NAME

MOHAMMAD SHAAD

REGISTRATION NUMBER

21BCE1542

CLASS

COMPUTER NETWORKS

FACULTY

PUNITHA K

LAB

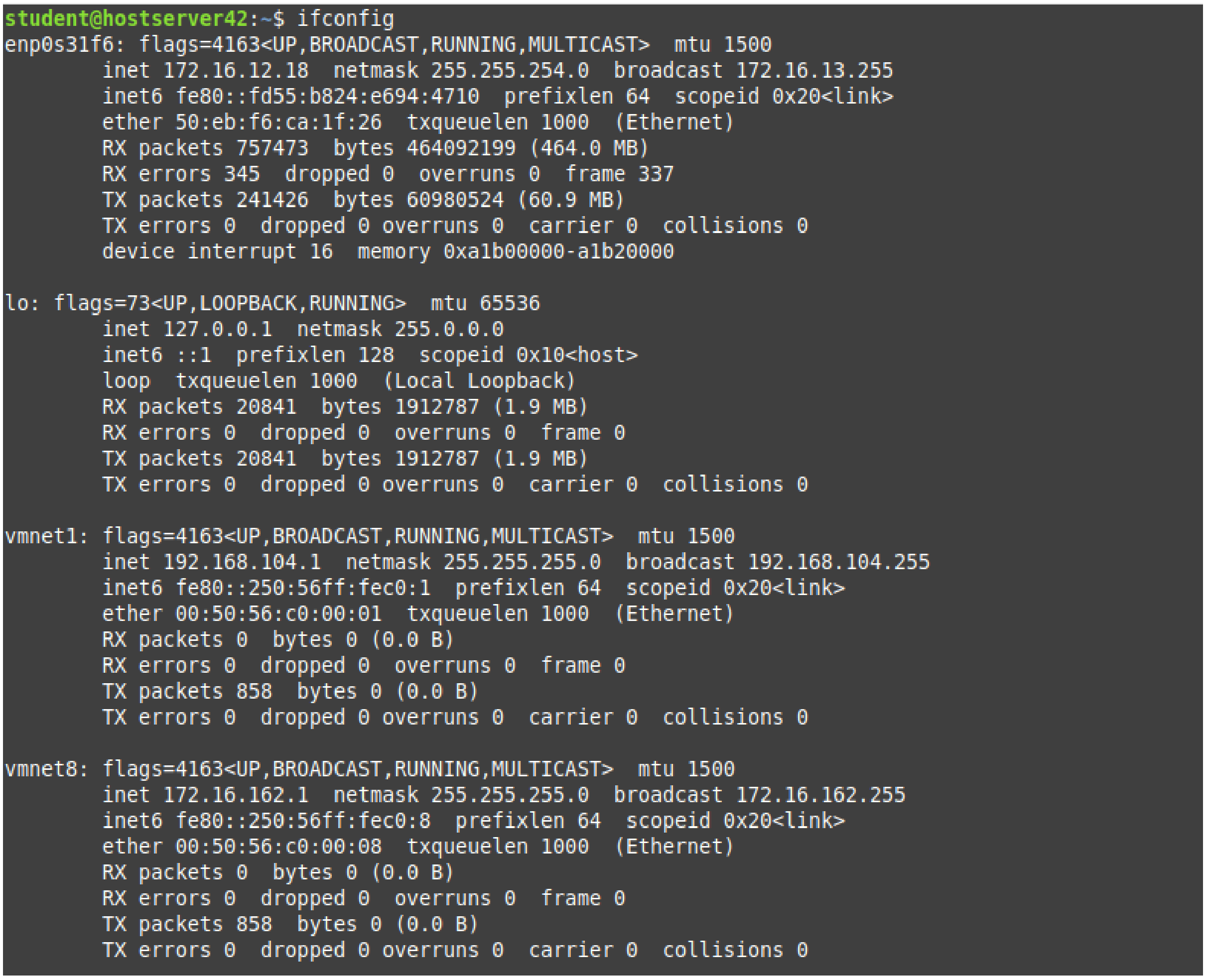
EXERCISE 1

1. Ifconfig

- Linux ifconfig stands for interface configurator. It is one of the most basic commands used in network inspection.
- ifconfig is used to initialize an interface, configure it with an IP address, and enable or disable it. It is also used to display the route and the network interface.
- Basic information displayed upon using ifconfig are:

1. IP address
2. MAC address
3. MTU(Maximum Transmission Unit)

OUTPUT



```
student@hostserver42:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.12.18  netmask 255.255.254.0  broadcast 172.16.13.255
        inet6 fe80::fd55:b824:e694:4710  prefixlen 64  scopeid 0x20<link>
        ether 50:eb:f6:ca:1f:26  txqueuelen 1000  (Ethernet)
        RX packets 757473  bytes 464092199 (464.0 MB)
        RX errors 345  dropped 0  overruns 0  frame 337
        TX packets 241426  bytes 60980524 (60.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 16  memory 0xa1b00000-a1b20000

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 20841  bytes 1912787 (1.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20841  bytes 1912787 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.104.1  netmask 255.255.255.0  broadcast 192.168.104.255
        inet6 fe80::250:56ff:fec0:1  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:01  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 858  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vmnet8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.162.1  netmask 255.255.255.0  broadcast 172.16.162.255
        inet6 fe80::250:56ff:fec0:8  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:c0:00:08  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 858  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2.ip

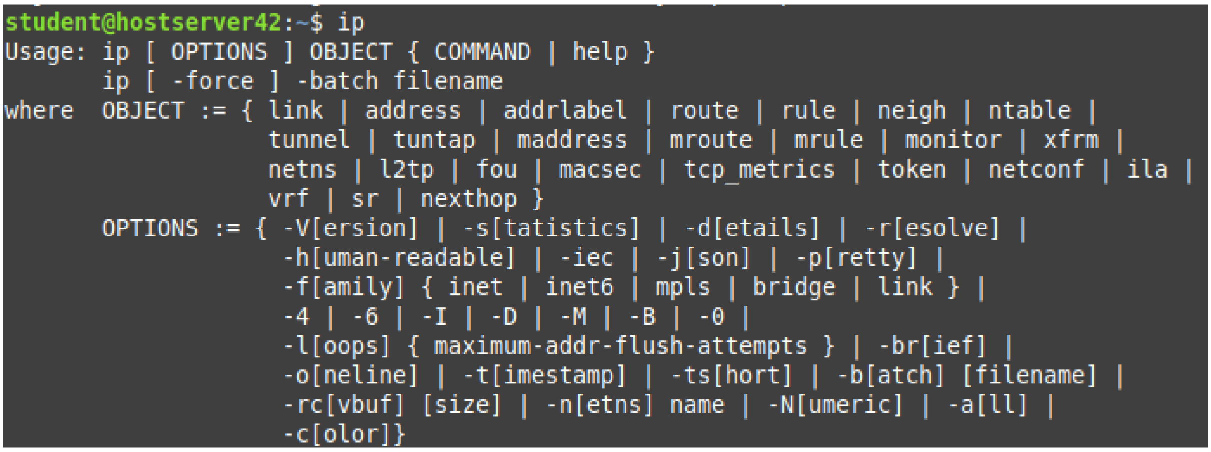
This is the latest and updated version of ifconfig command.

- Syntax:

1. ip a
2. ip addr

- This command gives the details of all networks like ifconfig.
- This command can also be used to get the details of a specific interface.

OUTPUT

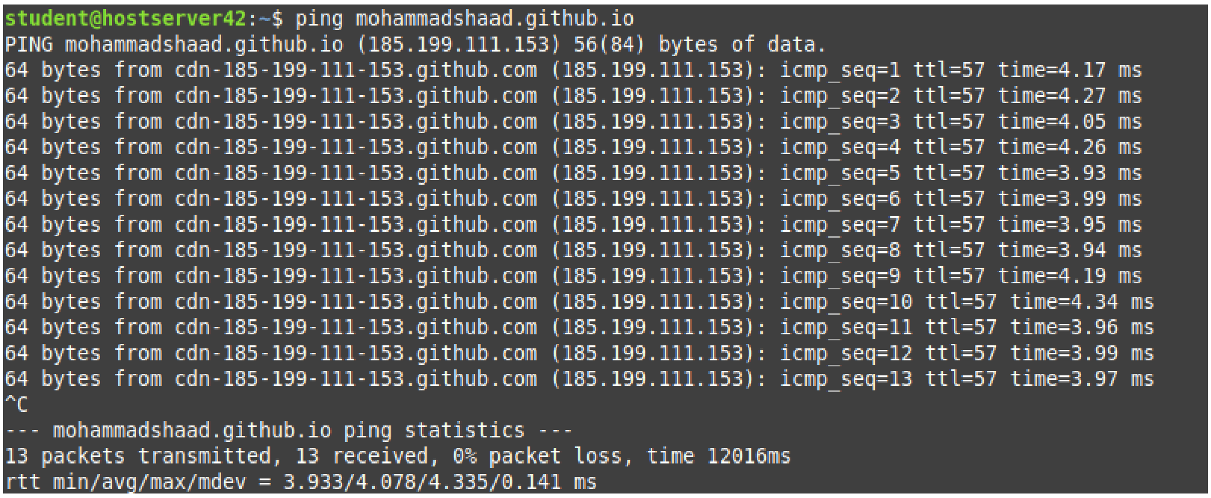


```
student@hostserver42:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                   tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm |
                   netns | l2tp | fou | macsec | tcp_metrics | token | netconf | ila |
                   vrf | sr | nexthop }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                    -h[uman-readable] | -iec | -j[son] | -p[retty] |
                    -f[amily] { inet | inet6 | mpls | bridge | link } |
                    -4 | -6 | -I | -D | -M | -B | -0 |
                    -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                    -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename] |
                    -rc[vbuf] [size] | -n[etns] name | -N[umeric] | -a[ll] |
                    -c[olor]}
```

3.ping mohammadshaad.github.io

- Linux ping is one of the most used network troubleshooting commands. It basically checks for the network connectivity between two nodes.
- ping stands for Packet INternet Groper.
- The ping command sends the ICMP echo request to check the network connectivity.
- It keeps executing until it is interrupted.
- Use Ctrl+C Key to interrupt the execution.

OUTPUT



```
student@hostserver42:~$ ping mohammadshaad.github.io
PING mohammadshaad.github.io (185.199.111.153) 56(84) bytes of data.
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=1 ttl=57 time=4.17 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=2 ttl=57 time=4.27 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=3 ttl=57 time=4.05 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=4 ttl=57 time=4.26 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=5 ttl=57 time=3.93 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=6 ttl=57 time=3.99 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=7 ttl=57 time=3.95 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=8 ttl=57 time=3.94 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=9 ttl=57 time=4.19 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=10 ttl=57 time=4.34 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=11 ttl=57 time=3.96 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=12 ttl=57 time=3.99 ms
64 bytes from cdn-185-199-111-153.github.com (185.199.111.153): icmp_seq=13 ttl=57 time=3.97 ms
^C
--- mohammadshaad.github.io ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12016ms
rtt min/avg/max/mdev = 3.933/4.078/4.335/0.141 ms
```

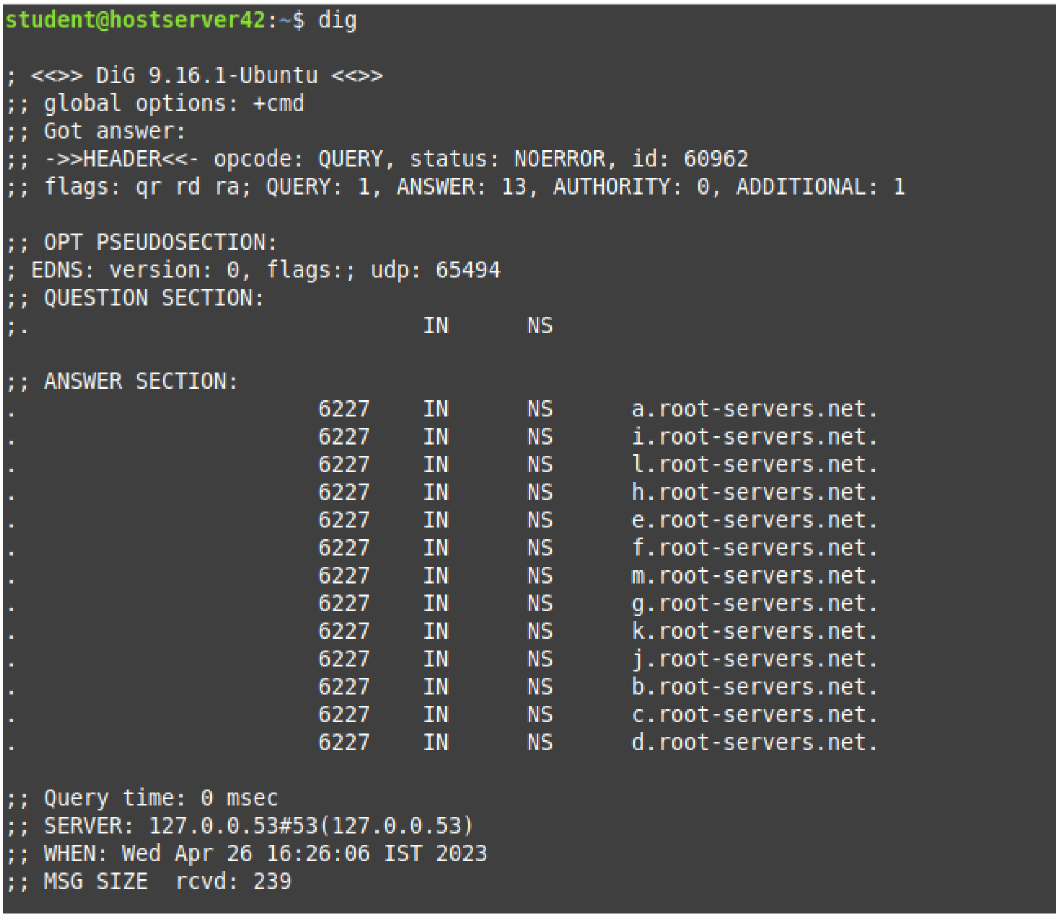
4. dig

Linux dig command stands for Domain Information Groper. This command is used in DNS lookup to query the DNS name server. It is also used to troubleshoot DNS related issues.

It is mainly used to verify DNS mappings, MX Records, host addresses, and all other DNS records for a better understanding of the DNS topography.

This command is an improvised version of nslookup command.

OUTPUT



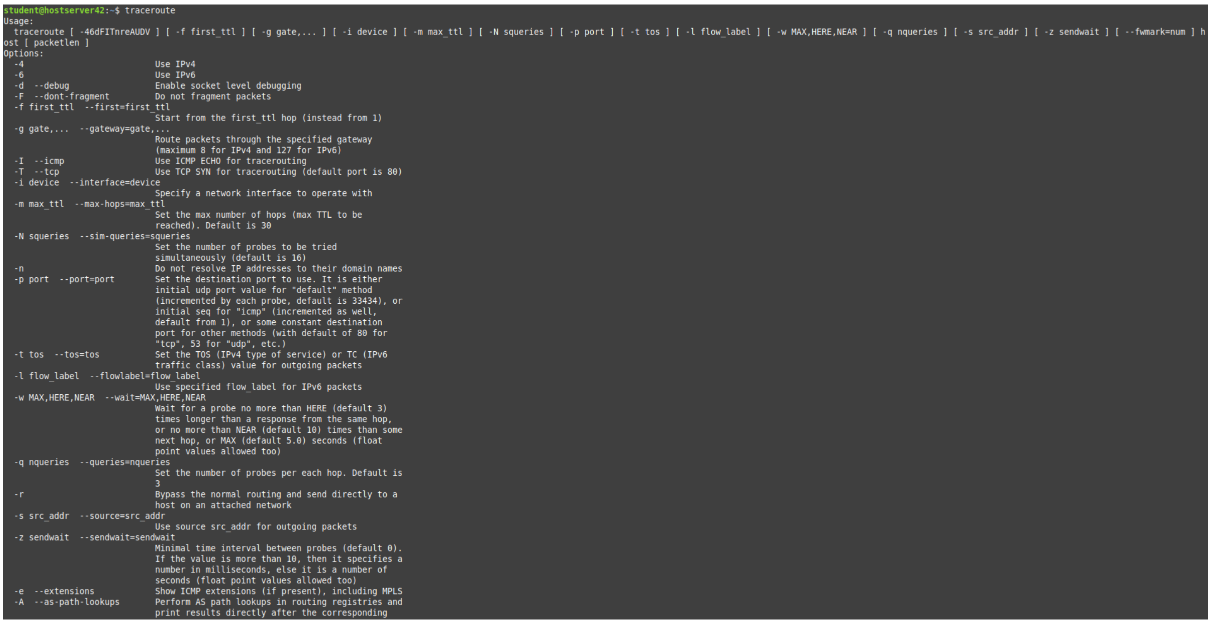
```
student@hostserver42:~$ dig

; <<>> DiG 9.16.1-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60962
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       6227    IN      NS      a.root-servers.net.
.                       6227    IN      NS      i.root-servers.net.
.                       6227    IN      NS      l.root-servers.net.
.                       6227    IN      NS      h.root-servers.net.
.                       6227    IN      NS      e.root-servers.net.
.                       6227    IN      NS      f.root-servers.net.
.                       6227    IN      NS      m.root-servers.net.
.                       6227    IN      NS      g.root-servers.net.
.                       6227    IN      NS      k.root-servers.net.
.                       6227    IN      NS      j.root-servers.net.
.                       6227    IN      NS      b.root-servers.net.
.                       6227    IN      NS      c.root-servers.net.
.                       6227    IN      NS      d.root-servers.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Wed Apr 26 16:26:06 IST 2023
;; MSG SIZE  rcvd: 239
```

5. traceroute

Linux traceroute is one of the most useful commands in networking. It is used to troubleshoot the network. It detects the delay and determines the pathway to your target. It basically helps in the following ways:

1. It provides the names and identifies every device on the path.
2. It follows the route to the destination
3. It determines where the network latency comes from and reports it.

OUTPUT



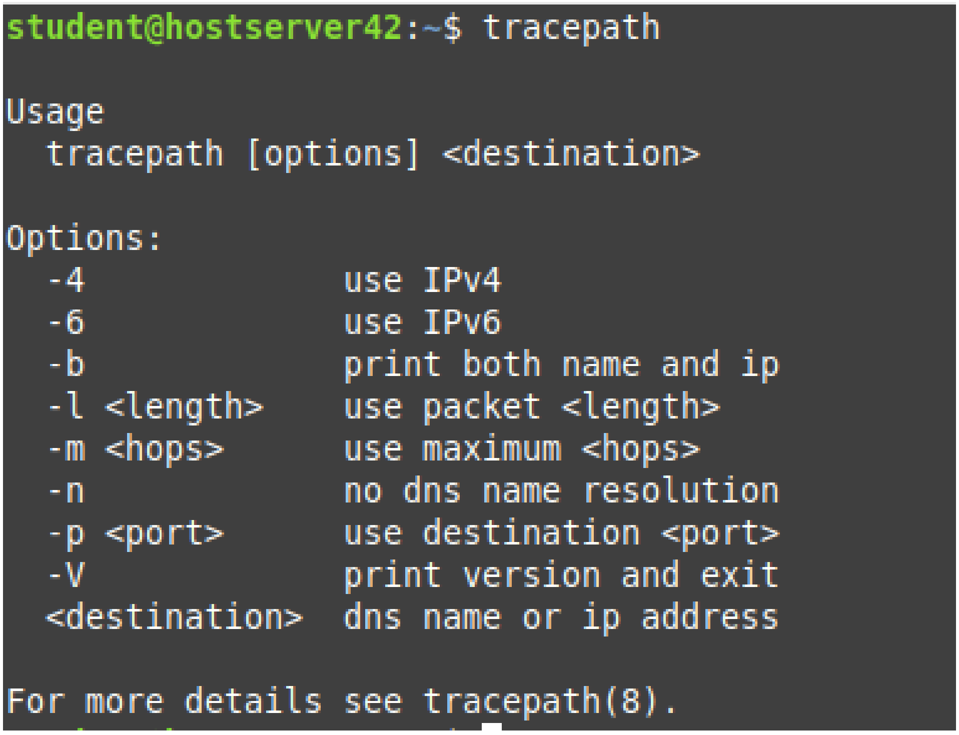
```
student@hostserver42:~$ traceroute
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w MAX,HERE,NEAR ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [ --fwmark=num ] h
ost [ packetlen ]
Options:
  -4                          Use IPv4
  -6                          Use IPv6
  -d  --debug                 Enable socket level debugging
  -F  --dont-fragment         Do not fragment packets
  -f first_ttl  --first=first_ttl
                              Start from the first_ttl hop (instead from 1)
  -g gate,...  --gateway=gate,...
                              Route packets through the specified gateway
                              (maximum 8 for IPv4 and 127 for IPv6)
  -I  --icmp                  Use ICMP ECHO for tracerouting
  -T  --tcp                   Use TCP SYN for tracerouting (default port is 80)
  -i device  --interface=device
                              Specify a network interface to operate with
  -m max_ttl  --max-hops=max_ttl
                              Set the max number of hops (max TTL to be
                              reached). Default is 30
  -N squeries  --sim-queries=squeries
                              Set the number of probes to be tried
                              simultaneously (default is 16)
  -n                          Do not resolve IP addresses to their domain names
  -p port  --port=port        Set the destination port to use. It is either
                              initial udp port value for "default" method
                              (incremented by each probe, default is 33434), or
                              initial seq for "icmp" (incremented as well,
                              default from 1), or some constant destination
                              port for other methods (with default of 80 for
                              "tcp", 53 for "udp", etc.)
  -t tos  --tos=tos           Set the TOS (IPv4 type of service) or TC (IPv6
                              traffic class) value for outgoing packets
  -l flow_label  --flowlabel=flow_label
                              Use specified flow_label for IPv6 packets
  -w MAX,HERE,NEAR  --wait=MAX,HERE,NEAR
                              Wait for a probe no more than HERE (default 3)
                              times longer than a response from the same hop,
                              or no more than NEAR (default 10) times than some
                              next hop, or MAX (default 5.0) seconds (float
                              point values allowed too)
  -q nqueries  --queries=nqueries
                              Set the number of probes per each hop. Default is
                              3
  -r                          Bypass the normal routing and send directly to a
                              host on an attached network
  -s src_addr  --source=src_addr
                              Use source src_addr for outgoing packets
  -z sendwait  --sendwait=sendwait
                              Minimal time interval between probes (default 0).
                              If the value is more than 10, then it specifies a
                              number in milliseconds, else it is a number of
                              seconds (float point values allowed too)
  -e  --extensions            Show ICMP extensions (if present), including MPLS
  -A  --as-path-lookups       Perform AS path lookups in routing registries and
                              print results directly after the corresponding
```

6. tracepath

Linux tracepath is similar to traceroute command. It is used to detect network delays. However, it doesn't require root privileges.

1. It is installed in Ubuntu by default.
2. It traces the route to the specified destination and identifies each hop in it. If your network is weak, it recognizes the point where the network is weak.

OUTPUT



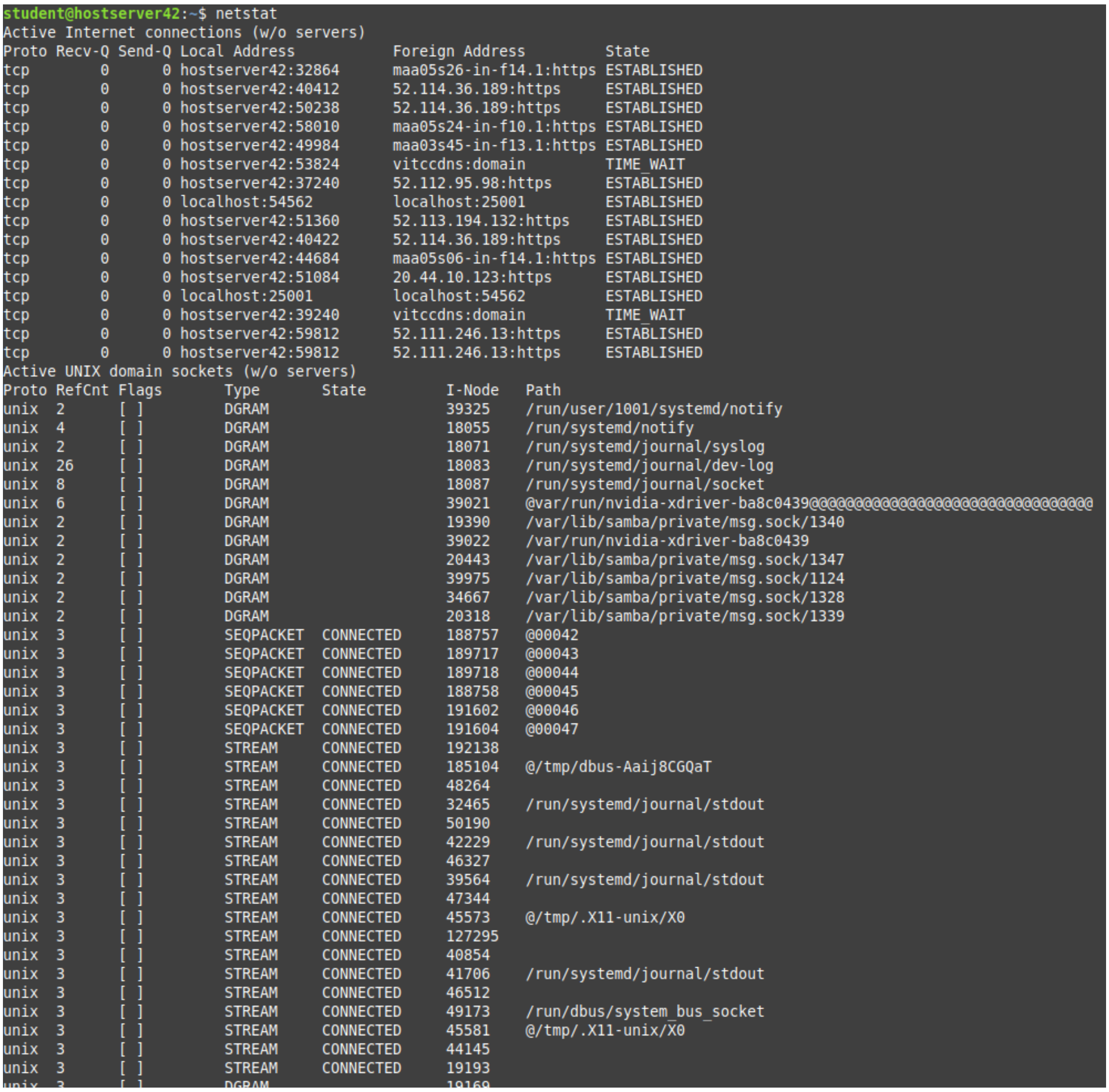
```
student@hostserver42:~$ tracepath

Usage
  tracepath [options] <destination>

Options:
  -4               use IPv4
  -6               use IPv6
  -b               print both name and ip
  -l <length>      use packet <length>
  -m <hops>        use maximum <hops>
  -n               no dns name resolution
  -p <port>        use destination <port>
  -V               print version and exit
  <destination>    dns name or ip address

For more details see tracepath(8).
```

7. netstat

Linux netstat command refers to the network statistics.

It provides statistical figures about different interfaces which include open sockets, routing tables, and connection information.

OUTPUT



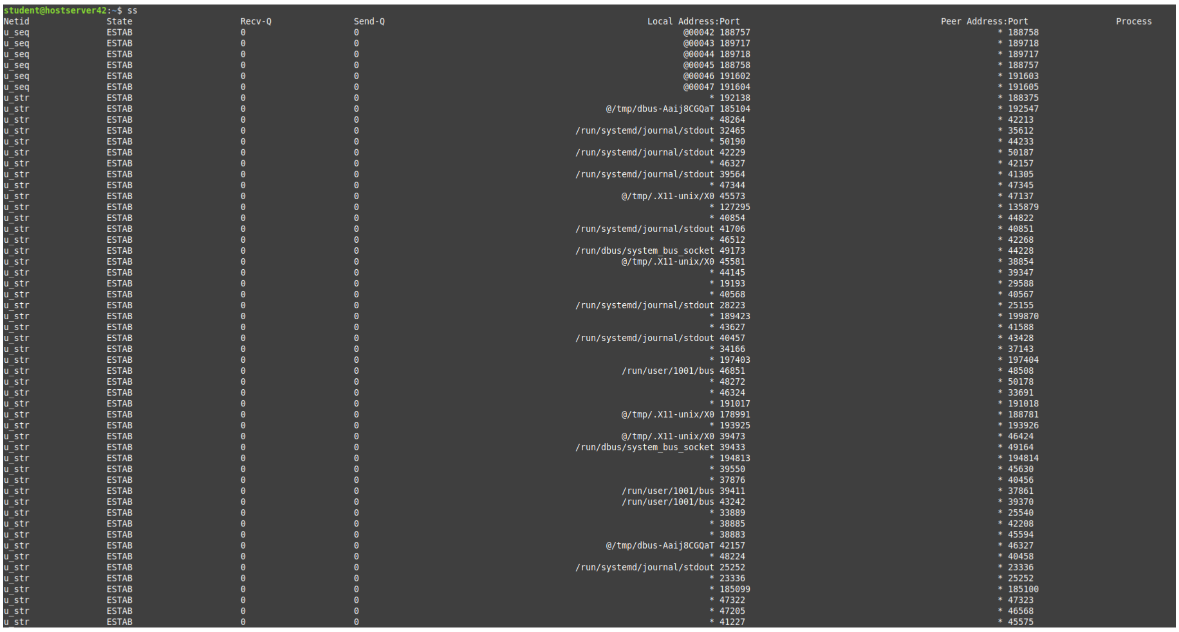
```
student@hostserver42:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 hostserver42:32864      maa05s26-in-f14.1:https ESTABLISHED
tcp        0      0 hostserver42:40412      52.114.36.189:https     ESTABLISHED
tcp        0      0 hostserver42:50238      52.114.36.189:https     ESTABLISHED
tcp        0      0 hostserver42:58010      maa05s24-in-f10.1:https ESTABLISHED
tcp        0      0 hostserver42:49984      maa03s45-in-f13.1:https ESTABLISHED
tcp        0      0 hostserver42:53824      vitccdns:domain         TIME_WAIT
tcp        0      0 hostserver42:37240      52.112.95.98:https      ESTABLISHED
tcp        0      0 localhost:54562         localhost:25001         ESTABLISHED
tcp        0      0 hostserver42:51360      52.113.194.132:https    ESTABLISHED
tcp        0      0 hostserver42:40422      52.114.36.189:https     ESTABLISHED
tcp        0      0 hostserver42:44684      maa05s06-in-f14.1:https ESTABLISHED
tcp        0      0 hostserver42:51084      20.44.10.123:https      ESTABLISHED
tcp        0      0 localhost:25001         localhost:54562         ESTABLISHED
tcp        0      0 hostserver42:39240      vitccdns:domain         TIME_WAIT
tcp        0      0 hostserver42:59812      52.111.246.13:https     ESTABLISHED
tcp        0      0 hostserver42:59812      52.111.246.13:https     ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    39325    /run/user/1001/systemd/notify
unix  4      [ ]         DGRAM                    18055    /run/systemd/notify
unix  2      [ ]         DGRAM                    18071    /run/systemd/journal/syslog
unix  26     [ ]         DGRAM                    18083    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    18087    /run/systemd/journal/socket
unix  6      [ ]         DGRAM                    39021    @var/run/nvidia-xdriver-ba8c0439@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
unix  2      [ ]         DGRAM                    19390    /var/lib/samba/private/msg.sock/1340
unix  2      [ ]         DGRAM                    39022    /var/run/nvidia-xdriver-ba8c0439
unix  2      [ ]         DGRAM                    20443    /var/lib/samba/private/msg.sock/1347
unix  2      [ ]         DGRAM                    39975    /var/lib/samba/private/msg.sock/1124
unix  2      [ ]         DGRAM                    34667    /var/lib/samba/private/msg.sock/1328
unix  2      [ ]         DGRAM                    20318    /var/lib/samba/private/msg.sock/1339
unix  3      [ ]         SEQPACKET  CONNECTED     188757   @00042
unix  3      [ ]         SEQPACKET  CONNECTED     189717   @00043
unix  3      [ ]         SEQPACKET  CONNECTED     189718   @00044
unix  3      [ ]         SEQPACKET  CONNECTED     188758   @00045
unix  3      [ ]         SEQPACKET  CONNECTED     191602   @00046
unix  3      [ ]         SEQPACKET  CONNECTED     191604   @00047
unix  3      [ ]         STREAM     CONNECTED     192138
unix  3      [ ]         STREAM     CONNECTED     185104   @/tmp/dbus-Aaij8CGQaT
unix  3      [ ]         STREAM     CONNECTED     48264
unix  3      [ ]         STREAM     CONNECTED     32465    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     50190
unix  3      [ ]         STREAM     CONNECTED     42229    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     46327
unix  3      [ ]         STREAM     CONNECTED     39564    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     47344
unix  3      [ ]         STREAM     CONNECTED     45573    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     127295
unix  3      [ ]         STREAM     CONNECTED     40854
unix  3      [ ]         STREAM     CONNECTED     41706    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     46512
unix  3      [ ]         STREAM     CONNECTED     49173    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     45581    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     44145
unix  3      [ ]         STREAM     CONNECTED     19193
unix  3      [ ]         DGRAM                    19169
```

8. SS

Linux ss command is the replacement for netstat command. It is regarded as a much faster and more informative command than netstat.

The faster response of ss is possible as it fetches all the information from within the kernel userspace.

OUTPUT:

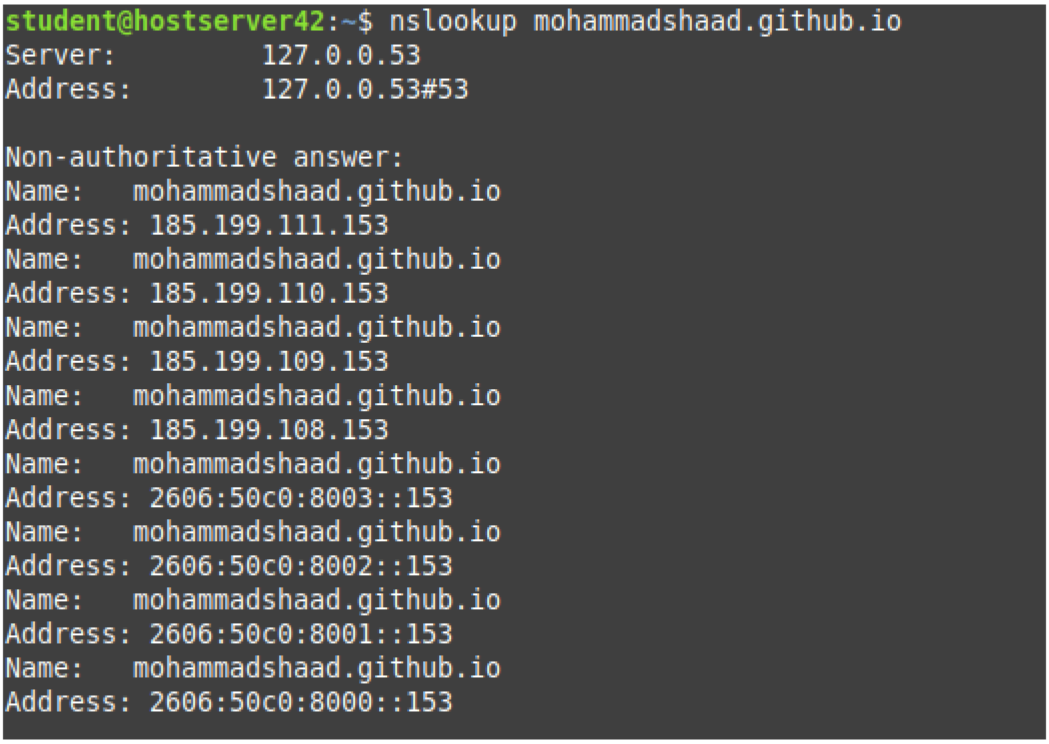


```
student@hostserver42:~$ ss
Netid  State  Recv-Q Send-Q                Local Address:Port     Peer Address:Port Process
u_seq  ESTAB  0      0                           @00042 188757    * 188758
u_seq  ESTAB  0      0                           @00043 189717    * 189718
u_seq  ESTAB  0      0                           @00044 189718    * 189717
u_seq  ESTAB  0      0                           @00045 188758    * 188757
u_seq  ESTAB  0      0                           @00046 191602    * 191603
u_seq  ESTAB  0      0                           @00047 191604    * 191605
u_str  ESTAB  0      0                                * 192138    * 188375
u_str  ESTAB  0      0            @/tmp/dbus-Aaij8CGQaT 185104    * 192547
u_str  ESTAB  0      0                                * 48264     * 42213
u_str  ESTAB  0      0      /run/systemd/journal/stdout 32465     * 35612
u_str  ESTAB  0      0                                * 50190     * 44233
u_str  ESTAB  0      0      /run/systemd/journal/stdout 42229     * 50187
u_str  ESTAB  0      0                                * 46327     * 42157
u_str  ESTAB  0      0      /run/systemd/journal/stdout 39564     * 41305
u_str  ESTAB  0      0                                * 47344     * 47345
u_str  ESTAB  0      0               @/tmp/.X11-unix/X0 45573     * 47137
u_str  ESTAB  0      0                                * 127295    * 135879
u_str  ESTAB  0      0                                * 40854     * 44822
u_str  ESTAB  0      0      /run/systemd/journal/stdout 41706     * 40851
u_str  ESTAB  0      0                                * 46512     * 42268
u_str  ESTAB  0      0      /run/dbus/system_bus_socket 49173     * 44228
u_str  ESTAB  0      0               @/tmp/.X11-unix/X0 45581     * 38854
u_str  ESTAB  0      0                                * 44145     * 39347
u_str  ESTAB  0      0                                * 19193     * 29588
u_str  ESTAB  0      0                                * 40568     * 40567
u_str  ESTAB  0      0      /run/systemd/journal/stdout 28223     * 25155
u_str  ESTAB  0      0                                * 189423    * 199870
u_str  ESTAB  0      0                                * 43627     * 41588
u_str  ESTAB  0      0      /run/systemd/journal/stdout 40457     * 43428
u_str  ESTAB  0      0                                * 34166     * 37143
u_str  ESTAB  0      0                                * 197403    * 197404
u_str  ESTAB  0      0               /run/user/1001/bus 46851     * 48508
u_str  ESTAB  0      0                                * 48272     * 50178
u_str  ESTAB  0      0                                * 46324     * 33691
u_str  ESTAB  0      0                                * 191017    * 191018
u_str  ESTAB  0      0               @/tmp/.X11-unix/X0 178991    * 188781
u_str  ESTAB  0      0                                * 193925    * 193926
u_str  ESTAB  0      0               @/tmp/.X11-unix/X0 39473     * 46424
u_str  ESTAB  0      0      /run/dbus/system_bus_socket 39433     * 49164
u_str  ESTAB  0      0                                * 194813    * 194814
u_str  ESTAB  0      0                                * 39550     * 45630
u_str  ESTAB  0      0                                * 37876     * 40456
u_str  ESTAB  0      0               /run/user/1001/bus 39411     * 37861
u_str  ESTAB  0      0               /run/user/1001/bus 43242     * 39370
u_str  ESTAB  0      0                                * 33889     * 25540
u_str  ESTAB  0      0                                * 38885     * 42208
u_str  ESTAB  0      0                                * 38883     * 45594
u_str  ESTAB  0      0            @/tmp/dbus-Aaij8CGQaT 42157     * 46327
u_str  ESTAB  0      0                                * 48224     * 40458
u_str  ESTAB  0      0      /run/systemd/journal/stdout 25252     * 23336
u_str  ESTAB  0      0                                * 23336     * 25252
u_str  ESTAB  0      0                                * 185099    * 185100
u_str  ESTAB  0      0                                * 47322     * 47323
u_str  ESTAB  0      0                                * 47205     * 46568
u_str  ESTAB  0      0                                * 41227     * 45575
```

9. nslookup

Linux nslookup is also a command used for DNS related queries. It is the older version of dig.

OUTPUT



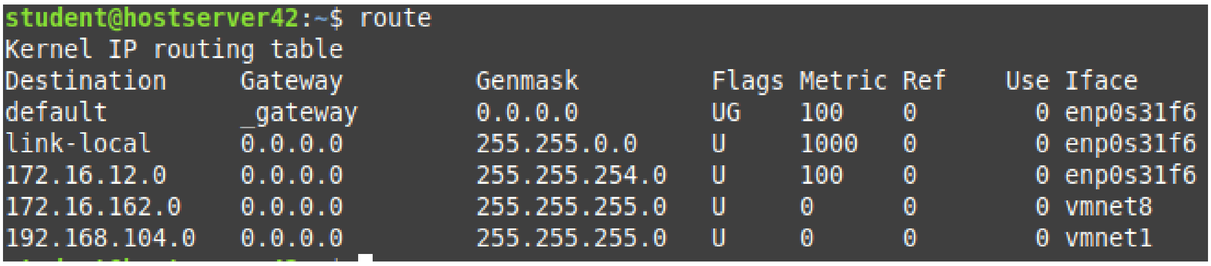
```
student@hostserver42:~$ nslookup mohammadshaad.github.io
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mohammadshaad.github.io
Address: 185.199.111.153
Name:   mohammadshaad.github.io
Address: 185.199.110.153
Name:   mohammadshaad.github.io
Address: 185.199.109.153
Name:   mohammadshaad.github.io
Address: 185.199.108.153
Name:   mohammadshaad.github.io
Address: 2606:50c0:8003::153
Name:   mohammadshaad.github.io
Address: 2606:50c0:8002::153
Name:   mohammadshaad.github.io
Address: 2606:50c0:8001::153
Name:   mohammadshaad.github.io
Address: 2606:50c0:8000::153
```

10. route

Linux route command displays and manipulates the routing table existing for your system.

A router is basically used to find the best way to send the packets across to a destination.

OUTPUT

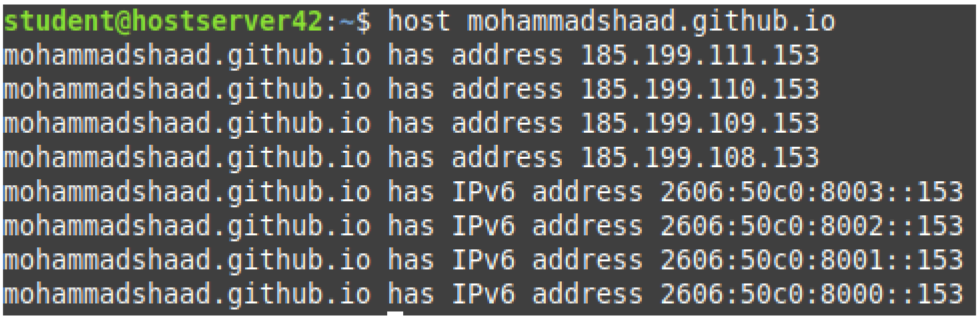


```
student@hostserver42:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s31f6
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s31f6
172.16.12.0     0.0.0.0         255.255.254.0   U     100    0        0 enp0s31f6
172.16.162.0    0.0.0.0         255.255.255.0   U     0      0        0 vmnet8
192.168.104.0   0.0.0.0         255.255.255.0   U     0      0        0 vmnet1
```

11. host mohammadshaad.github.io

Linux host command displays the domain name for a given IP address and IP address for a given hostname. It is also used to fetch DNS lookup for DNS related query.

OUTPUT

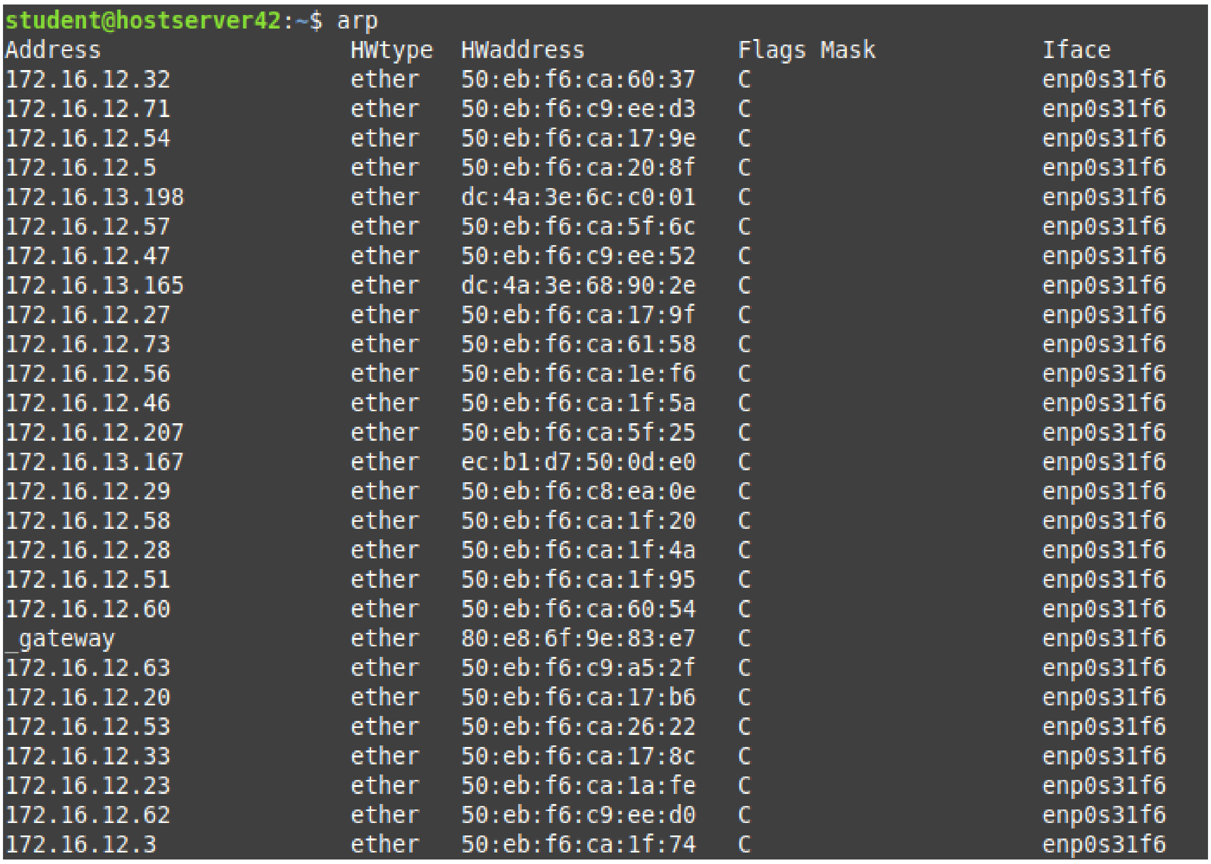


```
student@hostserver42:~$ host mohammadshaad.github.io
mohammadshaad.github.io has address 185.199.111.153
mohammadshaad.github.io has address 185.199.110.153
mohammadshaad.github.io has address 185.199.109.153
mohammadshaad.github.io has address 185.199.108.153
mohammadshaad.github.io has IPv6 address 2606:50c0:8003::153
mohammadshaad.github.io has IPv6 address 2606:50c0:8002::153
mohammadshaad.github.io has IPv6 address 2606:50c0:8001::153
mohammadshaad.github.io has IPv6 address 2606:50c0:8000::153
```

12. arp

Linux arp command stands for Address Resolution Protocol. It is used to view and add content to the kernel's ARP table.

OUTPUT

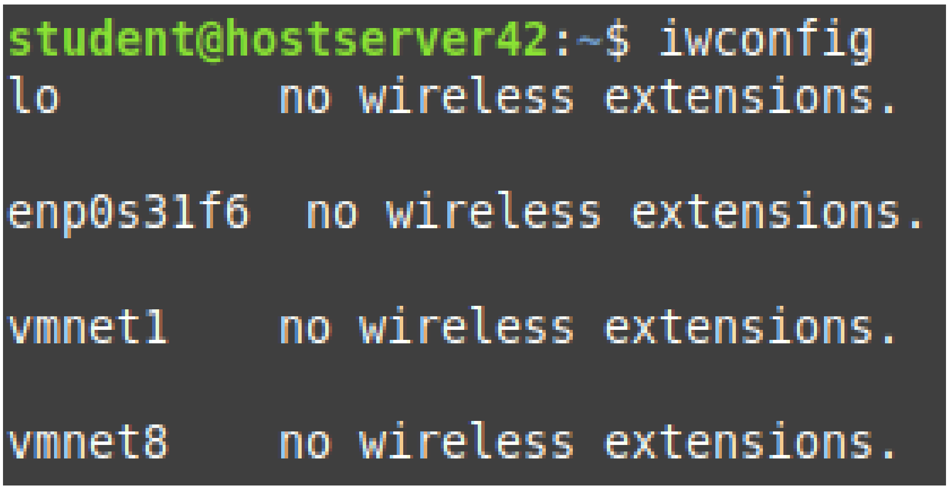


```
student@hostserver42:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
172.16.12.32             ether   50:eb:f6:ca:60:37   C                     enp0s31f6
172.16.12.71             ether   50:eb:f6:c9:ee:d3   C                     enp0s31f6
172.16.12.54             ether   50:eb:f6:ca:17:9e   C                     enp0s31f6
172.16.12.5              ether   50:eb:f6:ca:20:8f   C                     enp0s31f6
172.16.13.198            ether   dc:4a:3e:6c:c0:01   C                     enp0s31f6
172.16.12.57             ether   50:eb:f6:ca:5f:6c   C                     enp0s31f6
172.16.12.47             ether   50:eb:f6:c9:ee:52   C                     enp0s31f6
172.16.13.165            ether   dc:4a:3e:68:90:2e   C                     enp0s31f6
172.16.12.27             ether   50:eb:f6:ca:17:9f   C                     enp0s31f6
172.16.12.73             ether   50:eb:f6:ca:61:58   C                     enp0s31f6
172.16.12.56             ether   50:eb:f6:ca:1e:f6   C                     enp0s31f6
172.16.12.46             ether   50:eb:f6:ca:1f:5a   C                     enp0s31f6
172.16.12.207            ether   50:eb:f6:ca:5f:25   C                     enp0s31f6
172.16.13.167            ether   ec:b1:d7:50:0d:e0   C                     enp0s31f6
172.16.12.29             ether   50:eb:f6:c8:ea:0e   C                     enp0s31f6
172.16.12.58             ether   50:eb:f6:ca:1f:20   C                     enp0s31f6
172.16.12.28             ether   50:eb:f6:ca:1f:4a   C                     enp0s31f6
172.16.12.51             ether   50:eb:f6:ca:1f:95   C                     enp0s31f6
172.16.12.60             ether   50:eb:f6:ca:60:54   C                     enp0s31f6
_gateway                 ether   80:e8:6f:9e:83:e7   C                     enp0s31f6
172.16.12.63             ether   50:eb:f6:c9:a5:2f   C                     enp0s31f6
172.16.12.20             ether   50:eb:f6:ca:17:b6   C                     enp0s31f6
172.16.12.53             ether   50:eb:f6:ca:26:22   C                     enp0s31f6
172.16.12.33             ether   50:eb:f6:ca:17:8c   C                     enp0s31f6
172.16.12.23             ether   50:eb:f6:ca:1a:fe   C                     enp0s31f6
172.16.12.62             ether   50:eb:f6:c9:ee:d0   C                     enp0s31f6
172.16.12.3              ether   50:eb:f6:ca:1f:74   C                     enp0s31f6
```

13. iwconfig

Linux iwconfig is used to configure the wireless network interface. It is used to set and view the basic WI-FI details like SSID and encryption. To know more about this command, refer to the man page.

OUTPUT

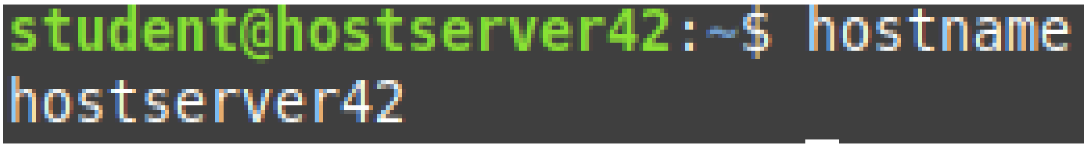


```
student@hostserver42:~$ iwconfig
lo          no wireless extensions.

enp0s31f6  no wireless extensions.

vmnet1     no wireless extensions.

vmnet8     no wireless extensions.
```

14. hostname

Linux hostname is the simple command used to view and set the hostname of a system.

OUTPUT



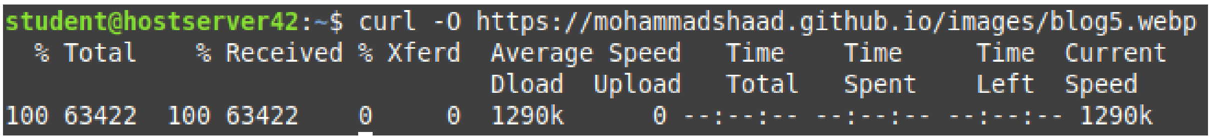
```
student@hostserver42:~$ hostname
hostserver42
```

15. curl

Linux curl and wget commands are used in downloading files from the internet through CLI. The curl command has to be used with the option "O" to fetch the file, while the wget command is used directly.

Below are the syntax and the example for the two commands.

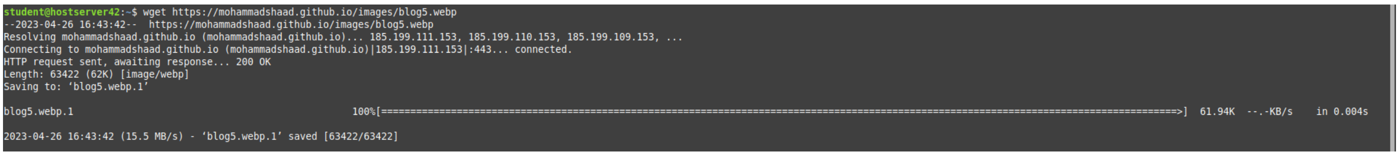
OUTPUT



```
student@hostserver42:~$ curl -O https://mohammadshaad.github.io/images/blog5.webp
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 63422  100 63422    0     0  1290k      0 --:--:-- --:--:-- --:--:-- 1290k
```

16. wget

OUTPUT

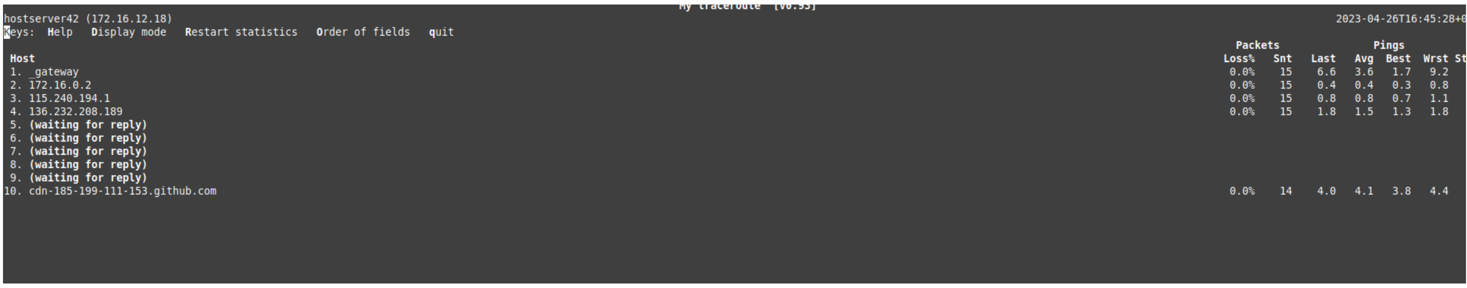


```
student@hostserver42:~$ wget https://mohammadshaad.github.io/images/blog5.webp
--2023-04-26 16:43:42--  https://mohammadshaad.github.io/images/blog5.webp
Resolving mohammadshaad.github.io (mohammadshaad.github.io)... 185.199.111.153, 185.199.110.153, 185.199.109.153, ...
Connecting to mohammadshaad.github.io (mohammadshaad.github.io)|185.199.111.153|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 63422 (62K) [image/webp]
Saving to: ‘blog5.webp.1’

blog5.webp.1                                    100%[=========================================================================================================================================>]  61.94K  --.-KB/s    in 0.004s

2023-04-26 16:43:42 (15.5 MB/s) - ‘blog5.webp.1’ saved [63422/63422]
```

17. mtr mohammadshaad.github.io

Linux mtr command is a combination of ping and the traceroute command. It continuously displays information regarding the packets sent with the ping time of each hop. It is also used to view the network issues.

OUTPUT

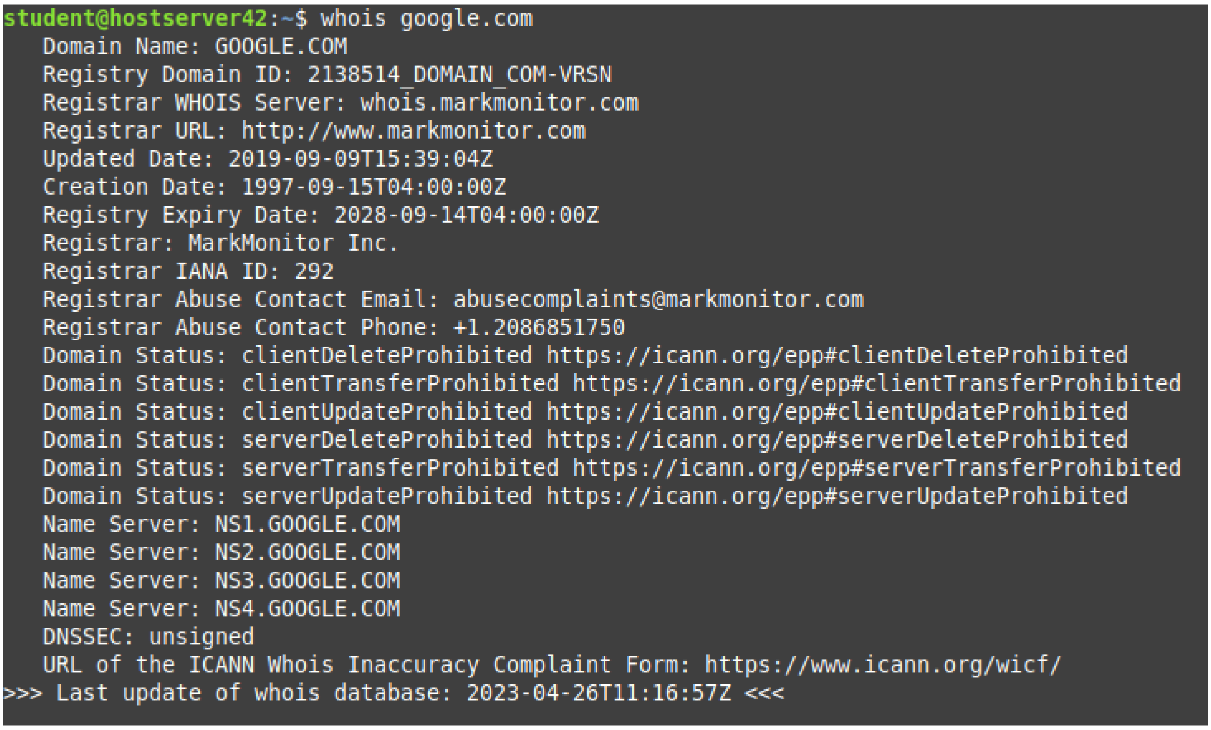


```
                                         My traceroute  [v0.95]
hostserver42 (172.16.12.18)                                                 2023-04-26T16:45:28+0
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                                 Packets               Pings
 Host                                                           Loss%   Snt   Last   Avg  Best  Wrst St
 1. _gateway                                                     0.0%    15    6.6   3.6   1.7   9.2
 2. 172.16.0.2                                                   0.0%    15    0.4   0.4   0.3   0.8
 3. 115.240.194.1                                                0.0%    15    0.8   0.8   0.7   1.1
 4. 136.232.208.189                                              0.0%    15    1.8   1.5   1.3   1.8
 5. (waiting for reply)
 6. (waiting for reply)
 7. (waiting for reply)
 8. (waiting for reply)
 9. (waiting for reply)
10. cdn-185-199-111-153.github.com                               0.0%    14    4.0   4.1   3.8   4.4
```

18. whois google.com

Linux whois command is used to fetch all the information related to a website. You can get all the information about a website including the registration and the owner information.

OUTPUT

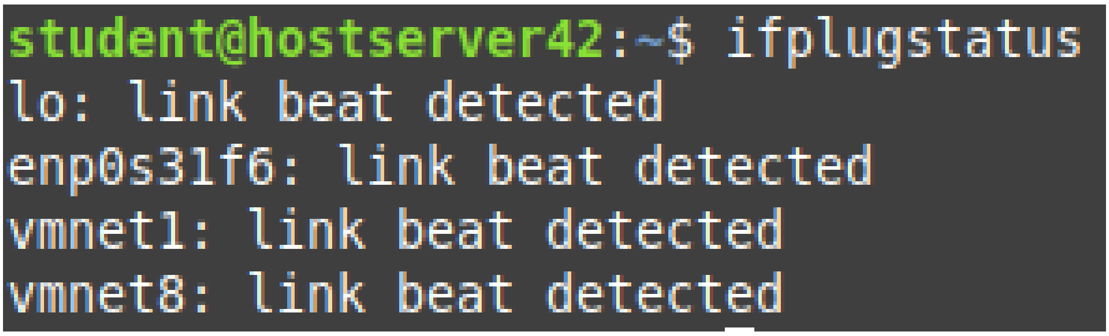


```
student@hostserver42:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-04-26T11:16:57Z <<<
```

19. ifplugstatus

Linux ifplugstatus command is used to check if a cable is plugged into the network interface. This command is not directly available on Ubuntu. You can install this using the command below:

OUTPUT



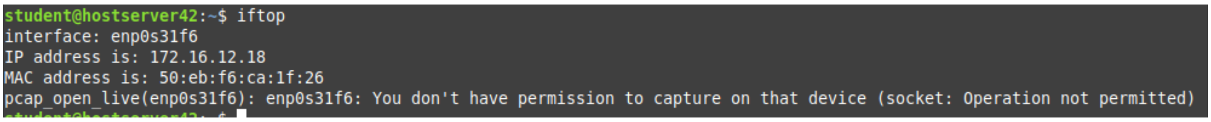
```
student@hostserver42:~$ ifplugstatus
lo: link beat detected
enp0s31f6: link beat detected
vmnet1: link beat detected
vmnet8: link beat detected
```

20. iftop

Linux iftop command is used in traffic monitoring.

Use the following command to download iftop on your system.

OUTPUT



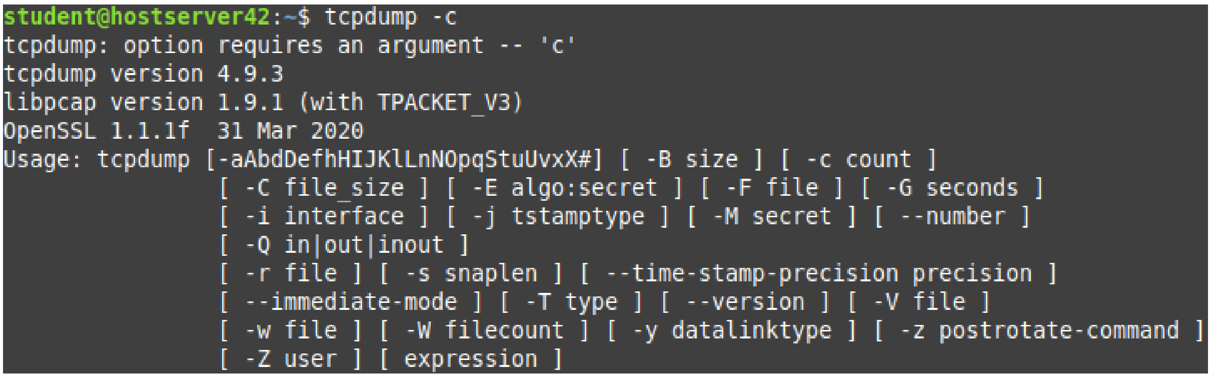
```
student@hostserver42:~$ iftop
interface: enp0s31f6
IP address is: 172.16.12.18
MAC address is: 50:eb:f6:ca:1f:26
pcap_open_live(enp0s31f6): enp0s31f6: You don't have permission to capture on that device (socket: Operation not permitted)
student@hostserver42:~$
```

21. tcpdump

Linux tcpdump command is the most used command in network analysis among other Linux network commands. It captures the traffic that is passing through the network interface and displays it.

This kind of access to the packet will be crucial when troubleshooting the network.

OUTPUT



```
student@hostserver42:~$ tcpdump -c
tcpdump: option requires an argument -- 'c'
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotate-command ]
                [ -Z user ] [ expression ]
```