ASSIGNMENT -01

REPORT

BASIC NETWORKING COMMANDS

SUBMITTED BY:

KOLLI JOGI NAIDU

B190605CS

CSE-B

Table of contents

INTRODUCTION:

The basic network commands will help us to understand how network works and get network information to troubleshoot and solve the network issues.

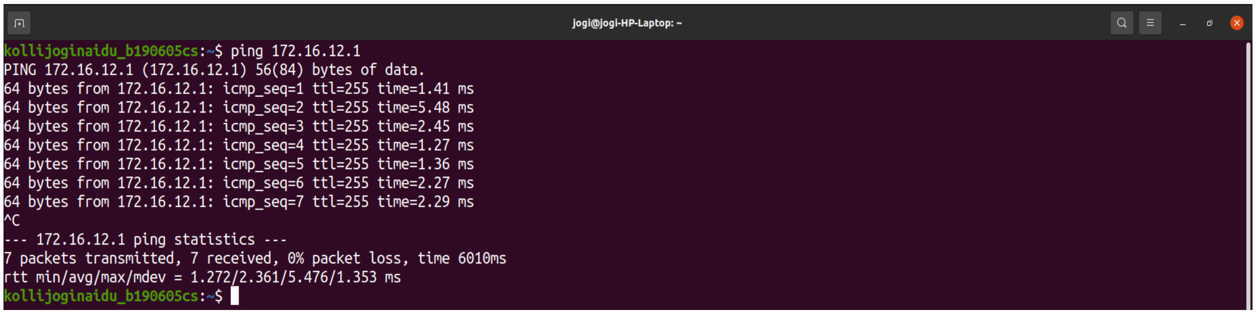
1.Ping:

Ping stands for “**Packet INternet Groper**”. It is used to test the connectivity between two hosts. It sends ICMP(Internet Control Message Protocol) echo request messages to the destination. The destination host replies with ICMP response messages. If the ping command gets a response from the destination host, it displays the reply along with the round-trip times.

General syntax:

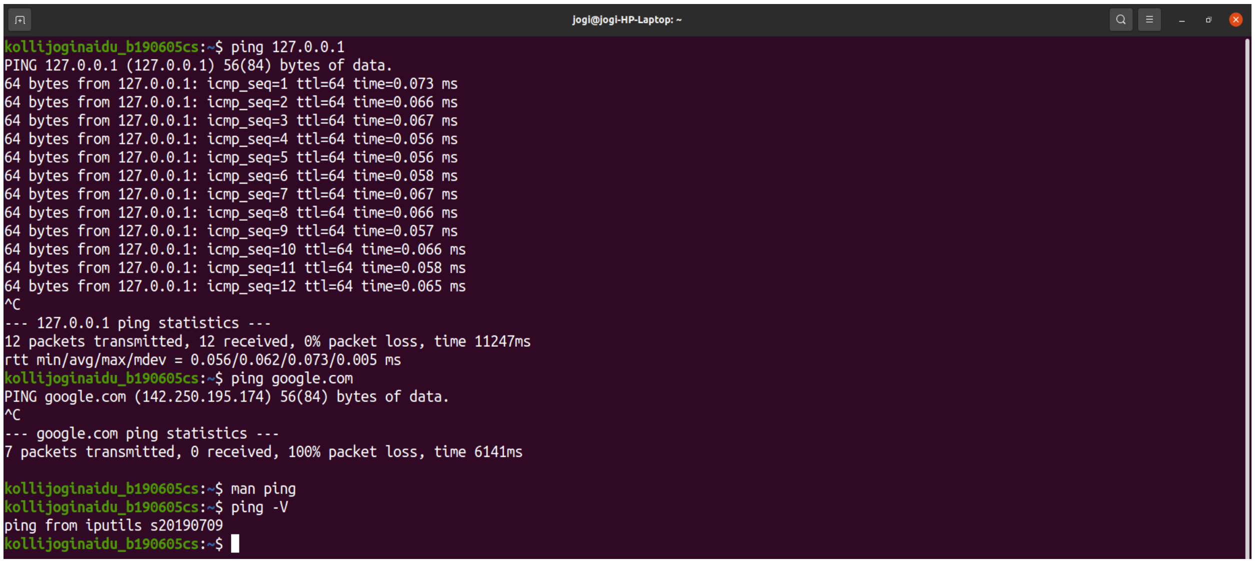
```
ping [destination host IP or domain name]
```

The following commands have been tested in the terminal to get more understanding. It shows the number of packets sent from the destination and the number of packets received by the destination.



```
kollijoginaidu_b190605cs:~$ ping 172.16.12.1
PING 172.16.12.1 (172.16.12.1) 56(84) bytes of data.
64 bytes from 172.16.12.1: icmp_seq=1 ttl=255 time=1.41 ms
64 bytes from 172.16.12.1: icmp_seq=2 ttl=255 time=5.48 ms
64 bytes from 172.16.12.1: icmp_seq=3 ttl=255 time=2.45 ms
64 bytes from 172.16.12.1: icmp_seq=4 ttl=255 time=1.27 ms
64 bytes from 172.16.12.1: icmp_seq=5 ttl=255 time=1.36 ms
64 bytes from 172.16.12.1: icmp_seq=6 ttl=255 time=2.27 ms
64 bytes from 172.16.12.1: icmp_seq=7 ttl=255 time=2.29 ms
^C
--- 172.16.12.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 1.272/2.361/5.476/1.353 ms
kollijoginaidu_b190605cs:~$
```

If you want to know whether you are connected to the internet or not, you can ping yourself to your local host(i.e. **127.0.0.1**)



```
kollijoginaidu_b190605cs:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.073 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.066 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.058 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.065 ms
^C
--- 127.0.0.1 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11247ms
rtt min/avg/max/mdev = 0.056/0.062/0.073/0.005 ms
kollijoginaidu_b190605cs:~$ ping google.com
PING google.com (142.250.195.174) 56(84) bytes of data.
^C
--- google.com ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6141ms

kollijoginaidu_b190605cs:~$ man ping
kollijoginaidu_b190605cs:~$ ping -V
ping from iputils s20190709
kollijoginaidu_b190605cs:~$
```

To know more about the ping command , type : ***man ping***

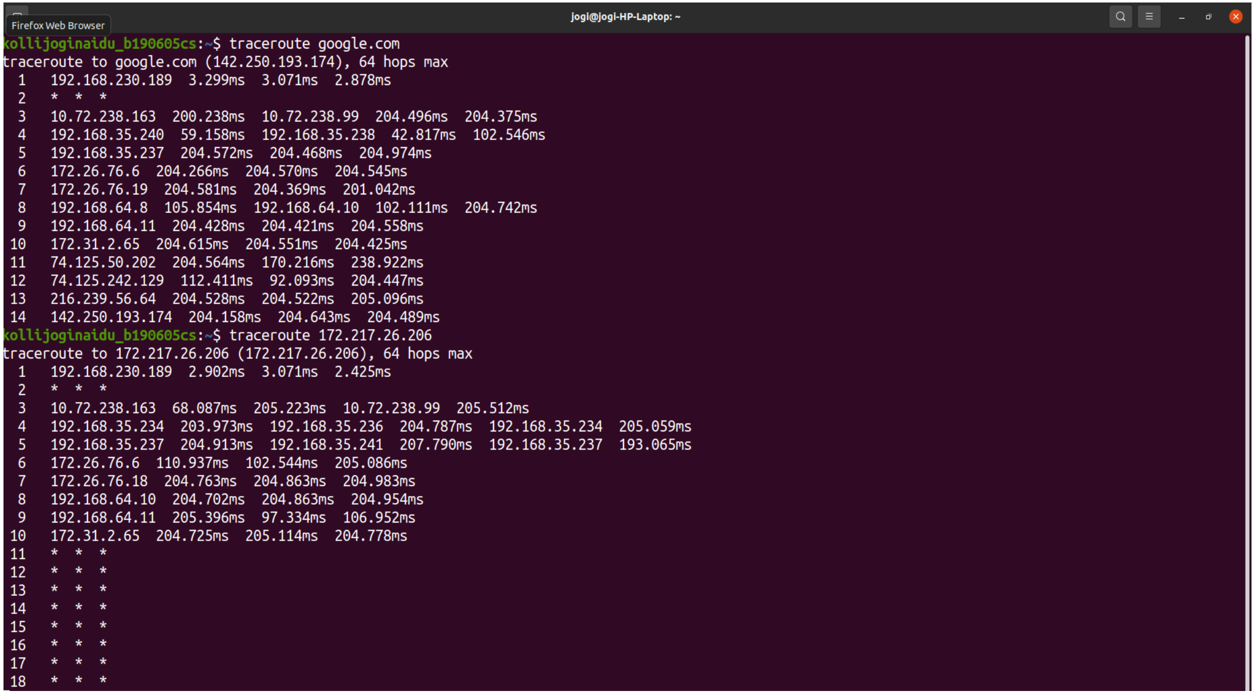
2.Traceroute:

This command gives the insight about how the network take a path to reach the destination. It is used to diagnose path-related problems. A path consists of all routers in a sequence that IP packets sent from the source host traverse to reach the destination host. This command prints the path. If any router is down on the path, this command prints the path up to the last operational router.

Note: The command **tracert** is used in windows.

General syntax:

traceroute [*destination name or IP address*]



```
kollijoginaidu_b190605cs:~$ traceroute google.com
traceroute to google.com (142.250.193.174), 64 hops max
  1   192.168.230.189  3.299ms  3.071ms  2.878ms
  2   *  *  *
  3   10.72.238.163  200.238ms  10.72.238.99  204.496ms  204.375ms
  4   192.168.35.240  59.158ms  192.168.35.238  42.817ms  102.546ms
  5   192.168.35.237  204.572ms  204.468ms  204.974ms
  6   172.26.76.6  204.266ms  204.570ms  204.545ms
  7   172.26.76.19  204.581ms  204.369ms  201.042ms
  8   192.168.64.8  105.854ms  192.168.64.10  102.111ms  204.742ms
  9   192.168.64.11  204.428ms  204.421ms  204.558ms
 10   172.31.2.65  204.615ms  204.551ms  204.425ms
 11   74.125.50.202  204.564ms  170.216ms  238.922ms
 12   74.125.242.129  112.411ms  92.093ms  204.447ms
 13   216.239.56.64  204.528ms  204.522ms  205.096ms
 14   142.250.193.174  204.158ms  204.643ms  204.489ms
kollijoginaidu_b190605cs:~$ traceroute 172.217.26.206
traceroute to 172.217.26.206 (172.217.26.206), 64 hops max
  1   192.168.230.189  2.902ms  3.071ms  2.425ms
  2   *  *  *
  3   10.72.238.163  68.087ms  205.223ms  10.72.238.99  205.512ms
  4   192.168.35.234  203.973ms  192.168.35.236  204.787ms  192.168.35.234  205.059ms
  5   192.168.35.237  204.913ms  192.168.35.241  207.790ms  192.168.35.237  193.065ms
  6   172.26.76.6  110.937ms  102.544ms  205.086ms
  7   172.26.76.18  204.763ms  204.863ms  204.983ms
  8   192.168.64.10  204.702ms  204.863ms  204.954ms
  9   192.168.64.11  205.396ms  97.334ms  106.952ms
 10   172.31.2.65  204.725ms  205.114ms  204.778ms
 11   *  *  *
 12   *  *  *
 13   *  *  *
 14   *  *  *
 15   *  *  *
 16   *  *  *
 17   *  *  *
 18   *  *  *
```

To know more about the ping command , type : ***man traceroute***

3. ip/ifconfig/ipconfig:

The command ipconfig stands for “**interface configurator**”. It is used to initialize an interface or configure it with an IP address and enable/disable it. It displays all current TCP/IP network configuration values and DNS entries.The **ip** command is the latest and updated version of ifconfig command.

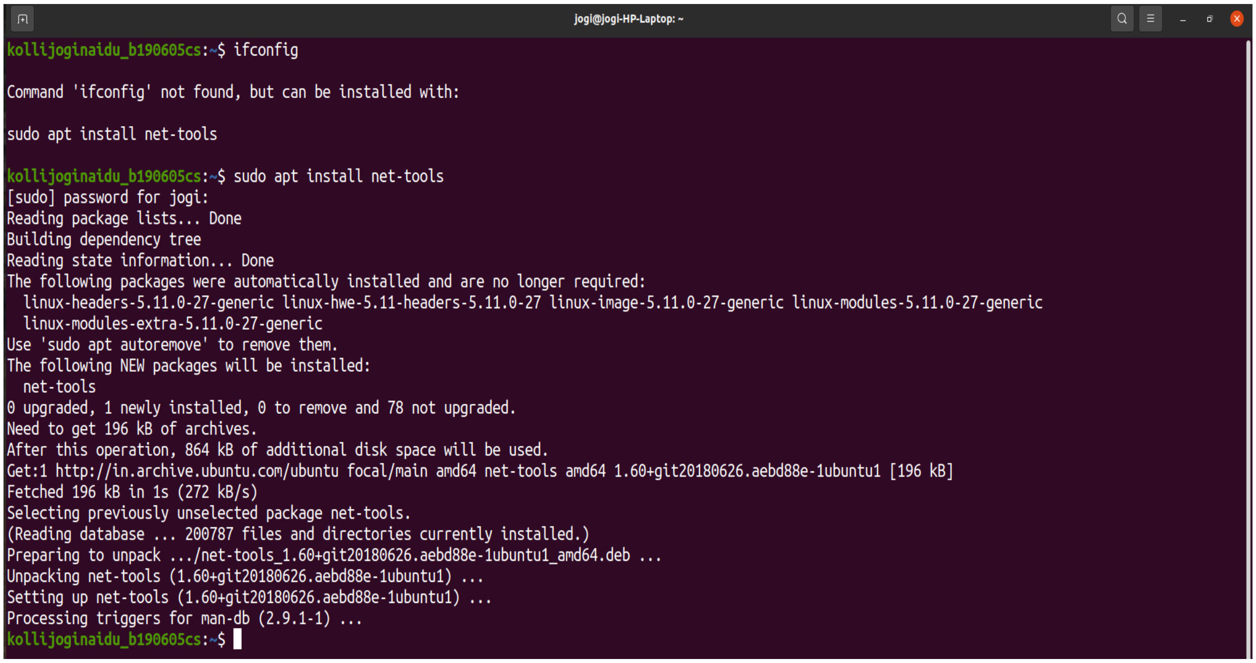
General syntax:

ifconfig

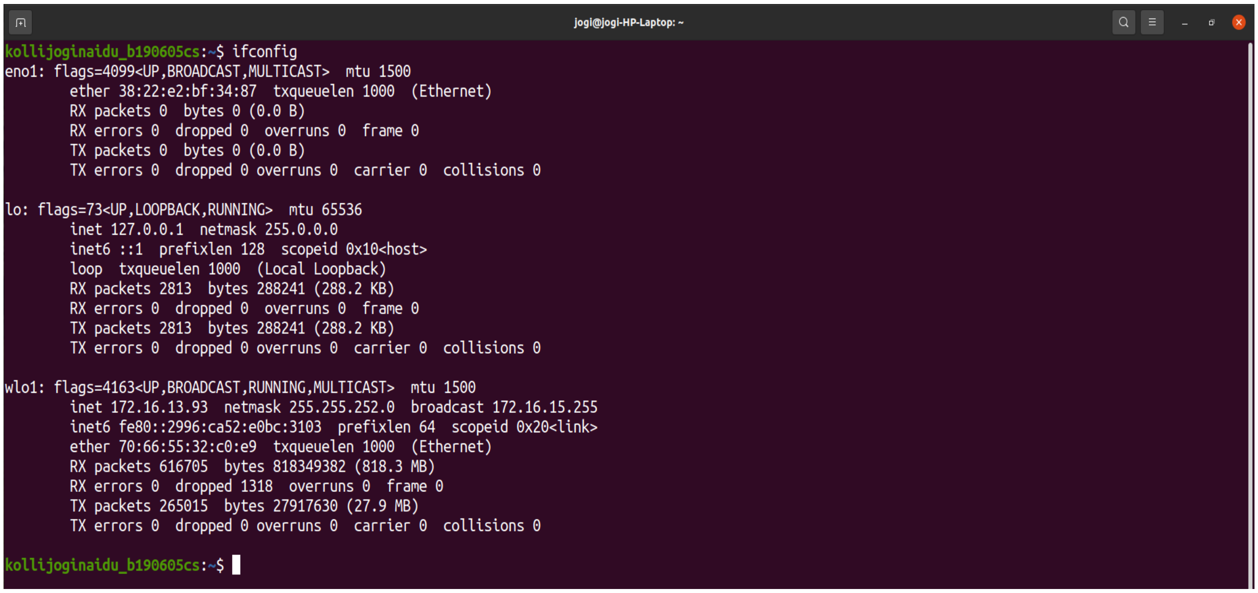
If the command is not found,install by the following command:

Sudo apt install net-tools

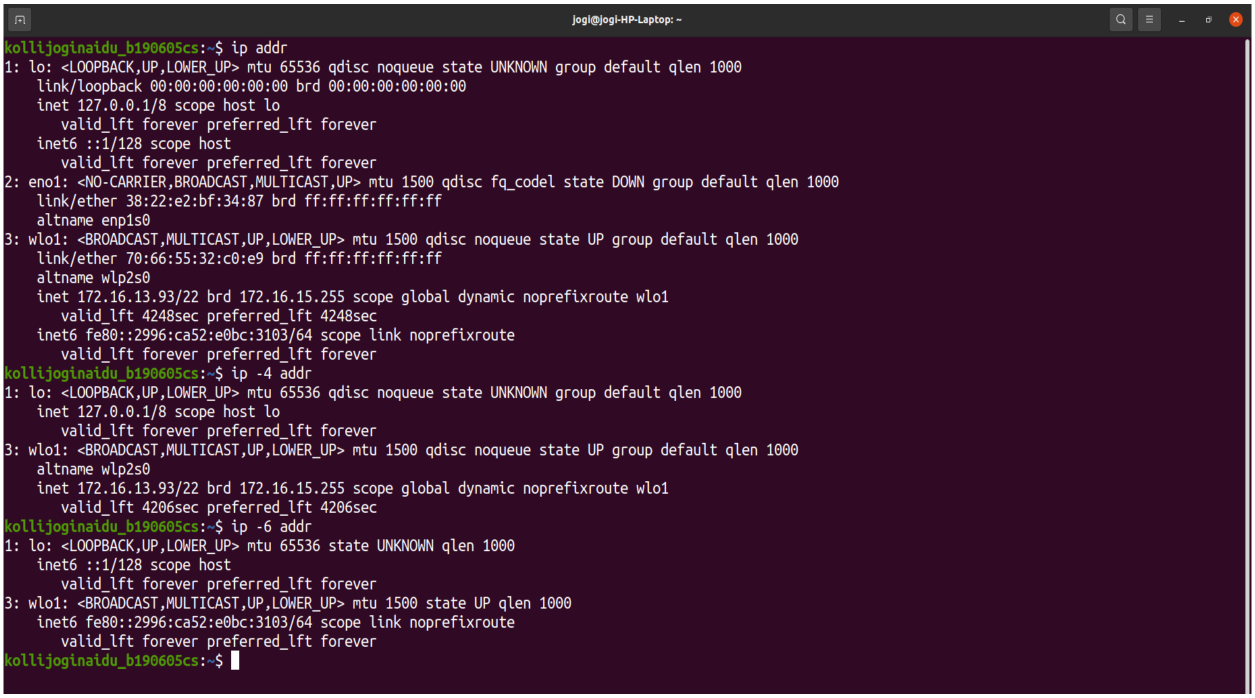
Note: The **ipconfig** command is used in the windows system.



```
kollijoginaidu_b190605cs:~$ ifconfig

Command 'ifconfig' not found, but can be installed with:

sudo apt install net-tools

kollijoginaidu_b190605cs:~$ sudo apt install net-tools
[sudo] password for jogi:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-5.11.0-27-generic linux-hwe-5.11-headers-5.11.0-27 linux-image-5.11.0-27-generic linux-modules-5.11.0-27-generic
  linux-modules-extra-5.11.0-27-generic
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  net-tools
0 upgraded, 1 newly installed, 0 to remove and 78 not upgraded.
Need to get 196 kB of archives.
After this operation, 864 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+git20180626.aebd88e-1ubuntu1 [196 kB]
Fetched 196 kB in 1s (272 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 200787 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ...
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
kollijoginaidu_b190605cs:~$ 
```



```
kollijoginaidu_b190605cs:~$ ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 38:22:e2:bf:34:87  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 2813  bytes 288241 (288.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2813  bytes 288241 (288.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.13.93  netmask 255.255.252.0  broadcast 172.16.15.255
        inet6 fe80::2996:ca52:e0bc:3103  prefixlen 64  scopeid 0x20<link>
        ether 70:66:55:32:c0:e9  txqueuelen 1000  (Ethernet)
        RX packets 616705  bytes 818349382 (818.3 MB)
        RX errors 0  dropped 1318  overruns 0  frame 0
        TX packets 265015  bytes 27917630 (27.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kollijoginaidu_b190605cs:~$ 
```

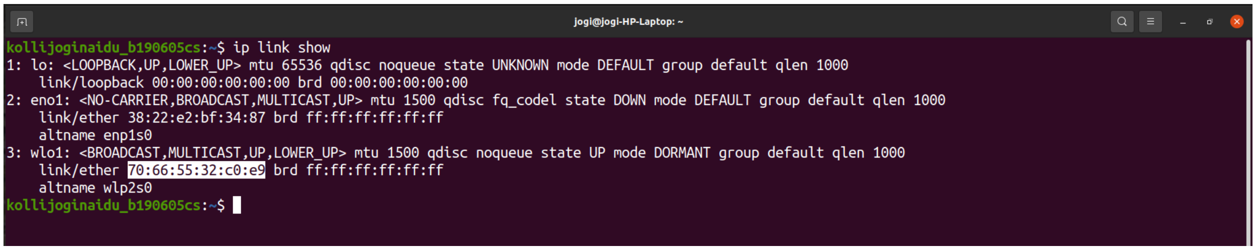


```
kollijoginaidu_b190605cs:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 38:22:e2:bf:34:87 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 70:66:55:32:c0:e9 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 172.16.13.93/22 brd 172.16.15.255 scope global dynamic noprefixroute wlo1
       valid_lft 4248sec preferred_lft 4248sec
    inet6 fe80::2996:ca52:e0bc:3103/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kollijoginaidu_b190605cs:~$ ip -4 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    altname wlp2s0
    inet 172.16.13.93/22 brd 172.16.15.255 scope global dynamic noprefixroute wlo1
       valid_lft 4206sec preferred_lft 4206sec
kollijoginaidu_b190605cs:~$ ip -6 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 state UNKNOWN qlen 1000
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 fe80::2996:ca52:e0bc:3103/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
kollijoginaidu_b190605cs:~$
```

To know more about the ifconfig command, type: **man ifconfig**

To get MAC Address:

The highlighted address is MAC address



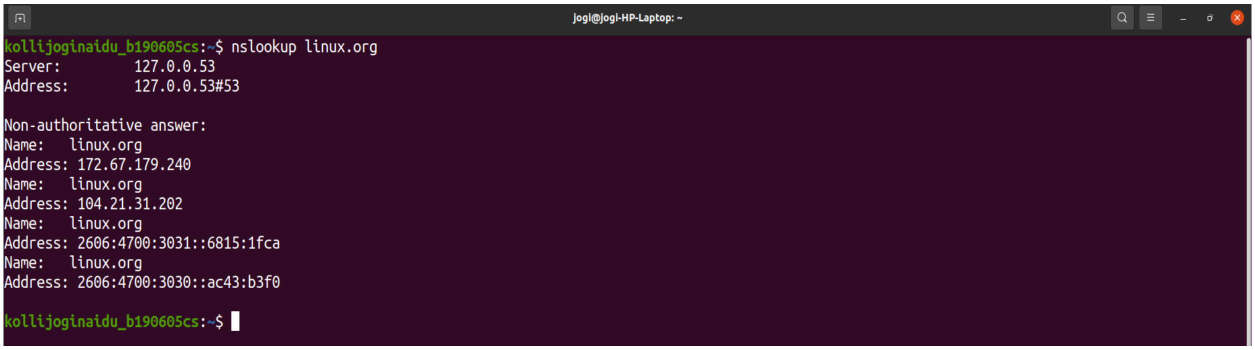
```
kollijoginaidu_b190605cs:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode DEFAULT group default qlen 1000
    link/ether 38:22:e2:bf:34:87 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default qlen 1000
    link/ether 70:66:55:32:c0:e9 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
kollijoginaidu_b190605cs:~$
```

4. dig/nslookup/host:

- **nslookup:** The command nslookup stands for “Name Server Lookup”. It is used to get information from the DNS server. It is used to query the DNS to obtain the domain name or IP address mapping or any other specific DNS record.

  General syntax:

  ```
  nslookup [option]
  ```

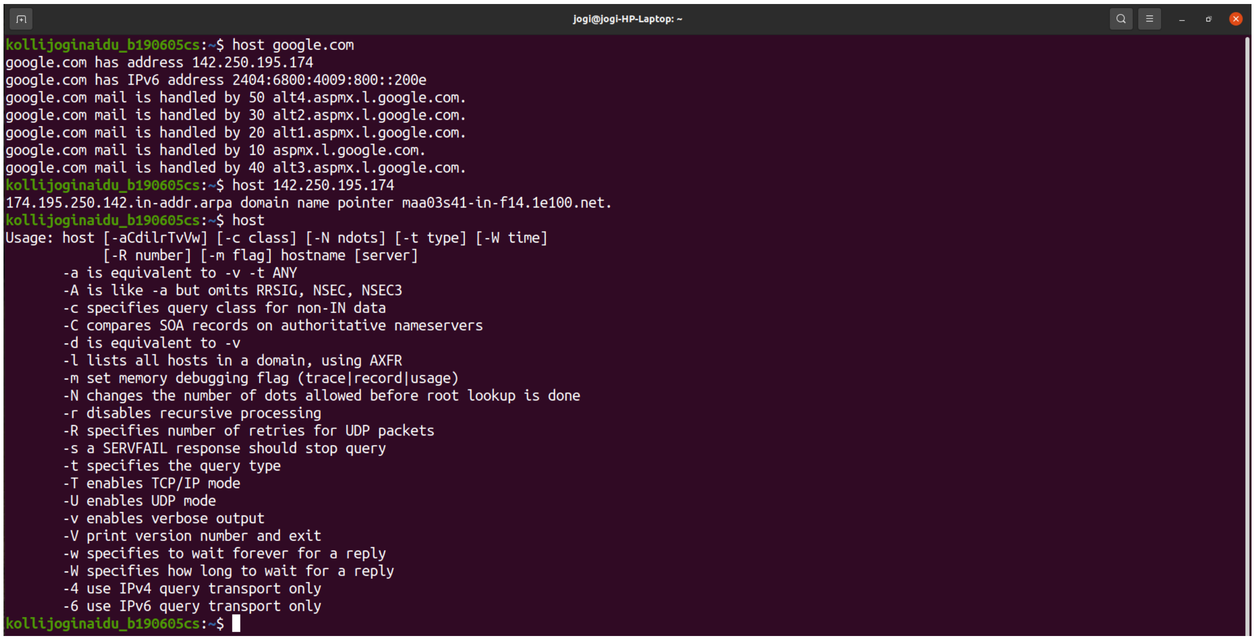


```
kollijoginaidu_b190605cs:~$ nslookup linux.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   linux.org
Address: 172.67.179.240
Name:   linux.org
Address: 104.21.31.202
Name:   linux.org
Address: 2606:4700:3031::6815:1fca
Name:   linux.org
Address: 2606:4700:3030::ac43:b3f0

kollijoginaidu_b190605cs:~$
```

host: It displays the domain name for a given IP address and vice versa.

General syntax:

host [-aCdlnrsTwv] [-c class] [-N ndots] [-R number] [-t type] [-W wait] [-m flag] [-4] [-6] {name} [server]

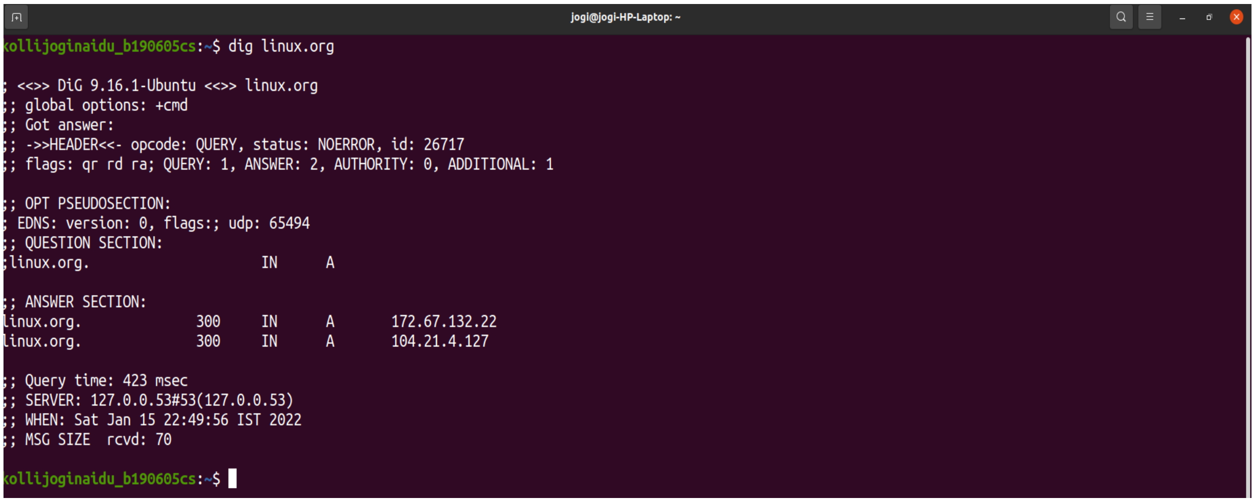


```
kollijoginaidu_b190605cs:~$ host google.com
google.com has address 142.250.195.174
google.com has IPv6 address 2404:6800:4009:800::200e
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
kollijoginaidu_b190605cs:~$ host 142.250.195.174
174.195.250.142.in-addr.arpa domain name pointer maa03s41-in-f14.1e100.net.
kollijoginaidu_b190605cs:~$ host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
            [-R number] [-m flag] hostname [server]
       -a is equivalent to -v -t ANY
       -A is like -a but omits RRSIG, NSEC, NSEC3
       -c specifies query class for non-IN data
       -C compares SOA records on authoritative nameservers
       -d is equivalent to -v
       -l lists all hosts in a domain, using AXFR
       -m set memory debugging flag (trace|record|usage)
       -N changes the number of dots allowed before root lookup is done
       -r disables recursive processing
       -R specifies number of retries for UDP packets
       -s a SERVFAIL response should stop query
       -t specifies the query type
       -T enables TCP/IP mode
       -U enables UDP mode
       -v enables verbose output
       -V print version number and exit
       -w specifies to wait forever for a reply
       -W specifies how long to wait for a reply
       -4 use IPv4 query transport only
       -6 use IPv6 query transport only
kollijoginaidu_b190605cs:~$
```

- **dig:**The command dig stands for “Domain Information Groper”. It replaces older tools such as nslookup and host.

  General syntax:

  dig [*server*] [*name*] [*type*]



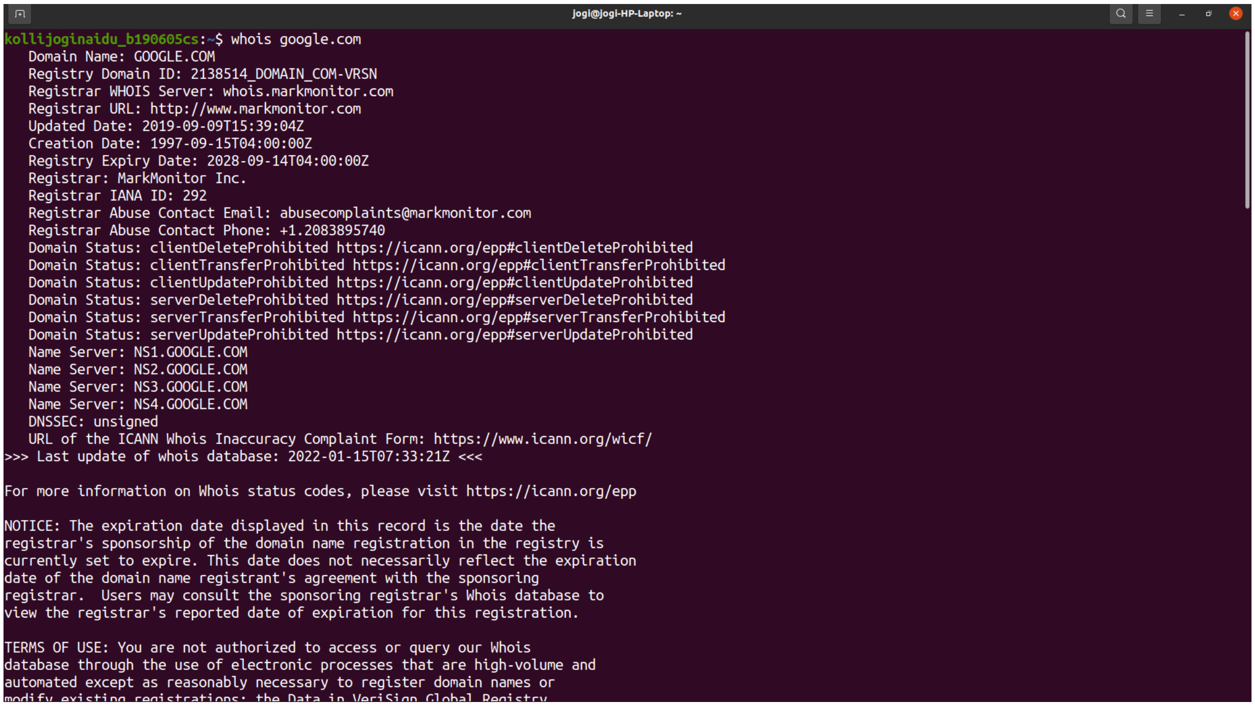
```
kollijoginaidu_b190605cs:~$ dig linux.org

; <<>> DiG 9.16.1-Ubuntu <<>> linux.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26717
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;linux.org.                     IN      A

;; ANSWER SECTION:
linux.org.              300     IN      A       172.67.132.22
linux.org.              300     IN      A       104.21.4.127

;; Query time: 423 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jan 15 22:49:56 IST 2022
;; MSG SIZE  rcvd: 70

kollijoginaidu_b190605cs:~$ 
```

5.whois:

It is used to find out information about a domain, such as the owner of the domain, the owner’s contact information, and the nameservers that the domain is using.

General syntax:

whois [*options*]...[*query*]

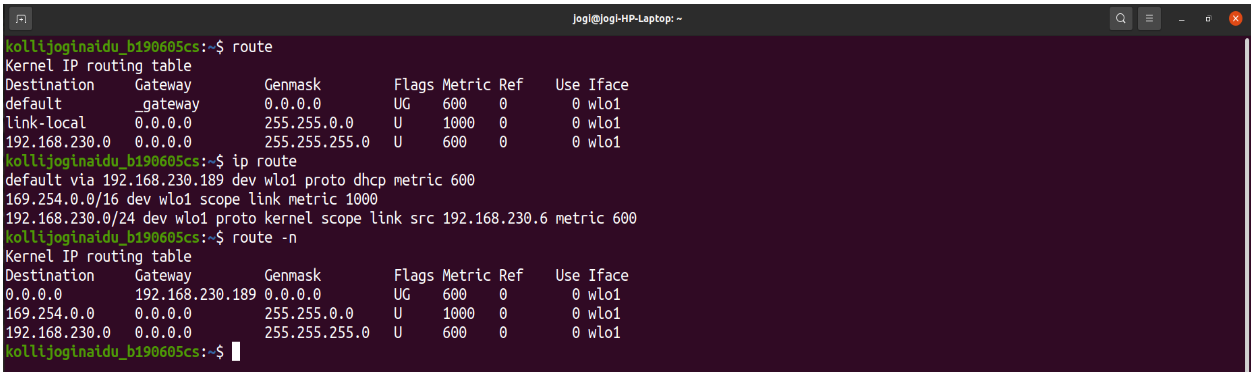


```
kollijoginaidu_b190605cs:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry 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: +1.2083895740
   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: 2022-01-15T07:33:21Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
```

6.route:

It is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.
General syntax:

```
route [option]
```



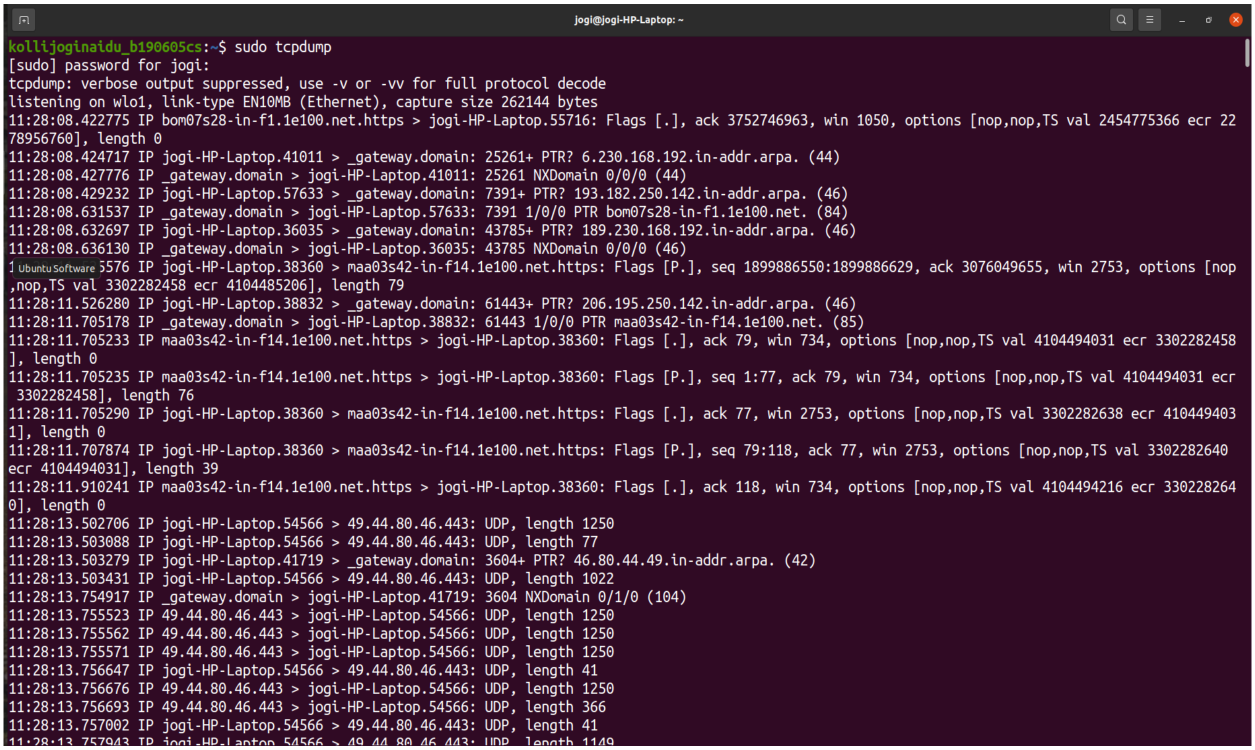
```
kollijoginaidu_b190605cs:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.230.0   0.0.0.0         255.255.255.0   U     600    0        0 wlo1
kollijoginaidu_b190605cs:~$ ip route
default via 192.168.230.189 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.230.0/24 dev wlo1 proto kernel scope link src 192.168.230.6 metric 600
kollijoginaidu_b190605cs:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.230.189 0.0.0.0         UG    600    0        0 wlo1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.230.0   0.0.0.0         255.255.255.0   U     600    0        0 wlo1
kollijoginaidu_b190605cs:~$ 
```

7.tcpdump:

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

To capture the packets of current network interface:

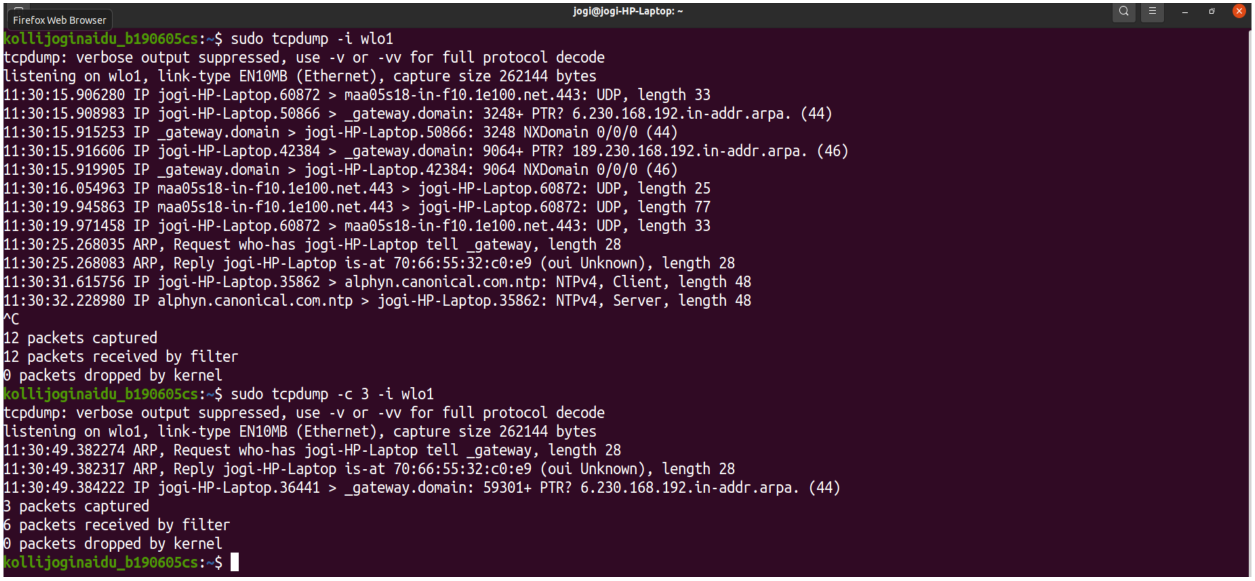
```
sudo tcpdump
```



```
kollijoginaidu_b190605cs:~$ sudo tcpdump
[sudo] password for jogi:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:28:08.422775 IP bom07s28-in-f1.1e100.net.https > jogi-HP-Laptop.55716: Flags [.], ack 3752746963, win 1050, options [nop,nop,TS val 2454775366 ecr 22
78956760], length 0
11:28:08.424717 IP jogi-HP-Laptop.41011 > _gateway.domain: 25261+ PTR? 6.230.168.192.in-addr.arpa. (44)
11:28:08.427776 IP _gateway.domain > jogi-HP-Laptop.41011: 25261 NXDomain 0/0/0 (44)
11:28:08.429232 IP jogi-HP-Laptop.57633 > _gateway.domain: 7391+ PTR? 193.182.250.142.in-addr.arpa. (46)
11:28:08.631537 IP _gateway.domain > jogi-HP-Laptop.57633: 7391 1/0/0 PTR bom07s28-in-f1.1e100.net. (84)
11:28:08.632697 IP jogi-HP-Laptop.36035 > _gateway.domain: 43785+ PTR? 189.230.168.192.in-addr.arpa. (46)
11:28:08.636130 IP _gateway.domain > jogi-HP-Laptop.36035: 43785 NXDomain 0/0/0 (46)
1[illegible]5576 IP jogi-HP-Laptop.38360 > maa03s42-in-f14.1e100.net.https: Flags [P.], seq 1899886550:1899886629, ack 3076049655, win 2753, options [nop
,nop,TS val 3302282458 ecr 4104485206], length 79
11:28:11.526280 IP jogi-HP-Laptop.38832 > _gateway.domain: 61443+ PTR? 206.195.250.142.in-addr.arpa. (46)
11:28:11.705178 IP _gateway.domain > jogi-HP-Laptop.38832: 61443 1/0/0 PTR maa03s42-in-f14.1e100.net. (85)
11:28:11.705233 IP maa03s42-in-f14.1e100.net.https > jogi-HP-Laptop.38360: Flags [.], ack 79, win 734, options [nop,nop,TS val 4104494031 ecr 3302282458
], length 0
11:28:11.705235 IP maa03s42-in-f14.1e100.net.https > jogi-HP-Laptop.38360: Flags [P.], seq 1:77, ack 79, win 734, options [nop,nop,TS val 4104494031 ecr
 3302282458], length 76
11:28:11.705290 IP jogi-HP-Laptop.38360 > maa03s42-in-f14.1e100.net.https: Flags [.], ack 77, win 2753, options [nop,nop,TS val 3302282638 ecr 410449403
1], length 0
11:28:11.707874 IP jogi-HP-Laptop.38360 > maa03s42-in-f14.1e100.net.https: Flags [P.], seq 79:118, ack 77, win 2753, options [nop,nop,TS val 3302282640
ecr 4104494031], length 39
11:28:11.910241 IP maa03s42-in-f14.1e100.net.https > jogi-HP-Laptop.38360: Flags [.], ack 118, win 734, options [nop,nop,TS val 4104494216 ecr 330228264
0], length 0
11:28:13.502706 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 1250
11:28:13.503088 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 77
11:28:13.503279 IP jogi-HP-Laptop.41719 > _gateway.domain: 3604+ PTR? 46.80.44.49.in-addr.arpa. (42)
11:28:13.503431 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 1022
11:28:13.754917 IP _gateway.domain > jogi-HP-Laptop.41719: 3604 NXDomain 0/1/0 (104)
11:28:13.755523 IP 49.44.80.46.443 > jogi-HP-Laptop.54566: UDP, length 1250
11:28:13.755562 IP 49.44.80.46.443 > jogi-HP-Laptop.54566: UDP, length 1250
11:28:13.755571 IP 49.44.80.46.443 > jogi-HP-Laptop.54566: UDP, length 1250
11:28:13.756647 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 41
11:28:13.756676 IP 49.44.80.46.443 > jogi-HP-Laptop.54566: UDP, length 1250
11:28:13.756693 IP 49.44.80.46.443 > jogi-HP-Laptop.54566: UDP, length 366
11:28:13.757002 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 41
11:28:13.757943 IP jogi-HP-Laptop.54566 > 49.44.80.46.443: UDP, length 1149
```

To capture the packets of specific network interface:

sudo tcpdump -i wlo1



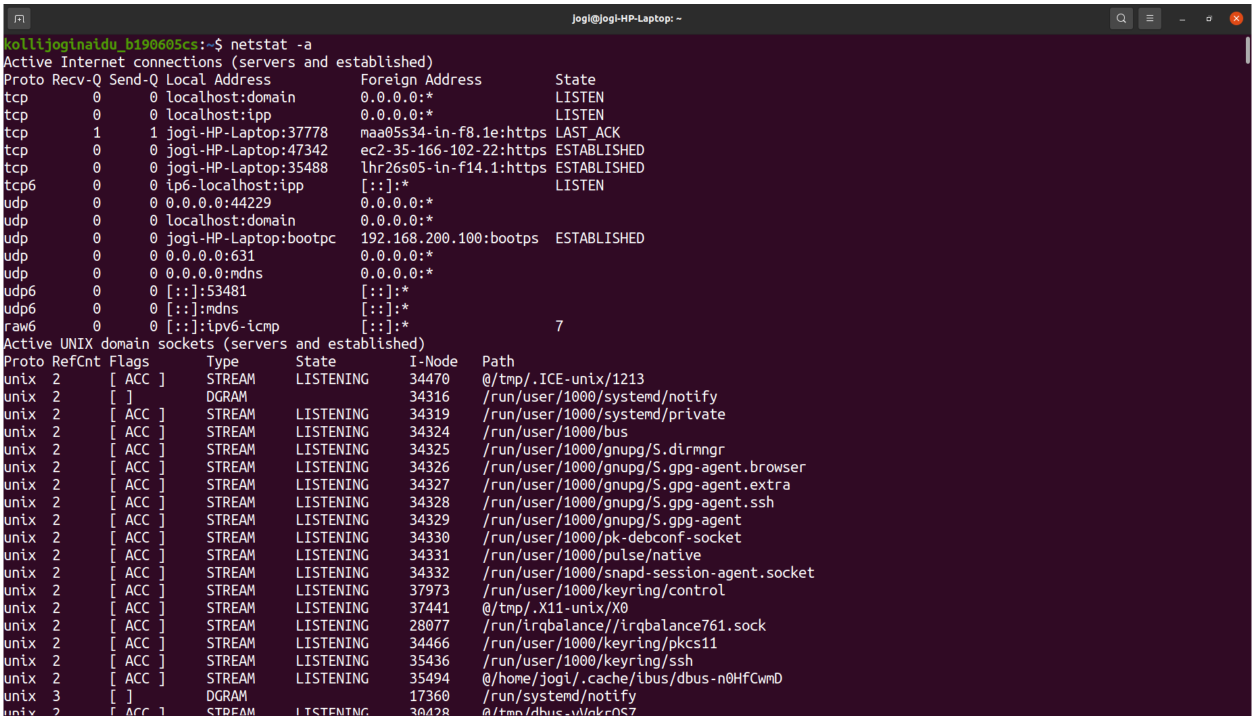
```
kollijoginaidu_b190605cs:~$ sudo tcpdump -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:30:15.906280 IP jogi-HP-Laptop.60872 > maa05s18-in-f10.1e100.net.443: UDP, length 33
11:30:15.908983 IP jogi-HP-Laptop.50866 > _gateway.domain: 3248+ PTR? 6.230.168.192.in-addr.arpa. (44)
11:30:15.915253 IP _gateway.domain > jogi-HP-Laptop.50866: 3248 NXDomain 0/0/0 (44)
11:30:15.916606 IP jogi-HP-Laptop.42384 > _gateway.domain: 9064+ PTR? 189.230.168.192.in-addr.arpa. (46)
11:30:15.919905 IP _gateway.domain > jogi-HP-Laptop.42384: 9064 NXDomain 0/0/0 (46)
11:30:16.054963 IP maa05s18-in-f10.1e100.net.443 > jogi-HP-Laptop.60872: UDP, length 25
11:30:19.945863 IP maa05s18-in-f10.1e100.net.443 > jogi-HP-Laptop.60872: UDP, length 77
11:30:19.971458 IP jogi-HP-Laptop.60872 > maa05s18-in-f10.1e100.net.443: UDP, length 33
11:30:25.268035 ARP, Request who-has jogi-HP-Laptop tell _gateway, length 28
11:30:25.268083 ARP, Reply jogi-HP-Laptop is-at 70:66:55:32:c0:e9 (oui Unknown), length 28
11:30:31.615756 IP jogi-HP-Laptop.35862 > alphyn.canonical.com.ntp: NTPv4, Client, length 48
11:30:32.228980 IP alphyn.canonical.com.ntp > jogi-HP-Laptop.35862: NTPv4, Server, length 48
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
kollijoginaidu_b190605cs:~$ sudo tcpdump -c 3 -i wlo1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
11:30:49.382274 ARP, Request who-has jogi-HP-Laptop tell _gateway, length 28
11:30:49.382317 ARP, Reply jogi-HP-Laptop is-at 70:66:55:32:c0:e9 (oui Unknown), length 28
11:30:49.384222 IP jogi-HP-Laptop.36441 > _gateway.domain: 59301+ PTR? 6.230.168.192.in-addr.arpa. (44)
3 packets captured
6 packets received by filter
0 packets dropped by kernel
kollijoginaidu_b190605cs:~$
```

8.netstat/ss:

- **netstat:**The command netstat stands for “**Network Statistics**”. It displays various network related information such as network connections, routing tables, interface statistics, connection information, port listening.

  General syntax:

netstat [*option*]

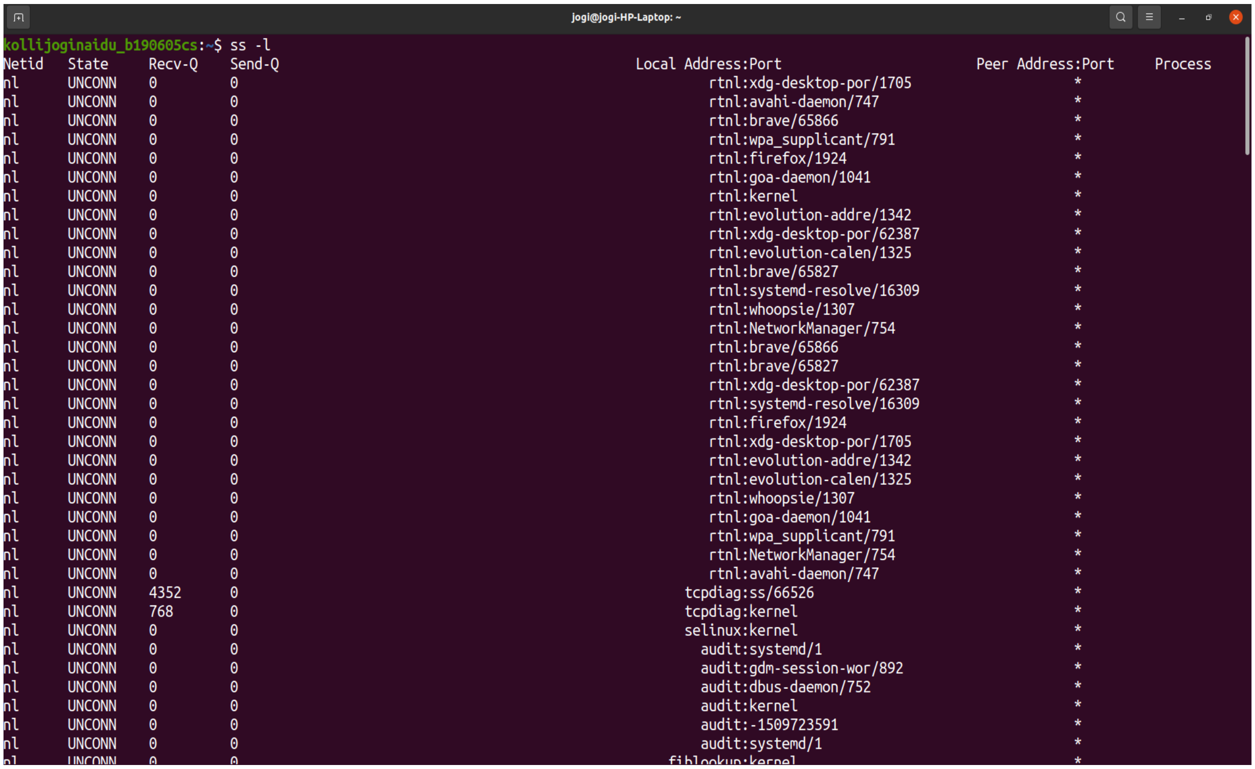


```
kollijoginaidu_b190605cs:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        1      1 jogi-HP-Laptop:37778    maa05s34-in-f8.1e:https LAST_ACK
tcp        0      0 jogi-HP-Laptop:47342    ec2-35-166-102-22:https ESTABLISHED
tcp        0      0 jogi-HP-Laptop:35488    lhr26s05-in-f14.1:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:44229           0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 jogi-HP-Laptop:bootpc   192.168.200.100:bootps  ESTABLISHED
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp6       0      0 [::]:53481              [::]:*
udp6       0      0 [::]:mdns               [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     34470    @/tmp/.ICE-unix/1213
unix  2      [ ]         DGRAM                    34316    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     34319    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     34324    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     34325    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     34326    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     34327    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     34328    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     34329    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     34330    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     34331    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     34332    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     37973    /run/user/1000/keyring/control
unix  2      [ ACC ]     STREAM     LISTENING     37441    @/tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     28077    /run/irqbalance//irqbalance761.sock
unix  2      [ ACC ]     STREAM     LISTENING     34466    /run/user/1000/keyring/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     35436    /run/user/1000/keyring/ssh
unix  2      [ ACC ]     STREAM     LISTENING     35494    @/home/jogi/.cache/ibus/dbus-n0HfCwmD
unix  3      [ ]         DGRAM                    17360    /run/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     30428    @/tmp/dbus-vVqkrOS7
```

- **ss:** It is the replacement of netstat command. It is faster and more informative than netstat command.

  General syntax:

ss [*option*]



```
kollijoginaidu_b190605cs:~$ ss -l
Netid  State    Recv-Q   Send-Q                                 Local Address:Port             Peer Address:Port     Process
nl     UNCONN   0        0                                          rtnl:xdg-desktop-por/1705                   *
nl     UNCONN   0        0                                          rtnl:avahi-daemon/747                       *
nl     UNCONN   0        0                                          rtnl:brave/65866                            *
nl     UNCONN   0        0                                          rtnl:wpa_supplicant/791                     *
nl     UNCONN   0        0                                          rtnl:firefox/1924                           *
nl     UNCONN   0        0                                          rtnl:goa-daemon/1041                        *
nl     UNCONN   0        0                                          rtnl:kernel                                 *
nl     UNCONN   0        0                                          rtnl:evolution-addre/1342                   *
nl     UNCONN   0        0                                          rtnl:xdg-desktop-por/62387                  *
nl     UNCONN   0        0                                          rtnl:evolution-calen/1325                   *
nl     UNCONN   0        0                                          rtnl:brave/65827                            *
nl     UNCONN   0        0                                          rtnl:systemd-resolve/16309                  *
nl     UNCONN   0        0                                          rtnl:whoopsie/1307                          *
nl     UNCONN   0        0                                          rtnl:NetworkManager/754                     *
nl     UNCONN   0        0                                          rtnl:brave/65866                            *
nl     UNCONN   0        0                                          rtnl:brave/65827                            *
nl     UNCONN   0        0                                          rtnl:xdg-desktop-por/62387                  *
nl     UNCONN   0        0                                          rtnl:systemd-resolve/16309                  *
nl     UNCONN   0        0                                          rtnl:firefox/1924                           *
nl     UNCONN   0        0                                          rtnl:xdg-desktop-por/1705                   *
nl     UNCONN   0        0                                          rtnl:evolution-addre/1342                   *
nl     UNCONN   0        0                                          rtnl:evolution-calen/1325                   *
nl     UNCONN   0        0                                          rtnl:whoopsie/1307                          *
nl     UNCONN   0        0                                          rtnl:goa-daemon/1041                        *
nl     UNCONN   0        0                                          rtnl:wpa_supplicant/791                     *
nl     UNCONN   0        0                                          rtnl:NetworkManager/754                     *
nl     UNCONN   0        0                                          rtnl:avahi-daemon/747                       *
nl     UNCONN   4352     0                                       tcpdiag:ss/66526                               *
nl     UNCONN   768      0                                       tcpdiag:kernel                                 *
nl     UNCONN   0        0                                       selinux:kernel                                 *
nl     UNCONN   0        0                                         audit:systemd/1                              *
nl     UNCONN   0        0                                         audit:gdm-session-wor/892                    *
nl     UNCONN   0        0                                         audit:dbus-daemon/752                        *
nl     UNCONN   0        0                                         audit:kernel                                 *
nl     UNCONN   0        0                                         audit:-1509723591                            *
nl     UNCONN   0        0                                         audit:systemd/1                              *
nl     UNCONN   0        0                                     fiblookup:kernel                                 *
```

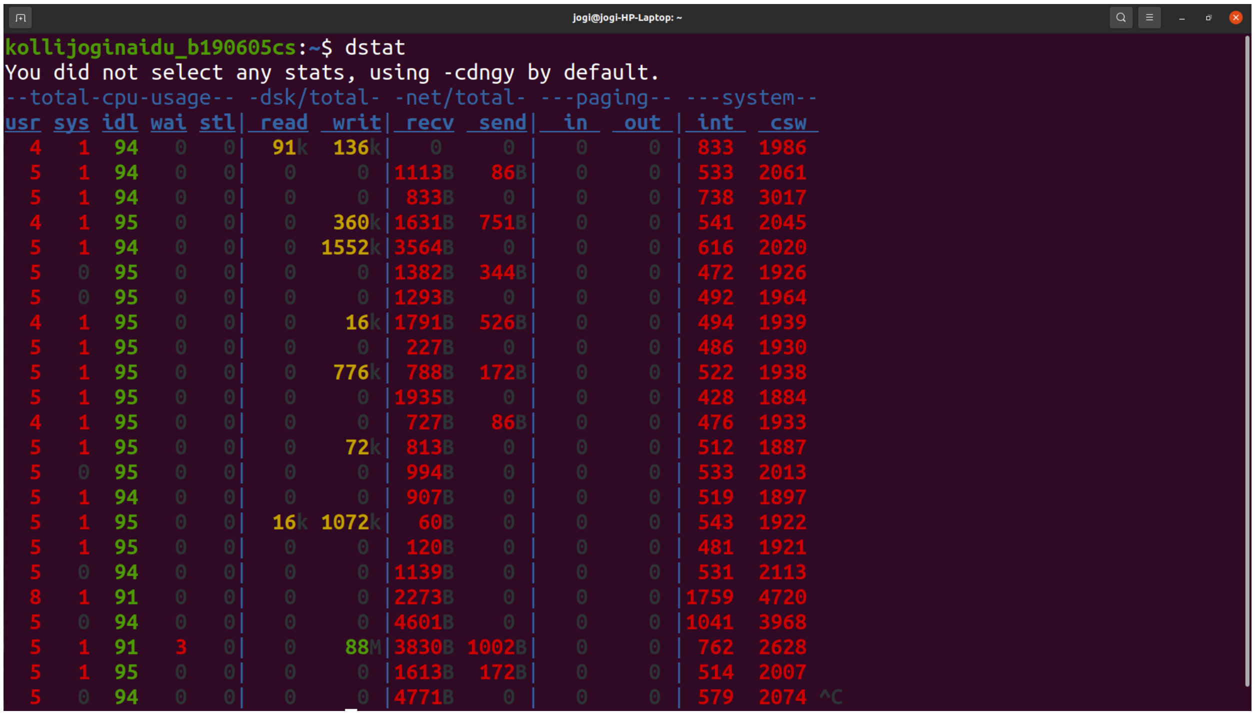
To know more about the ifconfig command, type: **man ss**

9.dstat:

It is used to display the statistics of major OS components such as network connections, I/O devices or CPU, disk, paging system statistics.

General syntax:

dstat [*option*]



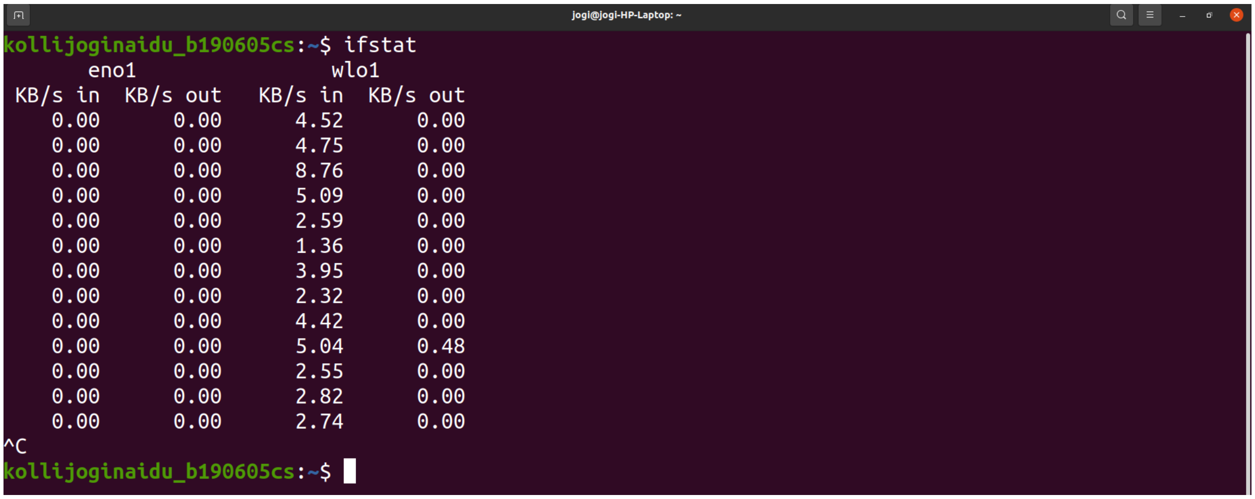
```
kollijoginaidu_b190605cs:~$ dstat
You did not select any stats, using -cdngy by default.
--total-cpu-usage-- -dsk/total- -net/total- ---paging-- ---system--
usr sys idl wai stl| read  writ| recv  send|  in   out | int   csw 
  4   1  94   0   0|  91k  136k|   0     0 |   0     0 | 833  1986 
  5   1  94   0   0|   0     0 |1113B   86B|   0     0 | 533  2061 
  5   1  94   0   0|   0     0 | 833B    0 |   0     0 | 738  3017 
  4   1  95   0   0|   0   360k|1631B  751B|   0     0 | 541  2045 
  5   1  94   0   0|   0  1552k|3564B    0 |   0     0 | 616  2020 
  5   0  95   0   0|   0     0 |1382B  344B|   0     0 | 472  1926 
  5   0  95   0   0|   0     0 |1293B    0 |   0     0 | 492  1964 
  4   1  95   0   0|   0    16k|1791B  526B|   0     0 | 494  1939 
  5   1  95   0   0|   0     0 | 227B    0 |   0     0 | 486  1930 
  5   1  95   0   0|   0   776k| 788B  172B|   0     0 | 522  1938 
  5   1  95   0   0|   0     0 |1935B    0 |   0     0 | 428  1884 
  4   1  95   0   0|   0     0 | 727B   86B|   0     0 | 476  1933 
  5   1  95   0   0|   0    72k| 813B    0 |   0     0 | 512  1887 
  5   0  95   0   0|   0     0 | 994B    0 |   0     0 | 533  2013 
  5   1  94   0   0|   0     0 | 907B    0 |   0     0 | 519  1897 
  5   1  95   0   0|  16k 1072k|  60B    0 |   0     0 | 543  1922 
  5   1  95   0   0|   0     0 | 120B    0 |   0     0 | 481  1921 
  5   0  94   0   0|   0     0 |1139B    0 |   0     0 | 531  2113 
  8   1  91   0   0|   0     0 |2273B    0 |   0     0 |1759  4720 
  5   0  94   0   0|   0     0 |4601B    0 |   0     0 |1041  3968 
  5   1  91   3   0|   0    88M|3830B 1002B|   0     0 | 762  2628 
  5   1  95   0   0|   0     0 |1613B  172B|   0     0 | 514  2007 
  5   0  94   0   0|   0     0 |4771B    0 |   0     0 | 579  2074 ^C
```

10.ifstat:

It neatly prints out network interface statistics. The utility keeps records of the previous data displayed in history files and by default only shows difference between the last and the current call.

General syntax:

```
ifstat [option]
```



```
kollijoginaidu_b190605cs:~$ ifstat
       eno1                 wlo1
 KB/s in  KB/s out   KB/s in  KB/s out
    0.00      0.00      4.52      0.00
    0.00      0.00      4.75      0.00
    0.00      0.00      8.76      0.00
    0.00      0.00      5.09      0.00
    0.00      0.00      2.59      0.00
    0.00      0.00      1.36      0.00
    0.00      0.00      3.95      0.00
    0.00      0.00      2.32      0.00
    0.00      0.00      4.42      0.00
    0.00      0.00      5.04      0.48
    0.00      0.00      2.55      0.00
    0.00      0.00      2.82      0.00
    0.00      0.00      2.74      0.00
^C
kollijoginaidu_b190605cs:~$ 
```

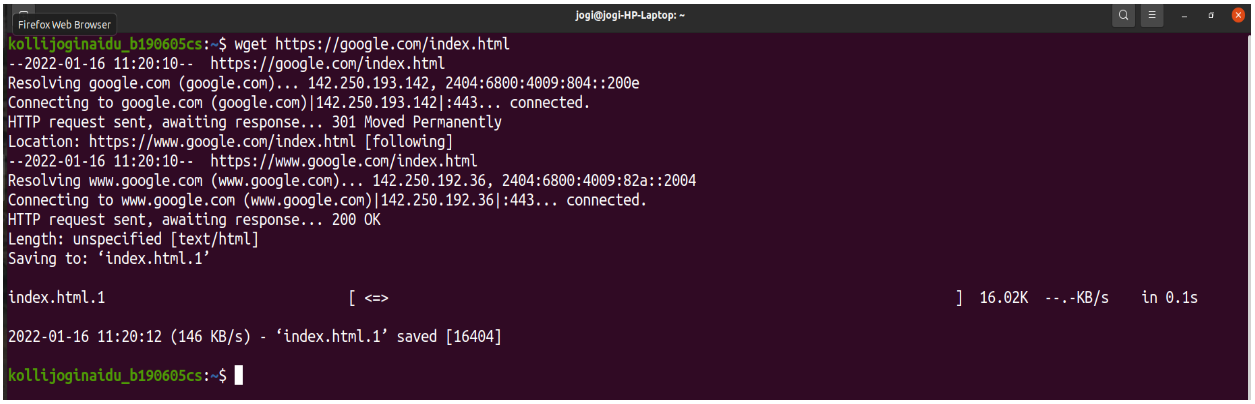
11.wget:

The command is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process.

General syntax:

wget [*option*] [*URL*]

The following image will illustrate the basic understanding of above command:



```
kollijoginaidu_b190605cs:~$ wget https://google.com/index.html
--2022-01-16 11:20:10--  https://google.com/index.html
Resolving google.com (google.com)... 142.250.193.142, 2404:6800:4009:804::200e
Connecting to google.com (google.com)|142.250.193.142|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com/index.html [following]
--2022-01-16 11:20:10--  https://www.google.com/index.html
Resolving www.google.com (www.google.com)... 142.250.192.36, 2404:6800:4009:82a::2004
Connecting to www.google.com (www.google.com)|142.250.192.36|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.1’

index.html.1                          [ <=>                                                            ]  16.02K  --.-KB/s    in 0.1s

2022-01-16 11:20:12 (146 KB/s) - ‘index.html.1’ saved [16404]

kollijoginaidu_b190605cs:~$ 
```

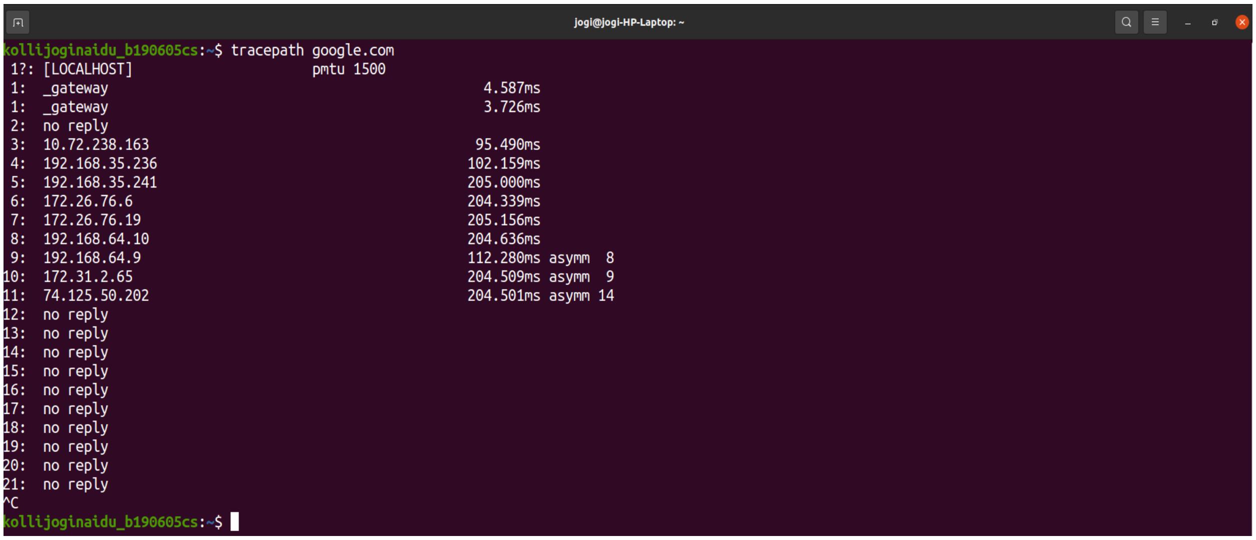
To know more about the ifconfig command, type: **man wget**

12.tracepath:

It is similar to traceroute but it does not require root privileges and it is installed by default.

General syntax:

```
tracepath  [-n] [-b] [-l pktlen] [-m max_hops] [-p port] destination
```



```
kollijoginaidu_b190605cs:~$ tracepath google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                              4.587ms
 1:  _gateway                                              3.726ms
 2:  no reply
 3:  10.72.238.163                                        95.490ms
 4:  192.168.35.236                                      102.159ms
 5:  192.168.35.241                                      205.000ms
 6:  172.26.76.6                                         204.339ms
 7:  172.26.76.19                                        205.156ms
 8:  192.168.64.10                                       204.636ms
 9:  192.168.64.9                                        112.280ms asymm  8
10:  172.31.2.65                                         204.509ms asymm  9
11:  74.125.50.202                                       204.501ms asymm 14
12:  no reply
13:  no reply
14:  no reply
15:  no reply
16:  no reply
17:  no reply
18:  no reply
19:  no reply
20:  no reply
21:  no reply
^C
kollijoginaidu_b190605cs:~$
```