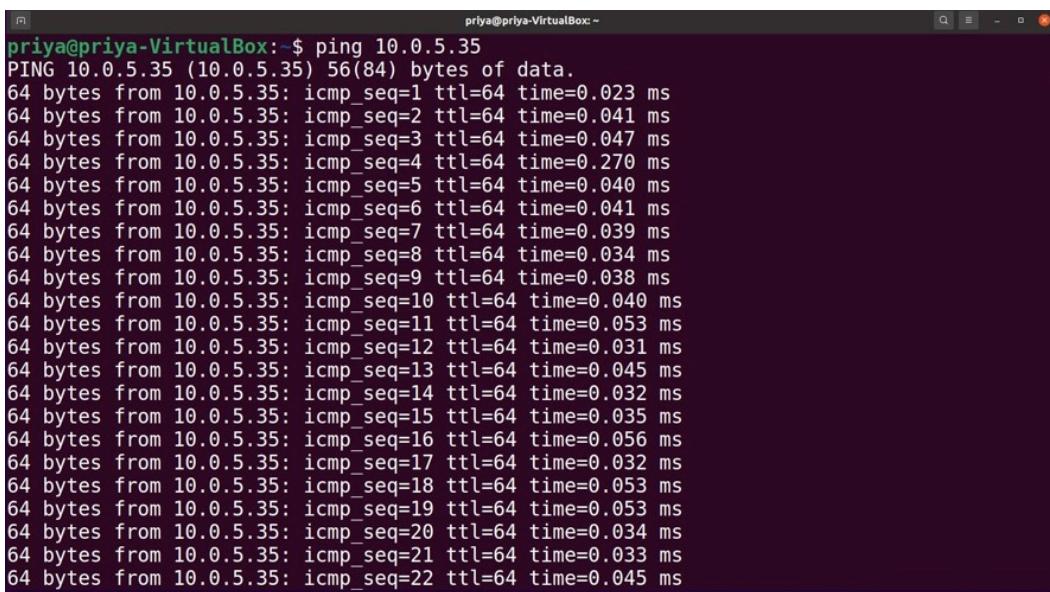
SCREENSHOT



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

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

Command Used : ping 10.0.5.35

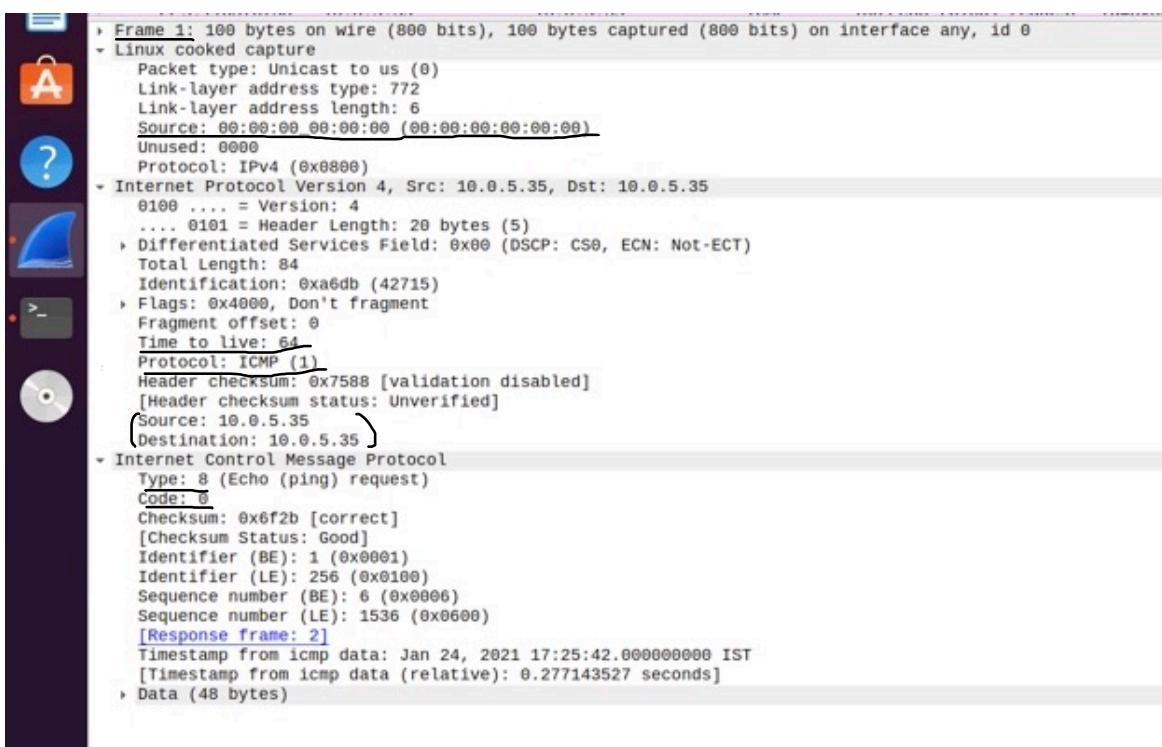


```
priya@priya-VirtualBox: $ ping 10.0.5.35
PING 10.0.5.35 (10.0.5.35) 56(84) bytes of data.
64 bytes from 10.0.5.35: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 10.0.5.35: icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from 10.0.5.35: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 10.0.5.35: icmp_seq=4 ttl=64 time=0.270 ms
64 bytes from 10.0.5.35: icmp_seq=5 ttl=64 time=0.040 ms
64 bytes from 10.0.5.35: icmp_seq=6 ttl=64 time=0.041 ms
64 bytes from 10.0.5.35: icmp_seq=7 ttl=64 time=0.039 ms
64 bytes from 10.0.5.35: icmp_seq=8 ttl=64 time=0.034 ms
64 bytes from 10.0.5.35: icmp_seq=9 ttl=64 time=0.038 ms
64 bytes from 10.0.5.35: icmp_seq=10 ttl=64 time=0.040 ms
64 bytes from 10.0.5.35: icmp_seq=11 ttl=64 time=0.053 ms
64 bytes from 10.0.5.35: icmp_seq=12 ttl=64 time=0.031 ms
64 bytes from 10.0.5.35: icmp_seq=13 ttl=64 time=0.045 ms
64 bytes from 10.0.5.35: icmp_seq=14 ttl=64 time=0.032 ms
64 bytes from 10.0.5.35: icmp_seq=15 ttl=64 time=0.035 ms
64 bytes from 10.0.5.35: icmp_seq=16 ttl=64 time=0.056 ms
64 bytes from 10.0.5.35: icmp_seq=17 ttl=64 time=0.032 ms
64 bytes from 10.0.5.35: icmp_seq=18 ttl=64 time=0.053 ms
64 bytes from 10.0.5.35: icmp_seq=19 ttl=64 time=0.053 ms
64 bytes from 10.0.5.35: icmp_seq=20 ttl=64 time=0.034 ms
64 bytes from 10.0.5.35: icmp_seq=21 ttl=64 time=0.033 ms
64 bytes from 10.0.5.35: icmp_seq=22 ttl=64 time=0.045 ms
```

OBSERVATIONS MADE

TTL	64
PROTOCOL USED BY PING	ICMP
TIME	ORDER OF (1/100) milliseconds Since I haven't pressed Ctrl+C Total time wasn't shown so I have written the order

REQUEST PACKET



The screenshot shows a single ICMP echo request packet captured by Wireshark. The packet details are as follows:

- Frame 1:** 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
- Linux cooked capture**
- Packet type:** Unicast to us (0)
- Link-layer address type:** 772
- Link-layer address length:** 6
- Source:** 00:00:00:00:00:00 (00:00:00:00:00:00)
- Unused:** 0000
- Protocol:** IPv4 (0x0800)
- Internet Protocol Version 4:** Src: 10.0.5.35, Dst: 10.0.5.35
 - Version:** 4
 - Header Length:** 20 bytes (5)
 - Differentiated Services Field:** 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length:** 84
 - Identification:** 0xa6db (42715)
 - Flags:** 0x4000, Don't fragment
 - Fragment offset:** 0
 - Time to live:** 64
 - Protocol:** ICMP (1)
 - Header checksum:** 0x7588 [validation disabled]
 - Checksum status:** Unverified
 - Source:** 10.0.5.35
 - Destination:** 10.0.5.35
- Internet Control Message Protocol**
 - Type:** 8 (Echo (ping) request)
 - Code:** 0
 - Csum:** 0x6f2b [correct]
 - Csum Status:** Good
 - Identifier (BE):** 1 (0x0001)
 - Identifier (LE):** 256 (0x0100)
 - Sequence number (BE):** 6 (0x0006)
 - Sequence number (LE):** 1536 (0x0600)
 - Response frame:** 2
 - Timestamp from icmp data:** Jan 24, 2021 17:25:42.000000000 IST
 - [Timestamp from icmp data (relative):** 0.277143527 seconds]
 - Data (48 bytes)**

Response Packet

```

> Frame 2: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
  Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 772
    Link-layer address length: 6
    Source: 00:00:00:00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
  + Internet Protocol Version 4, Src: 10.0.5.35, Dst: 10.0.5.35
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xa6dc (42716)
    Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xb587 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.0.5.35
    Destination: 10.0.5.35
  + Internet Control Message Protocol
    Type: 8 (Echo (ping) reply)
    Code: 0
    Checksum: 0x772b [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 6 (0x0006)
    Sequence number (LE): 1536 (0x0600)
    [Request frame: 1]
    [Response time: 0.012 ms]
    Timestamp from icmp data: Jan 24, 2021 17:25:42.000000000 IST
    [Timestamp from icmp data (relative): 0.277155328 seconds]
  > Data (48 bytes)

```

OBSERVATIONS MADE

DETAILS	FIRST ECHO REQUEST	FIRST ECHO REPLY
Frame Number	1	2
Source IP address	10.0.5.35	10.0.5.35
Destination IP address	10.0.5.35	10.0.5.35
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	ICMP- Version 4	ICMP- Version 4
Time To Live (TTL) Value	64	64

TASK 3: HTTP PDU Capture

Request packet (request to bbc.com)

Activities Wireshark ▾ Jan 24 18:43

Wireshark - Packet 445

Frame 4455: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits) on interface any, id 0
Linux cooked capture

Packet type: Sent by us (4)
Link-layer address type: 1
Link-layer address length: 6
Source: PcsCompu_a0:2c:49 (08:00:27:a0:2c:49)
Unused: 6800
Protocol: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.0.109, Dst: 151.101.158.169

0100 ... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 1062
Identification: 0x25f0 (9712)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x19be [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.0.109
Destination: 151.101.158.169

Transmission Control Protocol, Src Port: 46214, Dst Port: 80 Seq: 1, Ack: 1, Len: 1010

Source Port: 46214
Destination Port: 80
[Stream index: 83]
[TCP Segment Len: 1010]
Sequence number: 1 (relative sequence number)
Sequence number (raw): 614678687
[Next sequence number: 1011 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 1208325825
1000 ... = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window size value: 502
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0xb3c [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[Timestamps]
TCP payload (1010 bytes)

HyperText Transfer Protocol

GET / HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]

[GET / HTTP/1.1\r\n]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /

Request Version: HTTP/1.1

Host: www.bbc.com\r\n

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

[truncated]Cookie: optimizelyEndUserId=oeu1611493332977r0.06611335649701922; atuserId=%7B%22name%22%3A%22atuserId%22%2C%22val%22Upgrade-Insecure-Requests: 1\r\n

[Full request URI: http://www.bbc.com]
[HTTP request 1/1]
[Response in frame: 4459]

0000	00	04	00	01	00	06	08	00	27	a0	2c	49	68	00	08	00	1..	..,1h..
0010	45	00	04	26	25	f0	40	00	40	06	19	be	c0	a8	00	6d	E ..&%	0	0.....m
0020	97	65	9e	a9	b4	86	00	50	24	a3	40	9f	48	05	96	c1	e ..	-P	S @ H ..
0030	80	18	01	f6	fb	3c	00	00	01	01	08	0a	18	f7	63	39	<c9
0040	b7	1d	f7	c2	47	45	54	20	2f	20	48	54	54	50	2f	31	GET	/ HTTP/1

Help

Response packet

Activities Wireshark ▾

```

Frame 4459: 1363 bytes on wire (10904 bits), 1363 bytes captured (10904 bits) on interface any, id 0
  Linux cooked capture
    Packet type: Unicast to us (0)
    Link-layer address type: 1
    Link-layer address length: 6
    Source: Tp-LinkT_B0:b0:bf:c0 (98:da:c4:b0:bf:c0)
    Unused: 0000
    Protocol: IPv4 (0x0800)
  Internet Protocol Version 4 Src: 151.101.158.169, Dst: 192.168.0.109
    Version: 4
    ... 0100 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1347
    Identification: 0x02be (702)
    Flags: 0x0000 Don't fragment
    Fragment offset: 0
    Time to live: 55
    Protocol: TCP (6)
    Header checksum: 0x44d3 [validation disabled]
    [Header checksum status: Unverified]
    Source: 151.101.158.169
    Destination: 192.168.0.109
    Transmission Control Protocol, Src Port: 80, Dst Port: 46214, Seq: 1, Ack: 1011, Len: 1295
  Hypertext Transfer Protocol
    HTTP/1.1 301 Moved Permanently
      [Exploit Info: (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
      [HTTP/1.1 301 Moved Permanently\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
      Content-Type: text/html\r\n
      Location: https://www.bbc.com\r\n
      X-BBC-No-Scheme-Rewrite: 1\r\n
      Cache-Control: public, max-age=3600, stale-if-error=90, stale-while-revalidate=30\r\n
      Via: 1.1 39159a0d814f803c2a493823a4925c01.cloudflare.net (CloudFront), 1.1 varnish\r\n
      X-Amz-Cf-Pop: LHR-C1\r\n
      X-Amz-Cf-Id: pyif_MwWTKXJzKUf5UmHrlgb1wObmYVCKAIHUoXuTSnu3L9Pg==\r\n
      nel: {"reporter": "default", "max_age": 2592000, "include_subdomains": true, "failure_fraction": 0.05}\r\n
      report_to: {"group": "default", "max_age": 2592000, "endpoints": [{"url": "https://europe-west1-bbc-otg-traf-req-svc-chain: FASTLY_GTM\r\n
      req-svc-chain: FASTLY_GTM\r\n
      X-BBC-Edge-Cache-Status: MISS\r\n
      X-BBC-Origin-Response-Status: 301\r\n
      Server: BBC-GTM\r\n
      Content-Length: 162\r\n
      Accept-Ranges: bytes\r\n
      Date: Sun, 24 Jan 2021 13:11:43 GMT\r\n
      Age: 252\r\n
      Connection: keep-alive\r\n
      X-LB-NoCache: true\r\n
      X-Cloud-Edge-Cache-Status: HIT-CLUSTER\r\n
      X-Served-By: cloud-ama10248-MAA\r\n
      X-Cache: Hit from cloudfront, HIT\r\n
      X-Cache-Hits: 1\r\n
      X-Timer: S1611493903.097158,V80,VE1\r\n
      Vary: accept-encoding,x-bbc-edge-scheme\r\n
      \r\n
      [HTTP response 1/1]
      [Time since request: 0.143762321 seconds]
      [Request in frame: 4455]
      [Request URI: http://www.bbc.com/]
      File Data: 162 bytes
    Line-based text data: text/html (7 lines)
```

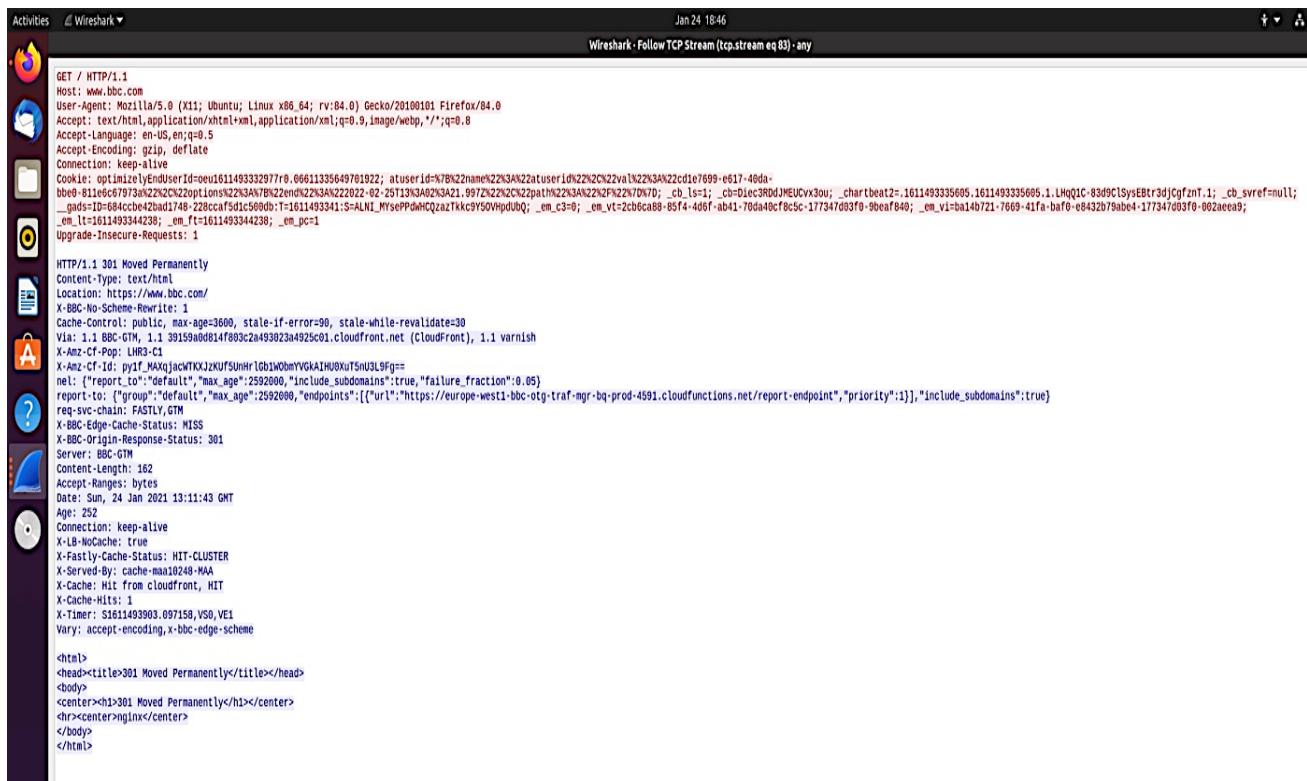
CONNECTION DETAILS

DETAILS	FIRST ECHO REQUEST	FIRST ECHO REPLY
Frame Number	4455	4459
Source Port	46214	80
Destination Port	80	46214
Source IP address	192.168.0.109	151.101.158.169
Destination IP address	151.101.158.169	192.168.0.109
Source Ethernet Address	08:00:27:a0:2c:49	98:da:c4:b0:bf:c0
Destination Ethernet Address	98:da:c4:b0:bf:c0	08:00:27:a0:2c:49

HTTP REQUEST AND RESPONSE

HTTP Request		HTTP Response	
Get	GET / HTTP/1.1\r\n	Server	BBC-GTM
Host	www.bbc.com	Content-Type	text/html
User-Agent	Mozilla/5.0	Date	Sun, 24 Jan 2021 13:11:43 GMT
Accept-Language	en-US	Location	https://www.bbc.com
Accept-Encoding	gzip,deflate	Content-Length	162
Connection	keep-alive	Connection	keep-alive

TCP STREAM



Task 4: Capturing packets with tcpdump

a)Viewing Interfaces available for packet capture

Command Used : sudo tcpdump -D

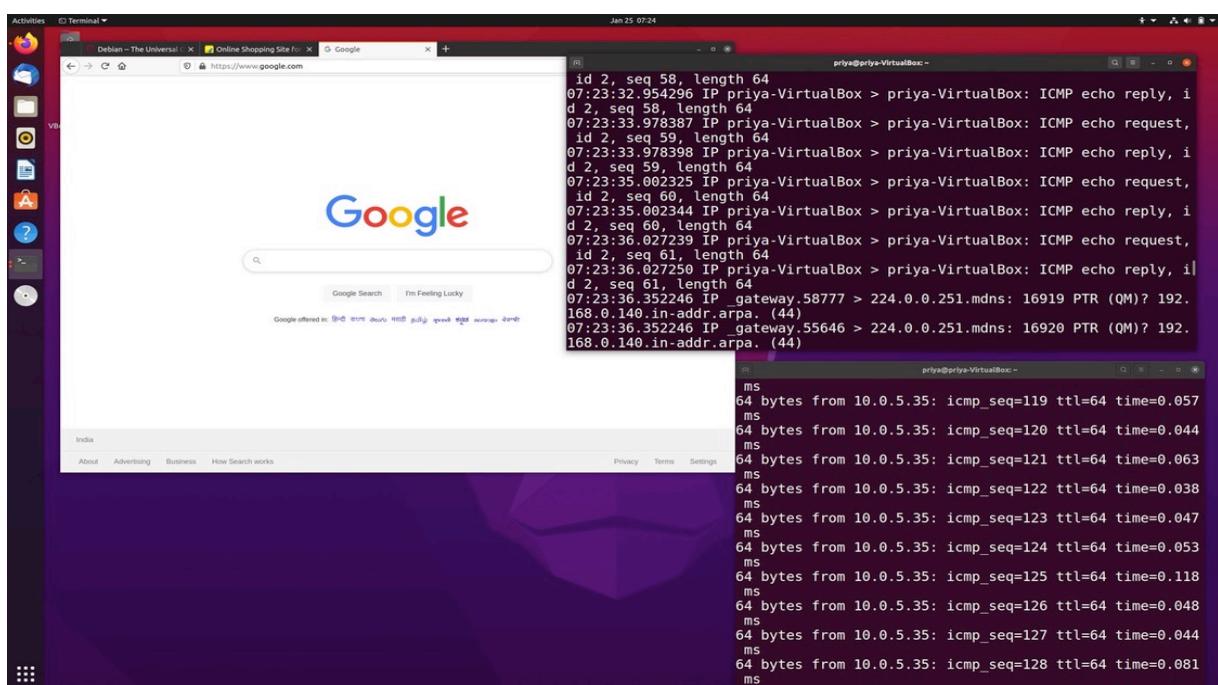
SCREENSHOT

```
priya@priya-VirtualBox:~$ sudo tcpdump -D
[sudo] password for priya:
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]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
priya@priya-VirtualBox:~$
```

b) Capturing packets in ‘any’ interface

Command Used : sudo tcpdump -i any

SCREENSHOT shows the browser with www.google.com the terminal with ping 10.0.5.35 and another terminal with **sudo tcpdump -i any**



c) Filtering packets based on the protocol (here its ICMP)

Command Used : `sudo tcpdump -i any -c5 icmp`

SCREENSHOT

```
priya@priya-VirtualBox: ~$ sudo tcpdump -i any -c5 icmp
[sudo] password for priya:
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
07:27:13.626563 IP priya-VirtualBox > priya-VirtualBox: ICMP echo request, id 3, seq 28, length 64
07:27:13.626573 IP priya-VirtualBox > priya-VirtualBox: ICMP echo reply, id 3, seq 28, length 64
07:27:14.651049 IP priya-VirtualBox > priya-VirtualBox: ICMP echo request, id 3, seq 29, length 64
07:27:14.651062 IP priya-VirtualBox > priya-VirtualBox: ICMP echo reply, id 3, seq 29, length 64
07:27:15.674342 IP priya-VirtualBox > priya-VirtualBox: ICMP echo request, id 3, seq 30, length 64
5 packets captured
12 packets received by filter
0 packets dropped by kernel
priya@priya-VirtualBox: ~
```



```
priya@priya-VirtualBox: ~$ sudo tcpdump -i any -c10 -nn -A port 80
64 bytes from 10.0.5.35: icmp_seq=38 ttl=64 time=0.044 ms
64 bytes from 10.0.5.35: icmp_seq=39 ttl=64 time=0.029 ms
64 bytes from 10.0.5.35: icmp_seq=40 ttl=64 time=0.033 ms
64 bytes from 10.0.5.35: icmp_seq=41 ttl=64 time=0.036 ms
64 bytes from 10.0.5.35: icmp_seq=42 ttl=64 time=0.032 ms
64 bytes from 10.0.5.35: icmp_seq=43 ttl=64 time=0.031 ms
64 bytes from 10.0.5.35: icmp_seq=44 ttl=64 time=0.041 ms
64 bytes from 10.0.5.35: icmp_seq=45 ttl=64 time=0.034 ms
64 bytes from 10.0.5.35: icmp_seq=46 ttl=64 time=0.051 ms
64 bytes from 10.0.5.35: icmp_seq=47 ttl=64 time=0.029 ms
64 bytes from 10.0.5.35: icmp_seq=48 ttl=64 time=0.029 ms
64 bytes from 10.0.5.35: icmp_seq=49 ttl=64 time=0.034 ms
64 bytes from 10.0.5.35: icmp_seq=50 ttl=64 time=0.036 ms
64 bytes from 10.0.5.35: icmp_seq=51 ttl=64 time=0.029 ms
64 bytes from 10.0.5.35: icmp_seq=52 ttl=64 time=0.028 ms
64 bytes from 10.0.5.35: icmp_seq=53 ttl=64 time=0.035 ms
64 bytes from 10.0.5.35: icmp_seq=54 ttl=64 time=0.027 ms
64 bytes from 10.0.5.35: icmp_seq=55 ttl=64 time=0.045 ms
64 bytes from 10.0.5.35: icmp_seq=56 ttl=64 time=0.038 ms
64 bytes from 10.0.5.35: icmp_seq=57 ttl=64 time=0.279 ms
64 bytes from 10.0.5.35: icmp_seq=58 ttl=64 time=0.037 ms
64 bytes from 10.0.5.35: icmp_seq=59 ttl=64 time=0.035 ms
64 bytes from 10.0.5.35: icmp_seq=60 ttl=64 time=0.045 ms
```

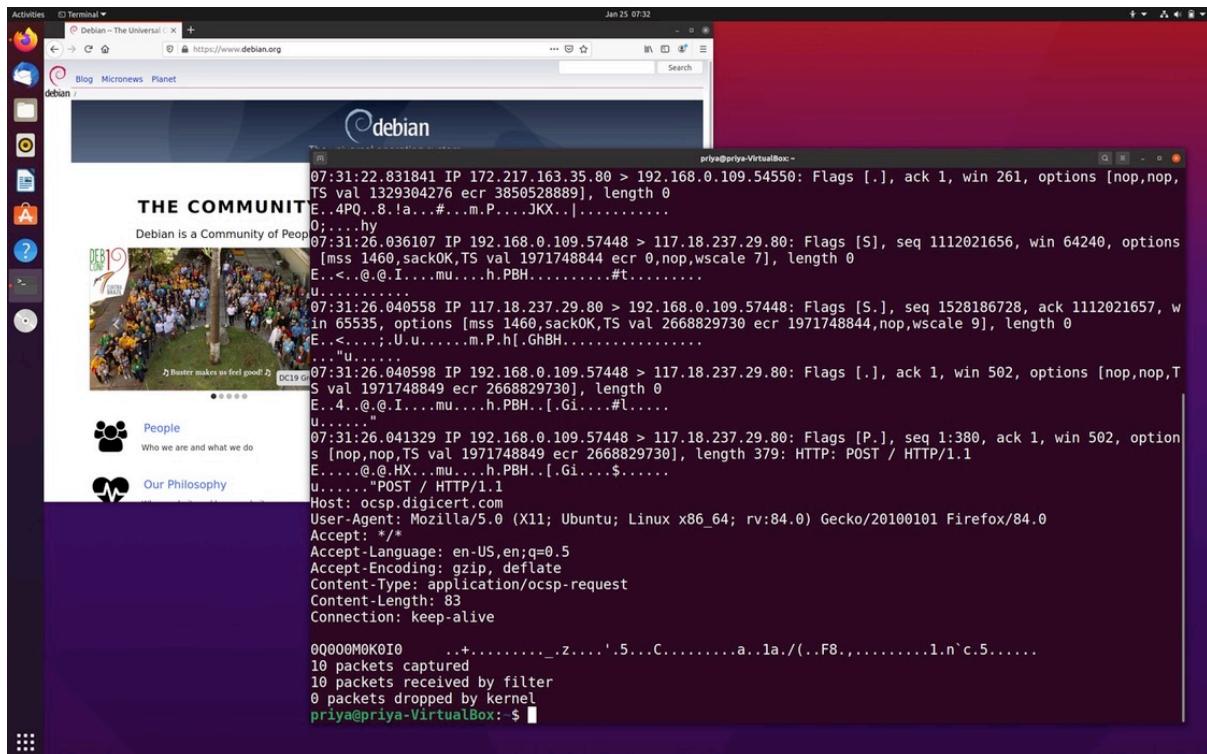
d)Checking packet content

Command Used : `sudo tcpdump -i any -c10 -nn -A port 80`

SCREENSHOTS show the HTTP content of a web request to www.debian.org

```
Activities Terminal Jan 25 07:32 priya@priya-VirtualBox ~
priya@priya-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
07:31:19.194251 IP 192.168.0.109.34888 > 34.107.221.82.80: Flags [.], ack 262138386, win 501, options [nop,nop,TS val 2585610420 ecr 20487
567741], length 0
E..4\..@..I..m"K.R.H.Pp.(.....
H.z.&
07:31:19.194380 IP 192.168.0.109.34892 > 34.107.221.82.80: Flags [.], ack 3524212015, win 501, options [nop,nop,TS val 2585610420 ecr 3020
485189], length 0
E..4[. @..0...m"K.R.L.P..<.5/.....
A..H....E
07:31:19.204854 IP 34.107.221.82.80 > 192.168.0.109.34888: Flags [.], ack 1, win 265, options [nop,nop,TS val 2048767003 ecr 2585528693],
length 0
E..4+W..8..z"K.R...m.P.H....p...)... E.....
?z.... u
07:31:19.205006 IP 34.107.221.82.80 > 192.168.0.109.34892: Flags [.], ack 1, win 265, options [nop,nop,TS val 3020495418 ecr 2585528706],
length 0
E..4.E..9..."K.R...m.P.L..5/....=... U8.....
:...
07:31:22.822517 IP 192.168.0.109.54550 > 172.217.163.35.80: Flags [.], ack 67848779, win 501, options [nop,nop,TS val 3850538893 ecr 13292
94268], length 0
E..4..@....m...#...PX.{.JK....9.....
0;k.
07:31:22.831841 IP 172.217.163.35.80 > 192.168.0.109.54550: Flags [.], ack 1, win 261, options [nop,nop,TS val 1329304276 ecr 3850528889],
length 0
E..4PQ..8.!a...#.m.P...JKX..|.....
0;....hy
07:31:26.036107 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [S], seq 1112021656, win 64240, options [mss 1460,sackOK,TS val 197174884
4 ecr 0,nop,wscale 7], length 0
E..<..@.I...mu...h.PBH.....#t.....
U.....
07:31:26.040558 IP 117.18.237.29.80 > 192.168.0.109.57448: Flags [S.], seq 1528186728, ack 1112021657, win 65535, options [mss 1460,sackOK
,TS val 2668829730 ecr 1971748844,nop,wscale 9], length 0
E..<...;U.0....m.P.h.GhBh.....
..."U.....
07:31:26.040598 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2668829730],
length 0
E..4..@.I...mu...h.PBH..[.6i....#l.....
U.....
07:31:26.041329 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [P.], seq 1:380, ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2
668829730], length 379: HTTP: POST / HTTP/1.1
E..<..@.Hx...mu...h.PBH..[.6i....$.....
U.....
Host: ocsp.digicert.com
```

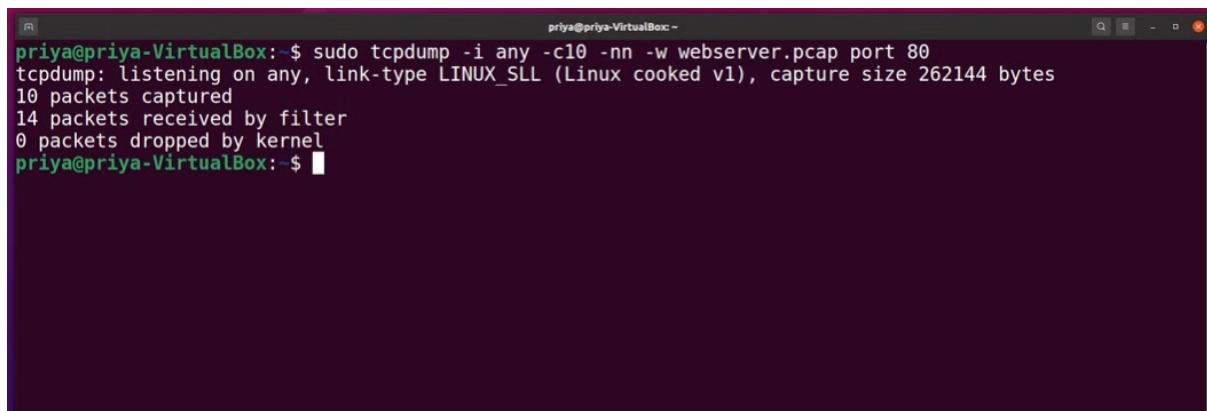
```
Activities Terminal Jan 25 07:32 priya@priya-VirtualBox ~
priya@priya-VirtualBox: $ sudo tcpdump -i any -c10 -nn -A port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX SLL (Linux cooked v1), capture size 262144 bytes
07:31:19.205006 IP 34.107.221.82.80 > 192.168.0.109.34892: Flags [.], ack 1, win 265, options [nop,nop,TS val 3020495418 ecr 2585528706],
length 0
E..4..@....m...#...PX.{.JK....9.....
:...
07:31:22.822517 IP 192.168.0.109.54550 > 172.217.163.35.80: Flags [.], ack 67848779, win 501, options [nop,nop,TS val 3850538893 ecr 13292
94268], length 0
E..4..@....m...#...PX.{.JK....9.....
0;k.
A..H....E
07:31:22.831841 IP 172.217.163.35.80 > 192.168.0.109.54550: Flags [.], ack 1, win 261, options [nop,nop,TS val 1329304276 ecr 3850528889],
length 0
E..4PQ..8.!a...#.m.P...JKX..|.....
0;....hy
07:31:26.036107 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [S], seq 1112021656, win 64240, options [mss 1460,sackOK,TS val 197174884
4 ecr 0,nop,wscale 7], length 0
E..<..@.I...mu...h.PBH.....#t.....
U.....
07:31:26.040558 IP 117.18.237.29.80 > 192.168.0.109.57448: Flags [S.], seq 1528186728, ack 1112021657, win 65535, options [mss 1460,sackOK
,TS val 2668829730 ecr 1971748844,nop,wscale 9], length 0
E..<...;U.0....m.P.h.GhBh.....
..."U.....
07:31:26.040598 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [.], ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2668829730],
length 0
E..4..@.I...mu...h.PBH..[.6i....#l.....
U.....
07:31:26.041329 IP 192.168.0.109.57448 > 117.18.237.29.80: Flags [P.], seq 1:380, ack 1, win 502, options [nop,nop,TS val 1971748849 ecr 2
668829730], length 379: HTTP: POST / HTTP/1.1
E..<..@.Hx...mu...h.PBH..[.6i....$.....
U.....
Host: ocsp.digicert.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: */
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/ocsp-request
Content-Length: 83
Connection: keep-alive
00000M0K0IO ..+....._z....'.5...C.....a..la./(..F8.,.....1.n`c.5.....
10 packets captured
10 packets received by filter
0 packets dropped by kernel
priya@priya-VirtualBox: $
```



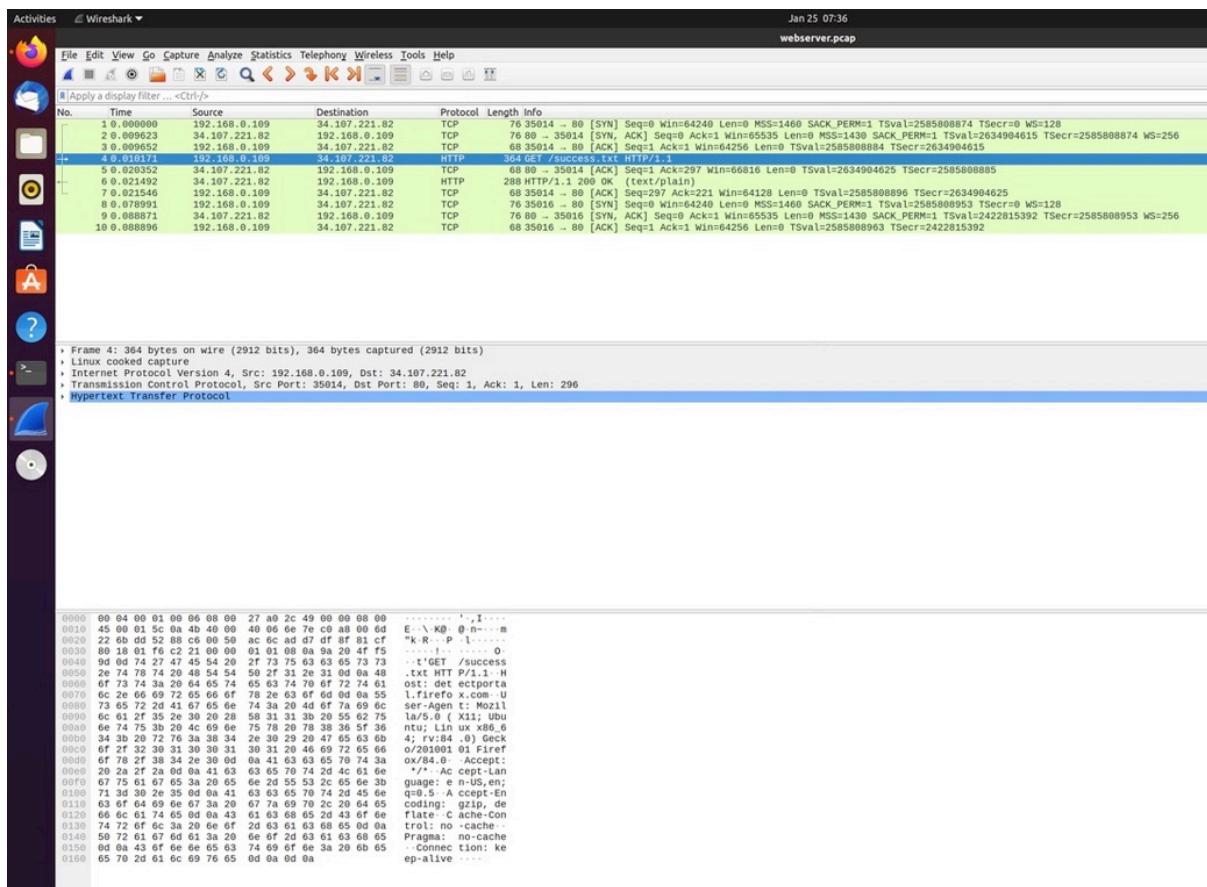
e) Saving the packet content in a file

Command Used : `sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80`

SCREENSHOT



THE FILE WEB SERVER.PCAP



Task 5: Perform Traceroute checks

a) Traceroute to www.google.com

Command Used : sudo traceroute www.google.com

SCREENSHOT

```
priya@priya-VirtualBox:~$ sudo traceroute www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  2.528 ms  2.469 ms  4.286 ms
 2  10.251.0.1 (10.251.0.1)  5.440 ms  5.416 ms  5.396 ms
 3  broadband.actcorp.in (202.83.20.43)  6.010 ms  5.962 ms  5.946 ms
 4  14.141.145.5.static-Bangalore.vsnl.net.in (14.141.145.5)  5.930 ms  5.915 ms  8.240 ms
 5  172.31.167.58 (172.31.167.58)  13.186 ms  12.982 ms  12.859 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  13.894 ms  11.027 ms  10.967 ms
 7  115.112.71.65.STDILL-Chennai.vsnl.net.in (115.112.71.65)  11.725 ms  11.688 ms  11.664 ms
 8  121.240.1.50 (121.240.1.50)  10.015 ms  10.919 ms  10.834 ms
 9  108.170.253.97 (108.170.253.97)  12.356 ms  108.170.253.113 (108.170.253.113)  11.533 ms  108.170.253.97
 10  142.250.233.143 (142.250.233.143)  14.746 ms  14.664 ms  14.641 ms
 11  maa03s35-in-f4.le100.net (142.250.71.36)  11.531 ms  11.430 ms  11.320 ms
priya@priya-VirtualBox:~$
```

Destination address is : 142.250.71.36

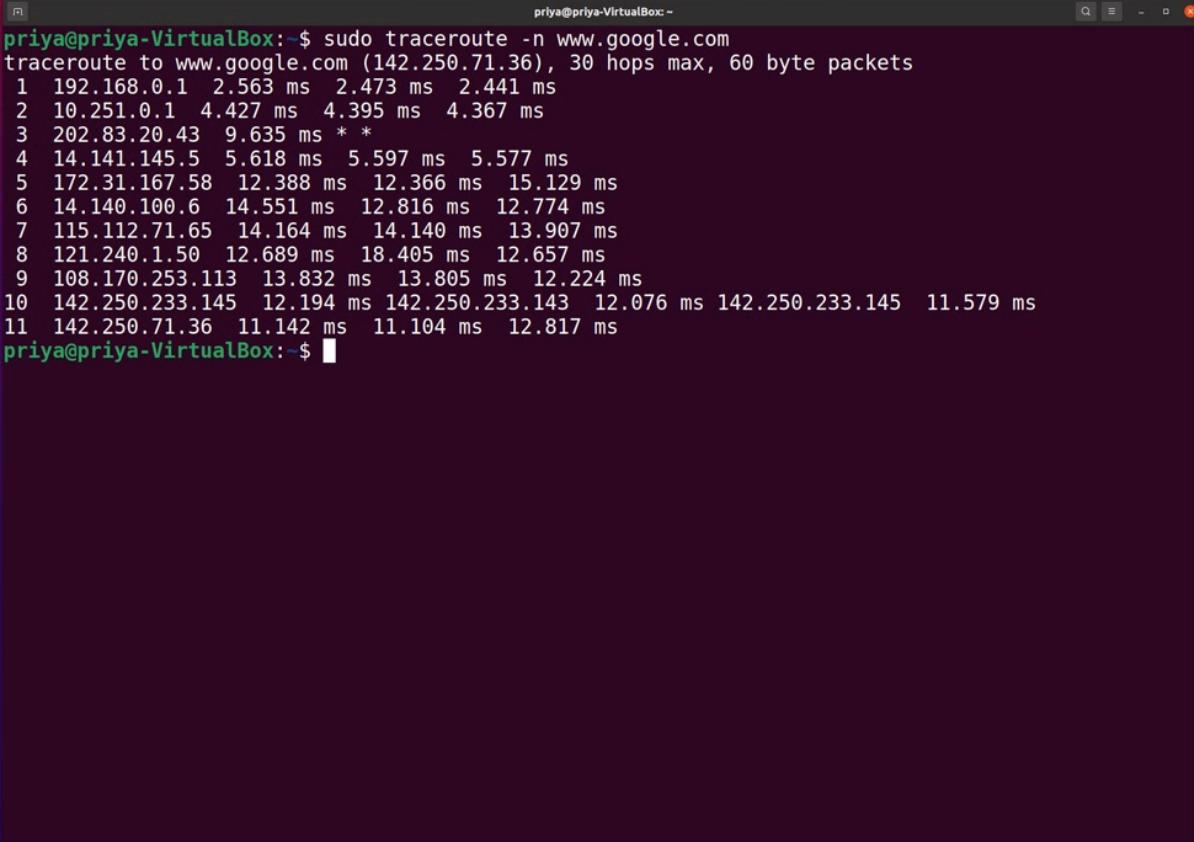
Number of Hops is :11

Maximum number of hops : 30

c) Disable the mapping of IP addresses with hostnames

Command Used : sudo traceroute -n www.google.com

SCREENSHOT

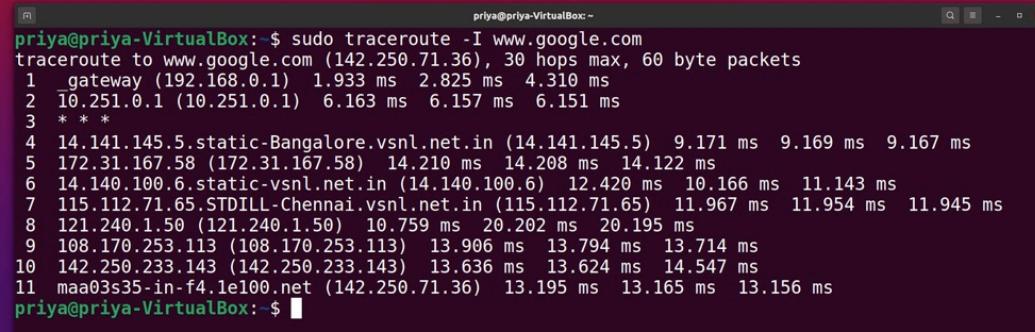


```
priya@priya-VirtualBox: $ sudo traceroute -n www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  192.168.0.1  2.563 ms  2.473 ms  2.441 ms
 2  10.251.0.1  4.427 ms  4.395 ms  4.367 ms
 3  202.83.20.43  9.635 ms * *
 4  14.141.145.5  5.618 ms  5.597 ms  5.577 ms
 5  172.31.167.58  12.388 ms  12.366 ms  15.129 ms
 6  14.140.100.6  14.551 ms  12.816 ms  12.774 ms
 7  115.112.71.65  14.164 ms  14.140 ms  13.907 ms
 8  121.240.1.50  12.689 ms  18.405 ms  12.657 ms
 9  108.170.253.113  13.832 ms  13.805 ms  12.224 ms
10  142.250.233.145  12.194 ms  142.250.233.143  12.076 ms  142.250.233.145  11.579 ms
11  142.250.71.36  11.142 ms  11.104 ms  12.817 ms
priya@priya-VirtualBox: $
```

d) Traceroute uses ICMP Protocol

Command Used : sudo traceroute -I www.google.com

SCREENSHOT

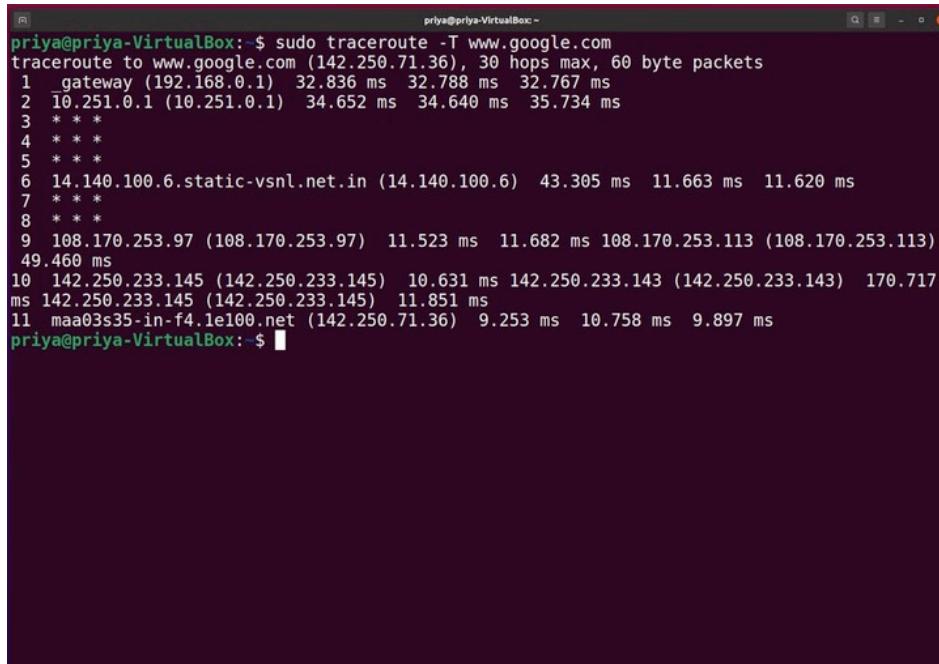


```
priya@priya-VirtualBox: $ sudo traceroute -I www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  1.933 ms  2.825 ms  4.310 ms
 2  10.251.0.1 (10.251.0.1)  6.163 ms  6.157 ms  6.151 ms
 3  * * *
 4  14.141.145.5.static-Bangalore.vsnl.net.in (14.141.145.5)  9.171 ms  9.169 ms  9.167 ms
 5  172.31.167.58 (172.31.167.58)  14.210 ms  14.208 ms  14.122 ms
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  12.420 ms  10.166 ms  11.143 ms
 7  115.112.71.65.STDILL-Chennai.vsnl.net.in (115.112.71.65)  11.967 ms  11.954 ms  11.945 ms
 8  121.240.1.50 (121.240.1.50)  10.759 ms  20.202 ms  20.195 ms
 9  108.170.253.113 (108.170.253.113)  13.906 ms  13.794 ms  13.714 ms
10  142.250.233.143 (142.250.233.143)  13.636 ms  13.624 ms  14.547 ms
11  maa03s35-in-f4.1e100.net (142.250.71.36)  13.195 ms  13.165 ms  13.156 ms
priya@priya-VirtualBox: $
```

e) Testing TCP Connection with traceroute

Command Used : sudo traceroute -I www.google.com

SCREENSHOT



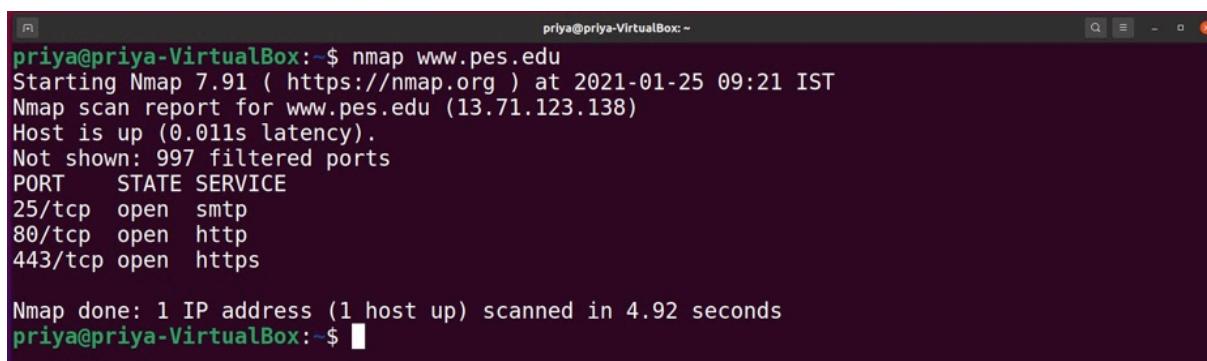
```
priya@priya-VirtualBox:~$ sudo traceroute -T www.google.com
traceroute to www.google.com (142.250.71.36), 30 hops max, 60 byte packets
 1  gateway (192.168.0.1)  32.836 ms  32.788 ms  32.767 ms
 2  10.251.0.1 (10.251.0.1)  34.652 ms  34.640 ms  35.734 ms
 3  * * *
 4  * * *
 5  * * *
 6  14.140.100.6.static-vsnl.net.in (14.140.100.6)  43.305 ms  11.663 ms  11.620 ms
 7  * * *
 8  * * *
 9  108.170.253.97 (108.170.253.97)  11.523 ms  11.682 ms  108.170.253.113 (108.170.253.113)
 49.460 ms
10  142.250.233.145 (142.250.233.145)  10.631 ms  142.250.233.143 (142.250.233.143)  170.717
ms 142.250.233.145 (142.250.233.145)  11.851 ms
11  maa03s35-in-f4.1e100.net (142.250.71.36)  9.253 ms  10.758 ms  9.897 ms
priya@priya-VirtualBox:~$
```

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

a) scan a host using its host name

Command Used : nmap www.pes.edu

SCREENSHOT



```
priya@priya-VirtualBox:~$ nmap www.pes.edu
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 09:21 IST
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.011s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds
priya@priya-VirtualBox:~$
```

b) Scan a host using IP Address

Command Used : nmap 163.53.78.128

SCREENSHOT

```
priya@priya-VirtualBox:~$ nmap 163.53.78.128
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 09:24 IST
Nmap scan report for 163.53.78.128
Host is up (0.011s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
priya@priya-VirtualBox:~$
```

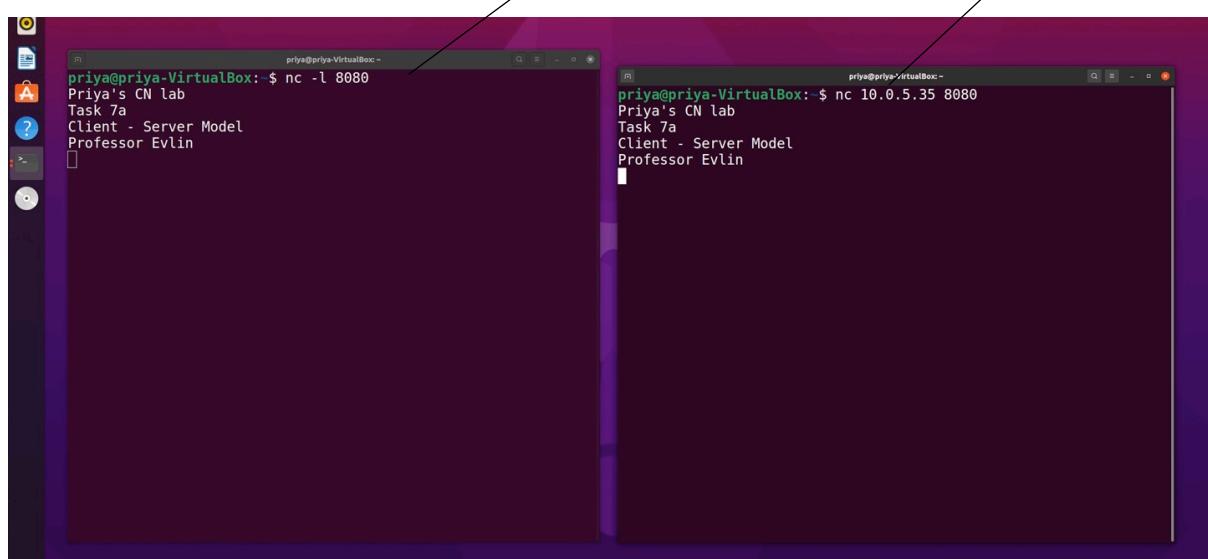
c) Scan multiple IP Addresses

Command Used : nmap 192.168.1.1 192.168.1.2 192.168.1.3

```
priya@priya-VirtualBox:~$ nmap 192.168.1.1 192.168.1.2 192.168.1.3
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 09:26 IST
Nmap done: 3 IP addresses (0 hosts up) scanned in 3.17 seconds
priya@priya-VirtualBox:~$
```

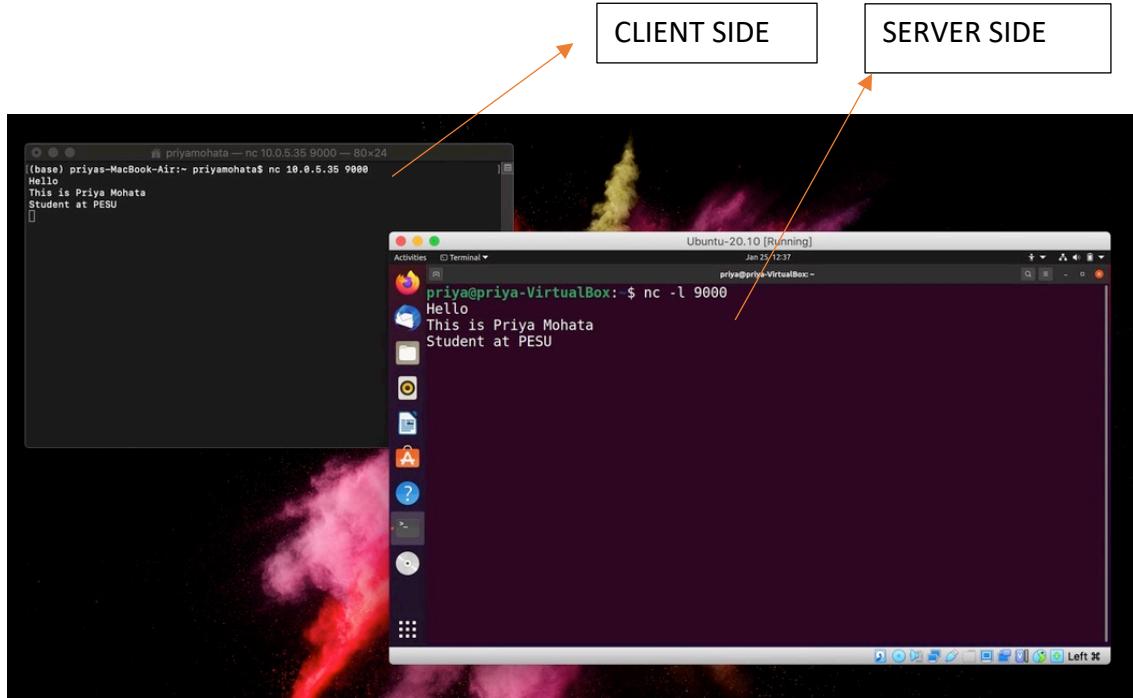
Task 7

a) Netcat as Chat tool



(i) Intra System Communication

(ii) Inter system communication

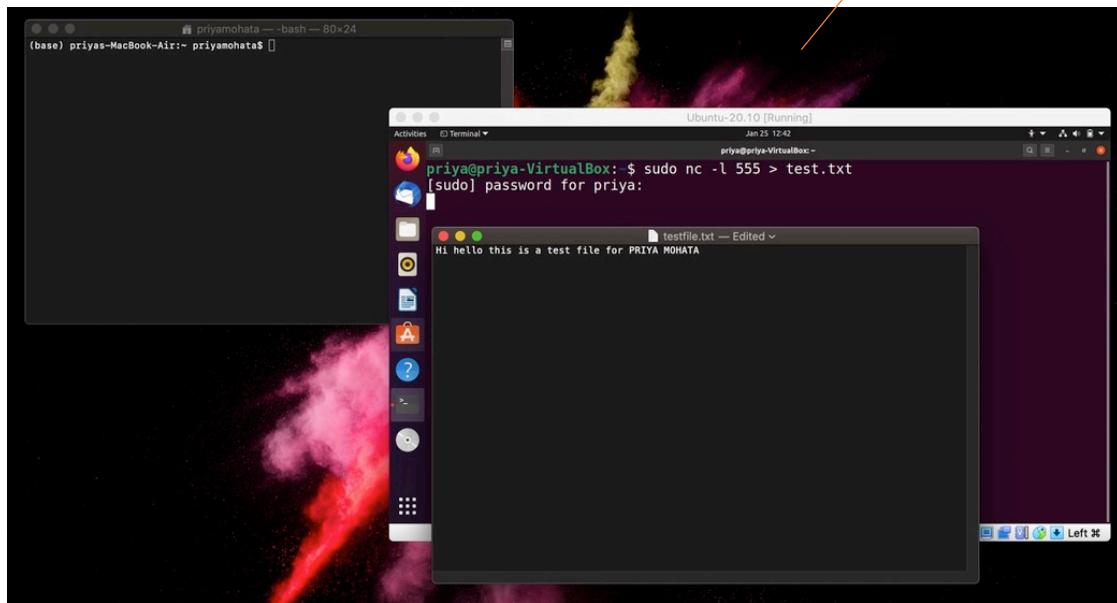


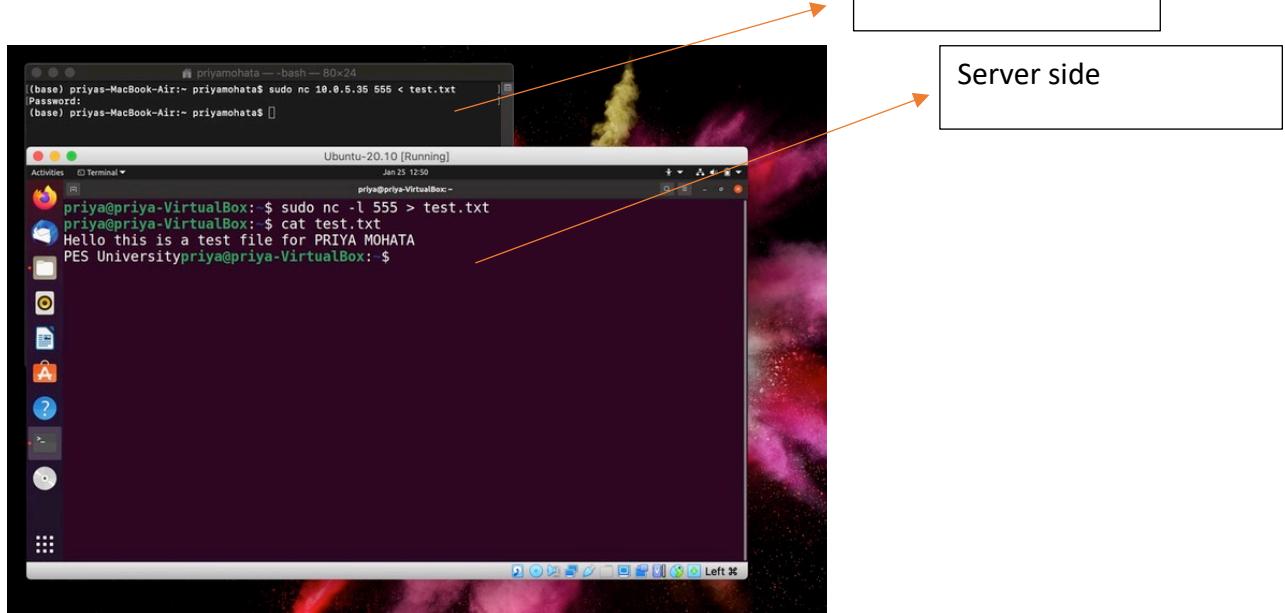
b) Use Netcat to Transfer Files

Command Used : sudo nc -l 555 > test.txt // Server Side

sudo nc 10.0.5.35 555 < test.txt //Client side

cat test.txt

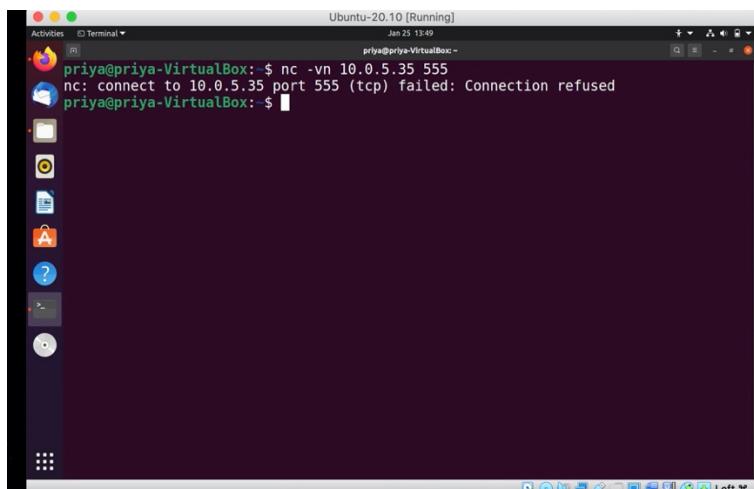




Task 7 c): Other Commands

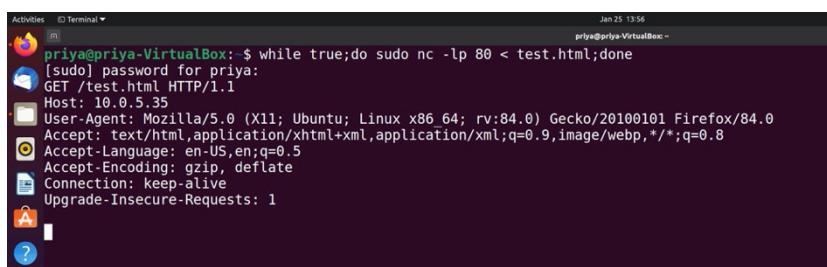
(i) To test if a particular TCP port of a remote host is open.

Command Used : nc -vn 10.0.5.35 555



(ii) Run a web server with a static web page.

Command Used : while true; do sudo nc -lp 80 < test.html; done



QUESTION & ANSWER

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

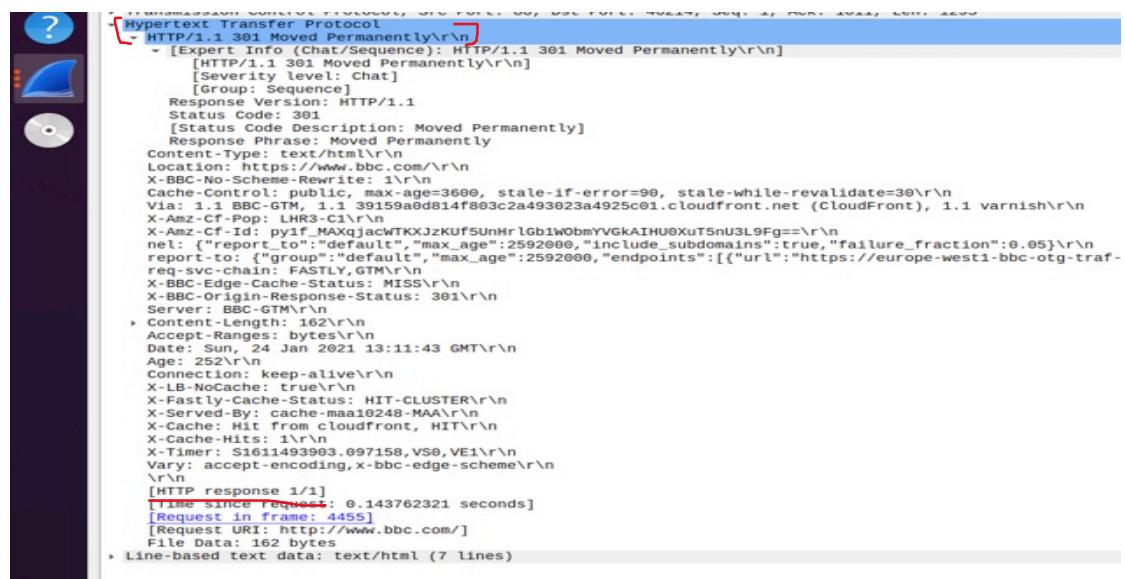
ANSWER : The Mozilla Firefox is running on the **HTTP Version 1.1**.

We can observe this in the screenshot below :

GET /HTTP/1.1\r\n



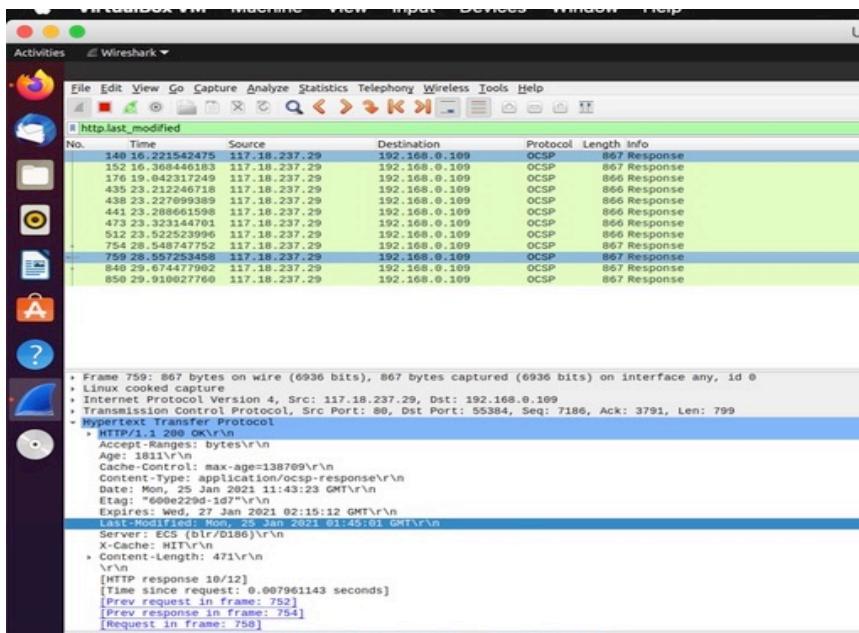
The web server also is running on the **HTTP Version 1.1**



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

ANSWER : In the filter tab of wireshark type 'http.last_modified'

Example : In the example below last modified is Mon,25 Jan 2021 , 01:45:01 GMT



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

ANSWER : Ping continuously sends the ICMP packets until it receives an interrupt signal. To specify the number of packets we use the **-c** flag followed by the number of packets

Command Used in the example : ping -c 10 www.edmodo.com

Example :

```
prya@priya-VirtualBox:~$ ping -c 10 www.edmodo.com
PING www.edmodo.com (99.86.19.126) 56(84) bytes of data.
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=1 ttl=245 time=3.88 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=2 ttl=245 time=3.45 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=3 ttl=245 time=3.27 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=4 ttl=245 time=3.97 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=5 ttl=245 time=5.65 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=6 ttl=245 time=4.12 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=7 ttl=245 time=3.82 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=8 ttl=245 time=11.0 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=9 ttl=245 time=3.90 ms
64 bytes from server-99-86-19-126.blr50.r.cloudfront.net (99.86.19.126): icmp_seq=10 ttl=245 time=3.75 ms

--- www.edmodo.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 3.270/4.681/11.016/2.196 ms
prya@priya-VirtualBox:~$
```

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

ANSWER : We can use nmap -O -v {domain name}

Example :

```
priya@priya-VirtualBox:~$ sudo nmap -O -v www.pes.edu
[sudo] password for priya:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-25 15:29 IST
Initiating Ping Scan at 15:29
Scanning www.pes.edu (13.71.123.138) [4 ports]
Completed Ping Scan at 15:29, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:29
Completed Parallel DNS resolution of 1 host. at 15:29, 0.10s elapsed
Initiating SYN Stealth Scan at 15:29
Scanning www.pes.edu (13.71.123.138) [1000 ports]
Discovered open port 25/tcp on 13.71.123.138
Discovered open port 443/tcp on 13.71.123.138
Discovered open port 80/tcp on 13.71.123.138
Completed SYN Stealth Scan at 15:29, 4.96s elapsed (1000 total ports)
Initiating OS detection (try #1) against www.pes.edu (13.71.123.138)
Nmap scan report for www.pes.edu (13.71.123.138)
Host is up (0.0097s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.27 - 2.6.28, Linux 2.6.9 - 2.6.27
Uptime guess: 12.664 days (since Tue Jan 12 23:34:25 2021)
TCP Sequence Prediction: Difficulty=202 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.38 seconds
Raw packets sent: 2043 (92.388KB) | Rcvd: 14 (712B)
priya@priya-VirtualBox:~$ █
```