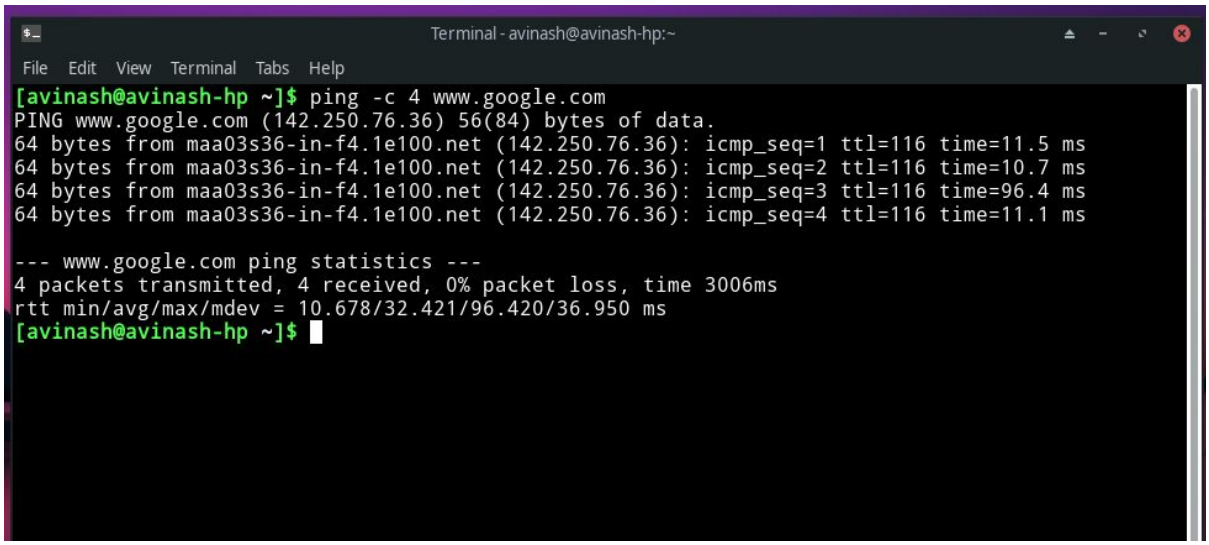
NETWORKS LAB

Experiment-1

Samudrala Aviansh
B180409CS

1. Ping :

Syntax : " ***ping [OPTIONS] DESTINATION*** "



The Linux ping command is a simple utility used to check whether a network is available and if a host is reachable. With this command, you can test if a server is up and running. It also helps with troubleshooting various connectivity issues.

The ping command resolves the domain name into an IP address and starts sending ICMP packages to the destination IP. If the destination IP is reachable it will respond back and the ping command prints a line that includes the following fields:

- The number of data bytes.
- The IP address of the destination.
- The ICMP sequence number for each packet.
- The Time to Live.
- The ping time, measured in milliseconds which is the round trip time for the packet to reach the host, and the response to return to the sender.

Here i used “ping -c 4 www.google.com” to set the count of packets to 4.

Once the command stops, it displays a statistic, including the percentage of packet loss. The packet loss means the data was dropped somewhere in the network, indicating an issue within the network. If there is a packet loss, you can use the traceroute command to identify where the packet loss occurs.

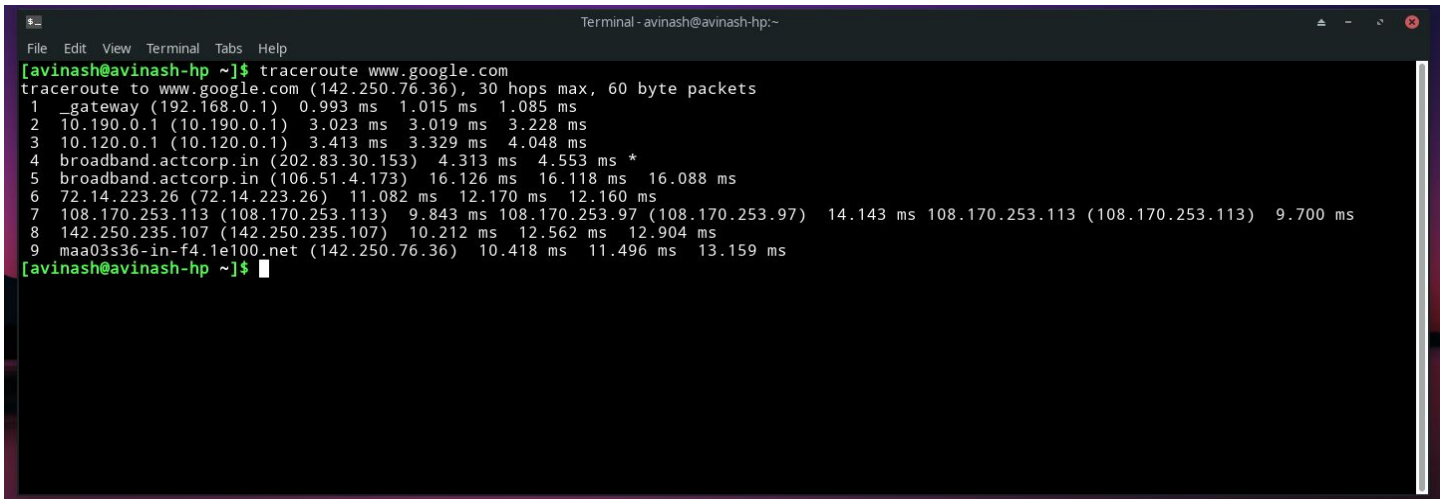
Options :

-c : to specify the count of packets to be sent to destination

-s : to specify the size of the packet that is to be sent.

-4 or -6 : to specify whether to use ipv4 or ipv6.

2. tracert / traceroute :



Syntax : ***“ traceroute [options] host_Address*** “

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Above image depicts how traceroute command is used to reach the Google (142.250.76.36) host from the local machine and it also prints detail about all the hops that it visits in between.

The first column corresponds to the hop count. The second column represents the address of that hop and after that, you see three space-separated time in milliseconds. *traceroute* command sends three packets to the hop and each of the time refers to the time taken by the packet to reach the hop. In our case maximum no.of hops to reach google host is 9.

Options:

-p : used to specify the destination port

-F : do not fragment packet.

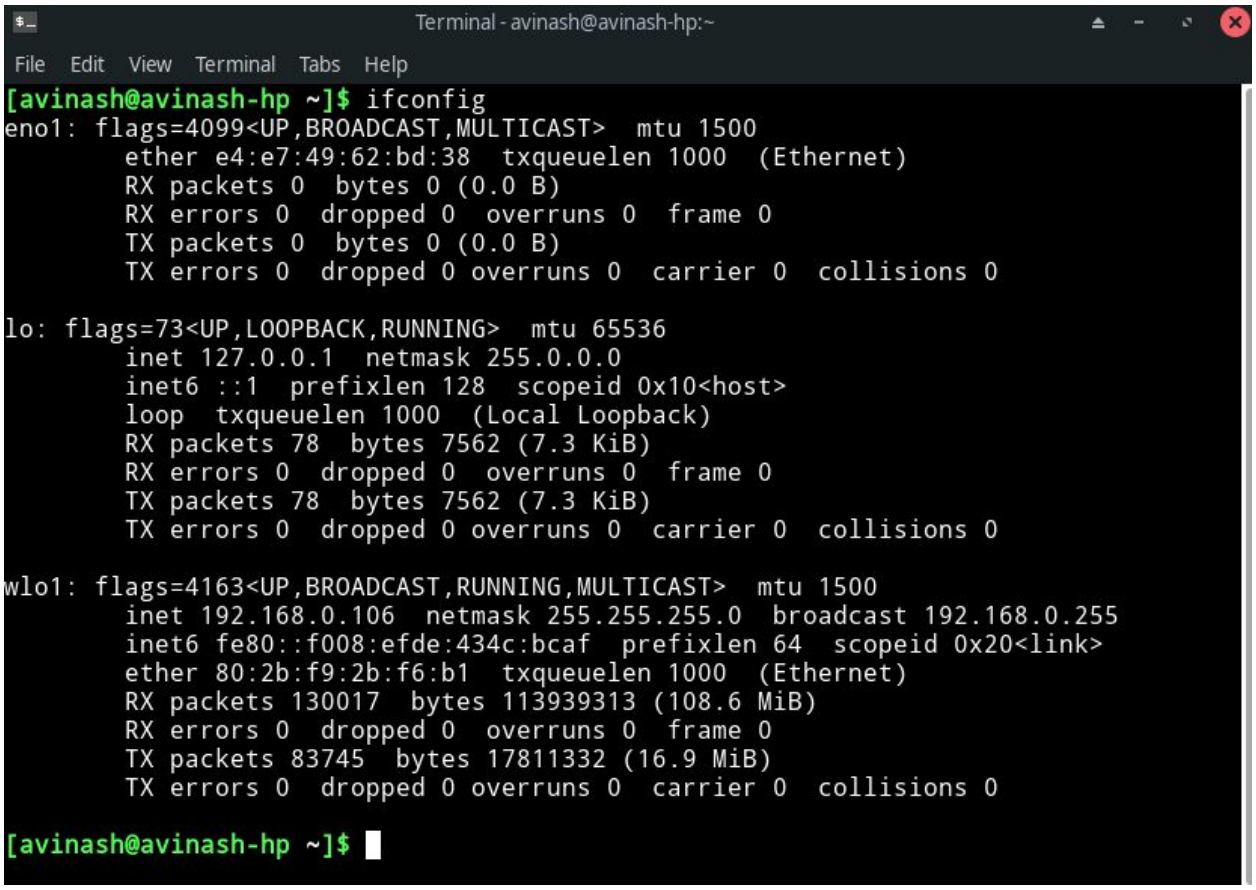
-g : Route the packet through gate.

-n : Do not resolve IP addresses to their domain names.

3. Ip / ifconfig / ipconfig :

Syntax : ***“ ifconfig [...OPTIONS] [INTERFACE] “***

This commands is used to configure the network interfaces.Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.



Here, **eno1**, **lo** and **wlo1** are the names of the active network interfaces on the system.

- **eno1** is the first Ethernet interface.
- **lo** is the loopback interface. This is a special network interface that the system uses to communicate with itself.
- **wlo1** is the name of the first wireless network interface on the system.

Options :

up : to activate driver for interface , **down :** to deactivate driver from interface

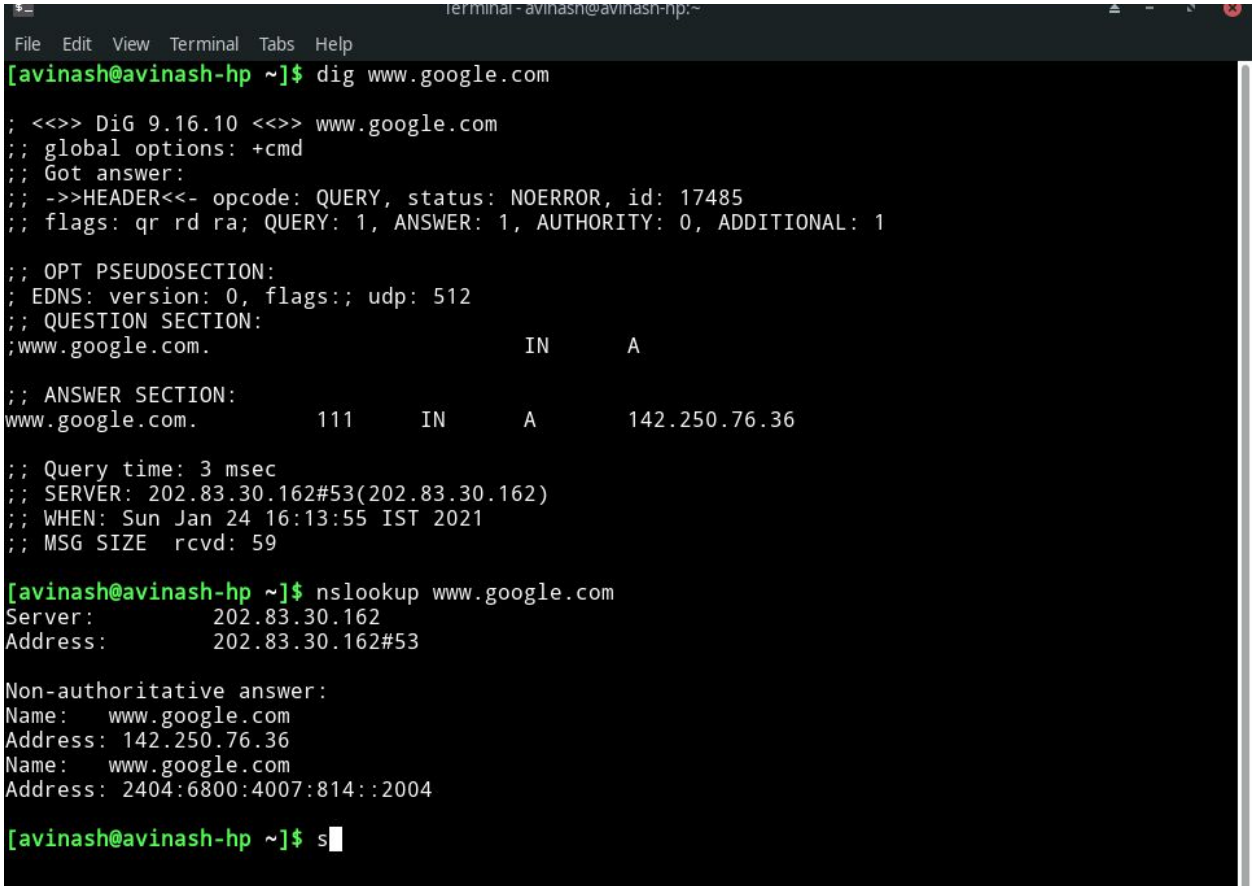
Here **inet** indicates the machine's ip address(ipv4) and **inet6** indicates the machine's ipv6 address.

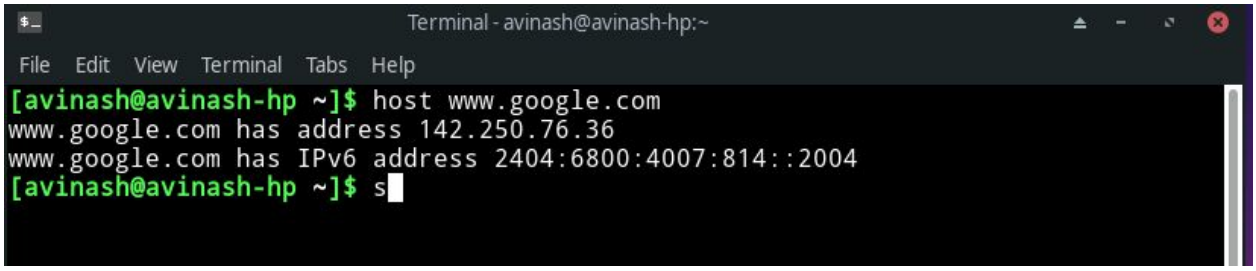
RX and TX are the number of received and transmitted packets.And the state <RUNNING> specifies that the interface is ready to accept the data.

In my case, my machine's ipv4 address is '192.168.0.106' and ipv6 address is 'fe80::f008:efde:434c:bcaf'

4. dig / nslookup / host :

Syntax : ***"host [OPTIONS] hostname [server]."***
"dig [SERVER] [NAME] [TYPE]"
"nslookup [OPTIONS] hostname [SERVER]"





These commands are basically used for DNS (Domain Name System) lookup operations. In simple words, these commands are used to find the IP address of a particular domain name or if you want to find out the domain name of a particular IP address these commands becomes handy. You can also find more specific details of a domain by specifying the corresponding option along with the domain name.

Options for host :

-a or -v: It used to enable the verbose output.

-t : It is used to specify the type of query(ns, SOA, txt).

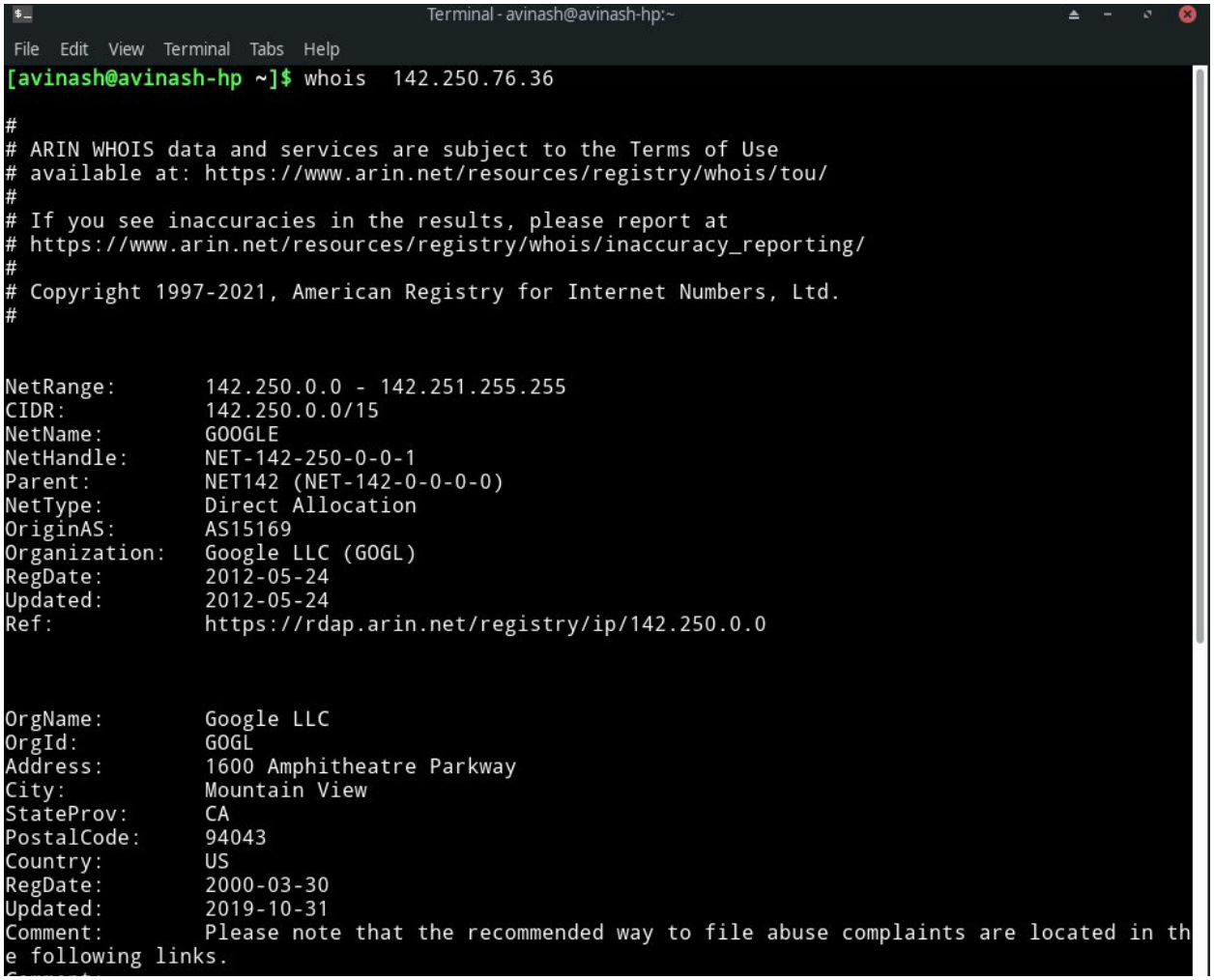
-R : In order to specify the number of retries you can do in case one try fails. If anyone succeeds then the command stops.

5. Whois :

Syntax : ***whois [-h HOST] [-p PORT] [-aCFHILMmrRSVx] [-g SOURCE:FIRST-LAST] [-i ATTR] [-S SOURCE] [-T TYPE] object***

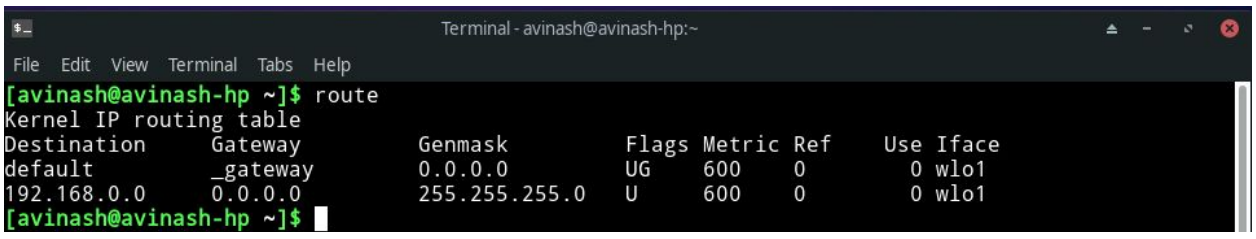
whois searches for an object in a WHOIS database. WHOIS is a query and response protocol that is widely used for querying databases that store the registered users of an Internet resource, such as a domain name or an IP address block, but is also used for a wider range of other information.

As you can see the ipv4 returned by **host** command for "www.google.com" is "142.250.76.36". So in the image below I checked whether the ipv4 "142.250.73.36" belongs to Google or not using **whois** command.



6. route :

route command in Linux 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. Syntax : "***route [OPTIONS]***"



We can get details of kernel/IP routing table using the command "***ip route"***

7. tcpdump :

tcpdump is a packet sniffing and packet analyzing tool 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.

Syntax : "***tcpdump [OPTIONS] [EXPRESSION]***

Output Format :

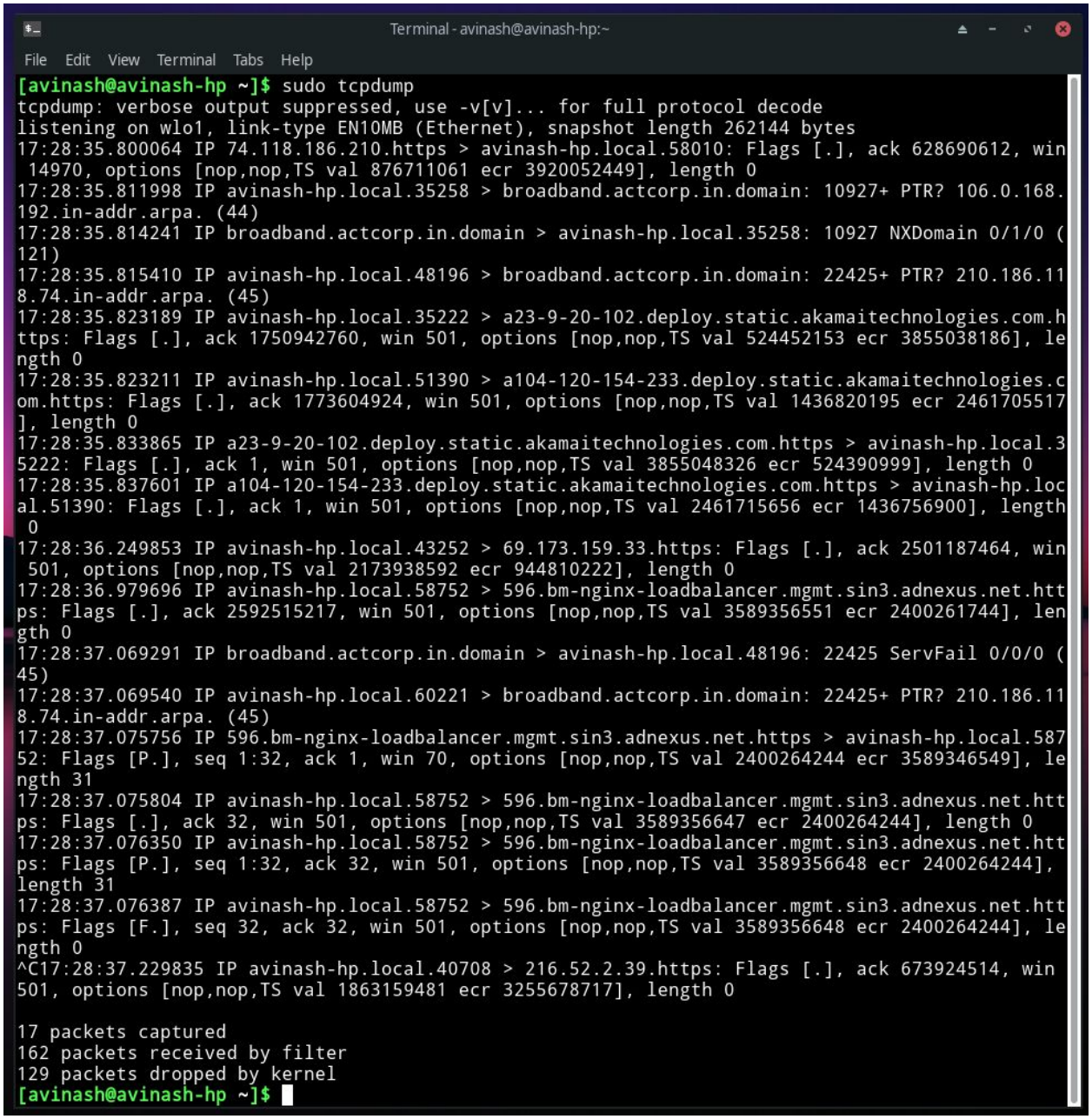
[Timestamp] [Protocol] [Src IP].[Src Port] > [Dst IP].[Dst Port]: [Flags], [Seq], [Ack], [Win Size], [Options], [Data Length]

Example:

15:47:24.248737 IP 192.168.1.185.22 > 192.168.1.150.37445: Flags [P.], seq 201747193:201747301, ack 1226568763, win 402, options [nop,nop,TS val 1051794587 ecr 2679218230], length 108

- 15:47:24.248737 - The timestamp of the captured packet (format: hours:minutes:seconds.frac)
- IP - The packet protocol. In this case, IP means the Internet protocol version 4 (IPv4).
- 192.168.1.185.22 - The source IP address and port, separated by a dot (.).
- 192.168.1.150.37445 - The destination IP address and port, separated by a dot (.).
- Flags [P.] - TCP Flags field. In this example, [P.] means Push Acknowledgment packet, which is used to acknowledge the previous packet and send data.
- seq 201747193:201747301 - The sequence number is in the first:last notation. It shows the number of data contained in the packet.
- ack 1226568763 The acknowledgment number is the sequence number of the next data expected by the other end of this connection.

- win 402 - The window number is the number of available bytes in the receiving buffer.
- options [nop,nop,TS val 1051794587 ecr 2679218230] - TCP options.
- length 108 - The length of payload data.

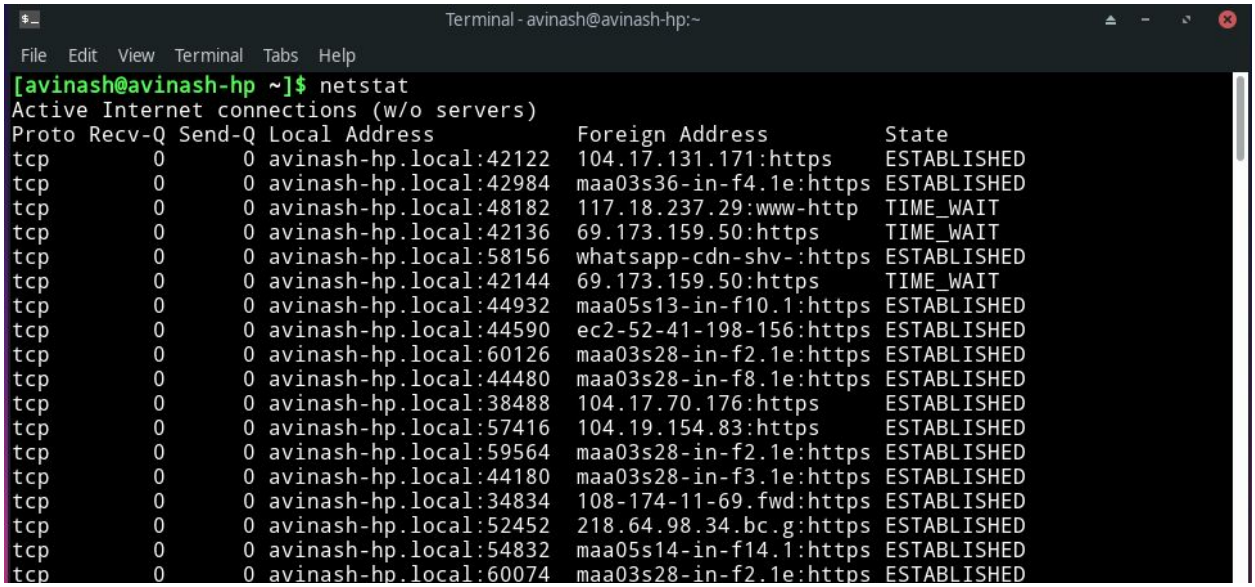


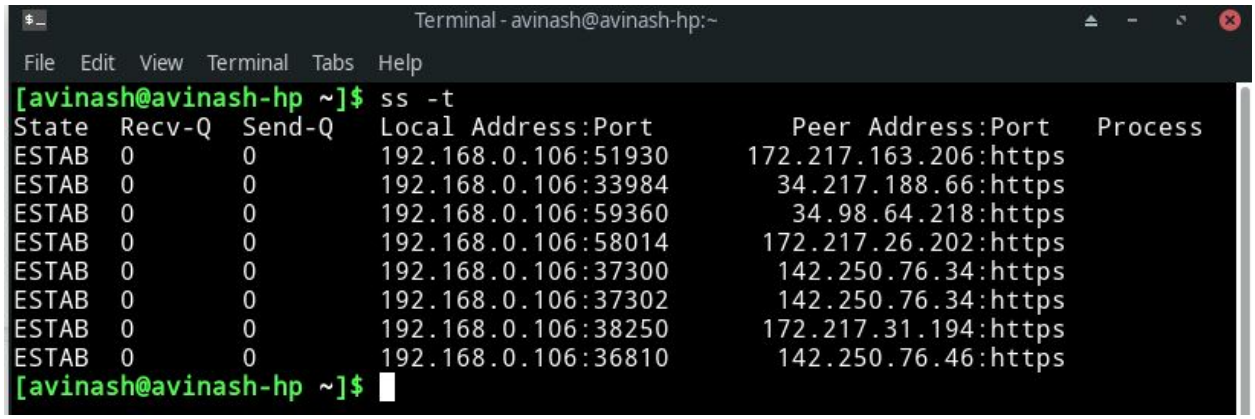
8. netstat / ss :

Syntax : ***"netstat [OPTIONS]" , "ss [OPTIONS]"***

netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,

The ***ss*** command is a tool used to dump socket statistics and displays information in similar fashion (although simpler and faster) to netstat. The ss command can also display even more TCP and state information than most other tools.





 # netstat -at : To list all tcp ports.

 # netstat -au : To list all udp ports.

 # netstat -l : To list only the listening ports.

Options for ss :

-t: display all TCP connections.

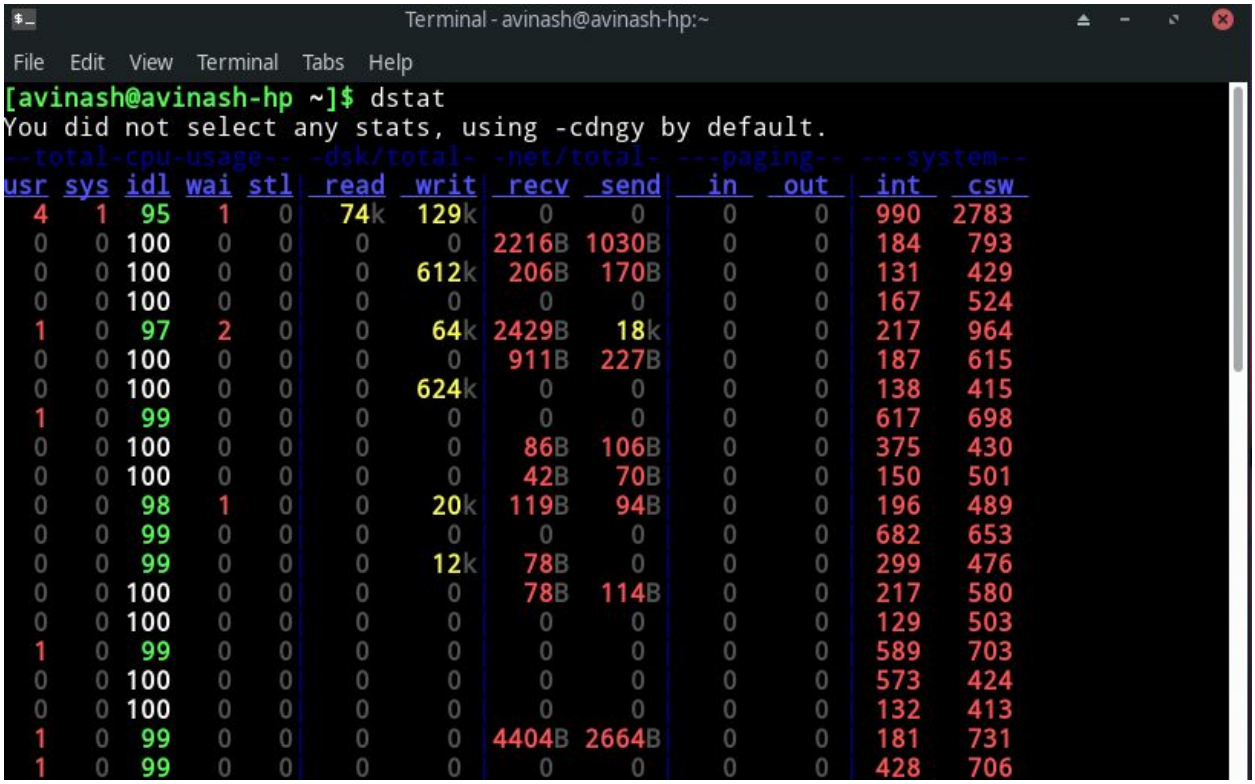
-u: display all UDP connections.

-x: display all UNIX connections.

9. dstat :

dstat is a tool that is used to retrieve information or statistics form components of the system such as network connections, IO devices, or CPU, etc.

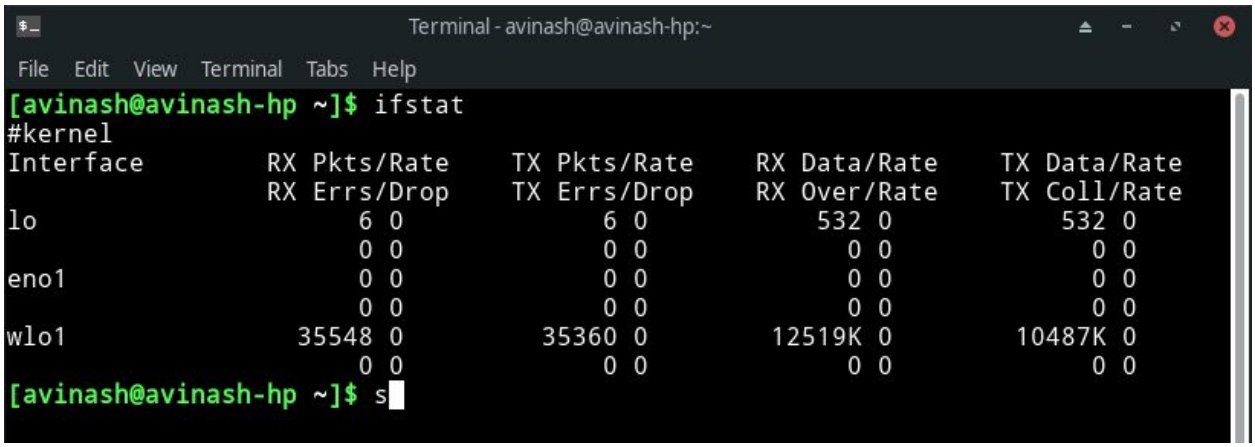
Syntax: "***dstat [OPTIONS]***"



10. Ifstat :

The ifstat command prints network interface statistics. The interface keeps records of the previous data displayed in history files.

Syntax : "***ifstat [OPTIONS][INTERFACE]***"



There are five columns of data per interface, with each interface having two rows. The first column is the interface name. The remaining columns contain two data fields each.

You see packets *received* and rate in the RX column, as well as any errors or drops on those packets. In the TX column, we have packets *transmitted* and rate, as well as errors and drops. After the packet columns, we change the unit of measure to data sent and received. This value is measured in kilobytes. We have data received and rate, as well as data transferred and rate.

11. wget :

Syntax : **“ *wget [OPTIONS] url* ”**

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.

- wget is non-interactive, meaning that it can work in the background, while the user is not logged on. This allows you to start a retrieval and disconnect from the system, letting wget finish the work. By contrast, most of the Web browsers require constant user’s presence, which can be a great hindrance when transferring a lot of data.
- wget can follow links in HTML and XHTML pages and create local versions of remote web sites, fully recreating the directory structure of the original site. This is sometimes referred to as recursive downloading. While doing that, wget respects the Robot Exclusion Standard (/robots.txt). wget can be instructed to convert the links in downloaded HTML files to the local files for offline viewing.
- wget has been designed for robustness over slow or unstable network connections; if a download fails due to a network problem, it will keep retrying until the whole file has been retrieved. If the server supports resuming, it will instruct the server to continue the download from where it left off.

Options :

-q : turn off output in terminal while downloading.

-b : to download file in background.

-c : To resume a partially downloaded file.