EX.No: 1B **Date : 30/07/2024**

Roll No: 231901004

Linux Networking Command

Aim:

To,study the various Linux Networking commands.

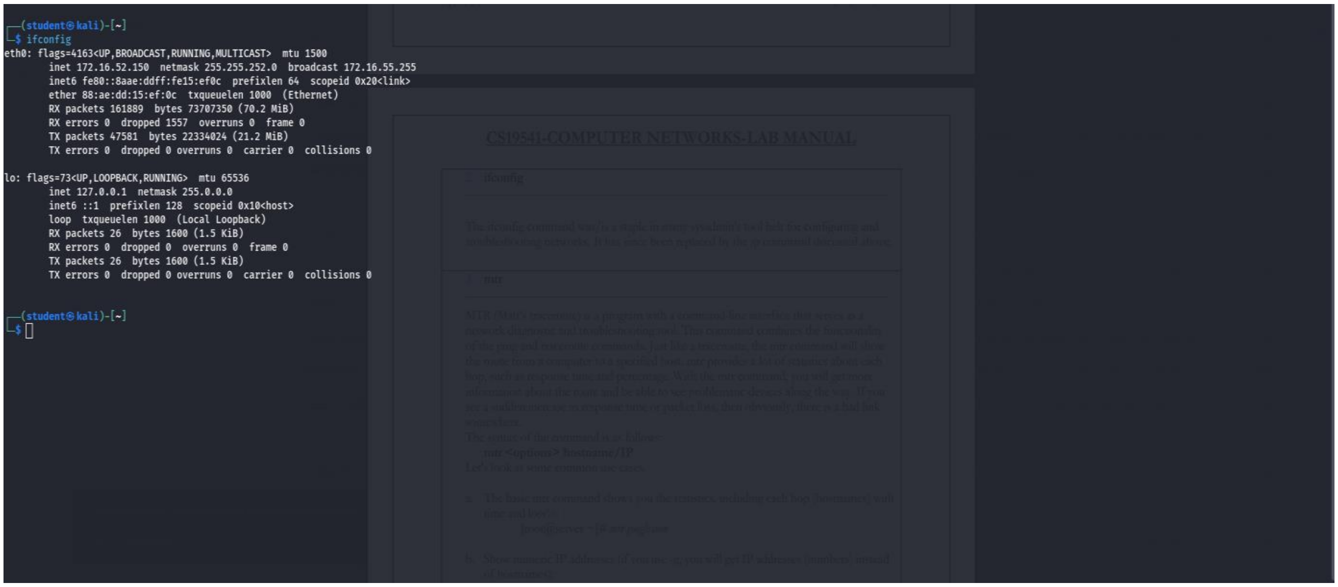
Theory:

Every computer is connected to some other computer through a network whether internally or externally to exchange some information. This network can be small as some computers connected in your home or office, or can be large or complicated as in large University or the entire Internet. Maintaining a system's network is a task of System/Network administrator. Their task includes network configuration and troubleshooting.

Here is a list of Networking and Troubleshooting commands:

Network Commands:

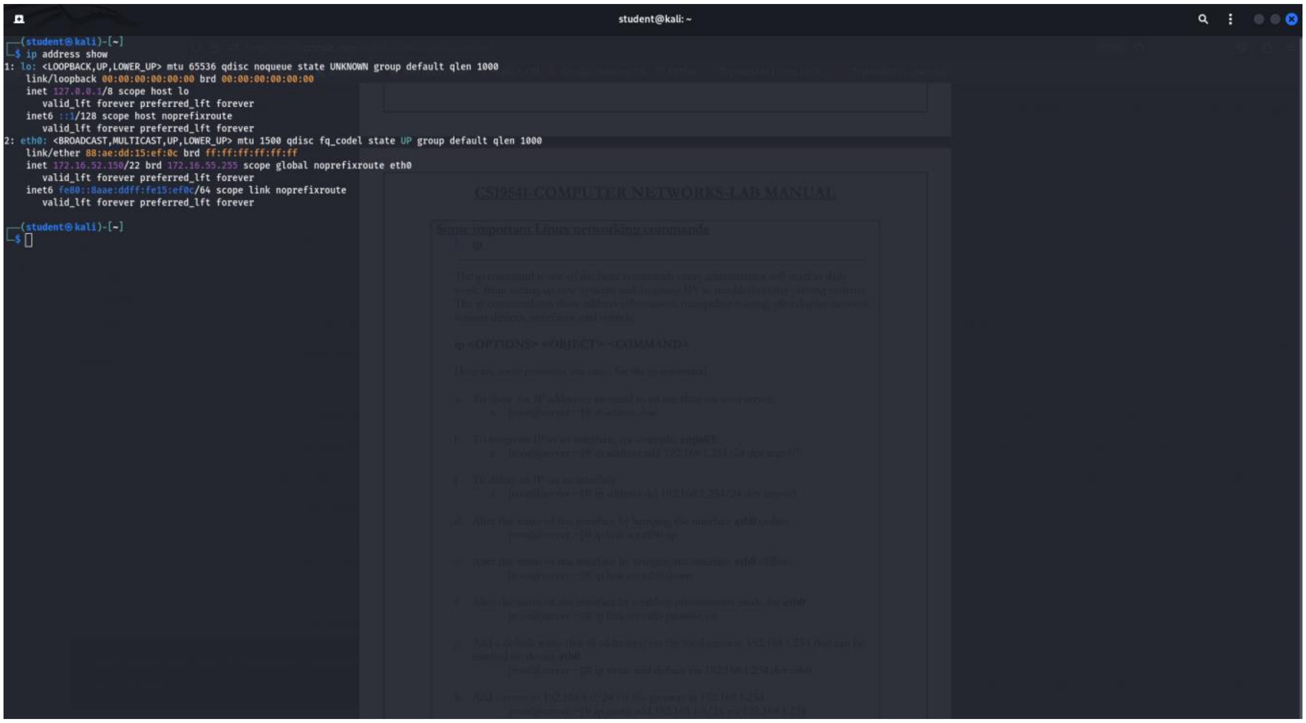
1. **ifconfig:** ifconfig is short for interface configurator. This command is utilized in network inspection, initializing the interface, enabling or disabling an IP address, and configuring an interface with an IP address. Also, it is used to show the network and route interface. **Syntax:** Ifconfig



```
┌──(student㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.52.150  netmask 255.255.252.0  broadcast 172.16.55.255
        inet6 fe80::8aae:ddff:fe15:ef0c  prefixlen 64  scopeid 0x20<link>
        ether 88:ae:dd:15:ef:0c  txqueuelen 1000  (Ethernet)
        RX packets 161889  bytes 73707350 (70.2 MiB)
        RX errors 0  dropped 1557  overruns 0  frame 0
        TX packets 47581  bytes 22334024 (21.2 MiB)
        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 26  bytes 1600 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 1600 (1.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(student㉿kali)-[~]
└─$ ▯
```

2. **ip:** It is the updated and latest edition of ifconfig command. The command provides the information of every network, such as ifconfig. Also, it can be used to get information about a particular interface. **Syntax:**

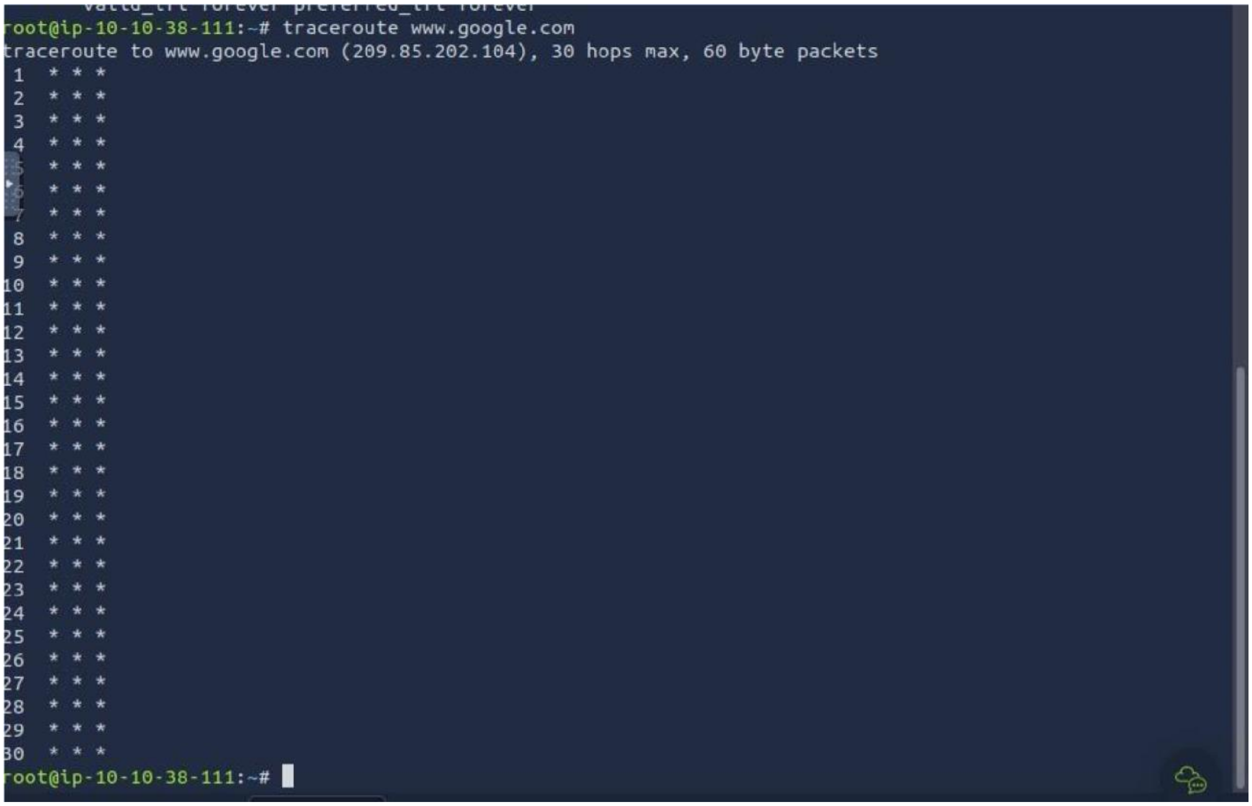
1. ip a
2. ip addr



```
┌──(student㉿kali)-[~]
└─$ ip address 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 88:ae:dd:15:ef:0c brd ff:ff:ff:ff:ff:ff
    inet 172.16.52.150/22 brd 172.16.55.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::8aae:ddff:fe15:ef0c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(student㉿kali)-[~]
└─$ 
```

3. **traceroute:** The traceroute command is one of the most helpful commands in the networking field. It's used to balance the network. It identifies the delay and decides the pathway to our target. Basically, it aids in the below ways:
   - It determines the location of the network latency and informs it.
   - It follows the path to the destination.
   - It gives the names and recognizes all devices on the path.

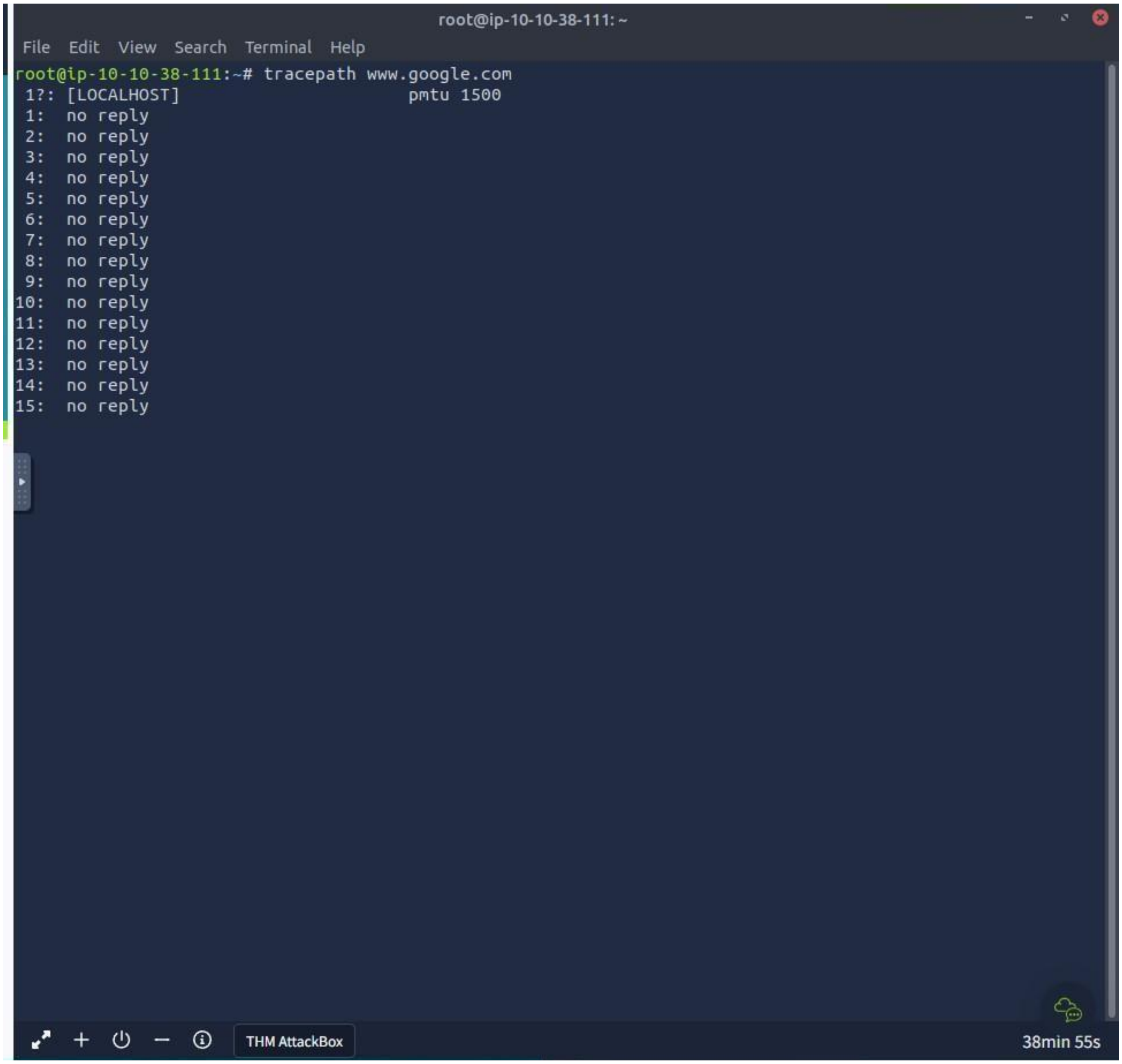
Syntax: traceroute
<destination>



```
    valid_lft forever preferred_lft forever
root@ip-10-10-38-111:~# traceroute www.google.com
traceroute to www.google.com (209.85.202.104), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
root@ip-10-10-38-111:~# 
```

4. **tracepath:** The tracepath command is the same as the traceroute command, and it is used to find network delays. Besides, it does not need root privileges. By default, it comes preinstalled in Ubuntu. It traces the path to the destination and recognizes all hops in it. It identifies the point at which the network is weak if our network is not strong enough.

Syntax: tracepath
<destination>

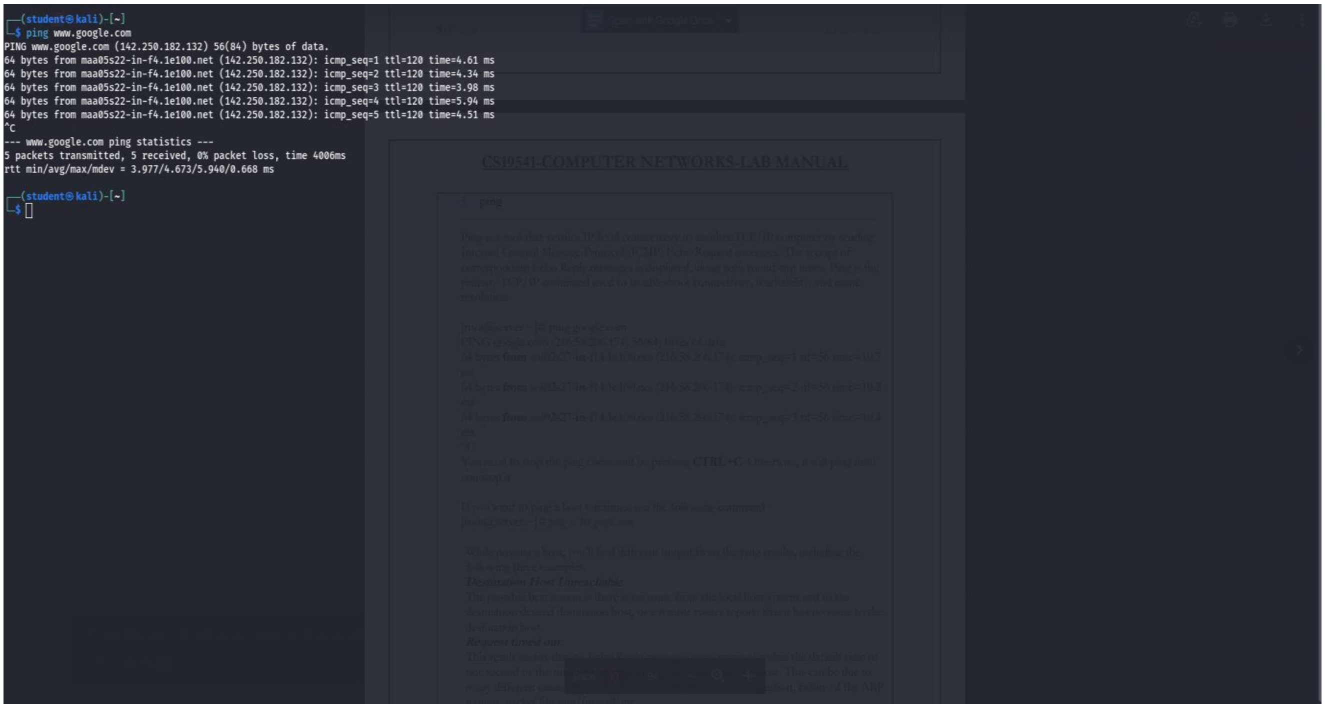


```
root@ip-10-10-38-111:~# tracepath www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  no reply
 2:  no reply
 3:  no reply
 4:  no reply
 5:  no reply
 6:  no reply
 7:  no reply
 8:  no reply
 9:  no reply
10:  no reply
11:  no reply
12:  no reply
13:  no reply
14:  no reply
15:  no reply
```

5. **ping:** It is short for Packet Internet Groper. The ping command is one of the widely used commands for network troubleshooting. Basically, it inspects the network connectivity between two different nodes.

Syntax:

ping **<destination>**

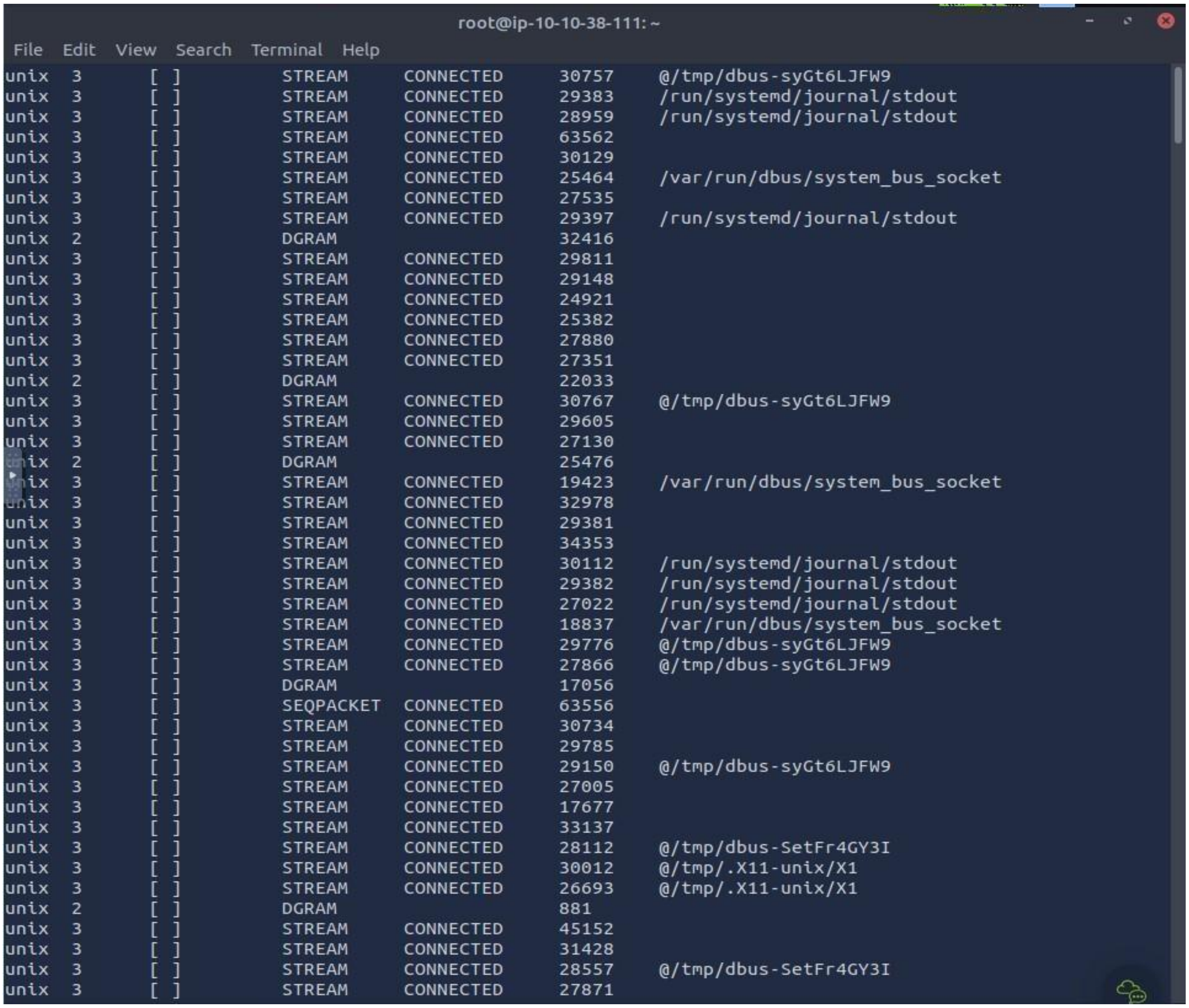


```
┌──(student㉿kali)-[~]
└─$ ping www.google.com
PING www.google.com (142.250.182.132) 56(84) bytes of data.
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=1 ttl=120 time=4.61 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=2 ttl=120 time=4.34 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=3 ttl=120 time=3.98 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=4 ttl=120 time=5.94 ms
64 bytes from maa05s22-in-f4.1e100.net (142.250.182.132): icmp_seq=5 ttl=120 time=4.51 ms
^C
--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 3.977/4.673/5.940/0.668 ms

┌──(student㉿kali)-[~]
└─$ 
```

6.netstat: It is short for network statistics. It gives statistical figures of many interfaces, which contain open sockets, connection information, and routing tables.

Syntax:

Netstat

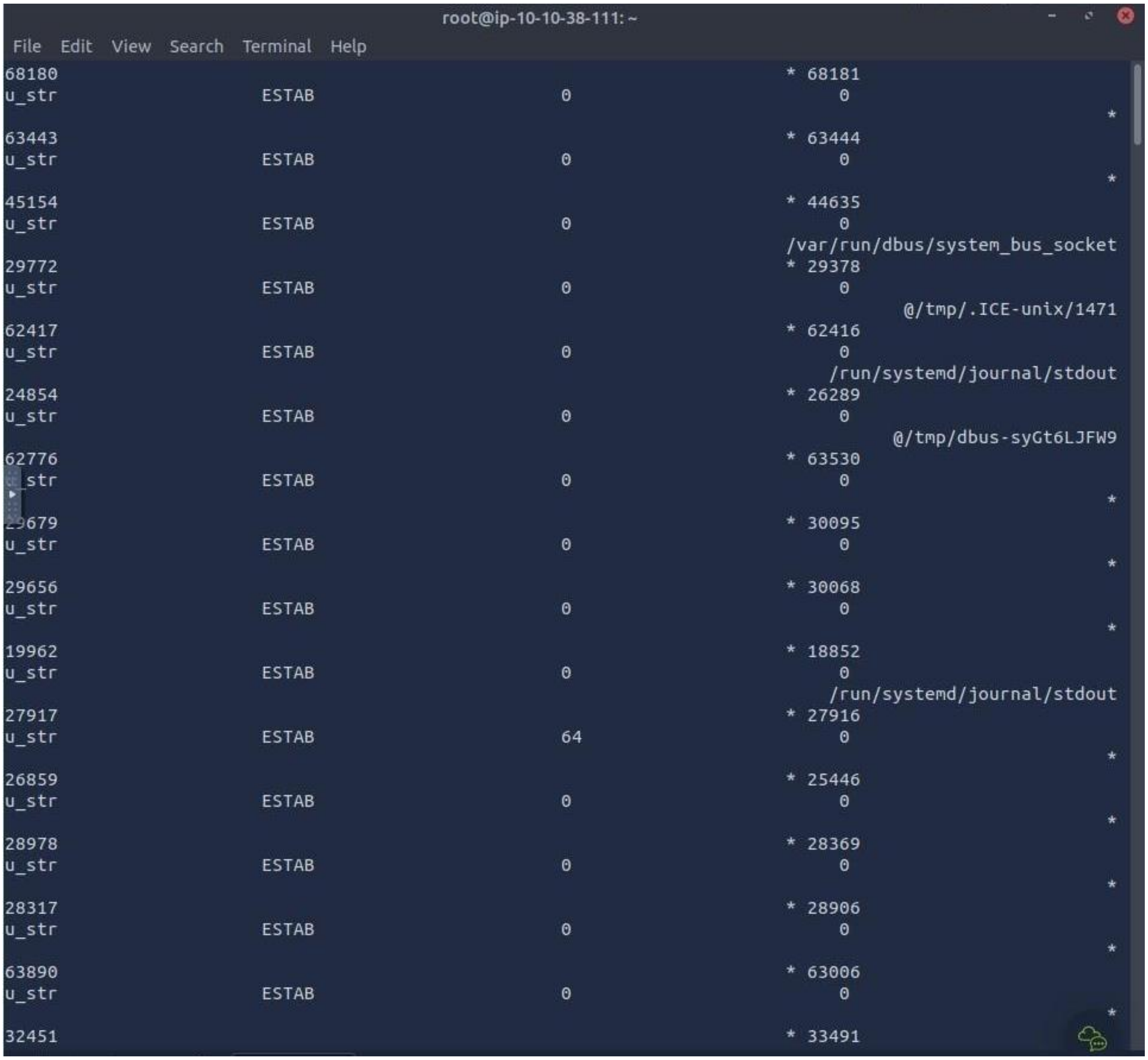


```
unix  3      [ ]         STREAM     CONNECTED     30757    @/tmp/dbus-syGt6LJFW9
unix  3      [ ]         STREAM     CONNECTED     29383    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28959    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     63562
unix  3      [ ]         STREAM     CONNECTED     30129
unix  3      [ ]         STREAM     CONNECTED     25464    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     27535
unix  3      [ ]         STREAM     CONNECTED     29397    /run/systemd/journal/stdout
unix  2      [ ]         DGRAM                    32416
unix  3      [ ]         STREAM     CONNECTED     29811
unix  3      [ ]         STREAM     CONNECTED     29148
unix  3      [ ]         STREAM     CONNECTED     24921
unix  3      [ ]         STREAM     CONNECTED     25382
unix  3      [ ]         STREAM     CONNECTED     27880
unix  3      [ ]         STREAM     CONNECTED     27351
unix  2      [ ]         DGRAM                    22033
unix  3      [ ]         STREAM     CONNECTED     30767    @/tmp/dbus-syGt6LJFW9
unix  3      [ ]         STREAM     CONNECTED     29605
unix  3      [ ]         STREAM     CONNECTED     27130
unix  2      [ ]         DGRAM                    25476
unix  3      [ ]         STREAM     CONNECTED     19423    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     32978
unix  3      [ ]         STREAM     CONNECTED     29381
unix  3      [ ]         STREAM     CONNECTED     34353
unix  3      [ ]         STREAM     CONNECTED     30112    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29382    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27022    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     18837    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     29776    @/tmp/dbus-syGt6LJFW9
unix  3      [ ]         STREAM     CONNECTED     27866    @/tmp/dbus-syGt6LJFW9
unix  3      [ ]         DGRAM                    17056
unix  3      [ ]         SEQPACKET  CONNECTED     63556
unix  3      [ ]         STREAM     CONNECTED     30734
unix  3      [ ]         STREAM     CONNECTED     29785
unix  3      [ ]         STREAM     CONNECTED     29150    @/tmp/dbus-syGt6LJFW9
unix  3      [ ]         STREAM     CONNECTED     27005
unix  3      [ ]         STREAM     CONNECTED     17677
unix  3      [ ]         STREAM     CONNECTED     33137
unix  3      [ ]         STREAM     CONNECTED     28112    @/tmp/dbus-SetFr4GY3I
unix  3      [ ]         STREAM     CONNECTED     30012    @/tmp/.X11-unix/X1
unix  3      [ ]         STREAM     CONNECTED     26693    @/tmp/.X11-unix/X1
unix  2      [ ]         DGRAM                    881
unix  3      [ ]         STREAM     CONNECTED     45152
unix  3      [ ]         STREAM     CONNECTED     31428
unix  3      [ ]         STREAM     CONNECTED     28557    @/tmp/dbus-SetFr4GY3I
unix  3      [ ]         STREAM     CONNECTED     27871
```

7. **ss:** This command is the substitution for the netstat command. The ss command is more informative and much faster than netstat. The ss command's faster response is possible because it fetches every information from inside the kernel userspace.

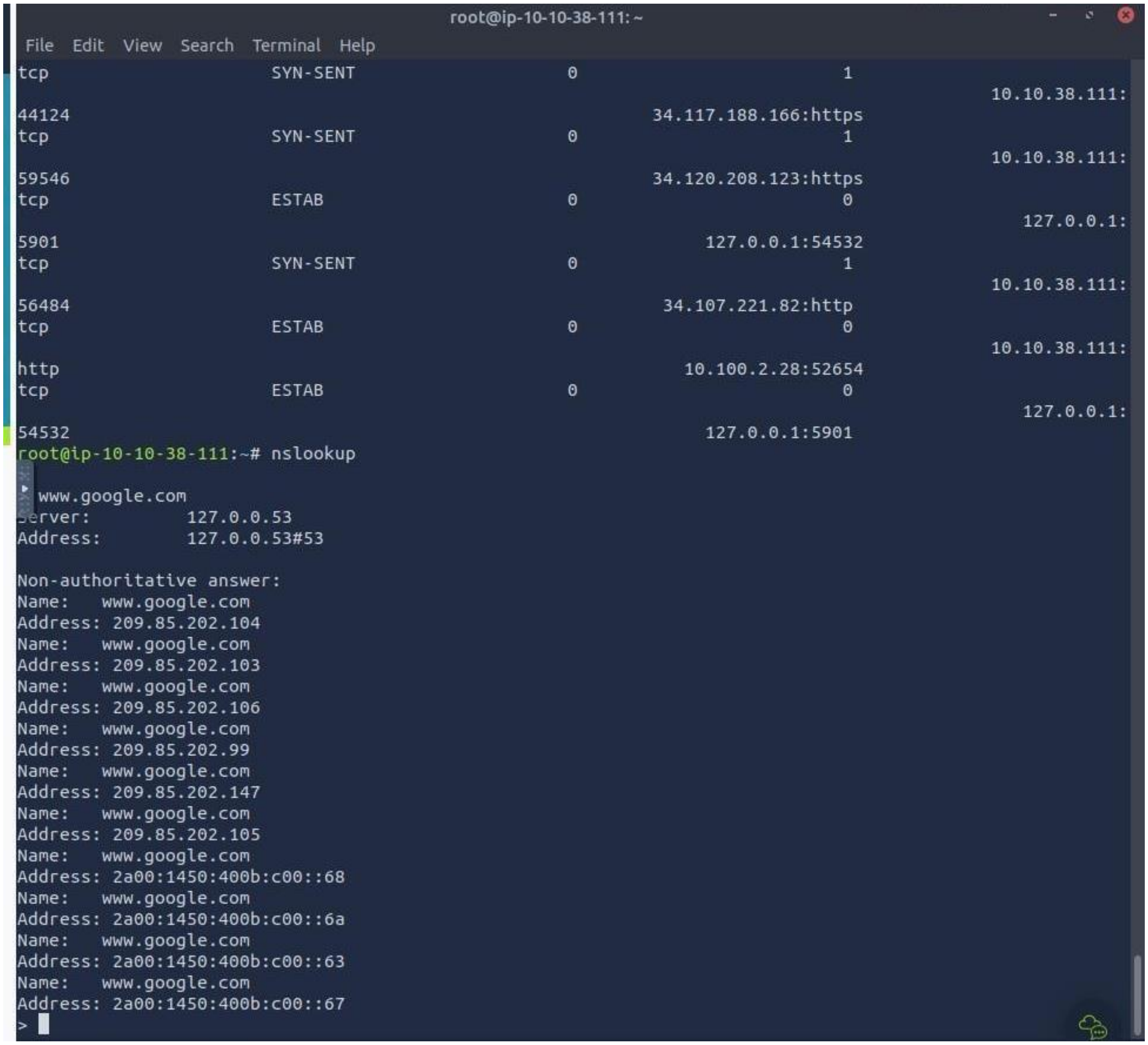
Syntax:

Ss



```
68180                                                                   * 68181
u_str                   ESTAB                       0                        0
                                                                                                      *
63443                                                                   * 63444
u_str                   ESTAB                       0                        0
                                                                                                      *
45154                                                                   * 44635
u_str                   ESTAB                       0                        0
                                                                        /var/run/dbus/system_bus_socket
29772                                                                   * 29378
u_str                   ESTAB                       0                        0
                                                                                   @/tmp/.ICE-unix/1471
62417                                                                   * 62416
u_str                   ESTAB                       0                        0
                                                                            /run/systemd/journal/stdout
24854                                                                   * 26289
u_str                   ESTAB                       0                        0
                                                                                  @/tmp/dbus-syGt6LJFW9
62776                                                                   * 63530
u_str                   ESTAB                       0                        0
                                                                                                      *
29679                                                                   * 30095
u_str                   ESTAB                       0                        0
                                                                                                      *
29656                                                                   * 30068
u_str                   ESTAB                       0                        0
                                                                                                      *
19962                                                                   * 18852
u_str                   ESTAB                       0                        0
                                                                            /run/systemd/journal/stdout
27917                                                                   * 27916
u_str                   ESTAB                       64                       0
                                                                                                      *
26859                                                                   * 25446
u_str                   ESTAB                       0                        0
                                                                                                      *
28978                                                                   * 28369
u_str                   ESTAB                       0                        0
                                                                                                      *
28317                                                                   * 28906
u_str                   ESTAB                       0                        0
                                                                                                      *
63890                                                                   * 63006
u_str                   ESTAB                       0                        0
                                                                                                      *
32451                                                                   * 33491
```

8. **nsloopup:** The nslookup command is an older edition of the dig command. Also, it is utilized for DNS related problems.



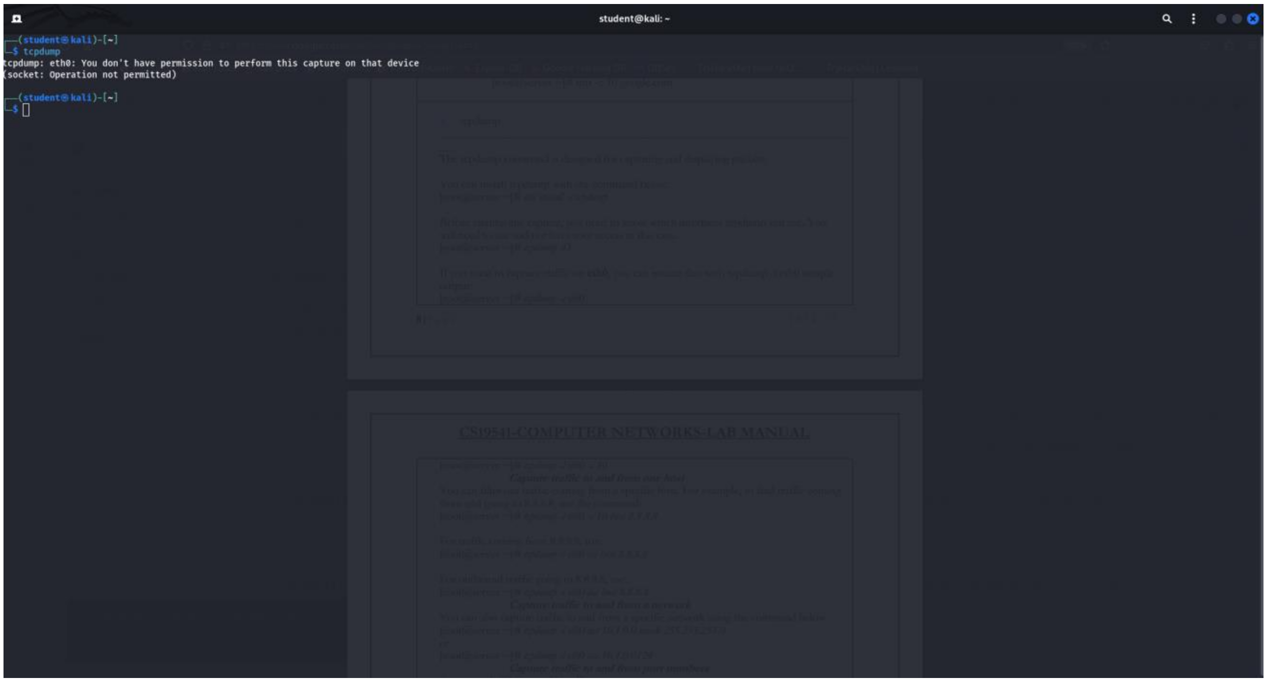
```
tcp                    SYN-SENT                 0                          1
                                                                                      10.10.38.111:
44124                                                          34.117.188.166:https
tcp                    SYN-SENT                 0                          1
                                                                                      10.10.38.111:
59546                                                          34.120.208.123:https
tcp                    ESTAB                    0                          0
                                                                                         127.0.0.1:
5901                                                                127.0.0.1:54532
tcp                    SYN-SENT                 0                          1
                                                                                      10.10.38.111:
56484                                                            34.107.221.82:http
tcp                    ESTAB                    0                          0
                                                                                      10.10.38.111:
http                                                              10.100.2.28:52654
tcp                    ESTAB                    0                          0
                                                                                         127.0.0.1:
54532                                                               127.0.0.1:5901
root@ip-10-10-38-111:~# nslookup
> www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 209.85.202.104
Name:   www.google.com
Address: 209.85.202.103
Name:   www.google.com
Address: 209.85.202.106
Name:   www.google.com
Address: 209.85.202.99
Name:   www.google.com
Address: 209.85.202.147
Name:   www.google.com
Address: 209.85.202.105
Name:   www.google.com
Address: 2a00:1450:400b:c00::68
Name:   www.google.com
Address: 2a00:1450:400b:c00::6a
Name:   www.google.com
Address: 2a00:1450:400b:c00::63
Name:   www.google.com
Address: 2a00:1450:400b:c00::67
> 
```

Syntax:

nslookup **<domainname>**

9.tcpdump

tcpdump -i **<network_device>**



student@kali: ~

```
┌──(student㉿kali)-[~]
└─$ tcpdump
tcpdump: eth0: You don't have permission to perform this capture on that device
(socket: Operation not permitted)

┌──(student㉿kali)-[~]
└─$ 
```

Result:

Thus, the various types of Linux networking commands were studied.