CS3009D: NETWORKS LABORATORY
(EXPERIMENT 1)

Name: BHUKYA VASANTH KUMAR	Batch: A
Roll Number: B180441CS	Date: 24th December 2021

Use the following tools to explore and summarize the network environment available in your system:

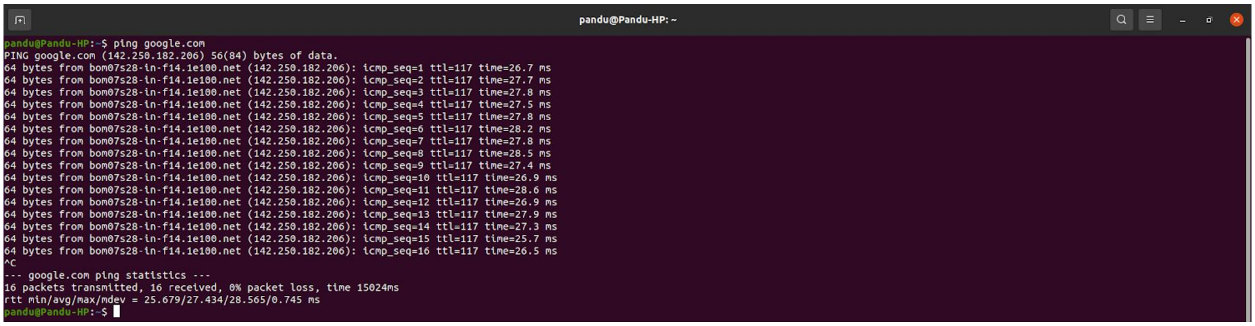
1. ping
2. tracert/traceroute
3. ip/ifconfig/ipconfig
4. dig/nslookup/host
5. whois
6. route
7. tcpdump
8. netstat/ss
9. dstat
10. ifstat
11. wget

1. ping

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. It is used to check whether a network is available and if a host is reachable. With this command, you can check if a server is up and running. When you "ping" a remote short, your machine starts sending ICMP (Internet Control Message Protocol) echo requests and waits for a response. If the connection is established, you'll receive an echo reply for every request. The output of the ping command contains the amount of time it takes for every packet to reach its destination and return. Also in the terminal, it keeps printing responses until it is stopped.

Ex:

```
ping google.com
ping nitc.ac.in
```



```
pandu@Pandu-HP:~$ ping google.com
PING google.com (142.250.182.206) 56(84) bytes of data.
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=1 ttl=117 time=26.7 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=2 ttl=117 time=27.7 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=3 ttl=117 time=27.8 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=4 ttl=117 time=27.5 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=5 ttl=117 time=27.8 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=6 ttl=117 time=28.2 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=7 ttl=117 time=27.8 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=8 ttl=117 time=28.5 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=9 ttl=117 time=27.4 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=10 ttl=117 time=26.9 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=11 ttl=117 time=28.6 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=12 ttl=117 time=26.9 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=13 ttl=117 time=27.9 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=14 ttl=117 time=27.3 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=15 ttl=117 time=25.7 ms
64 bytes from bom07s28-in-f14.1e100.net (142.250.182.206): icmp_seq=16 ttl=117 time=26.5 ms
^C
--- google.com ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15024ms
rtt min/avg/max/mdev = 25.679/27.434/28.565/0.745 ms
pandu@Pandu-HP:~$
```

Here,

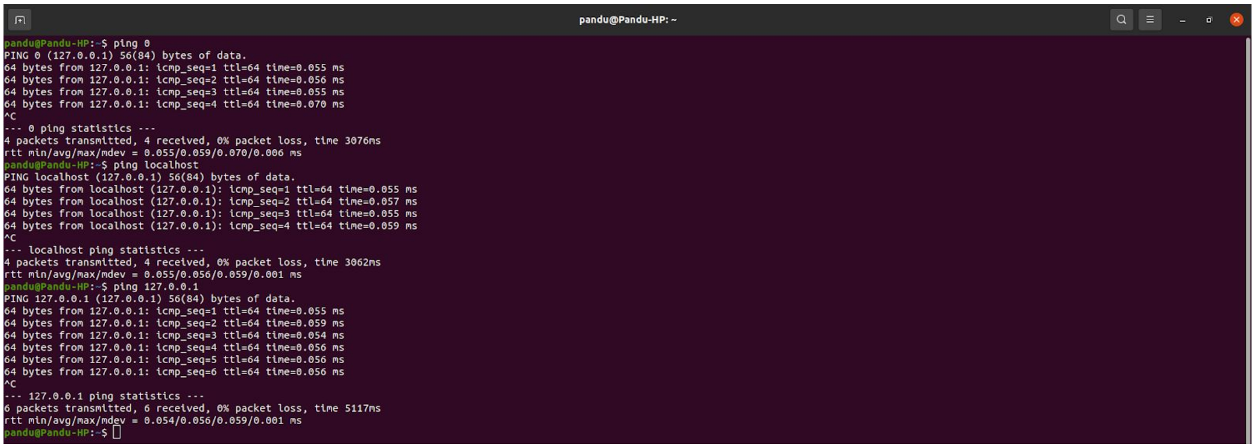
ttl = TTL (Time to Live) represents the number of network hops a packet can take before a router discards it.

icmp_seq = The sequence number of each ICMP packet. Increase by one for every echo request.

time = The time it took for a packet to reach its destination and comes back to the source. Expressed in milliseconds.

from = The destination and its IP address.

Note: You can ping to localhost using
ping 0 / ping localhost / ping 127.0.0.1



```
pandu@Pandu-HP:~$ ping 0
PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.056 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.070 ms
^C
--- 0 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.055/0.059/0.070/0.006 ms
pandu@Pandu-HP:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.055 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.059 ms
^C
--- localhost ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3062ms
rtt min/avg/max/mdev = 0.055/0.056/0.059/0.001 ms
pandu@Pandu-HP:~$ 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=0.055 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.054 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=0.056 ms
^C
--- 127.0.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5117ms
rtt min/avg/max/mdev = 0.054/0.056/0.059/0.001 ms
pandu@Pandu-HP:~$
```

OUTPUTS

Case1: If we did not get any reply from the destination then it means that there is no network connectivity between host and server/host.

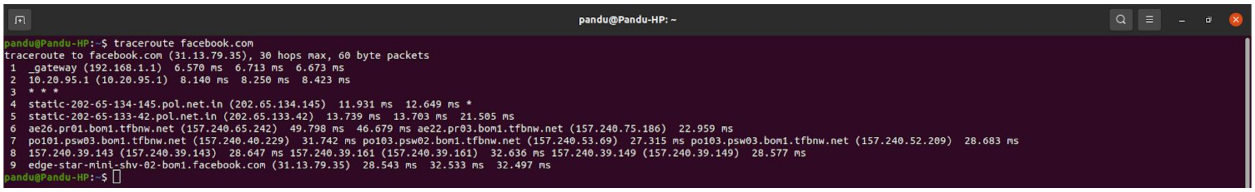
Case2: If the output is “request timed out” then it means the host is down or blocking our ICMP requests.

Case3: If the output is "destination not reachable” then it means that a route to the destination cannot be found.

2. tracert/traceroute

"traceroute" command in Linux prints the route that the packet takes to reach the host or destination. It displays details about all the hops that the packet visits in between i.e it displays IP addresses and the time it took between each hop. The main use of this tool is to find where the error lies in the network if a data packet is unable to reach the destination.

Ex: traceroute facebook.com



```
pandu@Pandu-HP:~$ traceroute facebook.com
traceroute to facebook.com (31.13.79.35), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  6.570 ms  6.713 ms  6.673 ms
 2  10.20.95.1 (10.20.95.1)  8.140 ms  8.250 ms  8.423 ms
 3  * * *
 4  static-202-65-134-145.pol.net.in (202.65.134.145)  11.931 ms  12.649 ms *
 5  static-202-65-133-42.pol.net.in (202.65.133.42)  13.739 ms  13.703 ms  21.505 ms
 6  ae26.pr01.bom1.tfbnw.net (157.240.65.242)  49.798 ms  46.679 ms ae22.pr03.bom1.tfbnw.net (157.240.75.186)  22.959 ms
 7  po101.psw03.bom1.tfbnw.net (157.240.40.229)  31.742 ms po103.psw02.bom1.tfbnw.net (157.240.53.69)  27.315 ms po103.psw03.bom1.tfbnw.net (157.240.52.209)  28.683 ms
 8  157.240.39.143 (157.240.39.143)  28.647 ms 157.240.39.161 (157.240.39.161)  32.636 ms 157.240.39.149 (157.240.39.149)  28.577 ms
 9  edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35)  28.543 ms  32.533 ms  32.497 ms
pandu@Pandu-HP:~$ 
```

3. ip/ifconfig/ipconfig

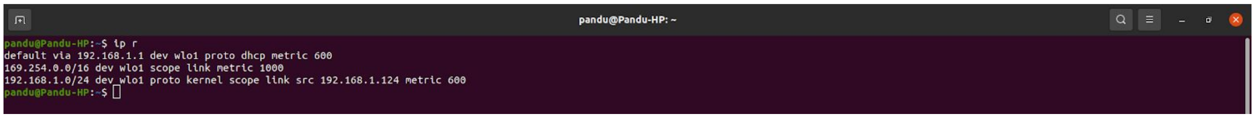
IP: IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your network and all over the world.

ipconfig stands for Internet Protocol Configuration, while ifconfig stands for Interface Configuration. It is often used for troubleshooting network connectivities. It's generally used to display the TCP/IP address of the system. Ifconfig is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning.

In ubuntu install them using : sudo apt-get install net-tools

ip r

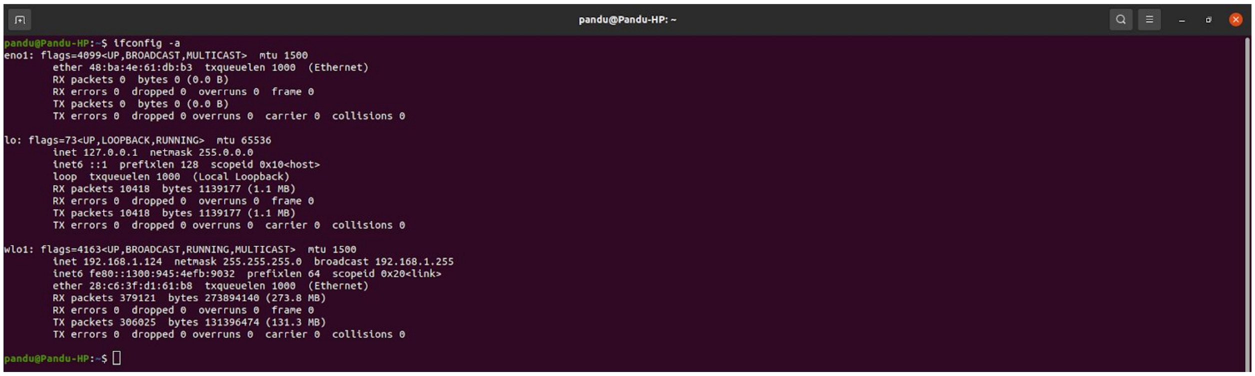
Find the gateway address in the starting line. 192.168.1.1 is the default gateway in the given image.



```
pandu@Pandu-HP:~$ ip r
default via 192.168.1.1 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.1.0/24 dev wlo1 proto kernel scope link src 192.168.1.124 metric 600
pandu@Pandu-HP:~$ 
```

Ifconfig -a

Check for IPv4 address beside inet below wlo1, 192.168.1.124 is the IP address in the given image.



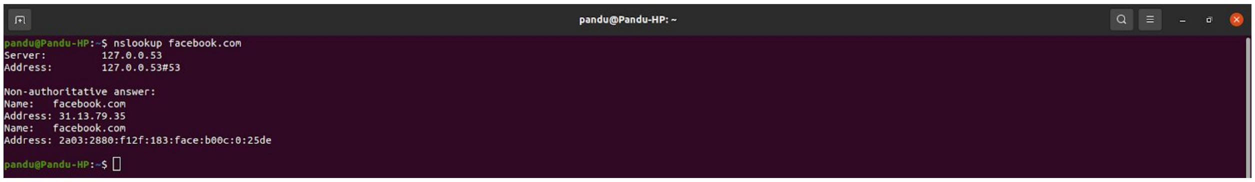
```
pandu@Pandu-HP:~$ ifconfig -a
eno1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:ba:4e:61:db:b3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 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 10418  bytes 1139177 (1.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10418  bytes 1139177 (1.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::1300:945:4efb:9032  prefixlen 64  scopeid 0x20<link>
        ether 28:c6:3f:d1:61:b8  txqueuelen 1000  (Ethernet)
        RX packets 379121  bytes 273894140 (273.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 306025  bytes 131396474 (131.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

pandu@Pandu-HP:~$ 
```

4. dig/nslookup/host

nslookup is a command-line administrative tool for testing and troubleshooting DNS servers (Domain Name Server). It is used to query specific DNS resource records (RR) as well.

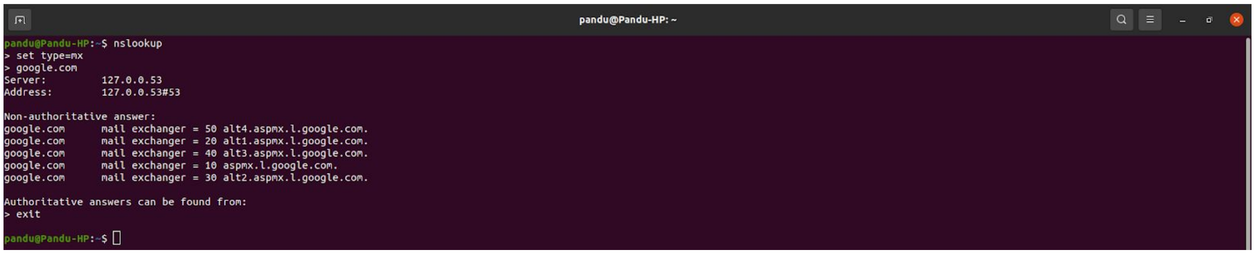
DNS: So basically, DNS is the phonebook of the internet. We can access information online through domain names, say linkedin.com or hackerrank.com. Web browsers interact through IP addresses. So, DNS translates domain names to IP addresses, so that the browsers can load internet resources.
Host by default is used to determine what domain a particular IP address resolves to.

Ex: nslookup facebook.com



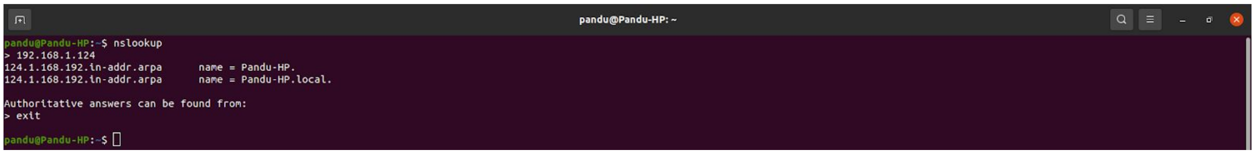
```
pandu@Pandu-HP:~$ nslookup facebook.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   facebook.com
Address: 31.13.79.35
Name:   facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de

pandu@Pandu-HP:~$ 
```

NOTE: Type nslookup without any arguments to enter into Interactive mode so that you can set the servers to mail servers.
> set type=mx
> google.com



```
pandu@Pandu-HP:~$ nslookup
> set type=mx
> google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
google.com      mail exchanger = 50 alt4.aspmx.l.google.com.
google.com      mail exchanger = 20 alt1.aspmx.l.google.com.
google.com      mail exchanger = 40 alt3.aspmx.l.google.com.
google.com      mail exchanger = 10 aspmx.l.google.com.
google.com      mail exchanger = 30 alt2.aspmx.l.google.com.

Authoritative answers can be found from:
> exit

pandu@Pandu-HP:~$ 
```

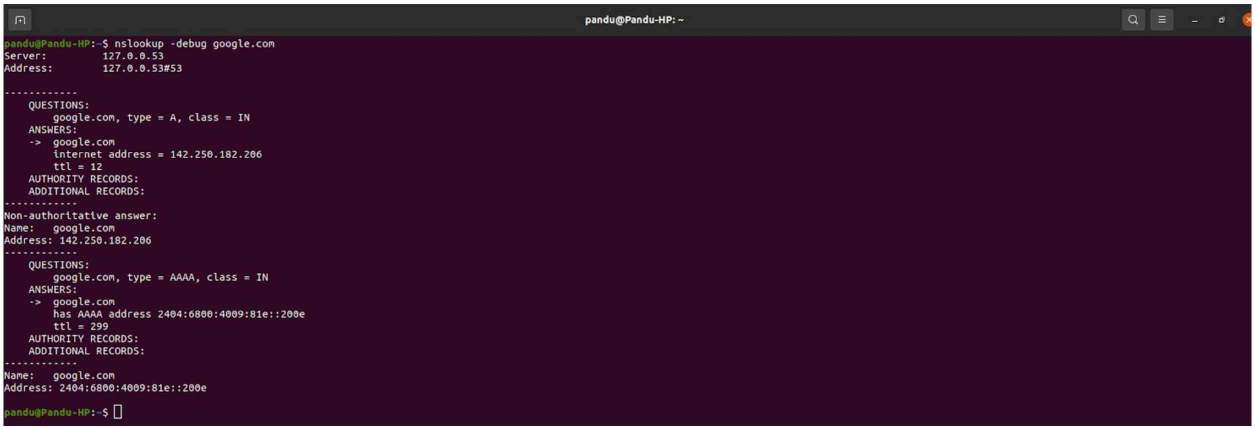
NOTE: Enter your ip address, to perform Reverse DNS.



```
pandu@Pandu-HP:~$ nslookup
> 192.168.1.124
124.1.168.192.in-addr.arpa      name = Pandu-HP.
124.1.168.192.in-addr.arpa      name = Pandu-HP.local.

Authoritative answers can be found from:
> exit

pandu@Pandu-HP:~$ 
```

NOTE : nslookup -debug google.com

You can troubleshoot DNS problems to perform DNS lookups, the answers for questions will be displayed.



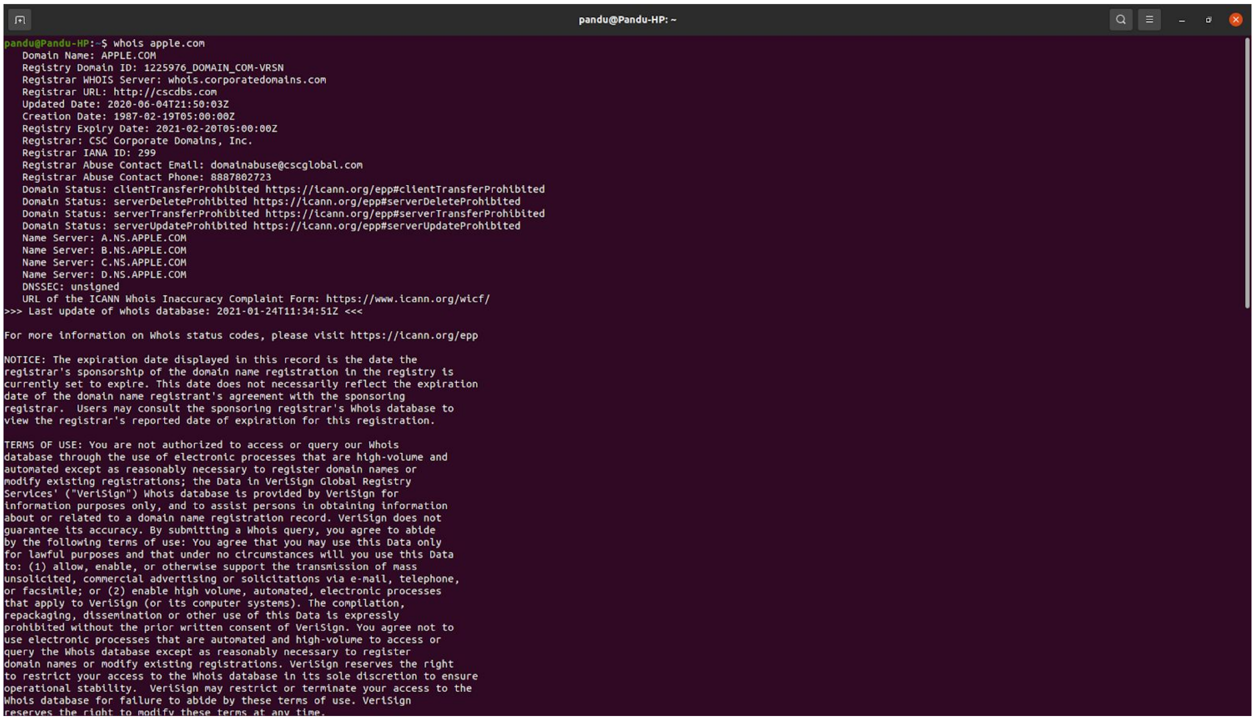
```
pandu@Pandu-HP:~$ nslookup -debug google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        google.com, type = A, class = IN
    ANSWERS:
    ->  google.com
        internet address = 142.250.182.206
        ttl = 12
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   google.com
Address: 142.250.182.206
------------
    QUESTIONS:
        google.com, type = AAAA, class = IN
    ANSWERS:
    ->  google.com
        has AAAA address 2404:6800:4009:81e::200e
        ttl = 299
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Name:   google.com
Address: 2404:6800:4009:81e::200e

pandu@Pandu-HP:~$ 
```

5. whois

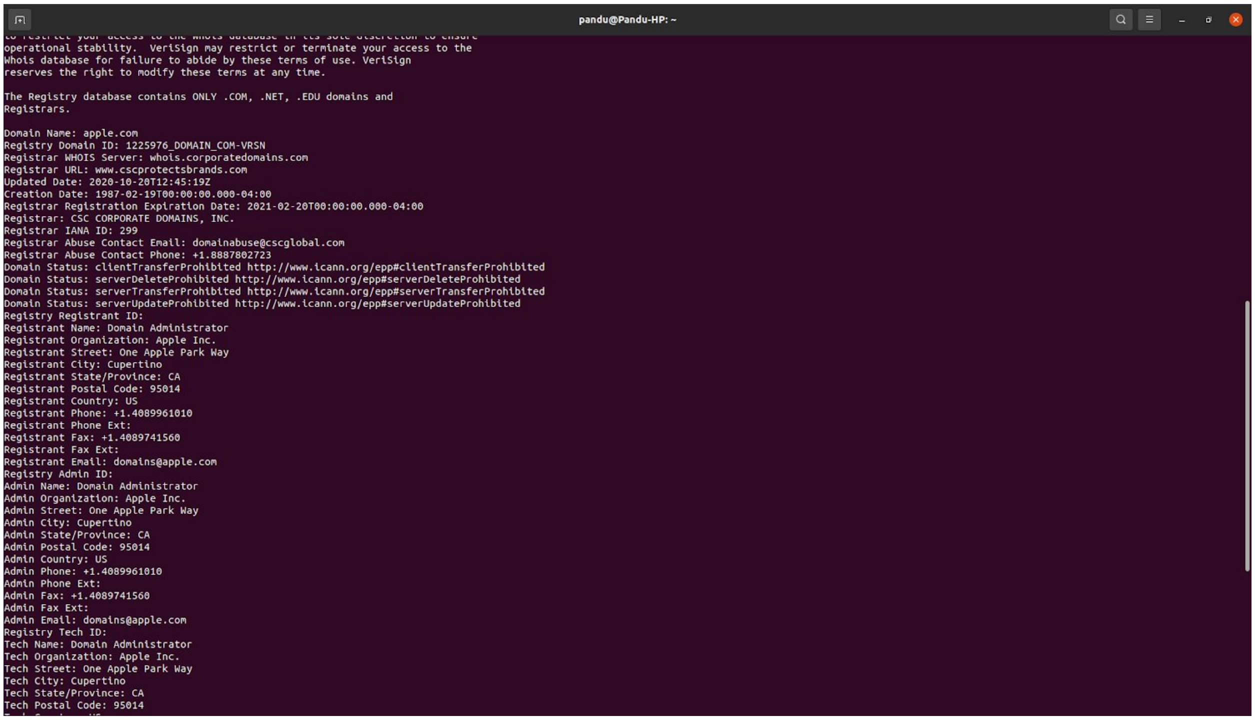
The whois system is a listing of records that contain details about the ownership of domains and the owners. The Internet corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership, but the list of records is held by many companies, known as registries. Anyone can query the list of records.
A whois record contains contact information with the person, company or other entity that registered the DOMAIN name.

Install it using : sudo install whois

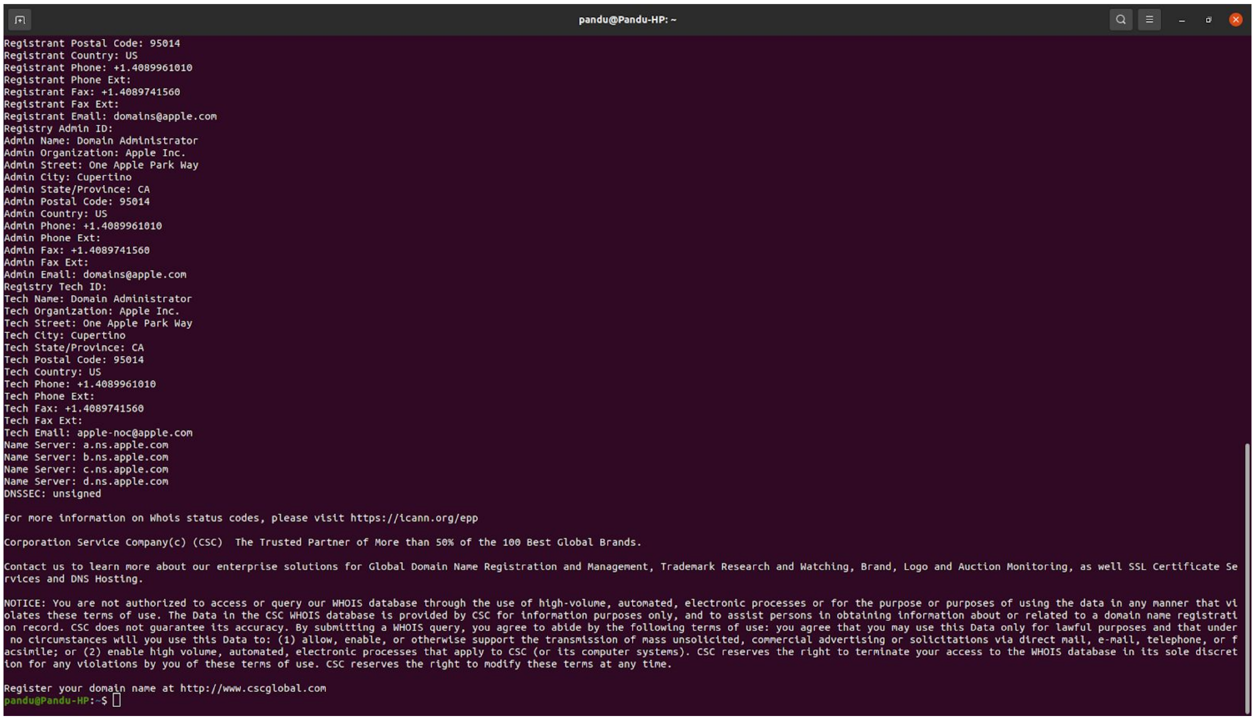
Ex: whois apple.com



```
pandu@Pandu-HP:~$ whois apple.com
   Domain Name: APPLE.COM
   Registry Domain ID: 1225976_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2020-06-04T21:50:03Z
   Creation Date: 1987-02-19T05:00:00Z
   Registry Expiry Date: 2021-02-20T05:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   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: A.NS.APPLE.COM
   Name Server: B.NS.APPLE.COM
   Name Server: C.NS.APPLE.COM
   Name Server: D.NS.APPLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-01-24T11:34:51Z <<<

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
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```



```
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

Domain Name: apple.com
Registry Domain ID: 1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-20T12:45:19Z
Creation Date: 1987-02-19T00:00:00.000-04:00
Registrar Registration Expiration Date: 2021-02-20T00:00:00.000-04:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Apple Inc.
Registrant Street: One Apple Park Way
Registrant City: Cupertino
Registrant State/Province: CA
Registrant Postal Code: 95014
Registrant Country: US
Registrant Phone: +1.4089961010
Registrant Phone Ext:
Registrant Fax: +1.4089741560
Registrant Fax Ext:
Registrant Email: domains@apple.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Apple Inc.
Admin Street: One Apple Park Way
Admin City: Cupertino
Admin State/Province: CA
Admin Postal Code: 95014
Admin Country: US
Admin Phone: +1.4089961010
Admin Phone Ext:
Admin Fax: +1.4089741560
Admin Fax Ext:
Admin Email: domains@apple.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Apple Inc.
Tech Street: One Apple Park Way
Tech City: Cupertino
Tech State/Province: CA
Tech Postal Code: 95014
```



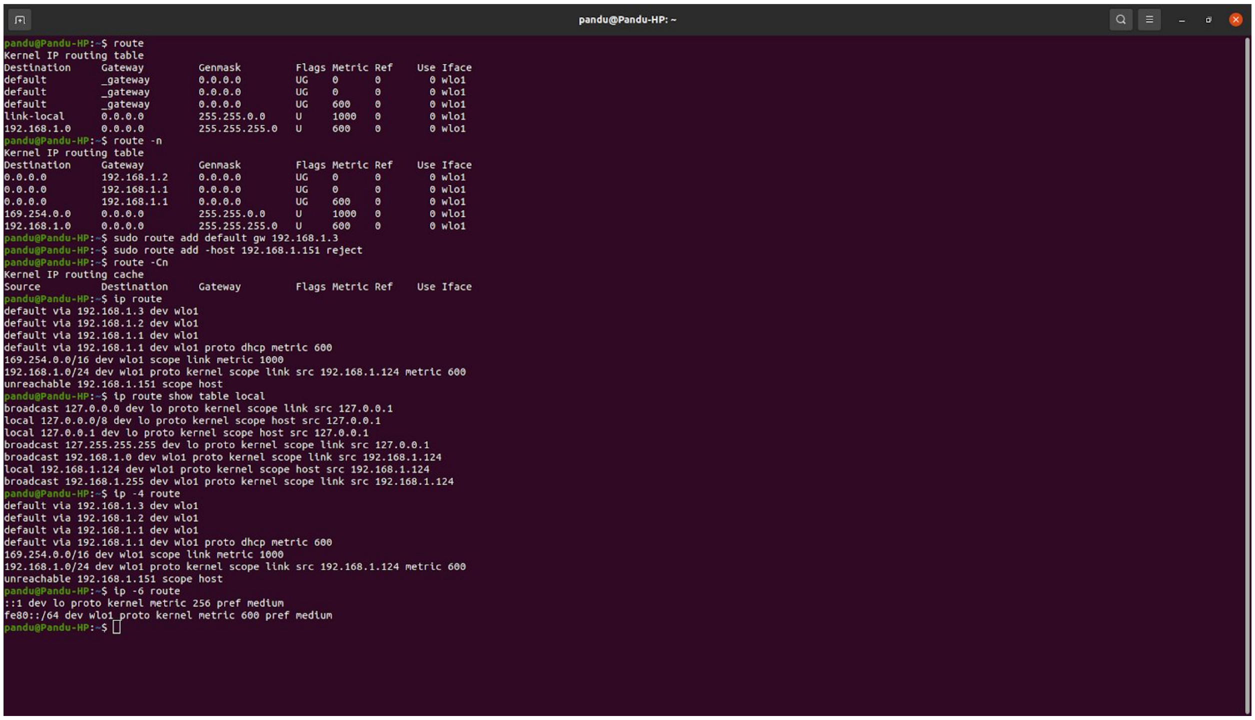
```
Registrant Postal Code: 95014
Registrant Country: US
Registrant Phone: +1.4089961010
Registrant Phone Ext:
Registrant Fax: +1.4089741560
Registrant Fax Ext:
Registrant Email: domains@apple.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Apple Inc.
Admin Street: One Apple Park Way
Admin City: Cupertino
Admin State/Province: CA
Admin Postal Code: 95014
Admin Country: US
Admin Phone: +1.4089961010
Admin Phone Ext:
Admin Fax: +1.4089741560
Admin Fax Ext:
Admin Email: domains@apple.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: Apple Inc.
Tech Street: One Apple Park Way
Tech City: Cupertino
Tech State/Province: CA
Tech Postal Code: 95014
Tech Country: US
Tech Phone: +1.4089961010
Tech Phone Ext:
Tech Fax: +1.4089741560
Tech Fax Ext:
Tech Email: apple-noc@apple.com
Name Server: a.ns.apple.com
Name Server: b.ns.apple.com
Name Server: c.ns.apple.com
Name Server: d.ns.apple.com
DNSSEC: unsigned

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

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and Auction Monitoring, as well SSL Certificate Se
rvices and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or purposes of using the data in any manner that vi
olates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes only, and to assist persons in obtaining information about or related to a domain name registrati
on record. CSC does not guarantee its accuracy. By submitting a WHOIS query, you agree to abide by the following terms of use: you agree that you may use this Data only for lawful purposes and that under
 no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via direct mail, e-mail, telephone, or f
acsimile; or (2) enable high volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserves the right to terminate your access to the WHOIS database in its sole discret
ion for any violations by you of these terms of use. CSC reserves the right to modify these terms at any time.

Register your domain name at http://www.cscglobal.com
pandu@Pandu-HP:~$ 
```

6. route (not done yet)

ROUTING TABLE : A routing table is a file containing information on how the information or packets should be transferred: the network path to all nodes or devices within a network. It is a map used by routers and gateways to track paths. The hop-by-hop routing is widely used, the packet contains the routing table to reach the next hop, once reached, it will read the routing table again to reach the next hop.

Using the route command you can communicate with subnets and different networks, you can also block the traffic between networks or devices by modifying the routing table.

Ex: route : To display routing table entries.
Ex: route -n : To display routing tables in full numerical entities.
Ex: sudo route add default gw 169.154.0.0 : To add default gateway.
Ex: sudo route add -host 192.168.1.151 reject : To reject a host/network.
Ex: route -Cn : To list routing cache information of Device
Ex: ip route : To get details of IP routing table
Ex: ip route show table local : To get details of local table with destination of localhost.
Ex: ip -4/-6 route : To get details of IPv4/IPv6 details.



```
pandu@Pandu-HP:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    0      0        0 wlo1
default         _gateway        0.0.0.0         UG    0      0        0 wlo1
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
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
pandu@Pandu-HP:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.2     0.0.0.0         UG    0      0        0 wlo1
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 wlo1
0.0.0.0         192.168.1.1     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
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
pandu@Pandu-HP:~$ sudo route add default gw 192.168.1.3
pandu@Pandu-HP:~$ sudo route add -host 192.168.1.151 reject
pandu@Pandu-HP:~$ route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
pandu@Pandu-HP:~$ ip route
default via 192.168.1.3 dev wlo1
default via 192.168.1.2 dev wlo1
default via 192.168.1.1 dev wlo1
default via 192.168.1.1 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.1.0/24 dev wlo1 proto kernel scope link src 192.168.1.124 metric 600
unreachable 192.168.1.151 scope host
pandu@Pandu-HP:~$ ip route show table local
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
broadcast 192.168.1.0 dev wlo1 proto kernel scope link src 192.168.1.124
local 192.168.1.124 dev wlo1 proto kernel scope host src 192.168.1.124
broadcast 192.168.1.255 dev wlo1 proto kernel scope link src 192.168.1.124
pandu@Pandu-HP:~$ ip -4 route
default via 192.168.1.3 dev wlo1
default via 192.168.1.2 dev wlo1
default via 192.168.1.1 dev wlo1
default via 192.168.1.1 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.1.0/24 dev wlo1 proto kernel scope link src 192.168.1.124 metric 600
unreachable 192.168.1.151 scope host
pandu@Pandu-HP:~$ ip -6 route
::1 dev lo proto kernel metric 256 pref medium
fe80::/64 dev wlo1 proto kernel metric 600 pref medium
pandu@Pandu-HP:~$
```

7. tcpdump

“tcpdump” tool allows you to capture and analyze network traffic such as TCP/IP packets going through the system. Normally used to troubleshoot network issues, also used as a security tool. It scans from all OSI layers (1-7) and saves the captured information as .pcap file which can be viewed on WIRESHARK or through the command tool itself.

Ex: sudo tcpdump

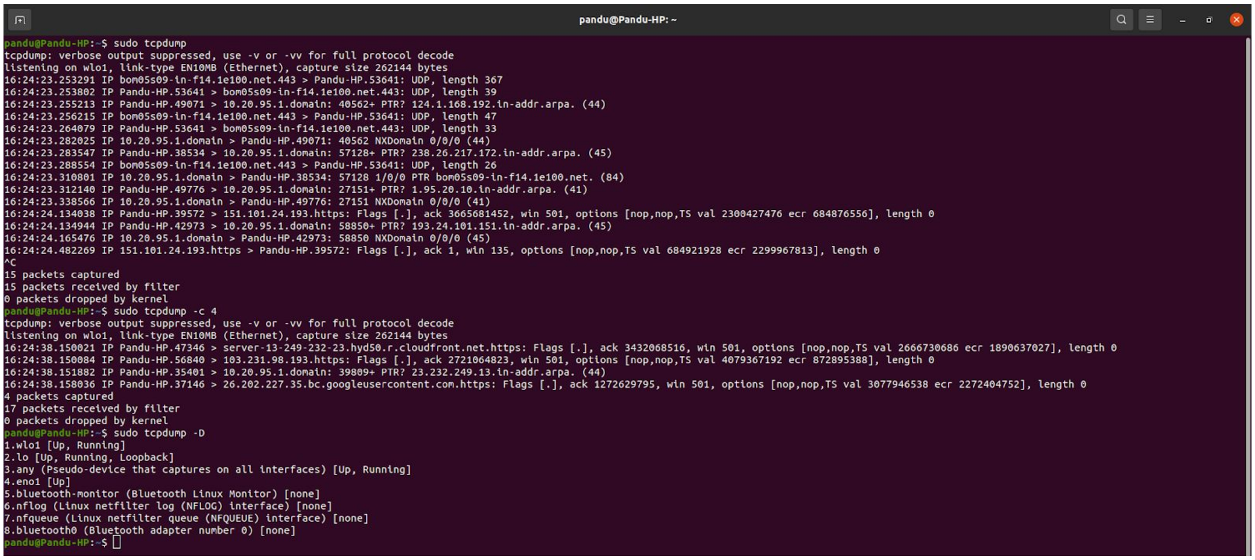
It will capture packets from the current interface of the network through which the system is connected to the internet.

Ex: sudo tcpdump -c 4

It will capture only 4 packets from the interface.

Ex: sudo tcpdump -D

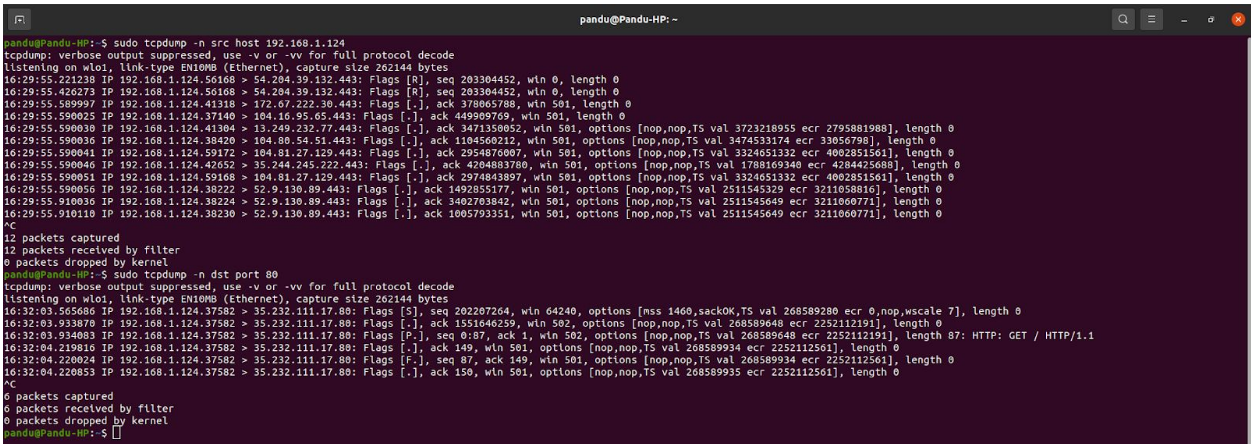
It will print all the list of available networks that this tool can capture packets from.



```
pandu@Pandu-HP:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
16:24:23.253291 IP bom05s09-in-f14.1e100.net.443 > Pandu-HP.53641: UDP, length 367
16:24:23.253802 IP Pandu-HP.53641 > bom05s09-in-f14.1e100.net.443: UDP, length 39
16:24:23.255213 IP Pandu-HP.49071 > 10.20.95.1.domain: 40562+ PTR? 124.1.168.192.in-addr.arpa. (44)
16:24:23.256215 IP bom05s09-in-f14.1e100.net.443 > Pandu-HP.53641: UDP, length 47
16:24:23.264079 IP Pandu-HP.53641 > bom05s09-in-f14.1e100.net.443: UDP, length 33
16:24:23.282025 IP 10.20.95.1.domain > Pandu-HP.49071: 40562 NXDomain 0/0/0 (44)
16:24:23.283547 IP Pandu-HP.38534 > 10.20.95.1.domain: 57128+ PTR? 238.26.217.172.in-addr.arpa. (45)
16:24:23.288554 IP bom05s09-in-f14.1e100.net.443 > Pandu-HP.53641: UDP, length 26
16:24:23.310801 IP 10.20.95.1.domain > Pandu-HP.38534: 57128 1/0/0 PTR bom05s09-in-f14.1e100.net. (84)
16:24:23.312140 IP Pandu-HP.49776 > 10.20.95.1.domain: 27151+ PTR? 1.95.20.10.in-addr.arpa. (41)
16:24:23.338566 IP 10.20.95.1.domain > Pandu-HP.49776: 27151 NXDomain 0/0/0 (41)
16:24:24.134038 IP Pandu-HP.39572 > 151.101.24.193.https: Flags [.], ack 3665681452, win 501, options [nop,nop,TS val 2300427476 ecr 684876556], length 0
16:24:24.134944 IP Pandu-HP.42973 > 10.20.95.1.domain: 58850+ PTR? 193.24.101.151.in-addr.arpa. (45)
16:24:24.165476 IP 10.20.95.1.domain > Pandu-HP.42973: 58850 NXDomain 0/0/0 (45)
16:24:24.482269 IP 151.101.24.193.https > Pandu-HP.39572: Flags [.], ack 1, win 135, options [nop,nop,TS val 684921928 ecr 2299967813], length 0
^C
15 packets captured
15 packets received by filter
0 packets dropped by kernel
pandu@Pandu-HP:~$ sudo tcpdump -c 4
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
16:24:38.150021 IP Pandu-HP.47346 > server-13-249-232-23.hyd50.r.cloudfront.net.https: Flags [.], ack 3432068516, win 501, options [nop,nop,TS val 2666730686 ecr 1890637027], length 0
16:24:38.150084 IP Pandu-HP.56840 > 103.231.98.193.https: Flags [.], ack 2721064823, win 501, options [nop,nop,TS val 4079367192 ecr 872895388], length 0
16:24:38.151882 IP Pandu-HP.35401 > 10.20.95.1.domain: 39809+ PTR? 23.232.249.13.in-addr.arpa. (44)
16:24:38.158036 IP Pandu-HP.37146 > 26.202.227.35.bc.googleusercontent.com.https: Flags [.], ack 1272629795, win 501, options [nop,nop,TS val 3077946538 ecr 2272404752], length 0
4 packets captured
17 packets received by filter
0 packets dropped by kernel
pandu@Pandu-HP:~$ sudo tcpdump -D
1.wlo1 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.eno1 [Up]
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]
6.nflog (Linux netfilter log (NFLOG) interface) [none]
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
8.bluetooth0 (Bluetooth adapter number 0) [none]
pandu@Pandu-HP:~$ 
```

Ex: sudo tcpdump -n host 142.250.182.206
To capture packets related to Specific host

Ex: sudo tcpdump -n src host 192.168.1.124 : packets from source host
sudo tcpdump -n dst port 80 : all packets to port 80



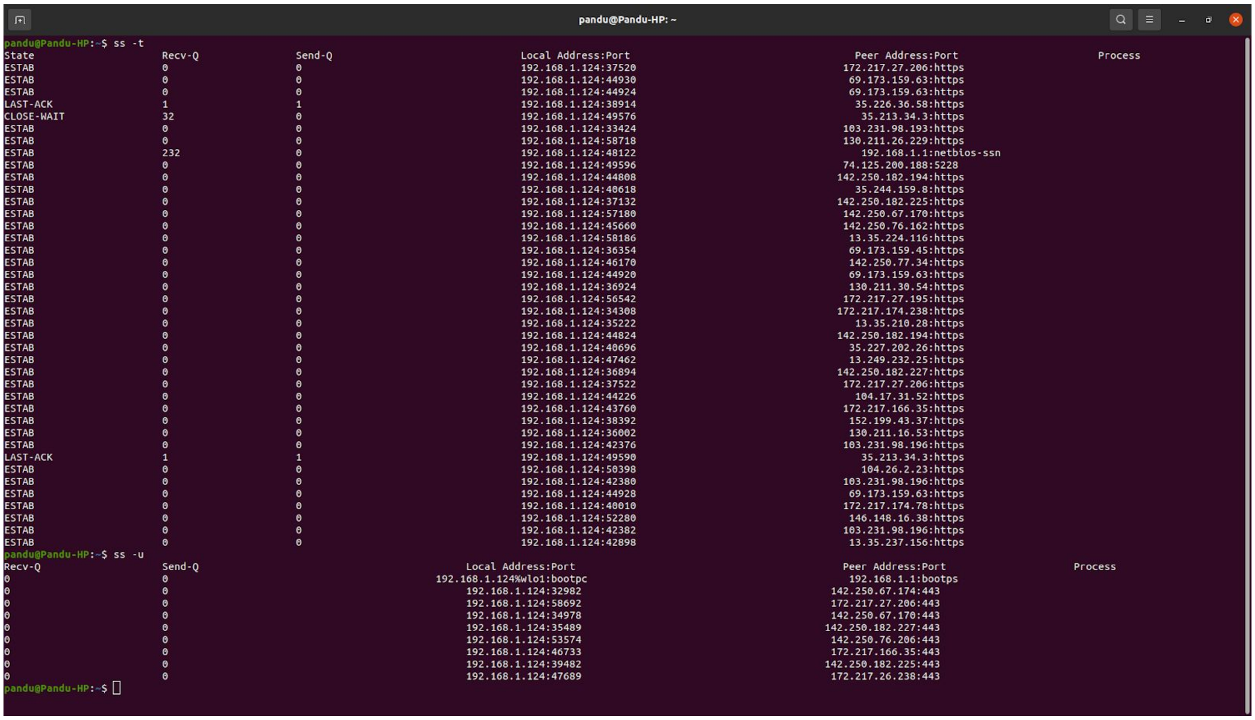
```
pandu@Pandu-HP:~$ sudo tcpdump -n src host 192.168.1.124
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
16:29:55.221238 IP 192.168.1.124.56168 > 54.204.39.132.443: Flags [R], seq 203304452, win 0, length 0
16:29:55.426273 IP 192.168.1.124.56168 > 54.204.39.132.443: Flags [R], seq 203304452, win 0, length 0
16:29:55.589997 IP 192.168.1.124.41318 > 172.67.222.30.443: Flags [.], ack 378065788, win 501, length 0
16:29:55.590025 IP 192.168.1.124.37140 > 104.16.95.65.443: Flags [.], ack 449909769, win 501, length 0
16:29:55.590030 IP 192.168.1.124.41304 > 13.249.232.77.443: Flags [.], ack 3471350052, win 501, options [nop,nop,TS val 3723218955 ecr 2795881988], length 0
16:29:55.590036 IP 192.168.1.124.38420 > 104.80.54.51.443: Flags [.], ack 1104560212, win 501, options [nop,nop,TS val 3474533174 ecr 33056798], length 0
16:29:55.590041 IP 192.168.1.124.59172 > 104.81.27.129.443: Flags [.], ack 2954876007, win 501, options [nop,nop,TS val 3324651332 ecr 4002851561], length 0
16:29:55.590046 IP 192.168.1.124.42652 > 35.244.245.222.443: Flags [.], ack 4204883780, win 501, options [nop,nop,TS val 1788169340 ecr 4284425688], length 0
16:29:55.590051 IP 192.168.1.124.59168 > 104.81.27.129.443: Flags [.], ack 2974843897, win 501, options [nop,nop,TS val 3324651332 ecr 4002851561], length 0
16:29:55.590056 IP 192.168.1.124.38222 > 52.9.130.89.443: Flags [.], ack 1492855177, win 501, options [nop,nop,TS val 2511545329 ecr 3211058816], length 0
16:29:55.910036 IP 192.168.1.124.38224 > 52.9.130.89.443: Flags [.], ack 3402703842, win 501, options [nop,nop,TS val 2511545649 ecr 3211060771], length 0
16:29:55.910110 IP 192.168.1.124.38230 > 52.9.130.89.443: Flags [.], ack 1005793351, win 501, options [nop,nop,TS val 2511545649 ecr 3211060771], length 0
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
pandu@Pandu-HP:~$ sudo tcpdump -n dst port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes
16:32:03.565686 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [S], seq 202207264, win 64240, options [mss 1460,sackOK,TS val 268589280 ecr 0,nop,wscale 7], length 0
16:32:03.933870 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [.], ack 1551646259, win 502, options [nop,nop,TS val 268589648 ecr 2252112191], length 0
16:32:03.934083 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [P.], seq 0:87, ack 1, win 502, options [nop,nop,TS val 268589648 ecr 2252112191], length 87: HTTP: GET / HTTP/1.1
16:32:04.219816 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [.], ack 149, win 501, options [nop,nop,TS val 268589934 ecr 2252112561], length 0
16:32:04.220024 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [F.], seq 87, ack 149, win 501, options [nop,nop,TS val 268589934 ecr 2252112561], length 0
16:32:04.220853 IP 192.168.1.124.37582 > 35.232.111.17.80: Flags [.], ack 150, win 501, options [nop,nop,TS val 268589935 ecr 2252112561], length 0
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
pandu@Pandu-HP:~$ 
```

8. netstat/ss

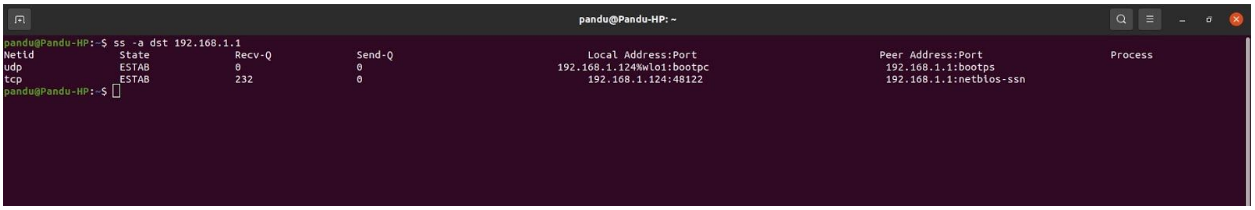
netstat is a command tool which displays network connections for TCP/UDP and stats for Interfaces, Network protocols, routing tables, etc. ss replaces netstat. ss command tool which dumps socket stats and displays information similarly but it is faster than netstat. With ss, we get detailed information about how Linux is communicating with other machines, networks, details about network stats, network protocols, linux socket connections. So, using this information, it’s easy to troubleshoot network issues.

Ex: ss	: Displays all connections
Ex: ss -a	: Displays non listening connections
Ex: ss -l	: Displays current listening connections
Ex: ss -t	: Displays TCP connections
Ex: ss -u	: Displays UDP connections
Ex: ss -x	: Displays UNIX connections
Ex: ss -s	: Displays summary stats
Ex: ss -t -r state established	: Displays sockets by state
Ex: ss -a dst 192.168.1.1	: Displays connections to specific address

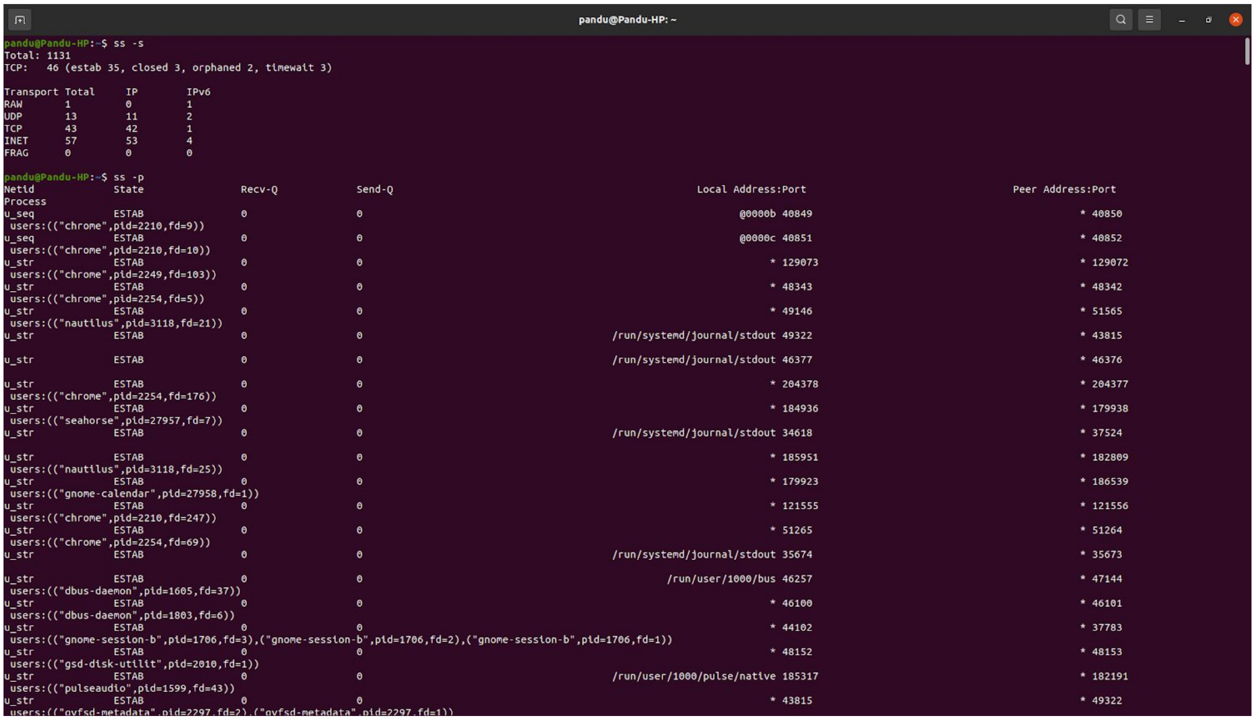
A listening connection means the socket is waiting for connection. A non listening socket implies the connection is already made.



```
pandu@Pandu-HP:~$ ss -t
State            Recv-Q        Send-Q                  Local Address:Port                    Peer Address:Port             Process
ESTAB            0             0                       192.168.1.124:37520                  172.217.27.206:https
ESTAB            0             0                       192.168.1.124:44930                   69.173.159.63:https
ESTAB            0             0                       192.168.1.124:44924                   69.173.159.63:https
LAST-ACK         1             1                       192.168.1.124:38914                    35.226.36.58:https
CLOSE-WAIT       32            0                       192.168.1.124:49576                     35.213.34.3:https
ESTAB            0             0                       192.168.1.124:33424                  103.231.98.193:https
ESTAB            0             0                       192.168.1.124:58718                  130.211.26.229:https
ESTAB            232           0                       192.168.1.124:48122                     192.168.1.1:netbios-ssn
ESTAB            0             0                       192.168.1.124:49596                  74.125.200.188:5228
ESTAB            0             0                       192.168.1.124:44808                 142.250.182.194:https
ESTAB            0             0                       192.168.1.124:40618                    35.244.159.8:https
ESTAB            0             0                       192.168.1.124:37132                 142.250.182.225:https
ESTAB            0             0                       192.168.1.124:57180                  142.250.67.170:https
ESTAB            0             0                       192.168.1.124:45660                  142.250.76.162:https
ESTAB            0             0                       192.168.1.124:58186                   13.35.224.116:https
ESTAB            0             0                       192.168.1.124:36354                   69.173.159.45:https
ESTAB            0             0                       192.168.1.124:46170                   142.250.77.34:https
ESTAB            0             0                       192.168.1.124:44920                   69.173.159.63:https
ESTAB            0             0                       192.168.1.124:36924                   130.211.30.54:https
ESTAB            0             0                       192.168.1.124:56542                  172.217.27.195:https
ESTAB            0             0                       192.168.1.124:34308                 172.217.174.238:https
ESTAB            0             0                       192.168.1.124:35222                    13.35.210.28:https
ESTAB            0             0                       192.168.1.124:44824                 142.250.182.194:https
ESTAB            0             0                       192.168.1.124:40696                   35.227.202.26:https
ESTAB            0             0                       192.168.1.124:47462                   13.249.232.25:https
ESTAB            0             0                       192.168.1.124:36894                 142.250.182.227:https
ESTAB            0             0                       192.168.1.124:37522                  172.217.27.206:https
ESTAB            0             0                       192.168.1.124:44226                    104.17.31.52:https
ESTAB            0             0                       192.168.1.124:43760                  172.217.166.35:https
ESTAB            0             0                       192.168.1.124:38392                   152.199.43.37:https
ESTAB            0             0                       192.168.1.124:36002                   130.211.16.53:https
ESTAB            0             0                       192.168.1.124:42376                  103.231.98.196:https
LAST-ACK         1             1                       192.168.1.124:49590                     35.213.34.3:https
ESTAB            0             0                       192.168.1.124:50398                     104.26.2.23:https
ESTAB            0             0                       192.168.1.124:42380                  103.231.98.196:https
ESTAB            0             0                       192.168.1.124:44928                   69.173.159.63:https
ESTAB            0             0                       192.168.1.124:40010                   172.217.174.78:https
ESTAB            0             0                       192.168.1.124:52280                   146.148.16.38:https
ESTAB            0             0                       192.168.1.124:42382                  103.231.98.196:https
ESTAB            0             0                       192.168.1.124:42898                   13.35.237.156:https
pandu@Pandu-HP:~$ ss -u
Recv-Q           Send-Q                      Local Address:Port                        Peer Address:Port               Process
0                0                      192.168.1.124%wlo1:bootpc                         192.168.1.1:bootps
0                0                           192.168.1.124:32982                       142.250.67.174:443
0                0                           192.168.1.124:58692                       172.217.27.206:443
0                0                           192.168.1.124:34978                       142.250.67.170:443
0                0                           192.168.1.124:35489                      142.250.182.227:443
0                0                           192.168.1.124:53574                       142.250.76.206:443
0                0                           192.168.1.124:46733                       172.217.166.35:443
0                0                           192.168.1.124:39482                      142.250.182.225:443
0                0                           192.168.1.124:47689                       172.217.26.238:443
pandu@Pandu-HP:~$ 
```



```
pandu@Pandu-HP:~$ ss -a dst 192.168.1.1
Netid          State          Recv-Q          Send-Q                    Local Address:Port                 Peer Address:Port            Process
udp            ESTAB          0               0                    192.168.1.124%wlo1:bootpc                192.168.1.1:bootps
tcp            ESTAB          232             0                         192.168.1.124:48122                 192.168.1.1:netbios-ssn
pandu@Pandu-HP:~$ 
```



```
pandu@Pandu-HP:~$ ss -s
Total: 1131
TCP:   46 (estab 35, closed 3, orphaned 2, timewait 3)

Transport Total     IP        IPv6
RAW       1         0         1
UDP       13        11        2
TCP       43        42        1
INET      57        53        4
FRAG      0         0         0

pandu@Pandu-HP:~$ ss -p
Netid             State               Recv-Q             Send-Q                                                 Local Address:Port                                 Peer Address:Port
Process
u_seq             ESTAB               0                  0                                                            @0000b 40849                                           * 40850
 users:(("chrome",pid=2210,fd=9))
u_seq             ESTAB               0                  0                                                            @0000c 40851                                           * 40852
 users:(("chrome",pid=2210,fd=10))
u_str             ESTAB               0                  0                                                                 * 129073                                          * 129072
 users:(("chrome",pid=2249,fd=103))
u_str             ESTAB               0                  0                                                                 * 48343                                           * 48342
 users:(("chrome",pid=2254,fd=5))
u_str             ESTAB               0                  0                                                                 * 49146                                           * 51565
 users:(("nautilus",pid=3118,fd=21))
u_str             ESTAB               0                  0                                       /run/systemd/journal/stdout 49322                                           * 43815

u_str             ESTAB               0                  0                                       /run/systemd/journal/stdout 46377                                           * 46376

u_str             ESTAB               0                  0                                                                 * 204378                                          * 204377
 users:(("chrome",pid=2254,fd=176))
u_str             ESTAB               0                  0                                                                 * 184936                                          * 179938
 users:(("seahorse",pid=27957,fd=7))
u_str             ESTAB               0                  0                                       /run/systemd/journal/stdout 34618                                           * 37524

u_str             ESTAB               0                  0                                                                 * 185951                                          * 182809
 users:(("nautilus",pid=3118,fd=25))
u_str             ESTAB               0                  0                                                                 * 179923                                          * 186539
 users:(("gnome-calendar",pid=27958,fd=1))
u_str             ESTAB               0                  0                                                                 * 121555                                          * 121556
 users:(("chrome",pid=2210,fd=247))
u_str             ESTAB               0                  0                                                                 * 51265                                           * 51264
 users:(("chrome",pid=2254,fd=69))
u_str             ESTAB               0                  0                                       /run/systemd/journal/stdout 35674                                           * 35673

u_str             ESTAB               0                  0                                                /run/user/1000/bus 46257                                           * 47144
 users:(("dbus-daemon",pid=1605,fd=37))
u_str             ESTAB               0                  0                                                                 * 46100                                           * 46101
 users:(("dbus-daemon",pid=1803,fd=6))
u_str             ESTAB               0                  0                                                                 * 44102                                           * 37783
 users:(("gnome-session-b",pid=1706,fd=3),("gnome-session-b",pid=1706,fd=2),("gnome-session-b",pid=1706,fd=1))
u_str             ESTAB               0                  0                                                                 * 48152                                           * 48153
 users:(("gsd-disk-utilit",pid=2010,fd=1))
u_str             ESTAB               0                  0                                       /run/user/1000/pulse/native 185317                                          * 182191
 users:(("pulseaudio",pid=1599,fd=43))
u_str             ESTAB               0                  0                                                                 * 43815                                           * 49322
 users:(("gvfsd-metadata",pid=2297,fd=2),("gvfsd-metadata",pid=2297,fd=1))
```

9. dstat

dstat is a tool that is used to retrieve information or statistics from components of the system such as network connections, IO devices, or CPU, etc. It is generally used by system administrators to retrieve a handful of information about the above-mentioned components of the system. It itself performs like vmsta, netstat, etc. By using this tool one can even see the throughput for block devices that make up a single filesystem or storage system.

Install it by : sudo apt install dstat

Ex: dstat --vmstat

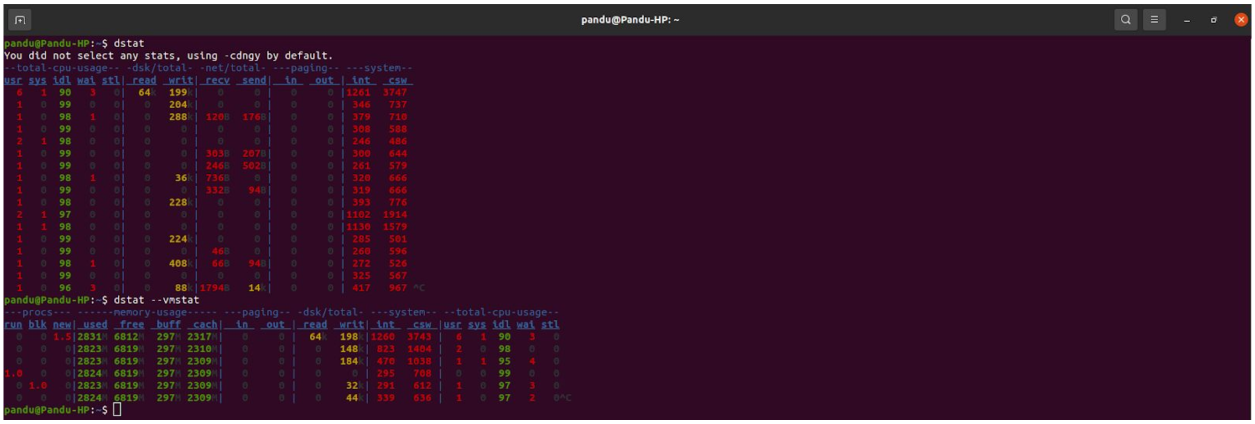
To display information displayed by vmstat. It displays process and memory stats.

Ex: dstat

The output indicates :

CPU Stats: CPU usage by user, system processes and number of idle processes, and Number of waiting processes, hardware and software interrupts.
Disk Stats: Total number of read and write operations on the disk.
Network Stats: Total amount of Bytes received and sent on network interfaces.

__Paging Stats:__ Number of times information is copied into and moved out of memory.
__System Stats:__ Number of interrupts and context switches.



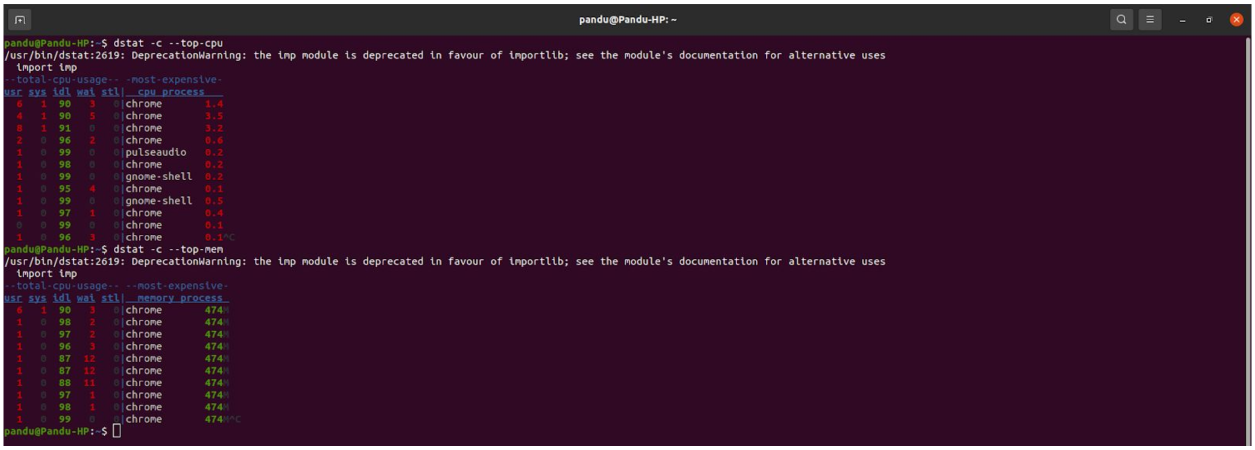
```
pandu@Pandu-HP:~$ dstat
You did not select any stats, using -cdngy by default.
--total-cpu-usage-- -dsk/total- -net/total- ---paging-- ---system--
usr sys idl wai stl| read  writ| recv  send|  in   out | int   csw 
  6   1  90   3   0|  64k  199k|   0     0 |   0     0 |1261  3747 
  1   0  99   0   0|   0   204k|   0     0 |   0     0 | 346   737 
  1   0  98   1   0|   0   288k| 120B  176B|   0     0 | 379   710 
  1   0  99   0   0|   0     0 |   0     0 |   0     0 | 308   588 
  2   1  98   0   0|   0     0 |   0     0 |   0     0 | 246   486 
  1   0  99   0   0|   0     0 | 303B  207B|   0     0 | 300   644 
  1   0  99   0   0|   0     0 | 246B  502B|   0     0 | 261   579 
  1   0  98   1   0|   0    36k| 736B    0 |   0     0 | 320   666 
  1   0  99   0   0|   0     0 | 332B   94B|   0     0 | 319   666 
  1   0  98   0   0|   0   228k|   0     0 |   0     0 | 393   776 
  2   1  97   0   0|   0     0 |   0     0 |   0     0 |1102  1914 
  1   1  98   0   0|   0     0 |   0     0 |   0     0 |1130  1579 
  1   0  99   0   0|   0   224k|   0     0 |   0     0 | 285   501 
  1   0  99   0   0|   0     0 |  46B    0 |   0     0 | 260   596 
  1   0  98   1   0|   0   408k|  66B   94B|   0     0 | 272   526 
  1   0  99   0   0|   0     0 |   0     0 |   0     0 | 325   567 
  1   0  96   3   0|   0    88k|1794B   14k|   0     0 | 417   967 ^C
pandu@Pandu-HP:~$ dstat --vmstat
---procs--- ------memory-usage----- ---paging-- -dsk/total- ---system-- --total-cpu-usage--
run blk new| used  free  buff  cach|  in   out | read  writ| int   csw |usr sys idl wai stl
  0   0 1.5|2831M 6812M  297M 2317M|   0     0 |  64k  198k|1260  3743 |  6   1  90   3   0
  0   0   0|2823M 6819M  297M 2310M|   0     0 |   0   148k| 823  1404 |  2   0  98   0   0
  0   0   0|2823M 6819M  297M 2309M|   0     0 |   0   184k| 470  1038 |  1   1  95   4   0
1.0   0   0|2824M 6819M  297M 2309M|   0     0 |   0     0 | 295   708 |  0   0  99   0   0
  0 1.0   0|2823M 6819M  297M 2309M|   0     0 |   0    32k| 291   612 |  1   0  97   3   0
  0   0   0|2824M 6819M  297M 2309M|   0     0 |   0    44k| 339   636 |  1   0  97   2   0^C
pandu@Pandu-HP:~$ 
```

Ex: dstat -c --top-cpu

To display stats of the process which is consuming most of the CPU.

Ex: dstat -c --top-mem

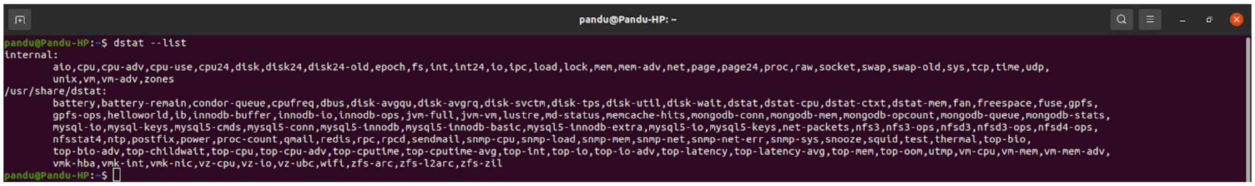
To display stats of the process which is consuming most of the memory.



```
pandu@Pandu-HP:~$ dstat -c --top-cpu
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
  import imp
--total-cpu-usage-- -most-expensive-
usr sys idl wai stl|  cpu process   
  6   1  90   3   0|chrome       1.4
  4   1  90   5   0|chrome       3.5
  8   1  91   0   0|chrome       3.2
  2   0  96   2   0|chrome       0.6
  1   0  99   0   0|pulseaudio   0.2
  1   0  98   0   0|chrome       0.2
  1   0  99   0   0|gnome-shell  0.2
  1   0  95   4   0|chrome       0.1
  1   0  99   0   0|gnome-shell  0.5
  1   0  97   1   0|chrome       0.4
  0   0  99   0   0|chrome       0.1
  1   0  96   3   0|chrome       0.1^C
pandu@Pandu-HP:~$ dstat -c --top-mem
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib; see the module's documentation for alternative uses
  import imp
--total-cpu-usage-- --most-expensive-
usr sys idl wai stl|  memory process 
  6   1  90   3   0|chrome       474M
  1   0  98   2   0|chrome       474M
  1   0  97   2   0|chrome       474M
  1   0  96   3   0|chrome       474M
  1   0  87  12   0|chrome       474M
  1   0  87  12   0|chrome       474M
  1   0  88  11   0|chrome       474M
  1   0  97   1   0|chrome       474M
  1   0  98   1   0|chrome       474M
  1   0  99   0   0|chrome       474M^C
pandu@Pandu-HP:~$ 
```

Ex: dstat --list

We can display stats of a few plugins. This command will display those plugins.



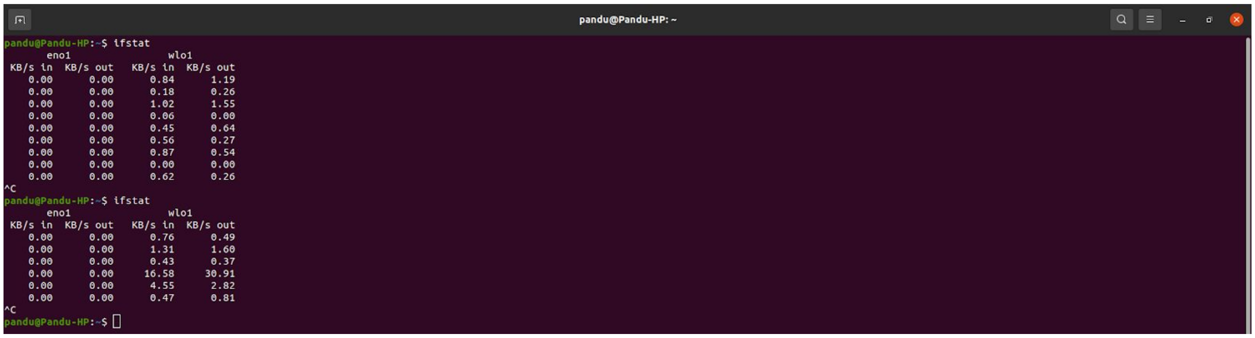
```
pandu@Pandu-HP:~$ dstat --list
internal:
	aio,cpu,cpu-adv,cpu-use,cpu24,disk,disk24,disk24-old,epoch,fs,int,int24,io,ipc,load,lock,mem,mem-adv,net,page,page24,proc,raw,socket,swap,swap-old,sys,tcp,time,udp,
	unix,vm,vm-adv,zones
/usr/share/dstat:
	battery,battery-remain,condor-queue,cpufreq,dbus,disk-avgqu,disk-avgrq,disk-svctm,disk-tps,disk-util,disk-wait,dstat,dstat-cpu,dstat-ctxt,dstat-mem,fan,freespace,fuse,gpfs,
	gpfs-ops,helloworld,ib,innodb-buffer,innodb-io,innodb-ops,jvm-full,jvm-vm,lustre,md-status,memcache-hits,mongodb-conn,mongodb-mem,mongodb-opcount,mongodb-queue,mongodb-stats,
	mysql-io,mysql-keys,mysql5-cmds,mysql5-conn,mysql5-innodb,mysql5-innodb-basic,mysql5-innodb-extra,mysql5-io,mysql5-keys,net-packets,nfs3,nfs3-ops,nfsd3,nfsd3-ops,nfsd4-ops,
	nfsstat4,ntp,postfix,power,proc-count,qmail,redis,rpc,rpcd,sendmail,snmp-cpu,snmp-load,snmp-mem,snmp-net,snmp-net-err,snmp-sys,snooze,squid,test,thermal,top-bio,
	top-bio-adv,top-childwait,top-cpu,top-cpu-adv,top-cputime,top-cputime-avg,top-int,top-io,top-io-adv,top-latency,top-latency-avg,top-mem,top-oom,utmp,vm-cpu,vm-mem,vm-mem-adv,
	vmk-hba,vmk-int,vmk-nic,vz-cpu,vz-io,vz-ubc,wifi,zfs-arc,zfs-l2arc,zfs-zil
pandu@Pandu-HP:~$ 
```

10. ifstat

As dstat, iostat, vmstat displays stats regarding the components of System. ifstat displays network interface statistics. This tool keeps records of the previous data files and displays differences between last and current calls.

Instal it using : sudo apt install ifstat

Ex: ifstat



```
pandu@Pandu-HP:~$ ifstat
       eno1                wlo1
 KB/s in  KB/s out   KB/s in  KB/s out
    0.00      0.00      0.84      1.19
    0.00      0.00      0.18      0.26
    0.00      0.00      1.02      1.55
    0.00      0.00      0.06      0.00
    0.00      0.00      0.45      0.64
    0.00      0.00      0.56      0.27
    0.00      0.00      0.87      0.54
    0.00      0.00      0.00      0.00
    0.00      0.00      0.62      0.26
^C
pandu@Pandu-HP:~$ ifstat
       eno1                wlo1
 KB/s in  KB/s out   KB/s in  KB/s out
    0.00      0.00      0.76      0.49
    0.00      0.00      1.31      1.60
    0.00      0.00      0.43      0.37
    0.00      0.00     16.58     30.91
    0.00      0.00      4.55      2.82
    0.00      0.00      0.47      0.81
^C
pandu@Pandu-HP:~$ 
```

11. wget

Wget is the non-interactive network downloader which 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. With Wget, you can download files using HTTP, HTTPS, and FTP protocols. Wget provides a number of options allowing you to download multiple files, resume downloads, limit the bandwidth, recursive downloads, download in the background, mirror a website, and much more.

Install it using : sudo apt install wget
Ex: wget [options] [url]

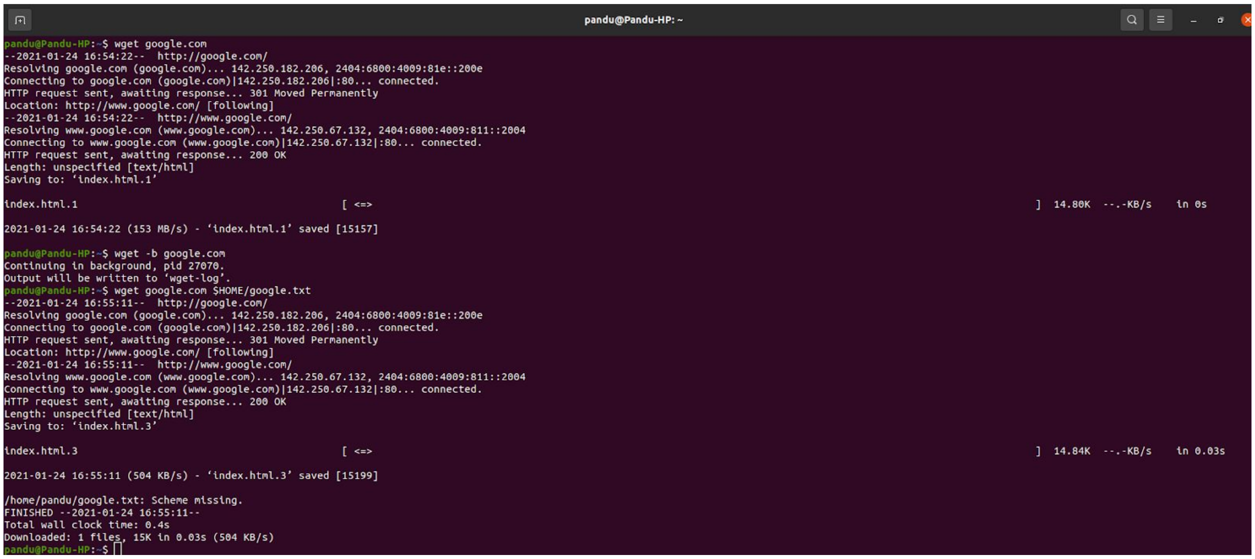
Ex: wget google.com

Ex: wget -b google.com
To download the file in background

Ex: wget google.com -o/path/filename.txt
To overwrite the log file of wget command.

Ex: wget -c google.com

To resume a partially downloaded file.



```
pandu@Pandu-HP:~$ wget google.com
--2021-01-24 16:54:22--  http://google.com/
Resolving google.com (google.com)... 142.250.182.206, 2404:6800:4009:81e::200e
Connecting to google.com (google.com)|142.250.182.206|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2021-01-24 16:54:22--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.67.132, 2404:6800:4009:811::2004
Connecting to www.google.com (www.google.com)|142.250.67.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.1’

index.html.1                                           [ <=>                                                                                                         ]  14.80K  --.-KB/s    in 0s

2021-01-24 16:54:22 (153 MB/s) - ‘index.html.1’ saved [15157]

pandu@Pandu-HP:~$ wget -b google.com
Continuing in background, pid 27070.
Output will be written to ‘wget-log’.
pandu@Pandu-HP:~$ wget google.com $HOME/google.txt
--2021-01-24 16:55:11--  http://google.com/
Resolving google.com (google.com)... 142.250.182.206, 2404:6800:4009:81e::200e
Connecting to google.com (google.com)|142.250.182.206|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2021-01-24 16:55:11--  http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.67.132, 2404:6800:4009:811::2004
Connecting to www.google.com (www.google.com)|142.250.67.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: ‘index.html.3’

index.html.3                                           [ <=>                                                                                                         ]  14.84K  --.-KB/s    in 0.03s

2021-01-24 16:55:11 (504 KB/s) - ‘index.html.3’ saved [15199]

/home/pandu/google.txt: Scheme missing.
FINISHED --2021-01-24 16:55:11--
Total wall clock time: 0.4s
Downloaded: 1 files, 15K in 0.03s (504 KB/s)
pandu@Pandu-HP:~$ 
```