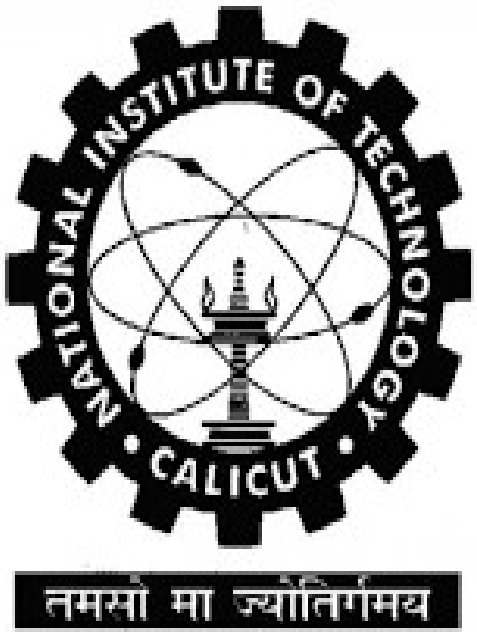
CS3009D: NETWORKS LABORATORY
(EXPERIMENT 1)

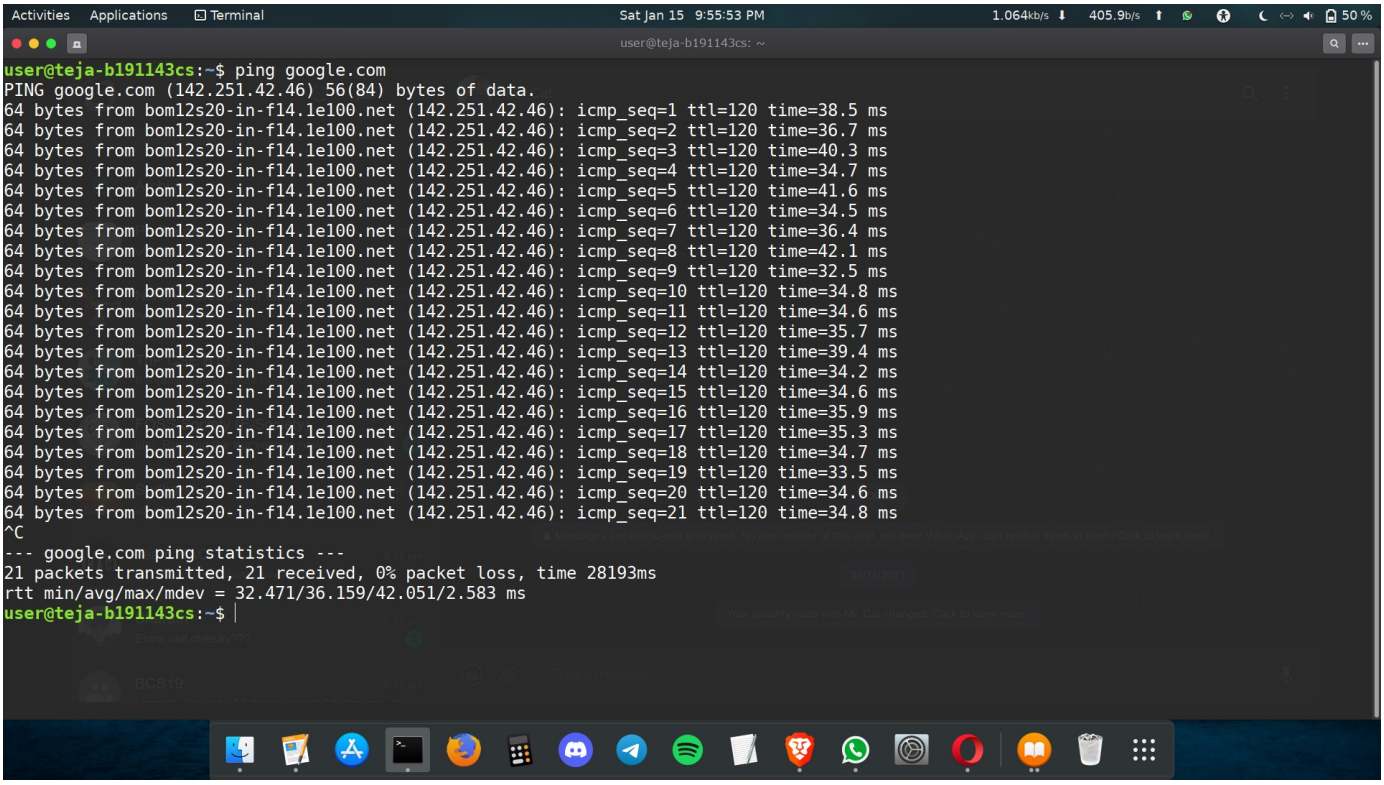


Name : Panasa Teja
ROLL : B191143CS
BATCH : B

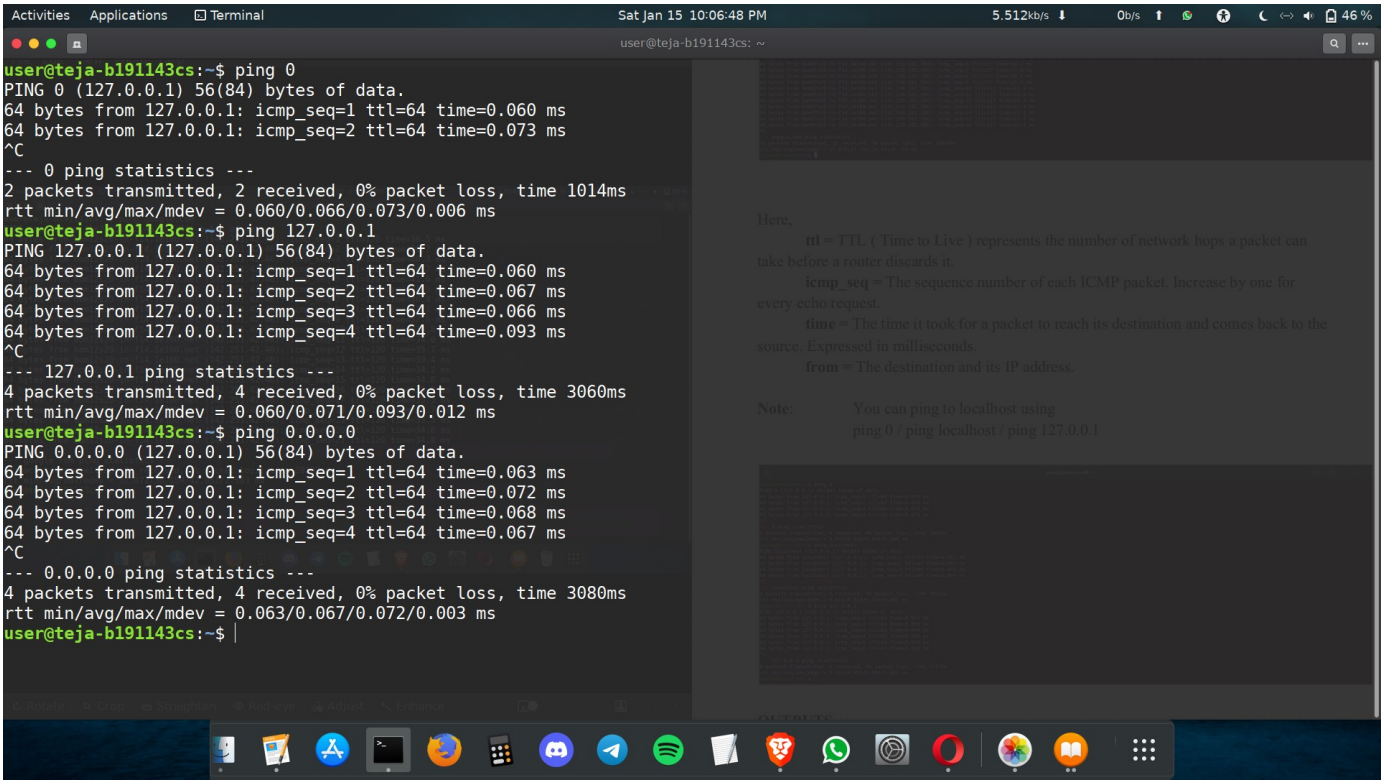
1. ping

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 www.amazon.com



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 127.0.0.1



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.

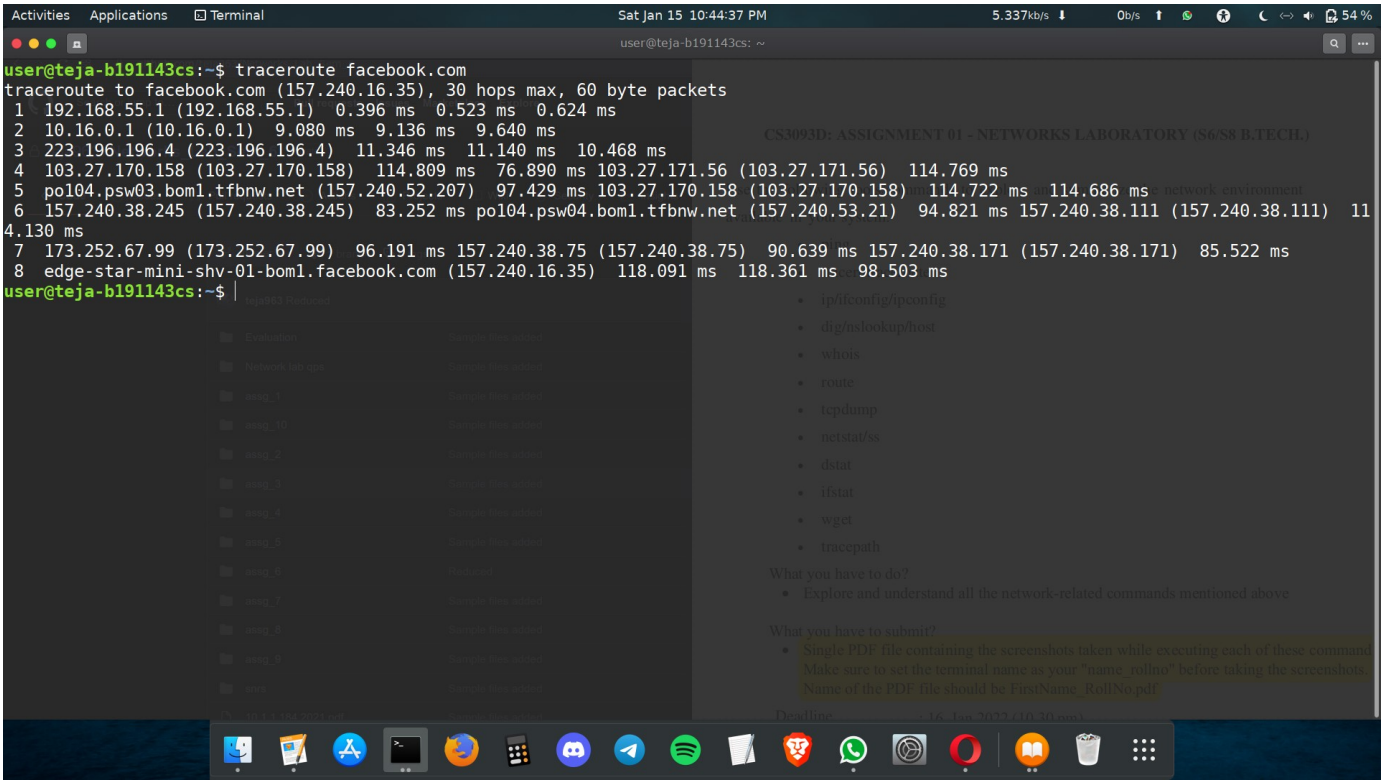
Case2: If the output is “request timed out” then it means the host is down or blocking our ICMP requests.

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



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**

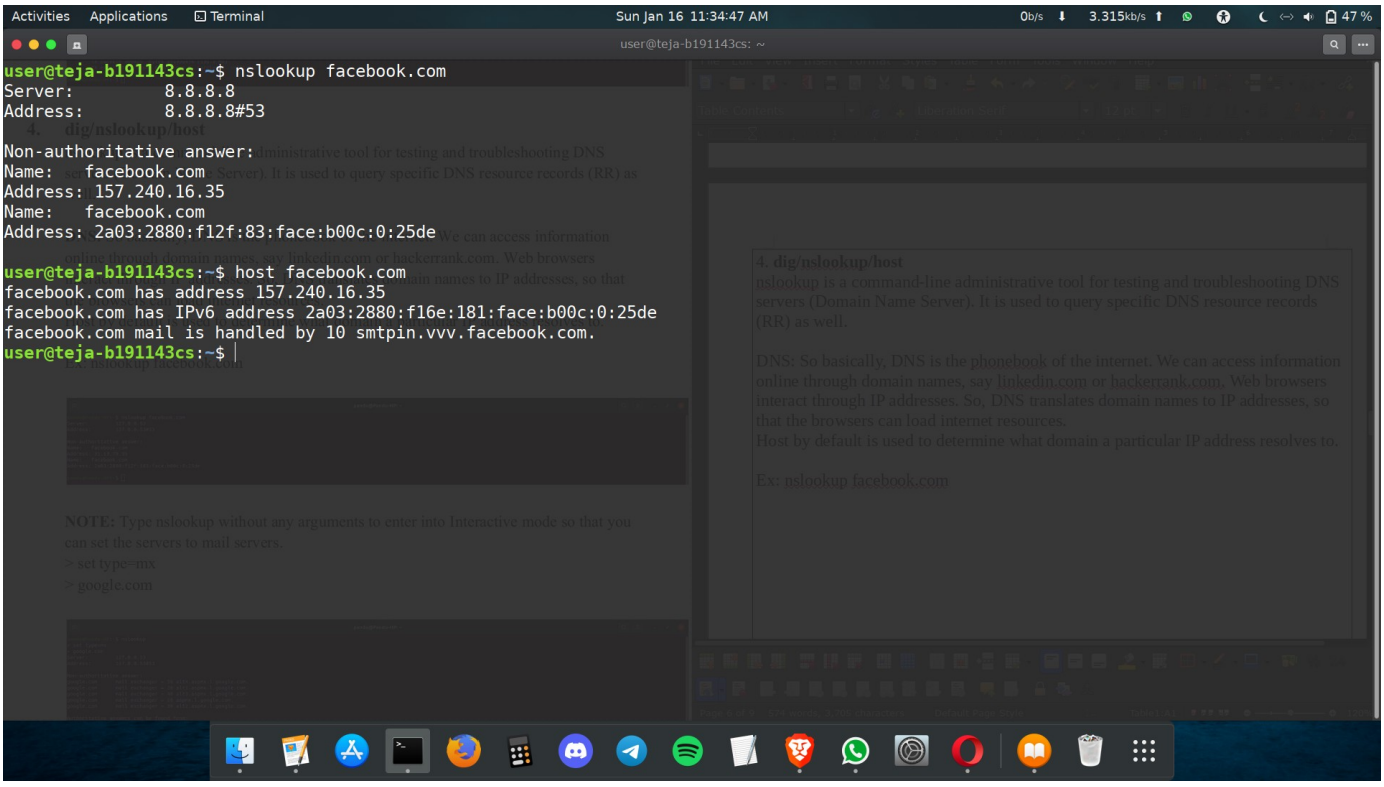
ip r
Find the gateway address in the starting line. 192.168.55.1 is the default gateway in the given image.

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.

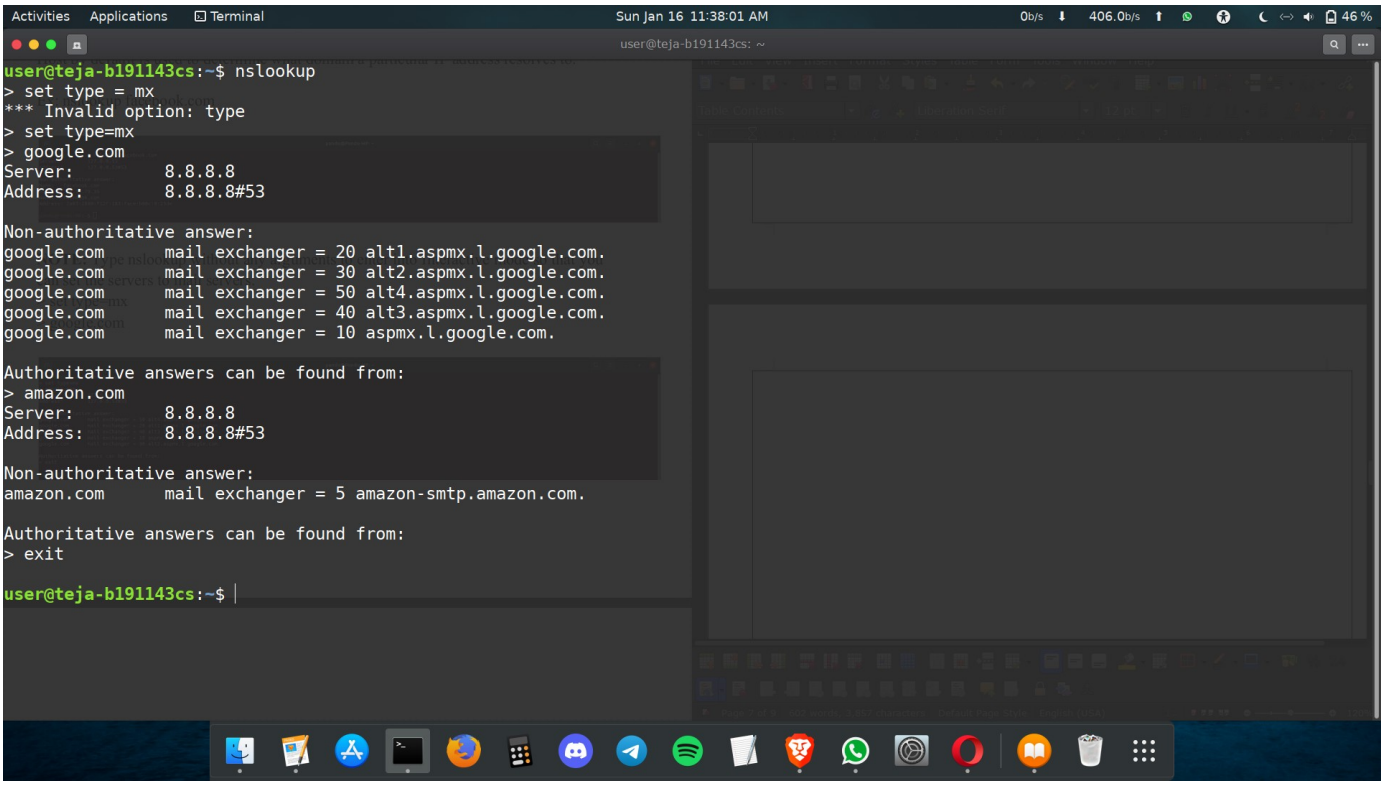
DNS: So basically, DNS is the phonebook of the internet. We can access information online through domain names, say linkedin.com or hackerrank.com. Web browsers interact through IP addresses. So, DNS translates domain names to IP addresses, so that the browsers can load internet resources.
Host by default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

Ex: nslookup facebook.com

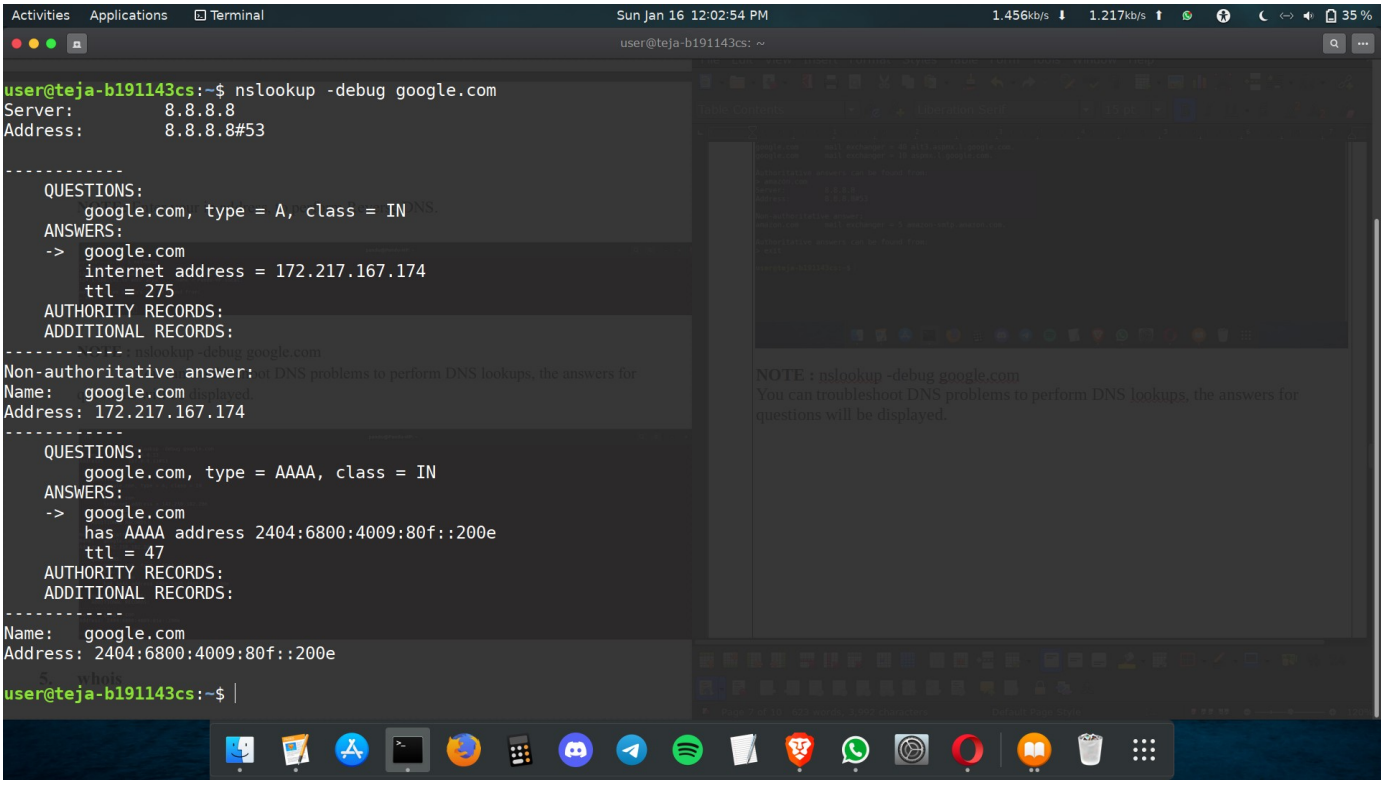


NOTE: Type nslookup without any arguments to enter into Interactive mode so that you
can set the servers to mail servers.
> set type = mx

> google.com



NOTE : nslookup -debug google.com
You can troubleshoot DNS problems to perform DNS lookups, the answers for questions will be displayed.

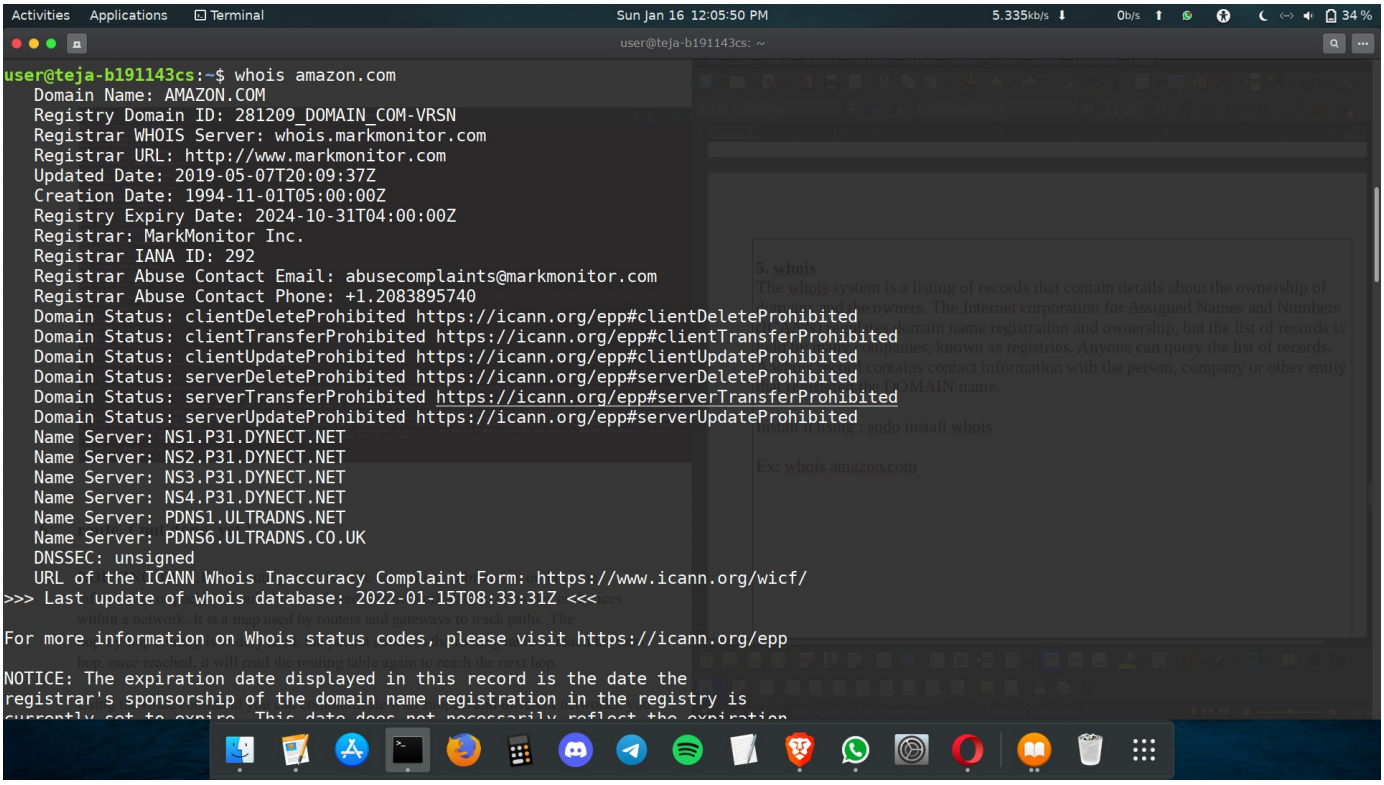


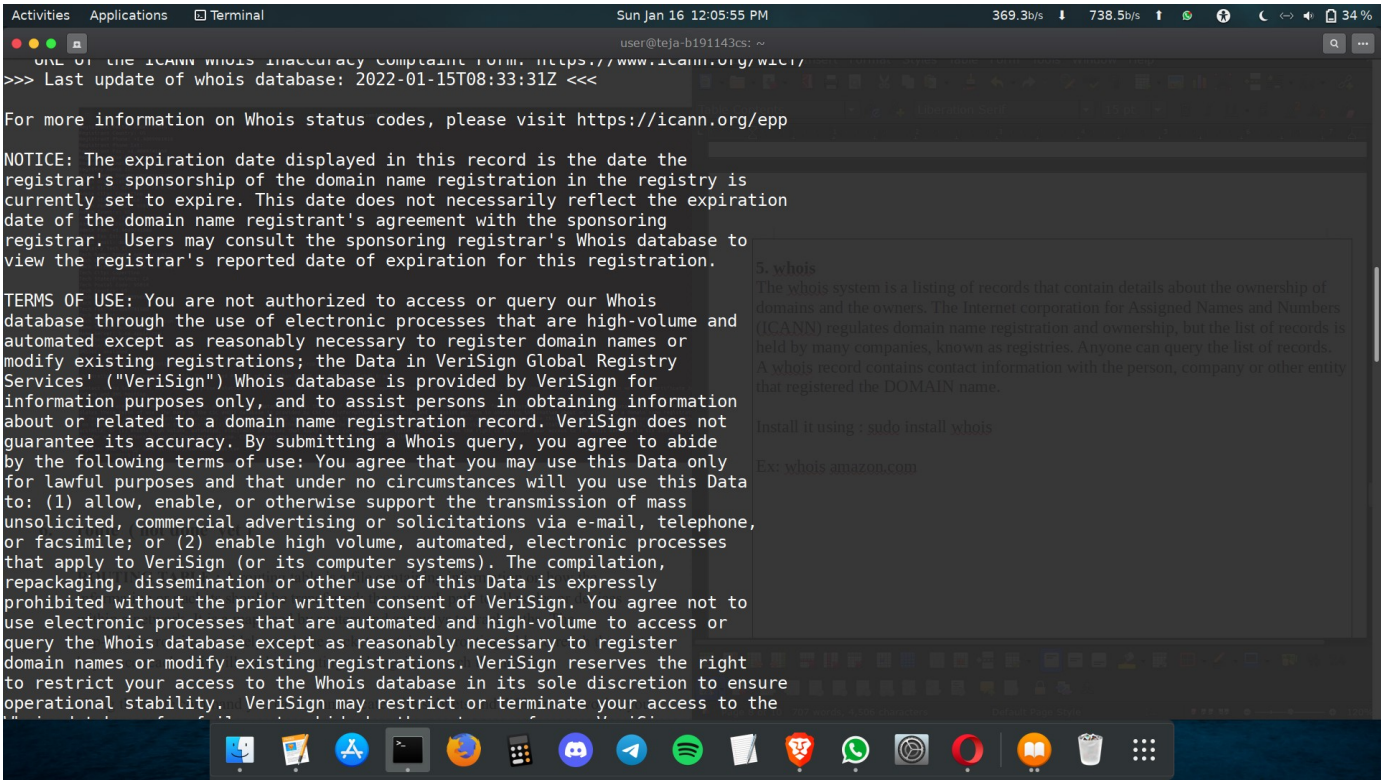
5. whois

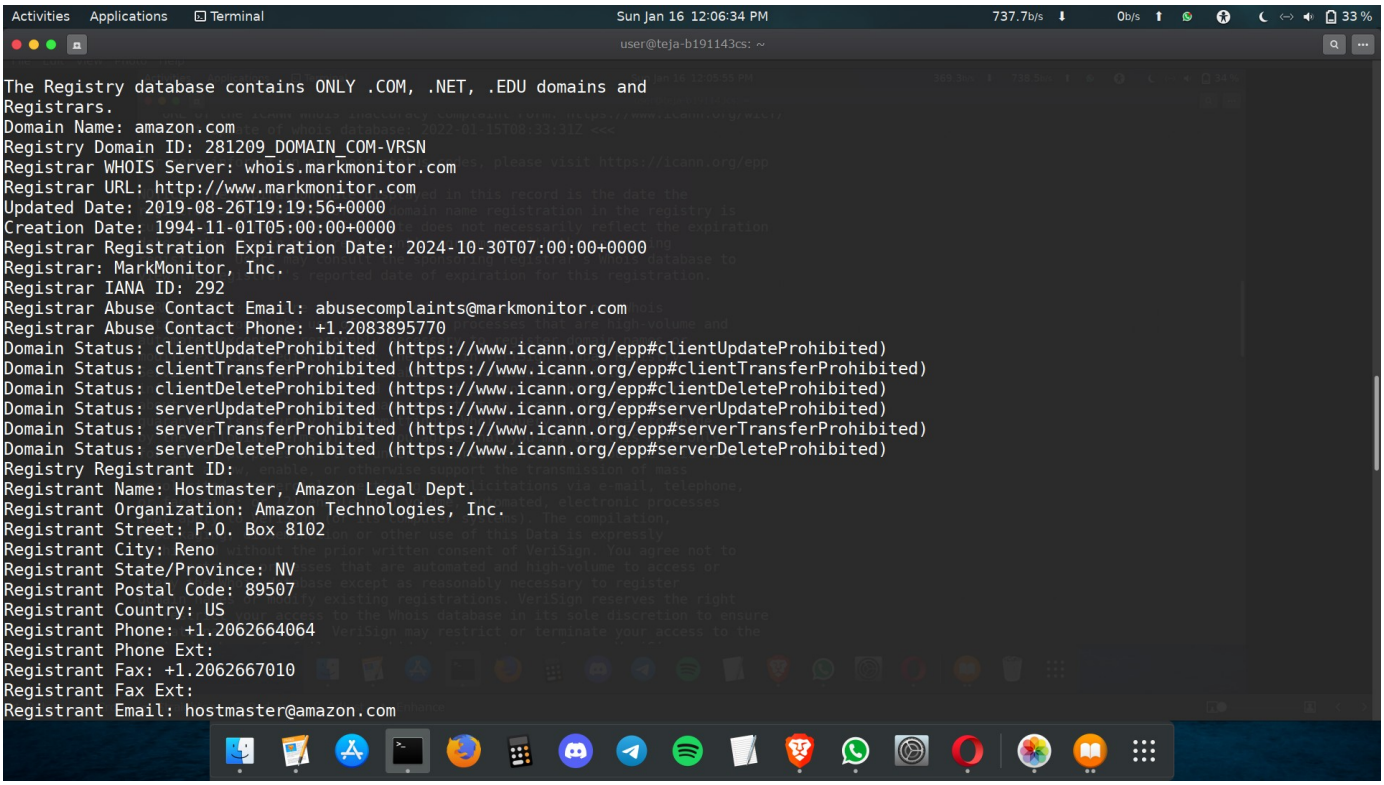
The whois system is a listing of records that contain details about the ownership of domains and the owners. The Internet corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership, but the list of records is held by many companies, known as registries. Anyone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

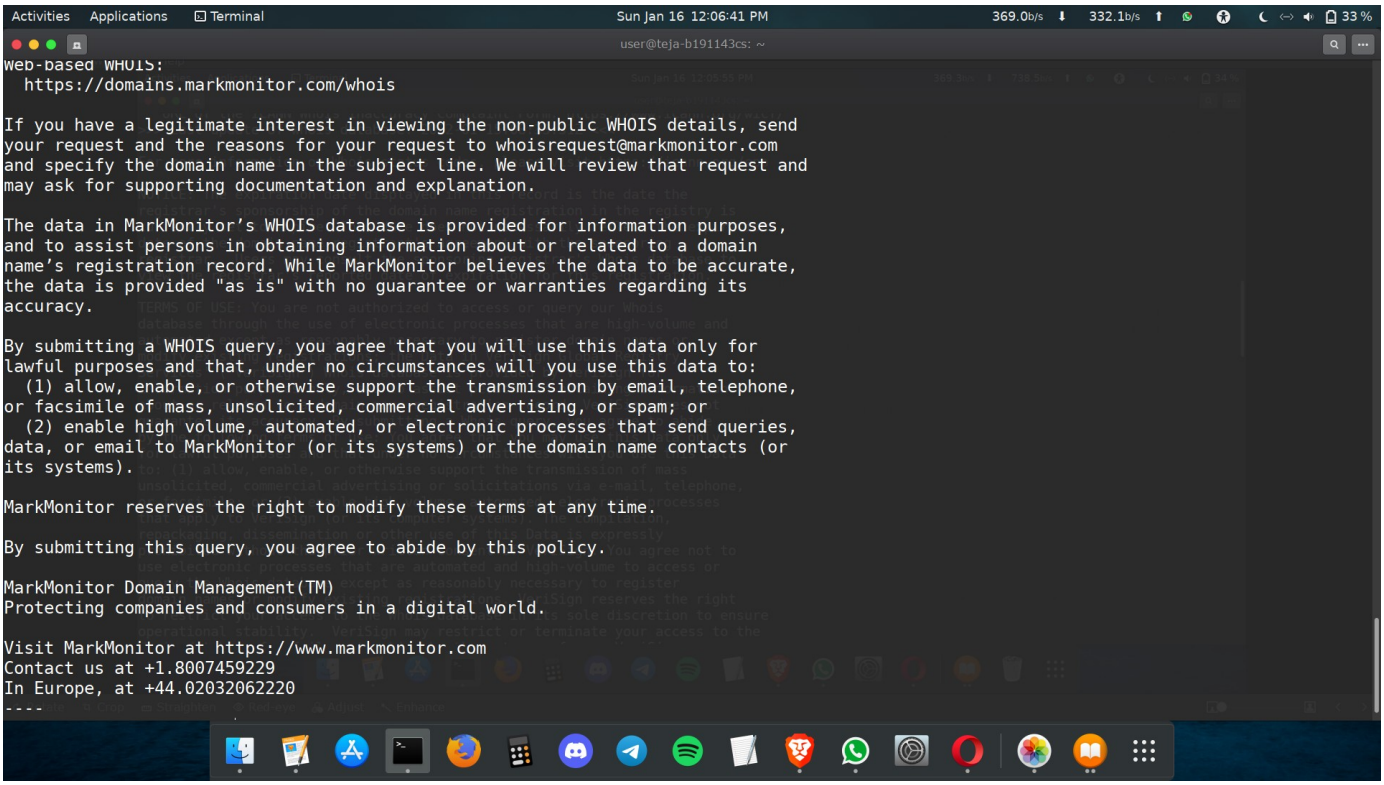
Install it using : sudo install whois

Ex: whois amazon.com




Activities Applications Terminal Sun Jan 16 12:05:55 PM 369.3b/s 738.5b/s 34 %
user@teja-b191143cs: ~
>>> Last update of whois database: 2022-01-15T08:33:31Z <<<
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

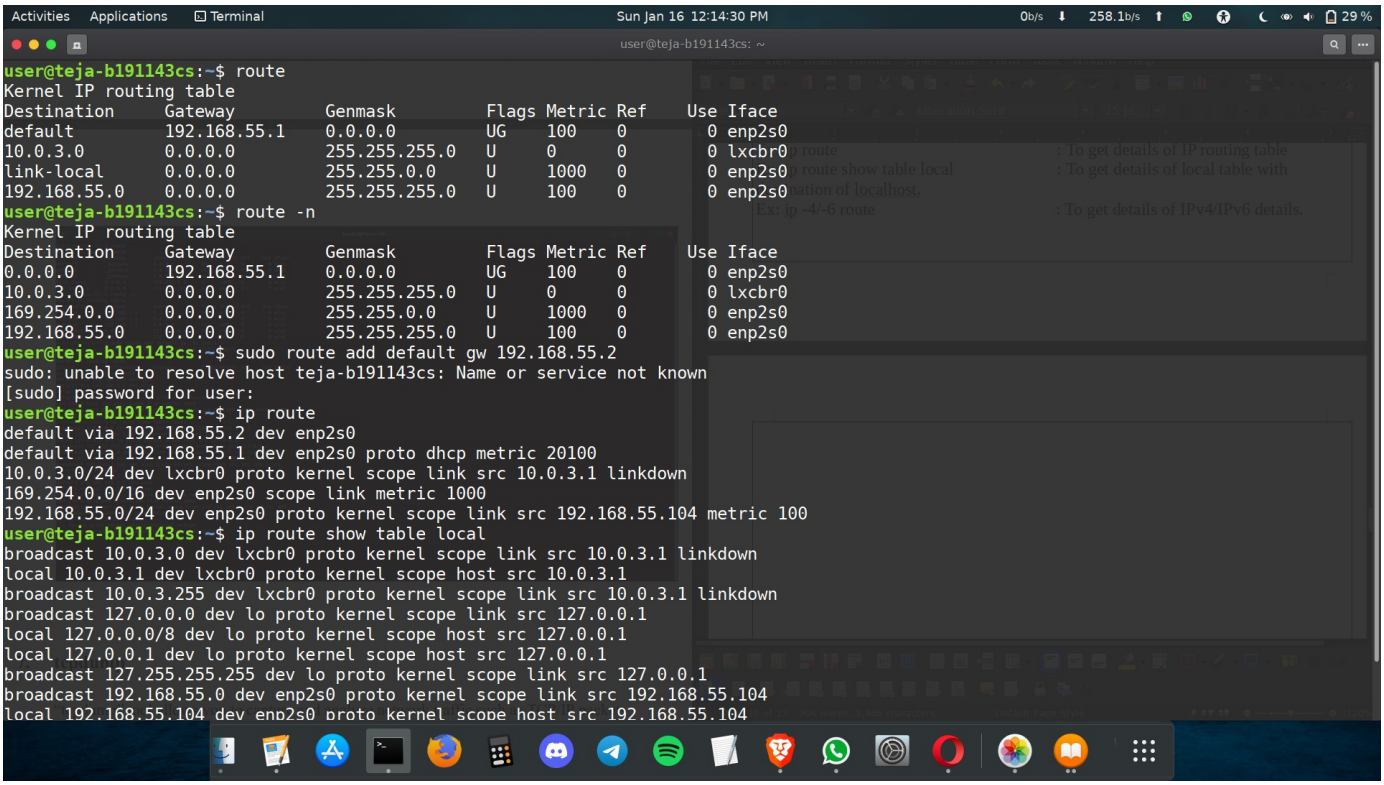

Activities Applications Terminal Sun Jan 16 12:06:34 PM 737.7b/s 0b/s 33 %
user@teja-b191143cs: ~
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: amazon.com
Registry Domain ID: 281209_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-08-26T19:19:56+0000
Creation Date: 1994-11-01T05:00:00+0000
Registrar Registration Expiration Date: 2024-10-30T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Hostmaster, Amazon Legal Dept.
Registrant Organization: Amazon Technologies, Inc.
Registrant Street: P.O. Box 8102
Registrant City: Reno
Registrant State/Province: NV
Registrant Postal Code: 89507
Registrant Country: US
Registrant Phone: +1.2062664064
Registrant Phone Ext:
Registrant Fax: +1.2062667010
Registrant Fax Ext:
Registrant Email: hostmaster@amazon.com



6. route

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.



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

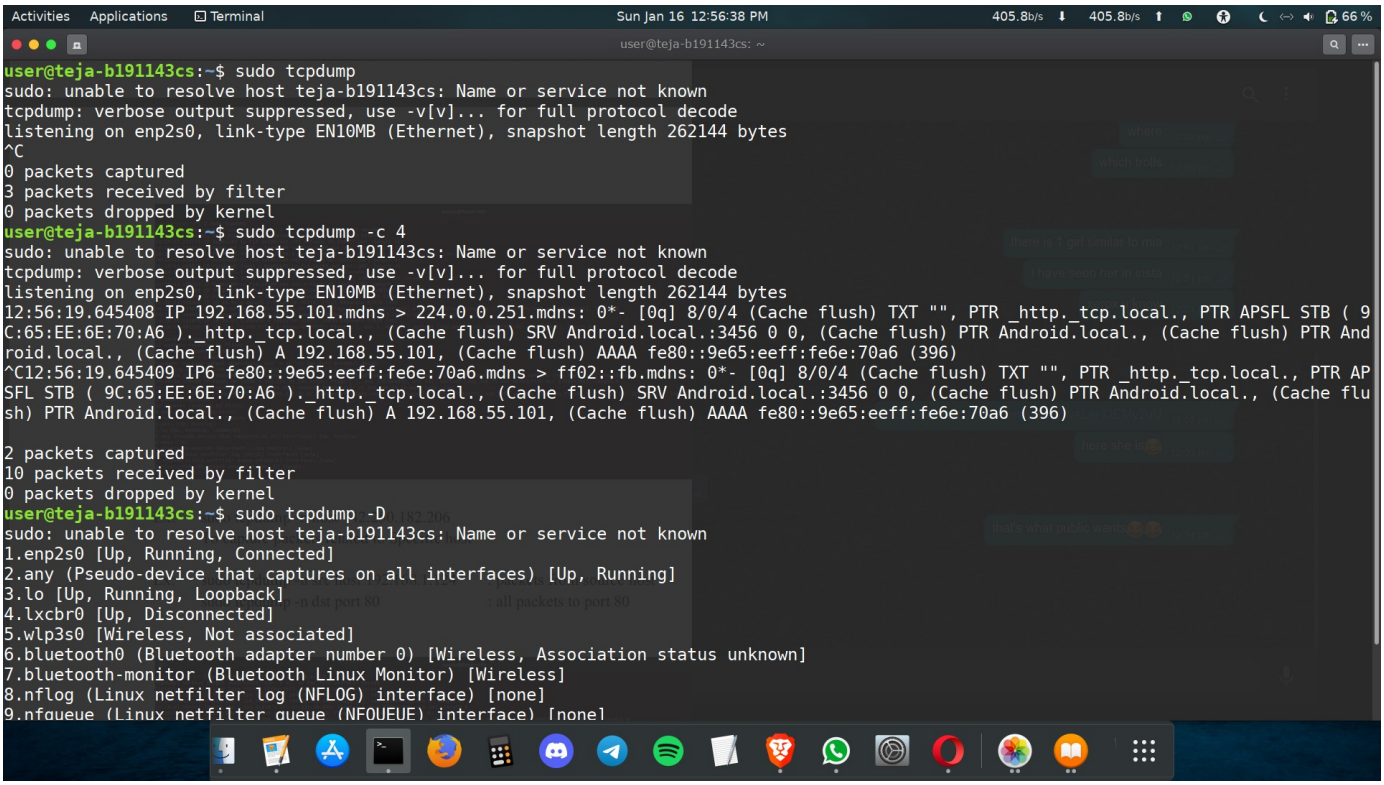
It will capture packets from the current interface of the network through which the system is connected to the internet.

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.



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

Ex: sudo tcpdump -n src host 192.168.55.104 : packets from source host
sudo tcpdump -n dst port 80 : all packets to port 80

8. netstat/ss

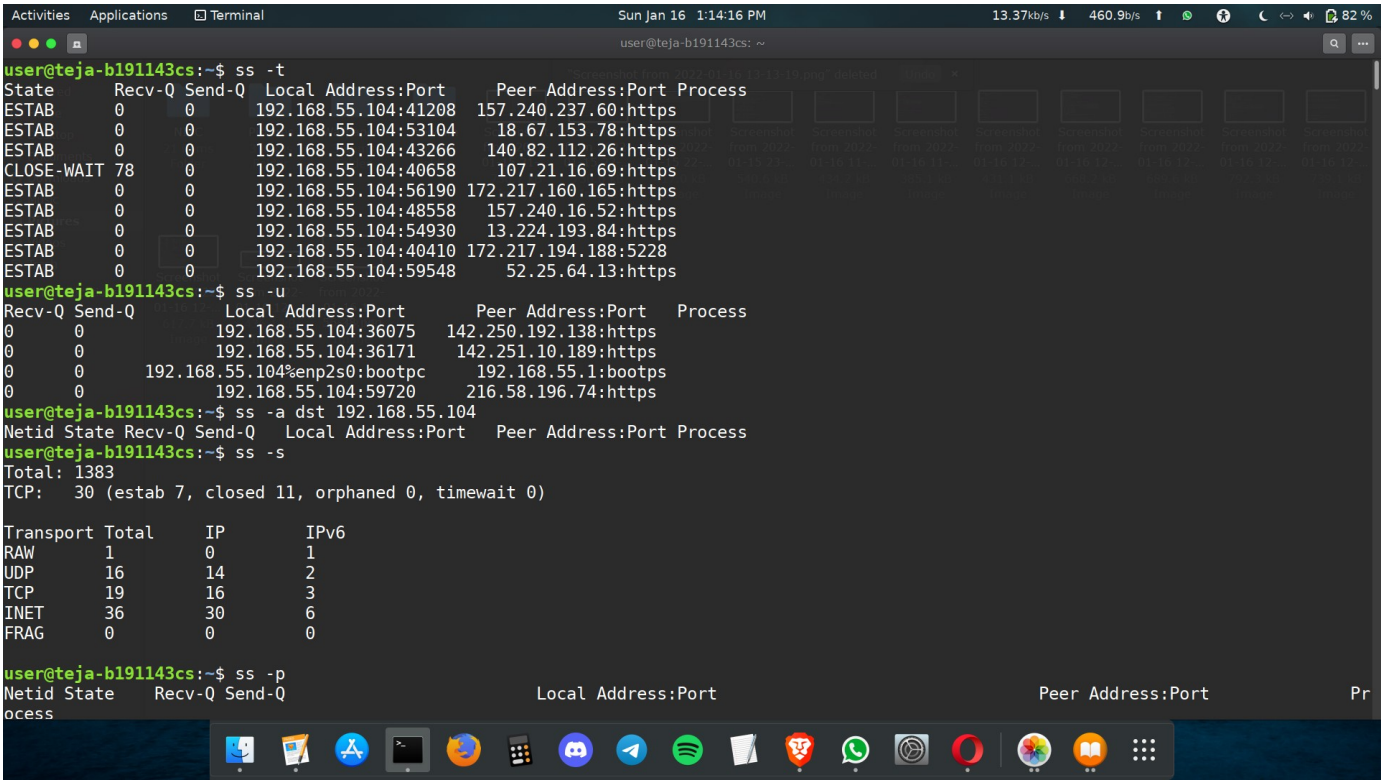
netstat is a command tool which displays network connections for TCP/UDP and stats for Interfaces, Network protocols, routing tables, etc. ss replaces netstat. ss command tool which dumps socket stats and displays information similarly but it is faster than netstat.

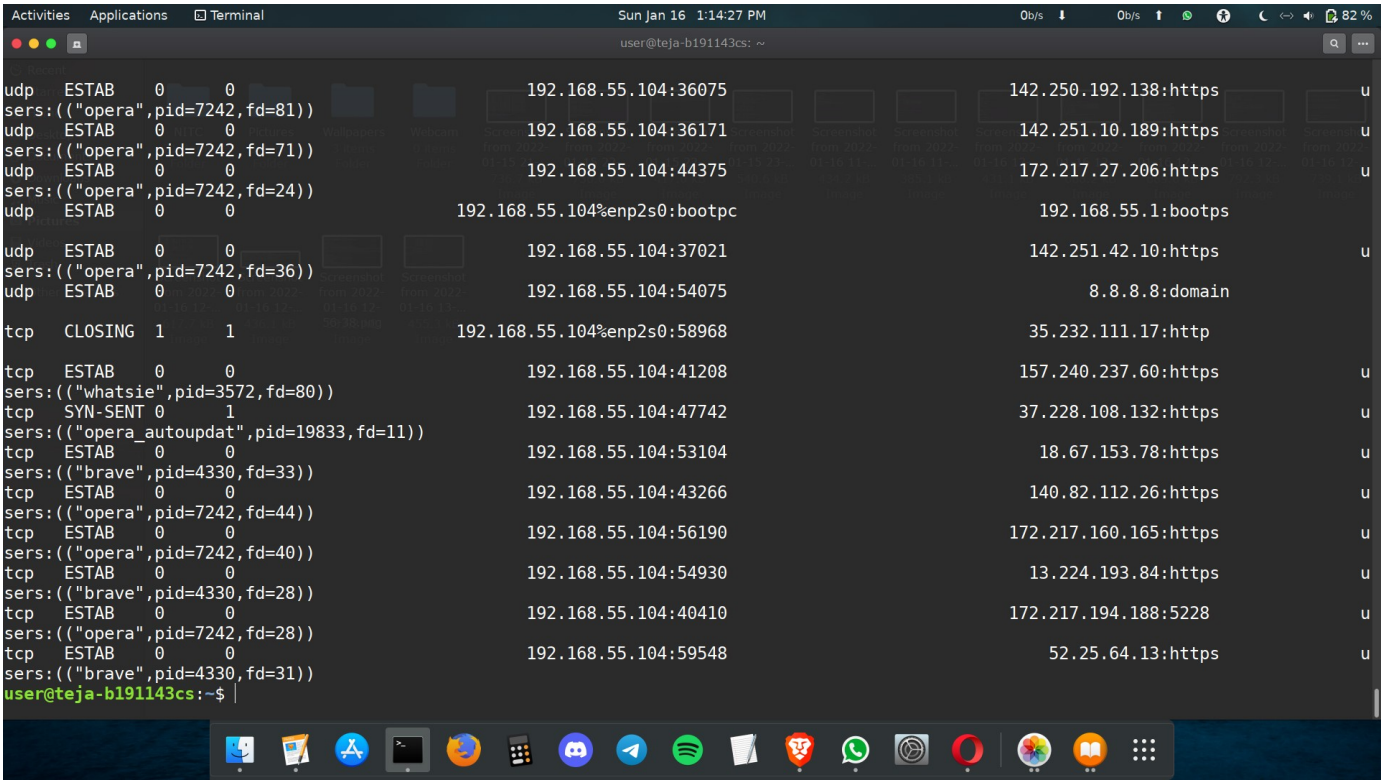
With ss, we get detailed information about how Linux is communicating with othermachines, networks, details about network stats, network protocols, linux socket connections. So, using this information, it's easy to troubleshoot network issues.

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.





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 :

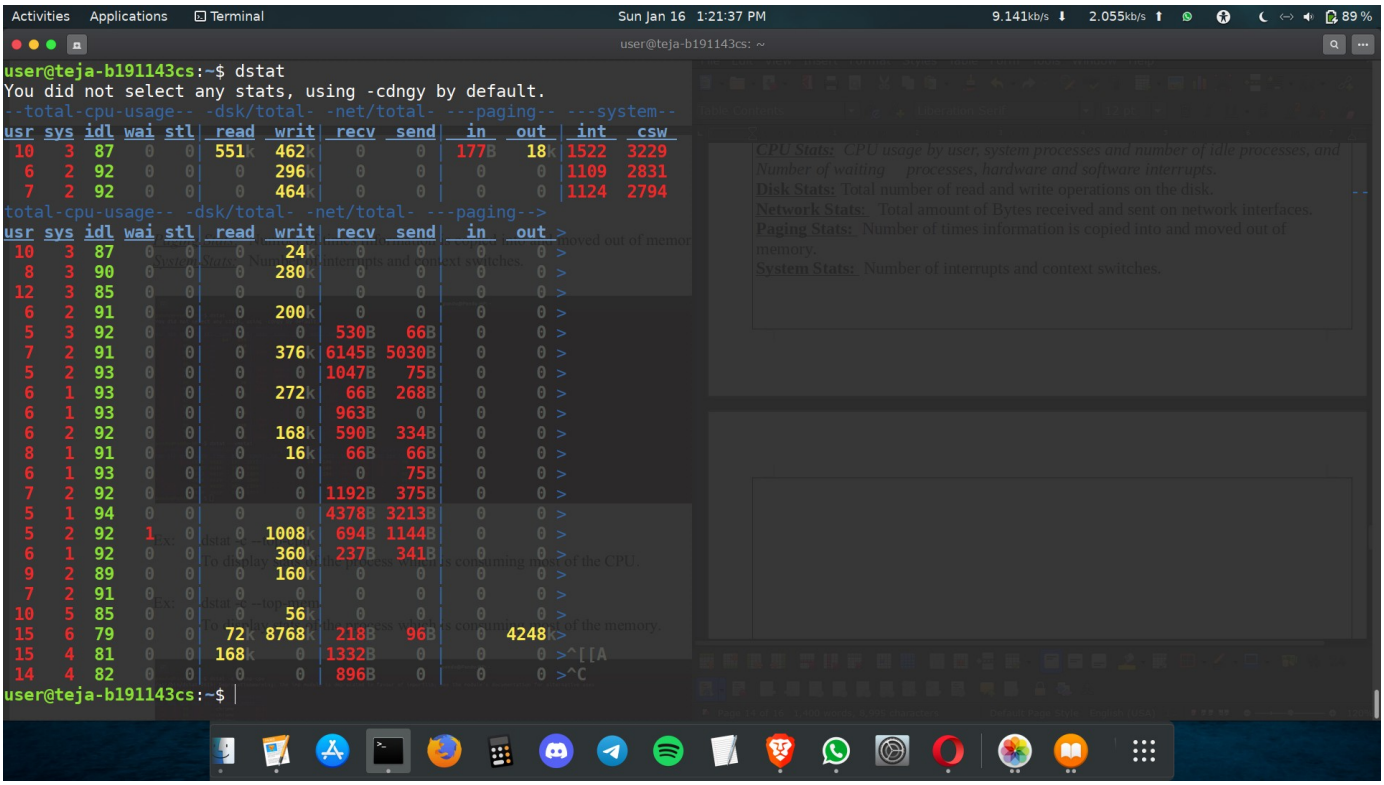
CPU Stats: *CPU usage by user, system processes and number of idle processes, and Number of waiting processes, hardware and software interrupts.*

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.

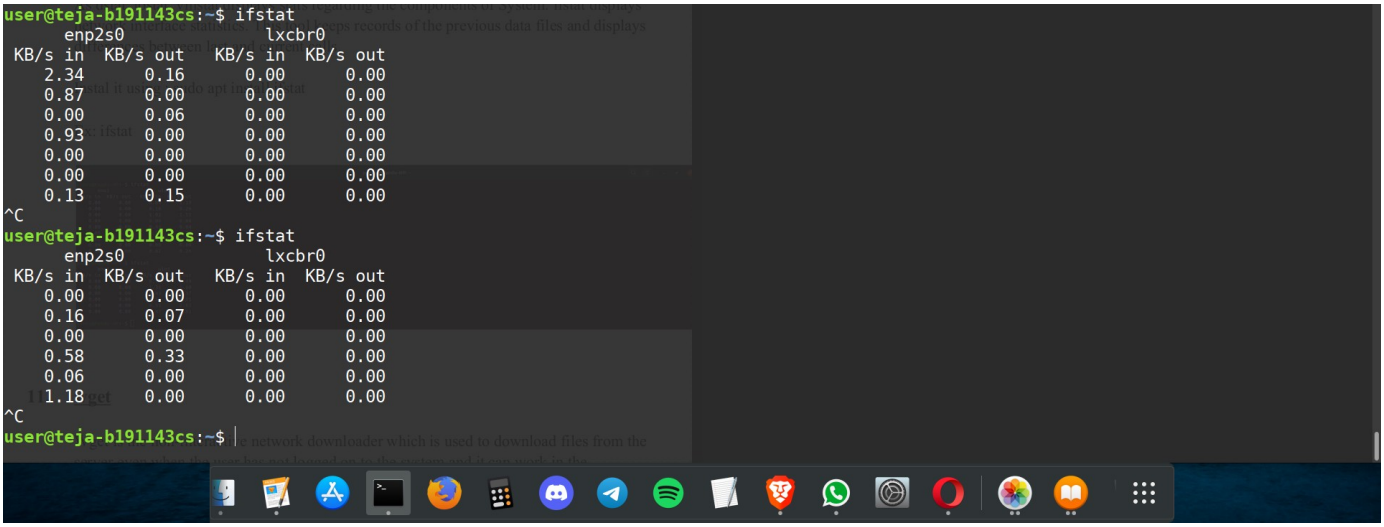


10. ifstat

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.

Install it using : $**sudo apt install ifstat**

Ex: ifstat



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.