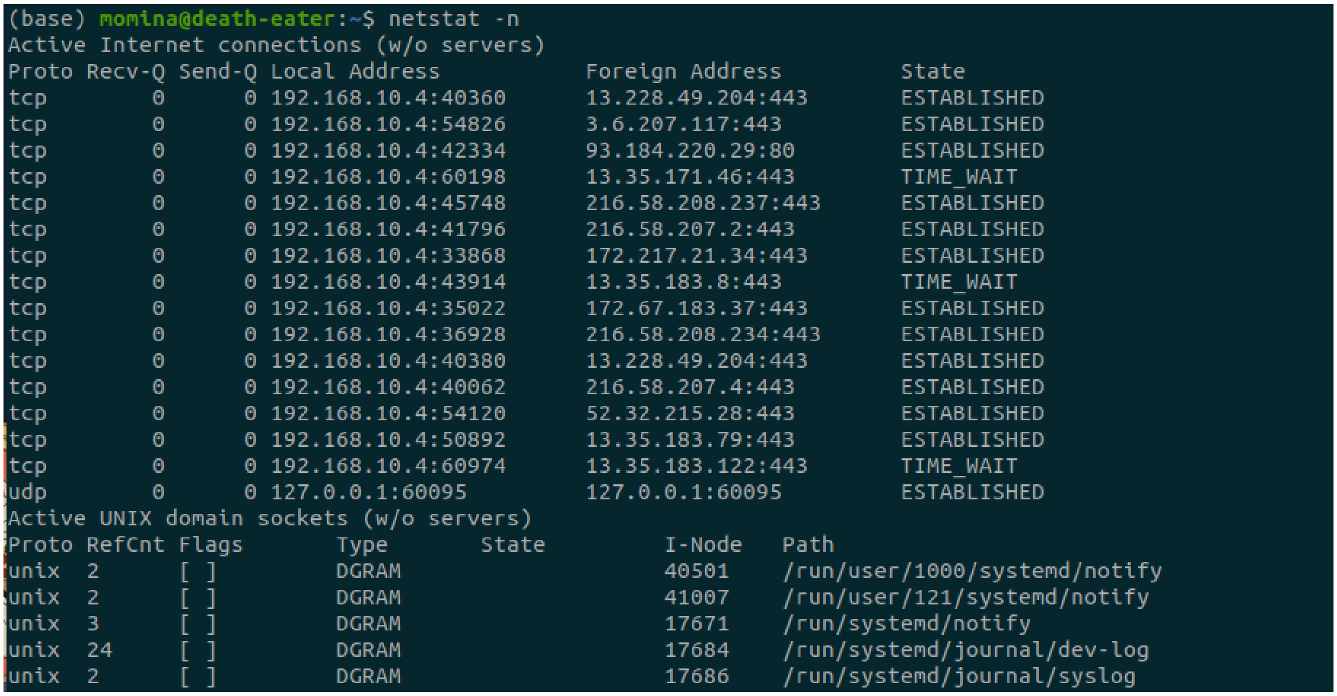
# Computer Networks Lab
# Task 01

Momina Atif Dar
P18-0030
Section B

1. netstat -n

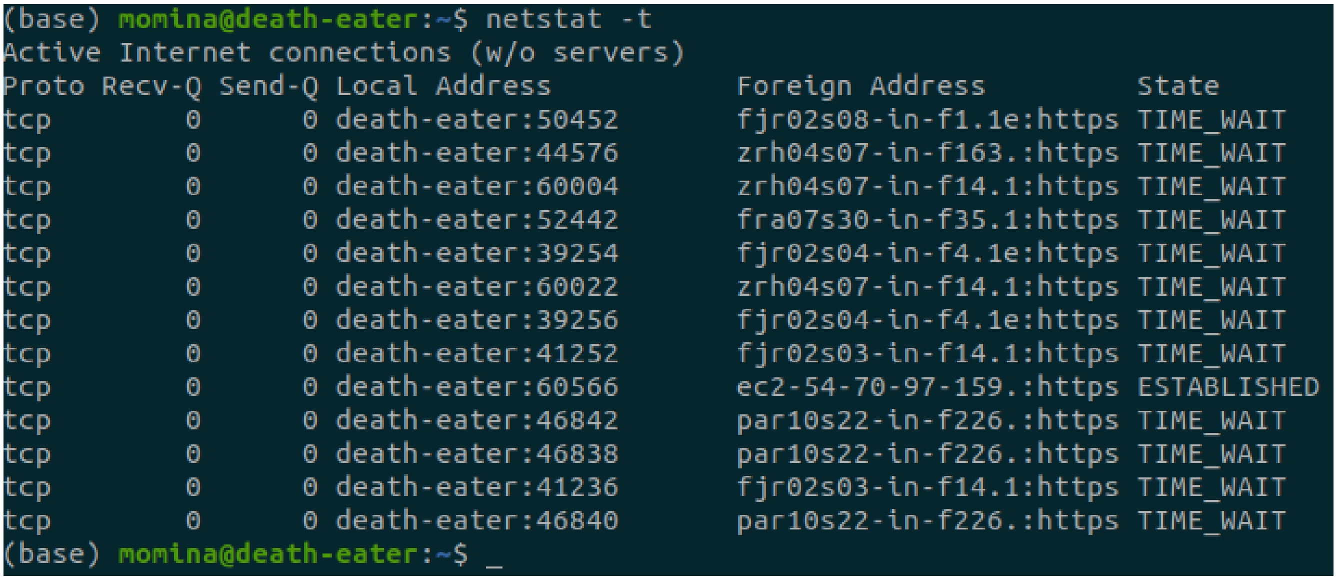
It displays local addresses along with their state for example 192.168.10.4's connection is established. It also shows the foreign addresses of local addresses. Along with that it shows active UNIX domain sockets, their type, state, I-node and path.



```
(base) momina@death-eater:~$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.10.4:40360      13.228.49.204:443       ESTABLISHED
tcp        0      0 192.168.10.4:54826      3.6.207.117:443         ESTABLISHED
tcp        0      0 192.168.10.4:42334      93.184.220.29:80        ESTABLISHED
tcp        0      0 192.168.10.4:60198      13.35.171.46:443        TIME_WAIT
tcp        0      0 192.168.10.4:45748      216.58.208.237:443      ESTABLISHED
tcp        0      0 192.168.10.4:41796      216.58.207.2:443        ESTABLISHED
tcp        0      0 192.168.10.4:33868      172.217.21.34:443       ESTABLISHED
tcp        0      0 192.168.10.4:43914      13.35.183.8:443         TIME_WAIT
tcp        0      0 192.168.10.4:35022      172.67.183.37:443       ESTABLISHED
tcp        0      0 192.168.10.4:36928      216.58.208.234:443      ESTABLISHED
tcp        0      0 192.168.10.4:40380      13.228.49.204:443       ESTABLISHED
tcp        0      0 192.168.10.4:40062      216.58.207.4:443        ESTABLISHED
tcp        0      0 192.168.10.4:54120      52.32.215.28:443        ESTABLISHED
tcp        0      0 192.168.10.4:50892      13.35.183.79:443        ESTABLISHED
tcp        0      0 192.168.10.4:60974      13.35.183.122:443       TIME_WAIT
udp        0      0 127.0.0.1:60095         127.0.0.1:60095         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    40501    /run/user/1000/systemd/notify
unix  2      [ ]         DGRAM                    41007    /run/user/121/systemd/notify
unix  3      [ ]         DGRAM                    17671    /run/systemd/notify
unix  24     [ ]         DGRAM                    17684    /run/systemd/journal/dev-log
unix  2      [ ]         DGRAM                    17686    /run/systemd/journal/syslog
```

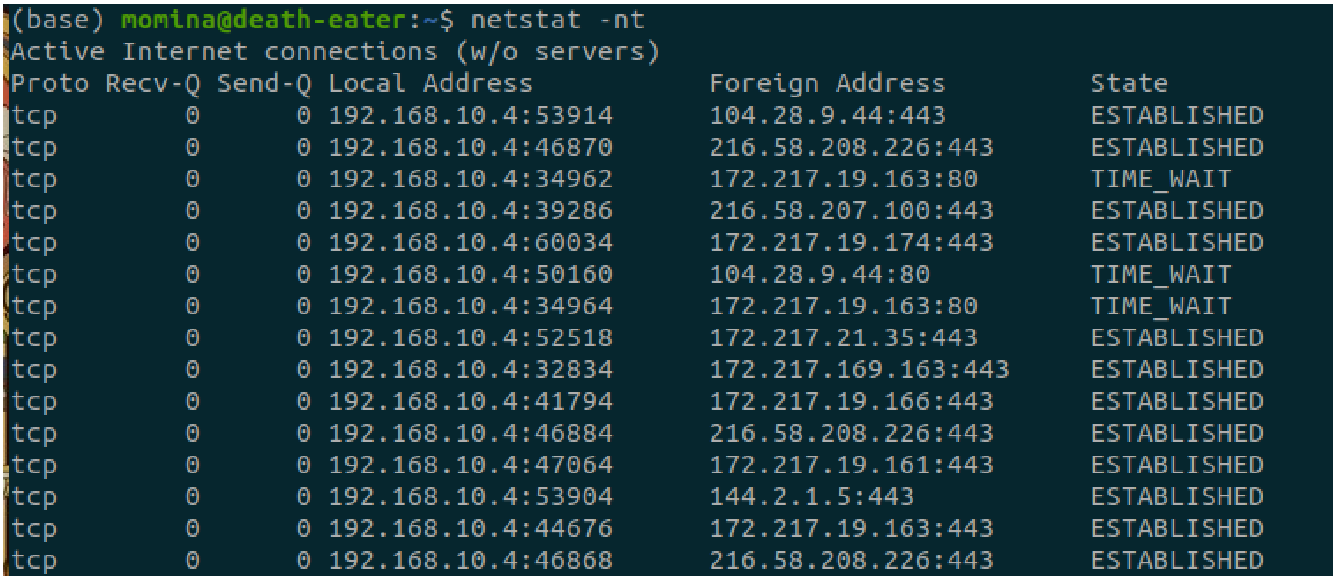
2. netstat -t

It tells us about tcp connections.



```
(base) momina@death-eater:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 death-eater:50452       fjr02s08-in-f1.1e:https TIME_WAIT
tcp        0      0 death-eater:44576       zrh04s07-in-f163.:https TIME_WAIT
tcp        0      0 death-eater:60004       zrh04s07-in-f14.1:https TIME_WAIT
tcp        0      0 death-eater:52442       fra07s30-in-f35.1:https TIME_WAIT
tcp        0      0 death-eater:39254       fjr02s04-in-f4.1e:https TIME_WAIT
tcp        0      0 death-eater:60022       zrh04s07-in-f14.1:https TIME_WAIT
tcp        0      0 death-eater:39256       fjr02s04-in-f4.1e:https TIME_WAIT
tcp        0      0 death-eater:41252       fjr02s03-in-f14.1:https TIME_WAIT
tcp        0      0 death-eater:60566       ec2-54-70-97-159.:https ESTABLISHED
tcp        0      0 death-eater:46842       par10s22-in-f226.:https TIME_WAIT
tcp        0      0 death-eater:46838       par10s22-in-f226.:https TIME_WAIT
tcp        0      0 death-eater:41236       fjr02s03-in-f14.1:https TIME_WAIT
tcp        0      0 death-eater:46840       par10s22-in-f226.:https TIME_WAIT
(base) momina@death-eater:~$ _
```

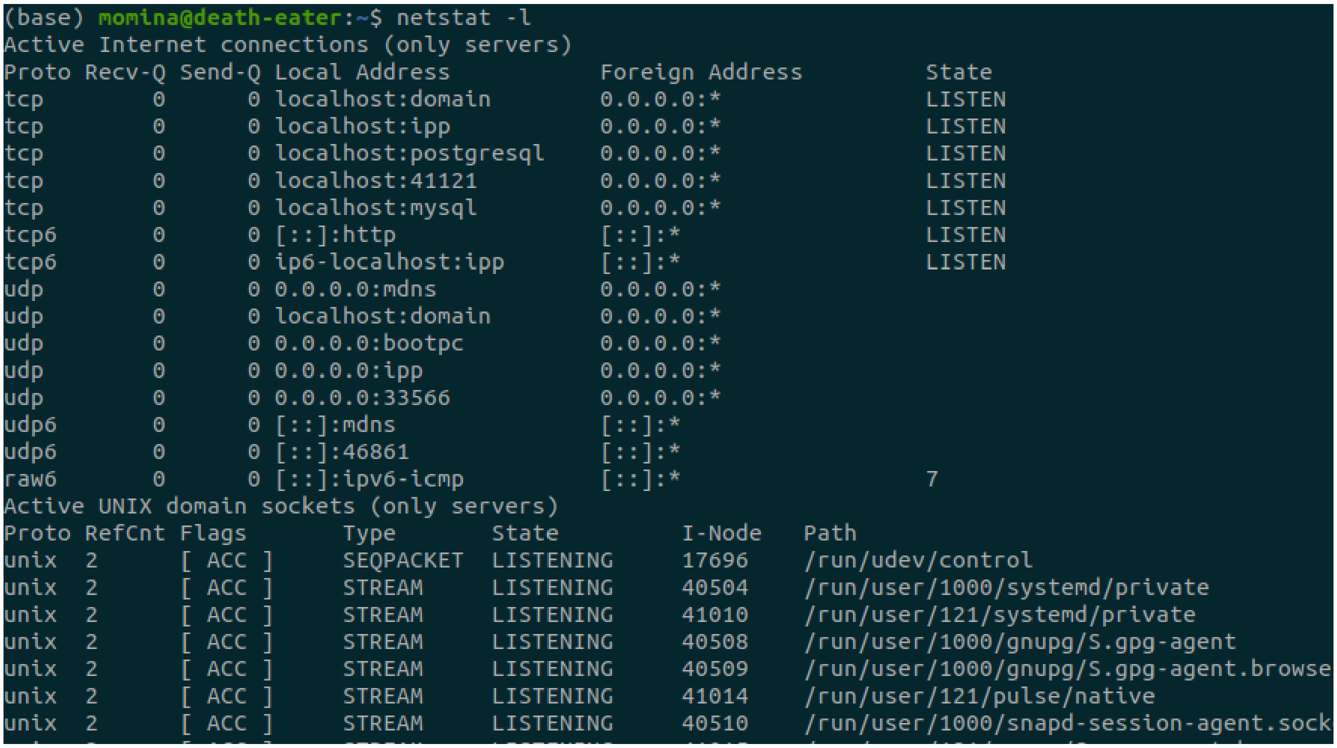
If we do option ‘-t’ with ‘-n’ we can get numerical IP addresses.



```
(base) momina@death-eater:~$ netstat -nt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.10.4:53914      104.28.9.44:443         ESTABLISHED
tcp        0      0 192.168.10.4:46870      216.58.208.226:443      ESTABLISHED
tcp        0      0 192.168.10.4:34962      172.217.19.163:80       TIME_WAIT
tcp        0      0 192.168.10.4:39286      216.58.207.100:443      ESTABLISHED
tcp        0      0 192.168.10.4:60034      172.217.19.174:443      ESTABLISHED
tcp        0      0 192.168.10.4:50160      104.28.9.44:80          TIME_WAIT
tcp        0      0 192.168.10.4:34964      172.217.19.163:80       TIME_WAIT
tcp        0      0 192.168.10.4:52518      172.217.21.35:443       ESTABLISHED
tcp        0      0 192.168.10.4:32834      172.217.169.163:443     ESTABLISHED
tcp        0      0 192.168.10.4:41794      172.217.19.166:443      ESTABLISHED
tcp        0      0 192.168.10.4:46884      216.58.208.226:443      ESTABLISHED
tcp        0      0 192.168.10.4:47064      172.217.19.161:443      ESTABLISHED
tcp        0      0 192.168.10.4:53904      144.2.1.5:443           ESTABLISHED
tcp        0      0 192.168.10.4:44676      172.217.19.163:443      ESTABLISHED
tcp        0      0 192.168.10.4:46868      216.58.208.226:443      ESTABLISHED
```

3. netstat -l

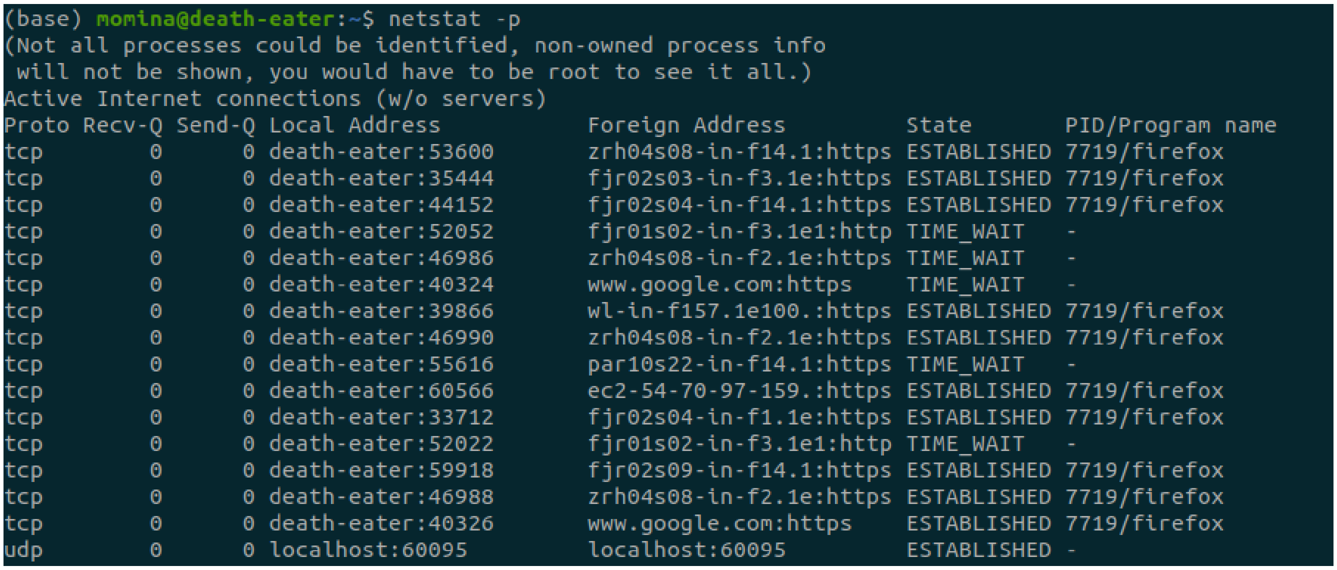
It shows only the ports that are in LISTENING state.



```
(base) momina@death-eater:~$ netstat -l
Active Internet connections (only servers)
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        0      0 localhost:postgresql    0.0.0.0:*               LISTEN
tcp        0      0 localhost:41121         0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 0.0.0.0:33566           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:46861              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     17696    /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     40504    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     41010    /run/user/121/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     40508    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     40509    /run/user/1000/gnupg/S.gpg-agent.browse
unix  2      [ ACC ]     STREAM     LISTENING     41014    /run/user/121/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     40510    /run/user/1000/snapd-session-agent.sock
```

4. netstat -p

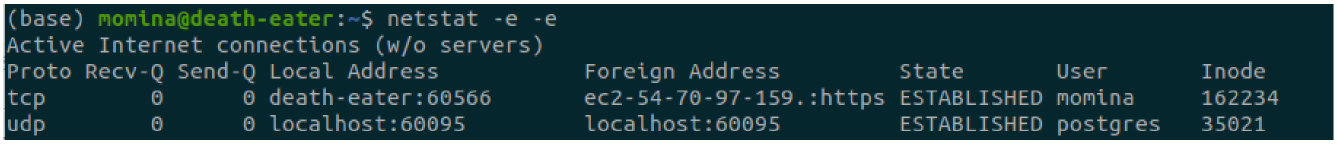
It shows the Program ID of the program to which a socket is belonging.



```
(base) momina@death-eater:~$ netstat -p
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 death-eater:53600       zrh04s08-in-f14.1:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:35444       fjr02s03-in-f3.1e:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:44152       fjr02s04-in-f14.1:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:52052       fjr01s02-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 death-eater:46986       zrh04s08-in-f2.1e:https TIME_WAIT   -
tcp        0      0 death-eater:40324       www.google.com:https    TIME_WAIT   -
tcp        0      0 death-eater:39866       wl-in-f157.1e100.:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:46990       zrh04s08-in-f2.1e:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:55616       par10s22-in-f14.1:https TIME_WAIT   -
tcp        0      0 death-eater:60566       ec2-54-70-97-159.:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:33712       fjr02s04-in-f1.1e:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:52022       fjr01s02-in-f3.1e1:http TIME_WAIT   -
tcp        0      0 death-eater:59918       fjr02s09-in-f14.1:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:46988       zrh04s08-in-f2.1e:https ESTABLISHED 7719/firefox
tcp        0      0 death-eater:40326       www.google.com:https    ESTABLISHED 7719/firefox
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED -
```

5. netstat -e

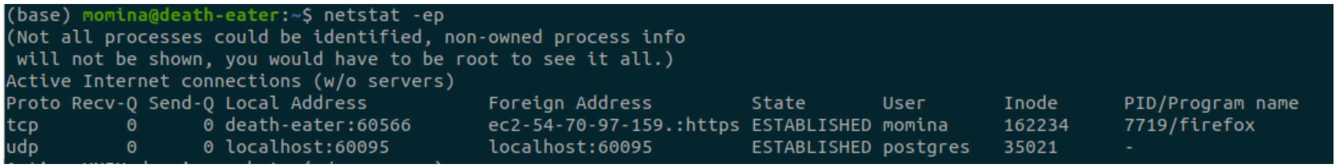
It tells us about the state of connection and which user is using it and also about the Inode.



```
(base) momina@death-eater:~$ netstat -e -e
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode
tcp        0      0 death-eater:60566       ec2-54-70-97-159.:https ESTABLISHED momina     162234
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED postgres   35021
```

6. netstat -ep

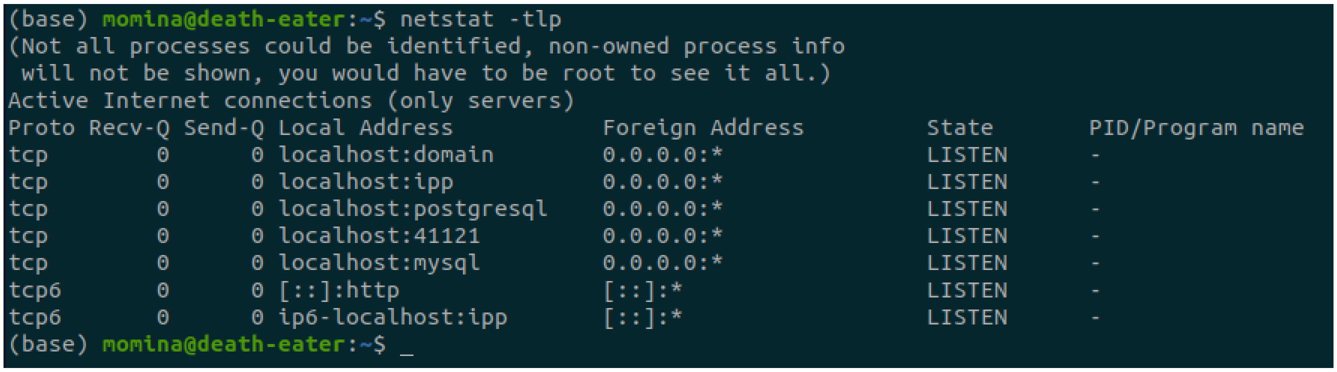
It tells us about the user and program to whata socket is belonging. With this you can easily check which user is using internet connection on what IP and what is using that connection.



```
(base) momina@death-eater:~$ netstat -ep
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 death-eater:60566       ec2-54-70-97-159.:https ESTABLISHED momina     162234     7719/firefox
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED postgres   35021      -
```

7. netstat -tlp

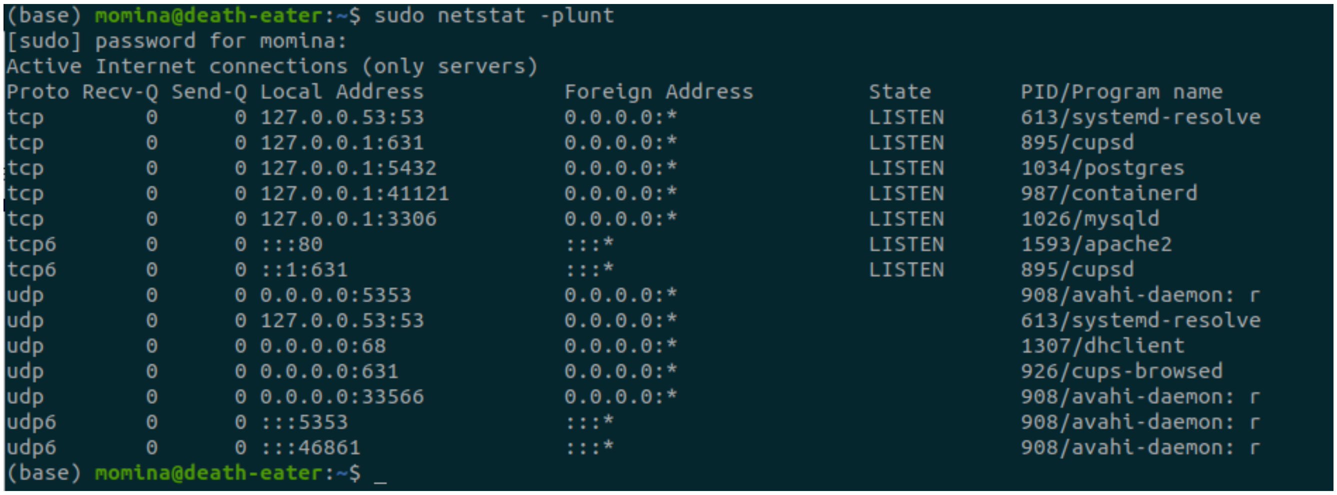
It shows active internet connections and their state along with Program ID/name.



```
(base) momina@death-eater:~$ netstat -tlp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:41121         0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN      -
tcp6       0      0 [::]:http               [::]:*                  LISTEN      -
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN      -
(base) momina@death-eater:~$ _
```

8. netstat -plunt

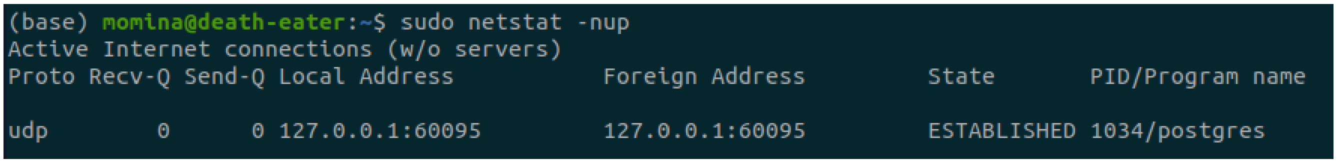
It shows active internet connections including IP address, ports they are listening on, state they are in and Program ID. Let’s say it’s a complete command to know about the connection with concise information.



```
(base) momina@death-eater:~$ sudo netstat -plunt
[sudo] password for momina:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      613/systemd-resolve
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      895/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      1034/postgres
tcp        0      0 127.0.0.1:41121         0.0.0.0:*               LISTEN      987/containerd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      1026/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN      1593/apache2
tcp6       0      0 ::1:631                 :::*                    LISTEN      895/cupsd
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           908/avahi-daemon: r
udp        0      0 127.0.0.53:53           0.0.0.0:*                           613/systemd-resolve
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1307/dhclient
udp        0      0 0.0.0.0:631             0.0.0.0:*                           926/cups-browsed
udp        0      0 0.0.0.0:33566           0.0.0.0:*                           908/avahi-daemon: r
udp6       0      0 :::5353                 :::*                                908/avahi-daemon: r
udp6       0      0 :::46861                :::*                                908/avahi-daemon: r
(base) momina@death-eater:~$ _
```

9. netstat -nup

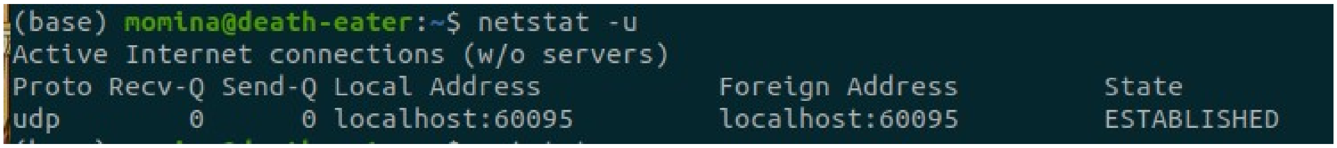
It tells us about udp connections with their numerical IP address, state, the program ID/name using it.



```
(base) momina@death-eater:~$ sudo netstat -nup
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name

udp        0      0 127.0.0.1:60095         127.0.0.1:60095         ESTABLISHED 1034/postgres
```

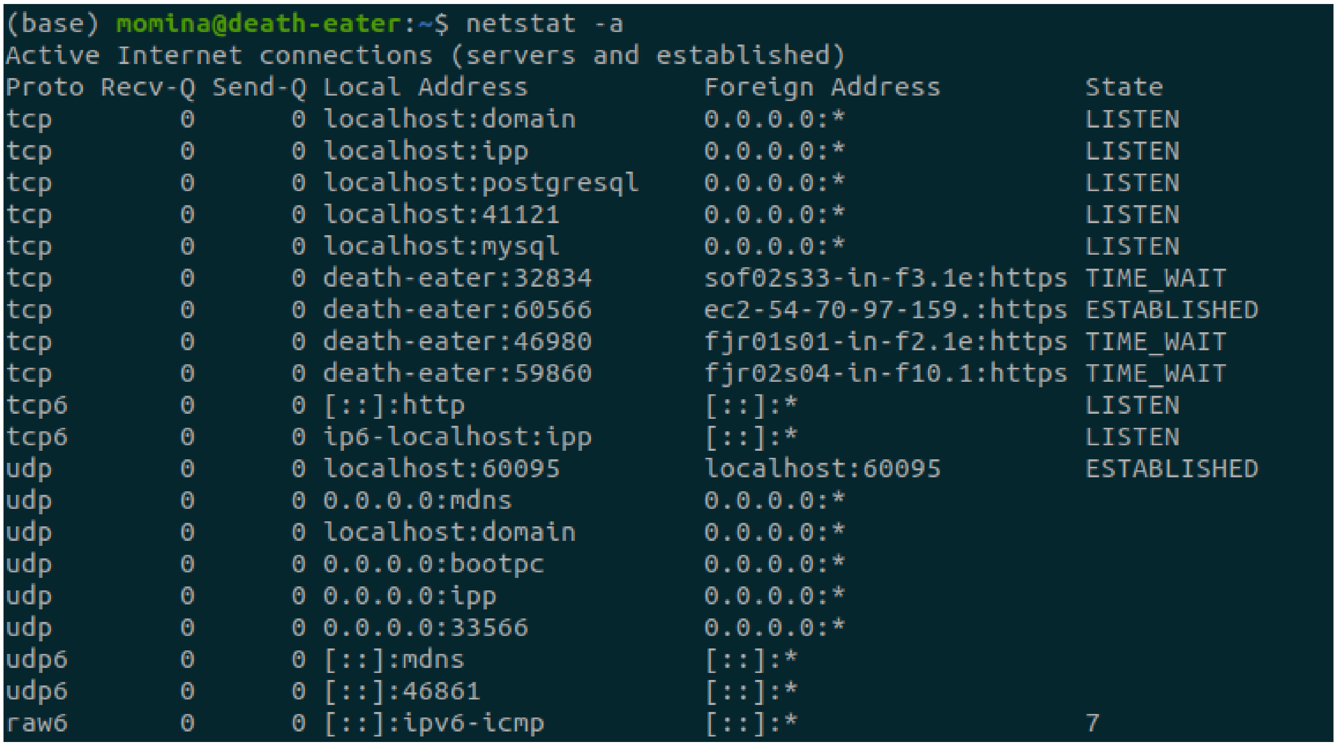
Option ‘-u’ alone tells us about udp connections.



```
(base) momina@death-eater:~$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED
```

10. netstat -a

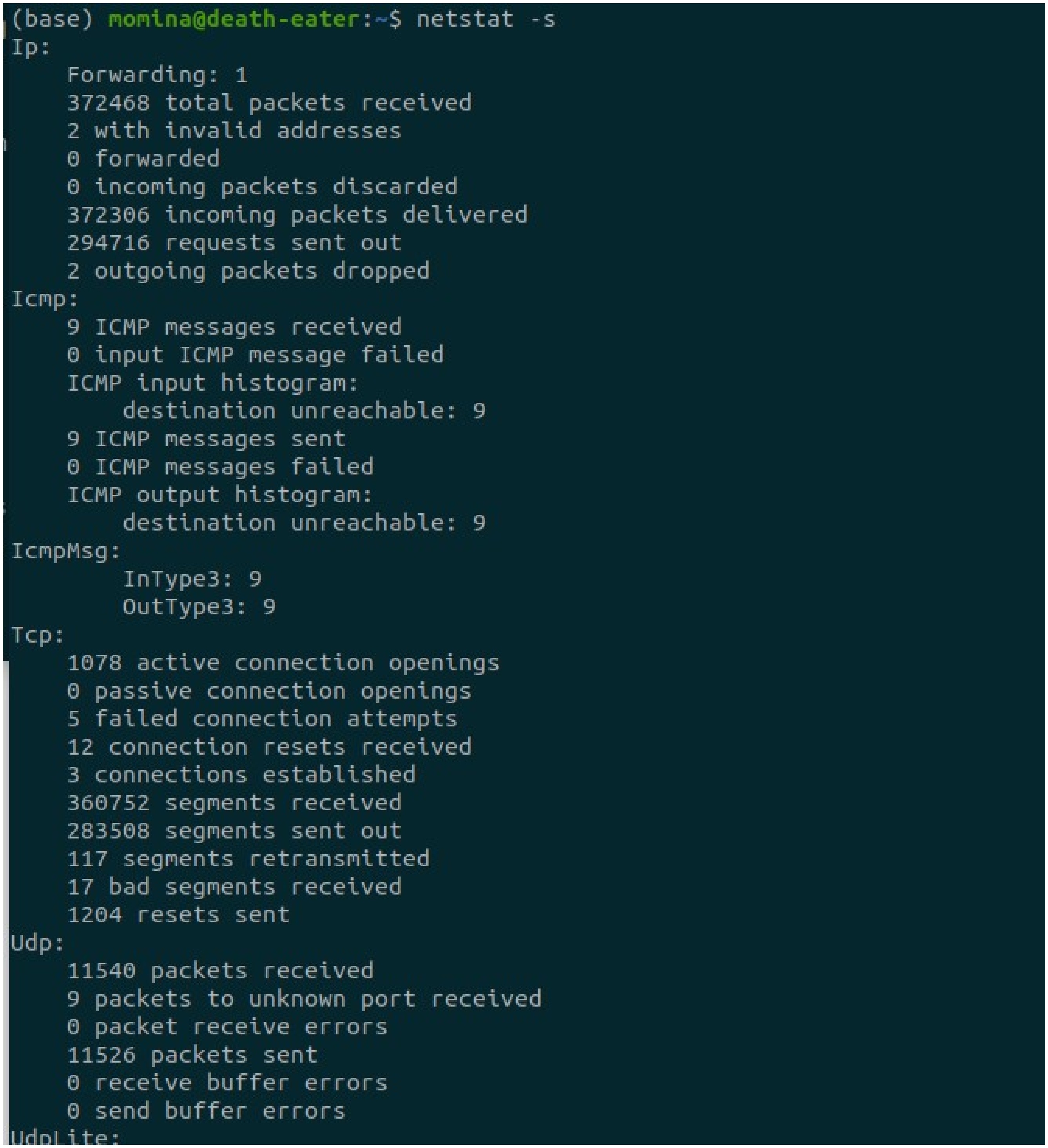
It shows us all the connections, including the ones that are in listen state or not in listen state.



```
(base) momina@death-eater:~$ 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        0      0 localhost:postgresql    0.0.0.0:*               LISTEN
tcp        0      0 localhost:41121         0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 death-eater:32834       sof02s33-in-f3.1e:https TIME_WAIT
tcp        0      0 death-eater:60566       ec2-54-70-97-159.:https ESTABLISHED
tcp        0      0 death-eater:46980       fjr01s01-in-f2.1e:https TIME_WAIT
tcp        0      0 death-eater:59860       fjr02s04-in-f10.1:https TIME_WAIT
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*
udp        0      0 0.0.0.0:ipp             0.0.0.0:*
udp        0      0 0.0.0.0:33566           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:46861              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
```

11. netstat -s

It displays the information about network statistics i.e. total number of packets received, forwarded, bad connections and more.

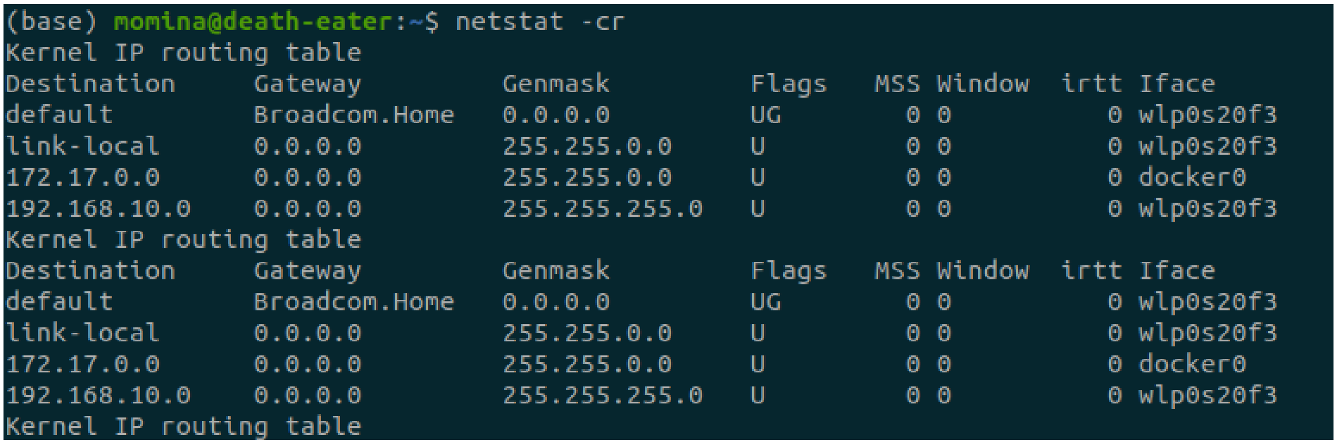


```
(base) momina@death-eater:~$ netstat -s
Ip:
    Forwarding: 1
    372468 total packets received
    2 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    372306 incoming packets delivered
    294716 requests sent out
    2 outgoing packets dropped
Icmp:
    9 ICMP messages received
    0 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 9
    9 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 9
IcmpMsg:
        InType3: 9
        OutType3: 9
Tcp:
    1078 active connection openings
    0 passive connection openings
    5 failed connection attempts
    12 connection resets received
    3 connections established
    360752 segments received
    283508 segments sent out
    117 segments retransmitted
    17 bad segments received
    1204 resets sent
Udp:
    11540 packets received
    9 packets to unknown port received
    0 packet receive errors
    11526 packets sent
    0 receive buffer errors
    0 send buffer errors
UdpLite:
```

12. netstat -c

Option ‘-c’ is mainly used with other options to get the output in a continuous manner. For continuity we use option ‘-c’.

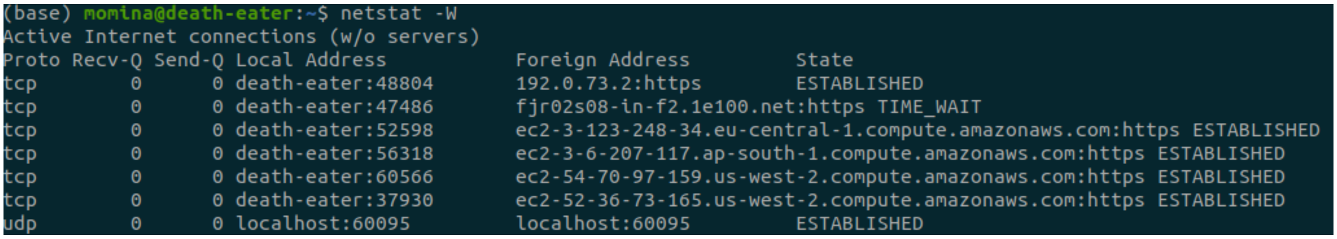
netstat -cr in the screenshot below is continuously telling us about routing information. We have to stop it manually by Ctrl+Z.



```
(base) momina@death-eater:~$ netstat -cr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         Broadcom.Home   0.0.0.0         UG        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp0s20f3
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
192.168.10.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp0s20f3
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         Broadcom.Home   0.0.0.0         UG        0 0          0 wlp0s20f3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 wlp0s20f3
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
192.168.10.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp0s20f3
Kernel IP routing table
```

13. netstat -W

It shows the information completely without keeping the tabular format in check.



```
(base) momina@death-eater:~$ netstat -W
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 death-eater:48804       192.0.73.2:https        ESTABLISHED
tcp        0      0 death-eater:47486       fjr02s08-in-f2.1e100.net:https TIME_WAIT
tcp        0      0 death-eater:52598       ec2-3-123-248-34.eu-central-1.compute.amazonaws.com:https ESTABLISHED
tcp        0      0 death-eater:56318       ec2-3-6-207-117.ap-south-1.compute.amazonaws.com:https ESTABLISHED
tcp        0      0 death-eater:60566       ec2-54-70-97-159.us-west-2.compute.amazonaws.com:https ESTABLISHED
tcp        0      0 death-eater:37930       ec2-52-36-73-165.us-west-2.compute.amazonaws.com:https ESTABLISHED
udp        0      0 localhost:60095         localhost:60095         ESTABLISHED
```