COMPUTER NETWORKS LABORATORY

COURSE CODE: UE19CS255

NAME : T.LOHITH SRINIVAS
SRN : PES2UG19CS203
SECTION : D
DATE : 2/02/2021
WEEK : 1

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

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

```
lohith@lohith-IdeaPad-3-15IIL05:~$ 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: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 98:8d:46:5e:37:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp0s20f3
       valid_lft 86329sec preferred_lft 86329sec
    inet6 fe80::ff14:1c0c:ae42:9399/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

INTERFACE NAME	IP ADDRESS (IPV4/IPV6)	MAC ADDRESS
lo	IPV4: 127.0.0.1/8 IPV6: 1/128	00:00:00:00:00:00
wlp0s20f3	IPV4: 192.168.1.12/24 IPV6: f280::ff14:1c0c:ae42:9399/64	98:8d:46:5e:37:f1

Step 2: To assign an IP address to an interface.

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo ip addr add 10.0.4.6/24 dev wlp0s20f3
[sudo] password for lohith:
lohith@lohith-IdeaPad-3-15IIL05:~$ 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: wlp0s20f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 98:8d:46:5e:37:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp0s20f3
       valid_lft 86266sec preferred_lft 86266sec
    inet 10.0.4.6/24 scope global wlp0s20f3
       valid_lft forever preferred_lft forever
    inet6 fe80::ff14:1c0c:ae42:9399/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Step 3: To activate / deactivate a network interface.

Deactivating network interface:

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo ifconfig wlp0s20f3 down
lohith@lohith-IdeaPad-3-15IIL05:~$ 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 168  bytes 13861 (13.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 168  bytes 13861 (13.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Activating network interface:

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo ifconfig wlp0s20f3 up
lohith@lohith-IdeaPad-3-15IIL05:~$ 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 192  bytes 15613 (15.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 192  bytes 15613 (15.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.1.12  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff14:1c0c:ae42:9399  prefixlen 64  scopeid 0x20<link>
        ether 98:8d:46:5e:37:f1  txqueuelen 1000  (Ethernet)
        RX packets 137  bytes 13890 (13.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 198  bytes 21748 (21.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 4: To show the current neighbour table in kernel.

```
lohith@lohith-IdeaPad-3-15IIL05:~$ ip neigh
192.168.1.1 dev wlp0s20f3 lladdr 18:45:93:7a:56:10 REACHABLE
fe80::1 dev wlp0s20f3 lladdr 18:45:93:7a:56:10 DELAY
```

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

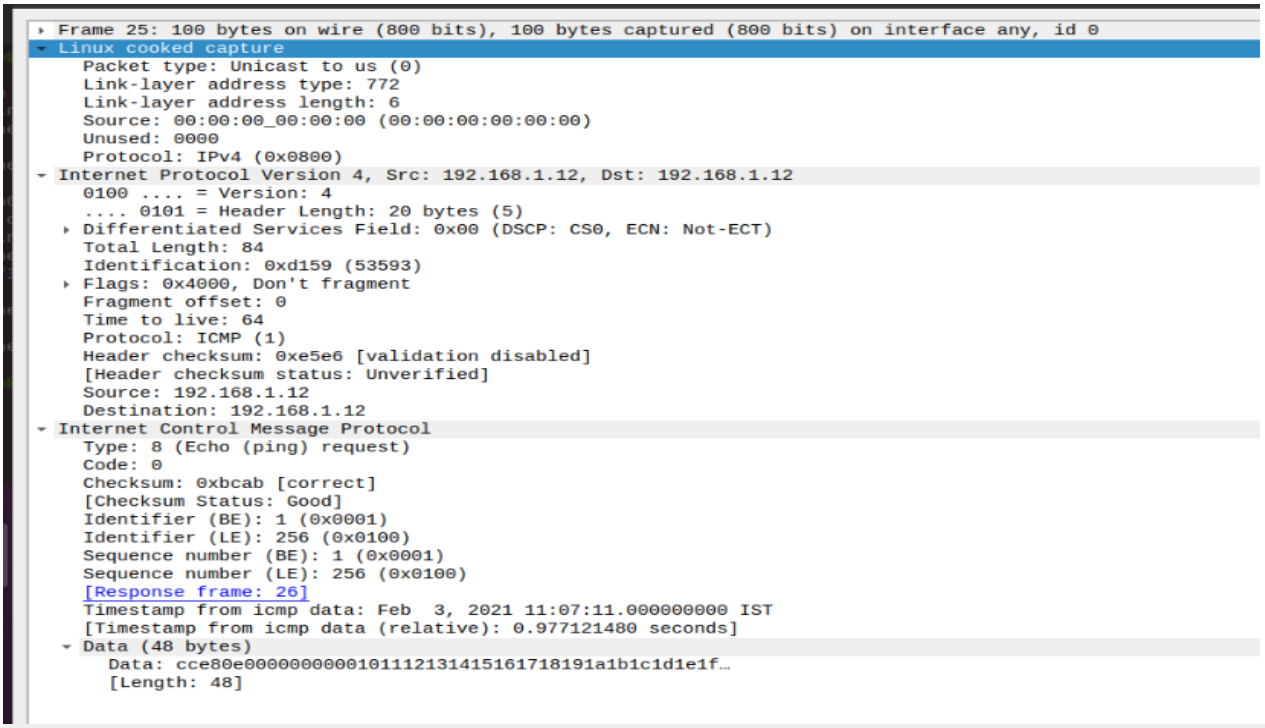
```
lohith@lohith-IdeaPad-3-15IIL05:~$ ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=0.053 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=0.040 ms
64 bytes from 192.168.1.12: icmp_seq=5 ttl=64 time=0.038 ms
64 bytes from 192.168.1.12: icmp_seq=6 ttl=64 time=0.040 ms
64 bytes from 192.168.1.12: icmp_seq=7 ttl=64 time=0.045 ms
64 bytes from 192.168.1.12: icmp_seq=8 ttl=64 time=0.051 ms
64 bytes from 192.168.1.12: icmp_seq=9 ttl=64 time=0.038 ms
64 bytes from 192.168.1.12: icmp_seq=10 ttl=64 time=0.044 ms
64 bytes from 192.168.1.12: icmp_seq=11 ttl=64 time=0.039 ms
64 bytes from 192.168.1.12: icmp_seq=12 ttl=64 time=0.043 ms
64 bytes from 192.168.1.12: icmp_seq=13 ttl=64 time=0.044 ms
64 bytes from 192.168.1.12: icmp_seq=14 ttl=64 time=0.034 ms
64 bytes from 192.168.1.12: icmp_seq=15 ttl=64 time=0.037 ms
64 bytes from 192.168.1.12: icmp_seq=16 ttl=64 time=0.037 ms
64 bytes from 192.168.1.12: icmp_seq=17 ttl=64 time=0.032 ms
64 bytes from 192.168.1.12: icmp_seq=18 ttl=64 time=0.042 ms
64 bytes from 192.168.1.12: icmp_seq=19 ttl=64 time=0.038 ms
64 bytes from 192.168.1.12: icmp_seq=20 ttl=64 time=0.037 ms
64 bytes from 192.168.1.12: icmp_seq=21 ttl=64 time=0.037 ms
64 bytes from 192.168.1.12: icmp_seq=22 ttl=64 time=0.033 ms
```

Observations to be made:

TTL : 64

Protocol use by ping : ICMP

Time : Order of 1/100 ms



```
▸ Frame 25: 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: 192.168.1.12, Dst: 192.168.1.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xd159 (53593)
  ▸ Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0xe5e6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.12
    Destination: 192.168.1.12
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xbcab [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 26]
    Timestamp from icmp data: Feb  3, 2021 11:07:11.000000000 IST
    [Timestamp from icmp data (relative): 0.977121480 seconds]
  ▾ Data (48 bytes)
      Data: cce80e0000000000101112131415161718191a1b1c1d1e1f…
      [Length: 48]
```

```
▸ Frame 26: 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: 192.168.1.12, Dst: 192.168.1.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xd15a (53594)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: ICMP (1)
    Header checksum: 0x25e6 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.12
    Destination: 192.168.1.12
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xc4ab [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Request frame: 25]
    [Response time: 0.013 ms]
    Timestamp from icmp data: Feb  3, 2021 11:07:11.000000000 IST
    [Timestamp from icmp data (relative): 0.977134013 seconds]
  ▾ Data (48 bytes)
      Data: cce80e0000000000101112131415161718191a1b1c1d1e1f…
      [Length: 48]
```

Observations made:

Details	First Echo Request	First Echo Response
Frame Number	25	26
Source IP address	192.168.1.12	192.168.1.12
Destination IP address	192.168.1.12	192.168.1.12
ICMP Type Value	8	0
ICMP Code Value	0	0
Source Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Destination Ethernet Address	00:00:00:00:00:00	00:00:00:00:00:00
Internet Protocol Version	4	4
Time To Live (TTL) Value	64	64

Task 4: Capturing packets with tcpdump

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

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo tcpdump -D
[sudo] password for lohith:
1.wlp0s20f3 [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.bluetooth0 (Bluetooth adapter number 0) [none]
```

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.

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo tcpdump -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
11:33:30.322645 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 32, length 64
11:33:30.322666 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo reply, id 2, seq 32, length 64
11:33:30.323391 IP localhost.50132 > localhost.domain: 31677+ [1au] PTR? 12.1.168.192.in-addr.arpa. (54)
11:33:30.323724 IP lohith-IdeaPad-3-15IIL05.59499 > _gateway.domain: 33204+ [1au] PTR? 12.1.168.192.in-addr.arpa. (54)
11:33:30.334745 IP _gateway.domain > lohith-IdeaPad-3-15IIL05.59499: 33204 NXDomain 0/1/1 (131)
11:33:30.335015 IP lohith-IdeaPad-3-15IIL05.59499 > _gateway.domain: 33204+ PTR? 12.1.168.192.in-addr.arpa. (43)
11:33:30.349352 IP localhost.55695 > localhost.domain: 3380+ [1au] PTR? 53.0.0.127.in-addr.arpa. (52)
11:33:30.349511 IP localhost.domain > localhost.55695: 3380 1/0/1 PTR localhost. (75)
11:33:31.346628 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 33, length 64
11:33:31.346645 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo reply, id 2, seq 33, length 64
11:33:31.964724 IP6 fe80::1 > lohith-IdeaPad-3-15IIL05: ICMP6, neighbor solicitation, who has lohith-IdeaPad-3-15IIL05, length 32
11:33:31.964770 IP6 lohith-IdeaPad-3-15IIL05 > fe80::1: ICMP6, neighbor advertisement, tgt is lohith-IdeaPad-3-15IIL05, length 24
11:33:31.964970 IP localhost.42244 > localhost.domain: 52583+ [1au] PTR? 9.9.3.9.2.4.e.a.c.0.c.1.4.1.f.f.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (101)
11:33:31.965501 IP lohith-IdeaPad-3-15IIL05.52163 > _gateway.domain: 23053+ PTR? 9.9.3.9.2.4.e.a.c.0.c.1.4.1.f.f.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:33:32.138378 IP _gateway.domain > lohith-IdeaPad-3-15IIL05.52163: 23053 NXDomain 0/1/0 (154)
11:33:32.138956 IP localhost.domain > localhost.42244: 52583 2/0/1 PTR lohith-IdeaPad-3-15IIL05., PTR lohith-IdeaPad-3-15IIL05.local. (183)
11:33:32.178594 IP6 lohith-IdeaPad-3-15IIL05 > fe80::1: ICMP6, neighbor solicitation, who has fe80::1, length 32
11:33:32.179737 IP6 fe80::1 > lohith-IdeaPad-3-15IIL05: ICMP6, neighbor advertisement, tgt is fe80::1, length 24
11:33:32.247369 IP 192.168.1.16.mdns > 224.0.0.251.mdns: 52 [2q] PTR (QM)? _%9E5E7C8F47989526C9BCD95D24084F6F0B27C5ED._sub._googlecast._tcp.local. PTR (QM)? _googlecast._tcp.local. (94)
11:33:32.247615 IP localhost.35750 > localhost.domain: 14805+ [1au] PTR? 251.0.0.224.in-addr.arpa. (53)
11:33:32.247903 IP lohith-IdeaPad-3-15IIL05.46633 > _gateway.domain: 16238+ PTR? 251.0.0.224.in-addr.arpa. (42)
11:33:32.258612 IP _gateway.domain > lohith-IdeaPad-3-15IIL05.46633: 16238 NXDomain 0/1/0 (99)
11:33:32.258968 IP localhost.domain > localhost.35750: 14805 NXDomain 0/0/1 (53)
11:33:32.370619 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 34, length 64
```

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

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo tcpdump -i any -c5 icmp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
11:33:51.826640 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 53, length 64
11:33:51.826654 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo reply, id 2, seq 53, length 64
11:33:52.850654 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 54, length 64
11:33:52.850668 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo reply, id 2, seq 54, length 64
11:33:53.874668 IP lohith-IdeaPad-3-15IIL05 > lohith-IdeaPad-3-15IIL05: ICMP echo request, id 2, seq 55, length 64
5 packets captured
12 packets received by filter
0 packets dropped by kernel
```

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

```
lohith@lohith-IdeaPad-3-15IIL05:~$ 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
11:34:30.802558 IP 192.168.1.12.57950 > 216.58.196.163.80: Flags [.], ack 1680893641, win 501, options [nop,nop,TS val 2940580405 ecr 1136692580], length 0
E..4.A@.@.....:...^.Pi..&d0f.....^.....
.E.5C..d
11:34:30.817864 IP 216.58.196.163.80 > 192.168.1.12.57950: Flags [.], ack 1, win 277, options [nop,nop,TS val 1136702820 ecr 2940498902], length 0
E..4.z..<.c7.:.....P.^d0f.i..'..........
C..d.Ds.
11:34:36.178597 IP 192.168.1.12.57944 > 216.58.196.163.80: Flags [.], ack 2912045798, win 501, options [nop,nop,TS val 2940585781 ecr 2032147264], length 0
E..4S.@.@.....:...X.P.Fd...J.....^.....
.E.5y .@
11:34:36.187858 IP 216.58.196.163.80 > 192.168.1.12.57944: Flags [.], ack 1, win 261, options [nop,nop,TS val 2032157501 ecr 2940493864], length 0
E..4Gd..<..M.:.....P.X..J..Fd.....    .....
y C=.D`(
11:34:41.042554 IP 192.168.1.12.57950 > 216.58.196.163.80: Flags [.], ack 1, win 501, options [nop,nop,TS val 2940590645 ecr 1136702820], length 0
E..4.B@.@.....:...^.Pi..&d0f.....^.....
.E.5C..d
11:34:41.061323 IP 216.58.196.163.80 > 192.168.1.12.57950: Flags [.], ack 1, win 277, options [nop,nop,TS val 1136713060 ecr 2940498902], length 0
E..4....<.M..:.....P.^d0f.i..'..........
C..d.Ds.
11:34:46.418569 IP 192.168.1.12.57944 > 216.58.196.163.80: Flags [.], ack 1, win 501, options [nop,nop,TS val 2940596021 ecr 2032157501], length 0
E..4S.@.@.....:...X.P.Fd...J.....^.....
.E.5y C=
11:34:46.431478 IP 216.58.196.163.80 > 192.168.1.12.57944: Flags [.], ack 1, win 261, options [nop,nop,TS val 2032167745 ecr 2940493864], length 0
E..4^ ..<....:.....P.X..J..Fd..........
y kA.D`(
11:34:51.282511 IP 192.168.1.12.57950 > 216.58.196.163.80: Flags [.], ack 1, win 501, options [nop,nop,TS val 2940600884 ecr 1136713060], length 0
E..4.C@.@.....:...^.Pi..&d0f.....^.....
.F.4C..d
11:34:51.297297 IP 216.58.196.163.80 > 192.168.1.12.57950: Flags [.], ack 1, win 277, options [nop,nop,TS val 1136723300 ecr 2940498902], length 0
E..4.y..<.88.:.....P.^d0f.i..'....|.....
C..d.Ds.
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

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

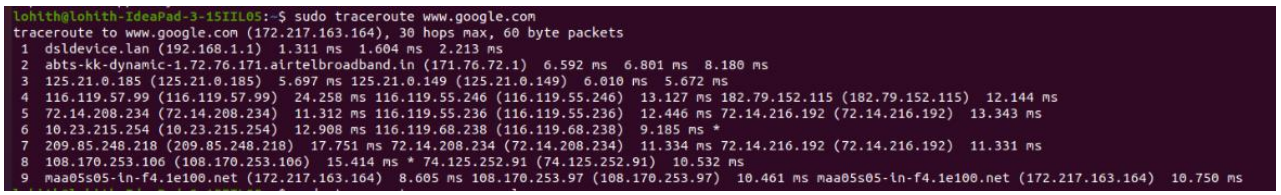
sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo tcpdump -i any -c10 -nn -w webserver.pcap port 80
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

Task 5: Perform Traceroute checks

Step 1: Run the traceroute using the following command.

sudo traceroute www.google.com



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

Destination Address **:** 172.217.163.164

No. of hops **:** 30

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

sudo traceroute -n www.google.com

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo traceroute -n www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  192.168.1.1  1.141 ms  1.599 ms  2.074 ms
 2  171.76.72.1  3.933 ms  4.913 ms  4.908 ms
 3  125.21.0.185  4.903 ms  5.257 ms 125.21.0.149  5.252 ms
 4  116.119.55.246  15.729 ms 182.79.152.115  14.497 ms 182.79.177.69  14.498 ms
 5  72.14.216.192  16.185 ms 72.14.208.234  15.284 ms 116.119.44.239  15.727 ms
 6  182.79.198.22  17.448 ms 182.79.141.174  16.304 ms 182.79.177.69  12.837 ms
 7  72.14.208.234  11.976 ms 72.14.216.192  13.025 ms 108.170.253.97  10.724 ms
 8  209.85.248.181  11.427 ms * *
 9  172.253.73.28  12.134 ms 108.170.236.196  11.884 ms 74.125.242.129  12.462 ms
10  74.125.252.91  15.585 ms 209.85.248.181  12.639 ms  12.770 ms
11  172.217.163.164  11.714 ms  10.963 ms  10.553 ms
```

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

sudo traceroute -I www.google.com

```
lohith@lohith-IdeaPad-3-15IIL05:~$ sudo traceroute -I www.google.com
traceroute to www.google.com (172.217.163.164), 30 hops max, 60 byte packets
 1  dsldevice.lan (192.168.1.1)  1.126 ms  1.389 ms  2.014 ms
 2  abts-kk-dynamic-1.72.76.171.airtelbroadband.in (171.76.72.1)  4.384 ms  4.729 ms  5.025 ms
 3  125.21.0.185 (125.21.0.185)  4.726 ms  5.022 ms  5.404 ms
 4  182.79.152.115 (182.79.152.115)  14.561 ms  14.558 ms  14.365 ms
 5  116.119.55.236 (116.119.55.236)  15.054 ms  16.398 ms  16.396 ms
 6  116.119.57.193 (116.119.57.193)  14.776 ms  12.545 ms  12.774 ms
 7  72.14.216.192 (72.14.216.192)  13.104 ms  13.260 ms  13.457 ms
 8  216.239.54.67 (216.239.54.67)  12.693 ms  12.689 ms  12.684 ms
 9  74.125.252.91 (74.125.252.91)  13.784 ms  15.856 ms  15.824 ms
10  maa05s05-in-f4.1e100.net (172.217.163.164)  13.939 ms  12.800 ms  14.777 ms
```

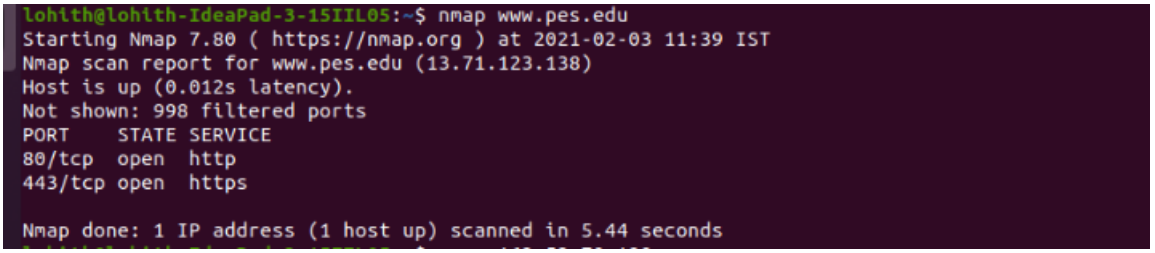
Step 5: By default, traceroute uses icmp (ping) packets. If you'd rather test a TCP connection to gather data more relevant to web server, you can use the -T flag.

sudo traceroute -T www.google.com

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

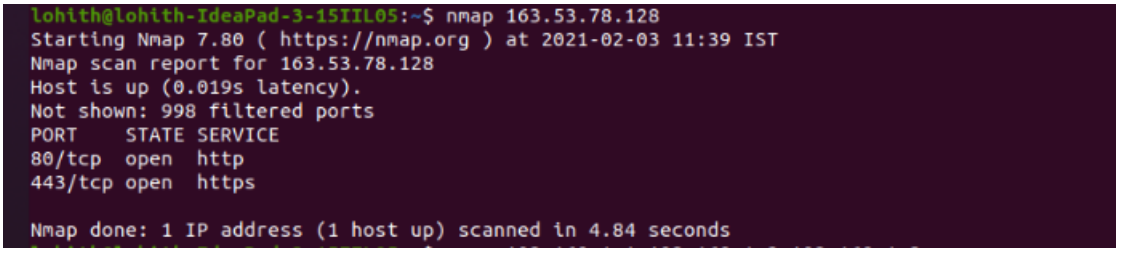
Step 1: You can scan a host using its host name or IP address, for instance.

nmap www.pes.edu



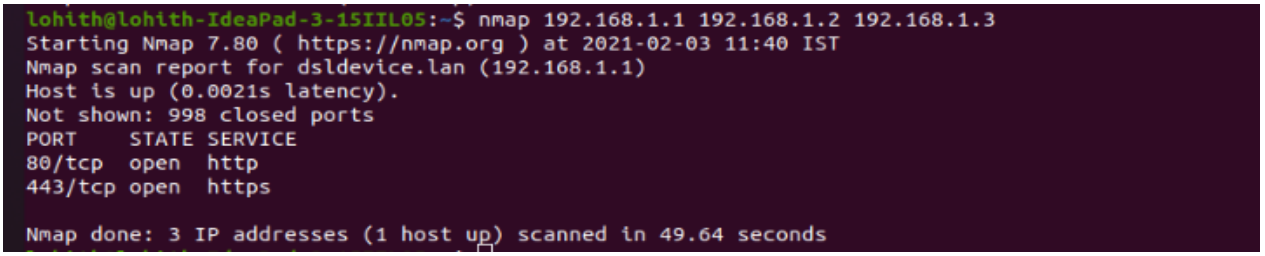
Step 2: Alternatively, use an IP address to scan.

nmap 163.53.78.128



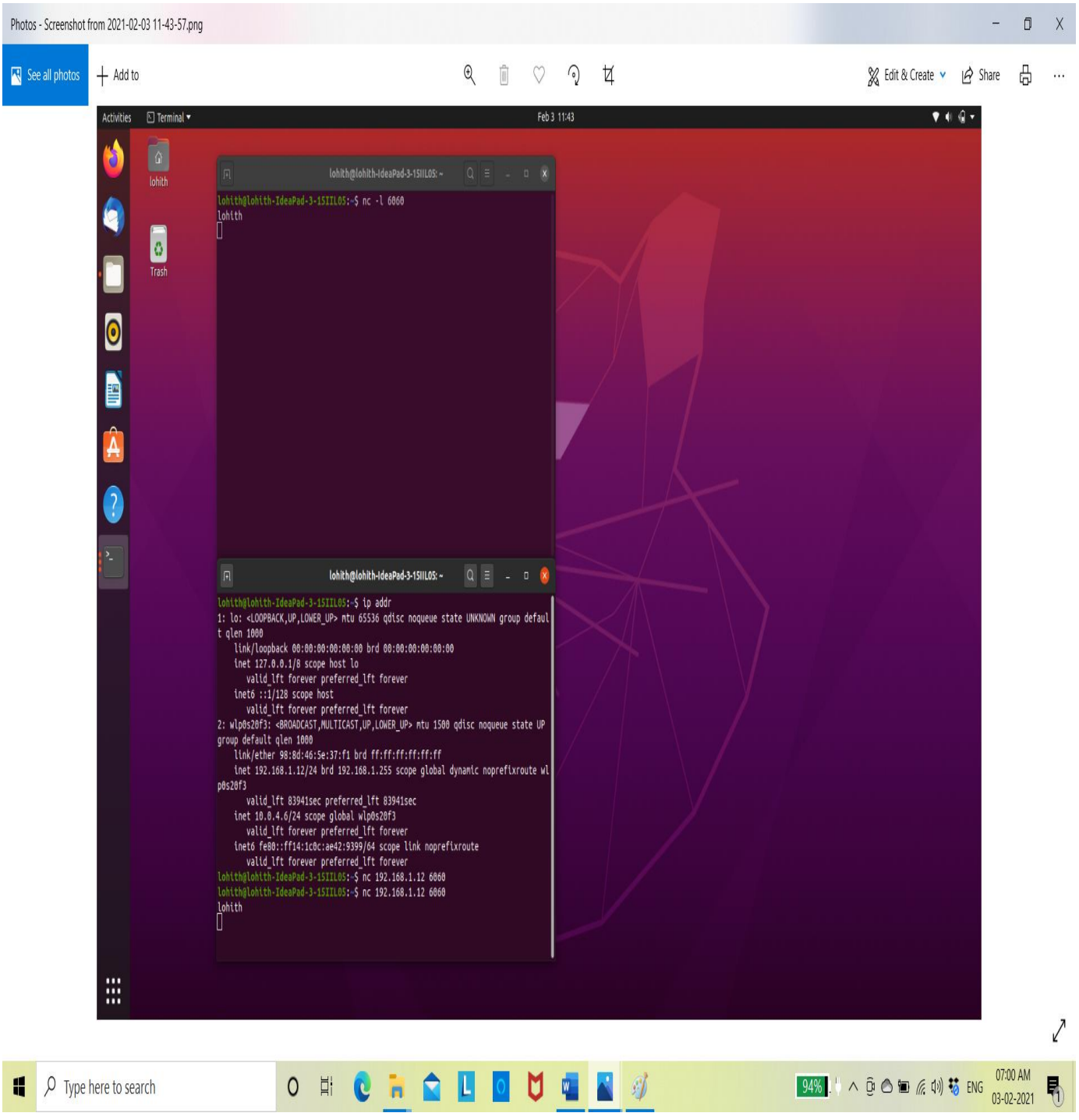
Step 3: Scan multiple IP address or subnet (IPv4)

nmap 192.168.1.1 192.168.1.2 192.168.1.3



Task 7 a): Netcat as Chat tool

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



Questions on above observations:

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

Answer: The browser and the web server both are running on the HTTP version 1.1.

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

Answer:

ping -c 10 www.edmodo.com

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

Answer: To identify remote host apps and OS:

nmap -0 -v {domain_name}