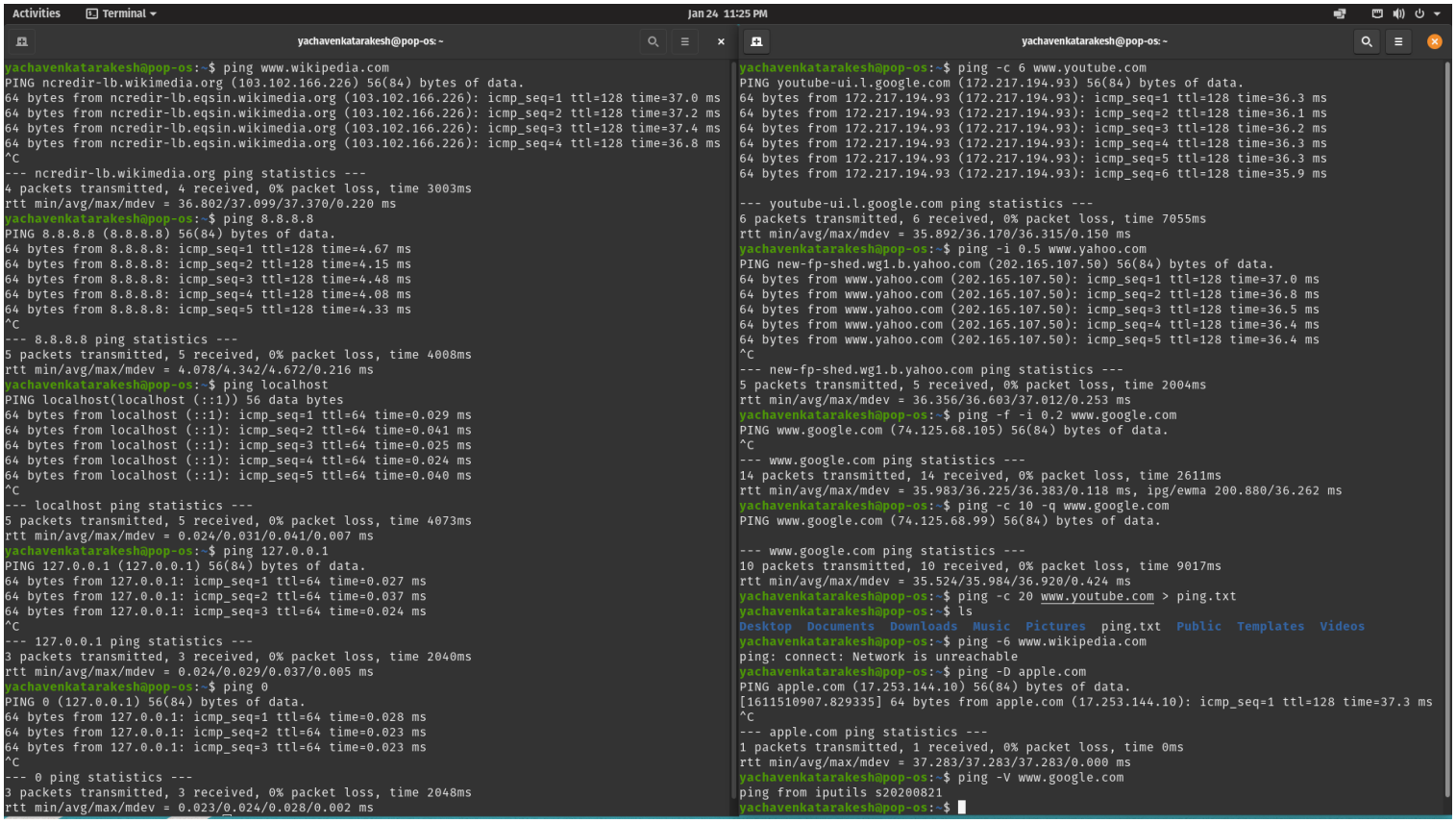
NETWORKS LAB EXPERIMENT – 1

YACHA VENKATA RAKESH

B180427CS



PING COMMAND

Ping command is a simple tool that can be used in troubleshooting network issues either connected to Local Area Network or the Internet and also test for network delay and packet losses or to test DNS issues such as name resolution. It works on network layer.

ICMP (Internet Control Message Protocol) echo request and the ICMP echo reply messages are commonly known as ping messages.

We can ping an IP address or domain name of a host. This host could be any network device such as computer, server, router or printer, whether its on local area network or in the internet. In terminal when we type ping www.wikipedia.com then domain name is sent to the dns server which maps this to the IP address of the server of that domain and send data packets to that server and then our computer wait for a response. Then the server will send the data packets back to us as a reply and these replies are called echo reply request and these replies inform you about what's happening with server we pinged.

If we received a reply then that means there is network connectivity between us and server. When we ping a server and get a message "request timed out" then that could mean that either server is powered down or server is up and running but it's using a firewall that's blocking all ping requests. When we ping a server and get a message "destination host unreachable" route to that destination can't be found. That is the router

doesn't have information on how to route data to the destination or it could also mean remote server is down or disconnected to network or it could also mean that our system is not connected to the network.

To test if network interface card is working

$ ping localhost or $ping 127.0.0.1

This is called a loopback test(will send out signals back to your system for testing)

To test DNS name resolution issues

$ ping domainname

And if we get "ping request could not find host domain name. Please check and try again" could be because of DNS name resolution issues.

Some other ping commands:

1. $ping Domainname or $ping IPaddress
from : The destination domain name and it's ip address
IP address of the destination website might change based on our geographical location.
icmp_seq: The sequence number of each ICMP packet. Increases for every subsequent echo request. It is also called as hop
ttl : The time to live value from 1 to 255. It can represents number of network hops a packet can take before router discards it.
A hop is occurred when a packet is passed from one network segment to another.
time: The time it took a packet to reach the destination and come back to source. It is expressed in milliseconds.

2. $ping -i 0.5 www.wikipedia.com
To increase time between two packets keep a number > 1
Else keep a number < 1 (minimum 0.2)

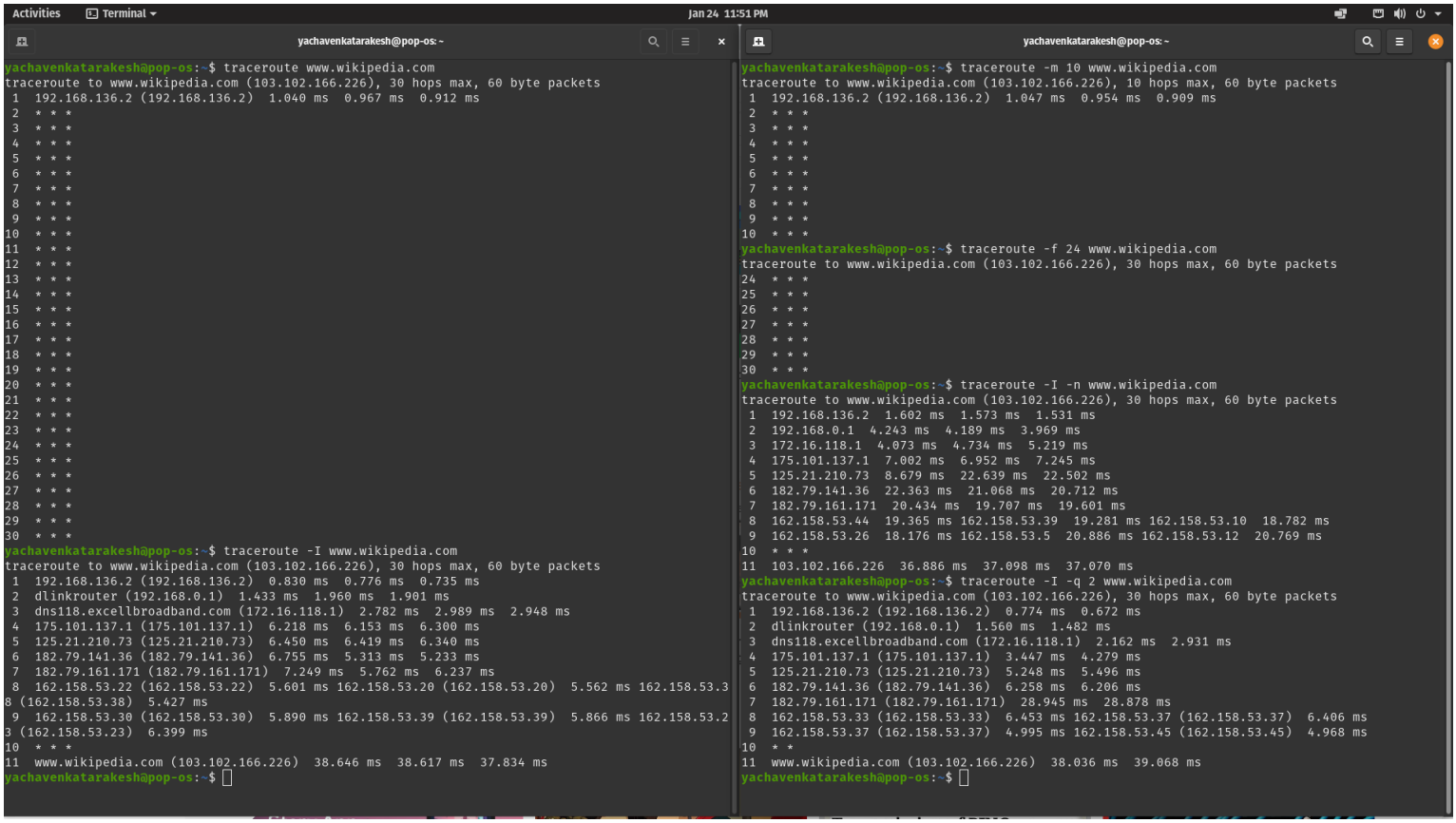
3. $ping -s 1000 www.wikipedia.com
To change packet size which is 64 bytes by default.

4.$ping -f -i 0.2 www.wikipedia.com
This prints '_' for every sent packet and backspace for every received packets

5.$ping -c 10 -q www.wikipedia.com
This print only summary statistics without complete details

6.$ping -c 20 www.wikipedia.com > ping.txt
This saves the details of the ping data received into ping.txt file

7.$ping -v www.wikipedia.com
To display the version of this ping utility



Traceroute

Traceroute is a command line utility that is used to show the exact route that is taken by the data packets as they travel across the internet to their destination. This tool is used to find problems like bottlenecks, such as why and where a connection to a server might be lagging.

Traceroute not only pings the final destination, but it also pings each router on its way to the destination and measures the round trip time that the data packets took from each router and destination. Note that this shows route from source server or device to the destination server.

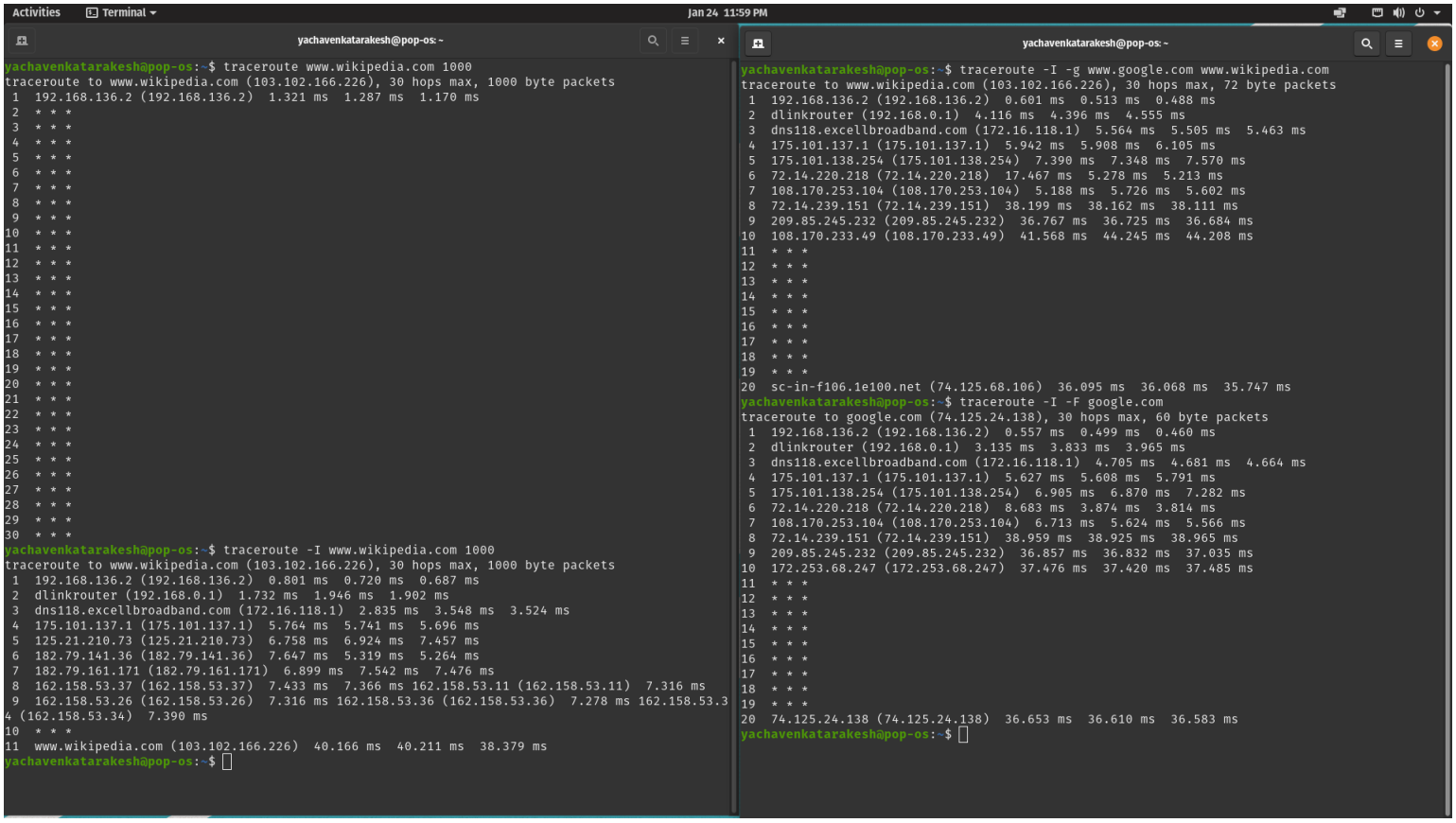
Each time three data packets are sent to each router on its way to the destination. This is just to ensure that if in case something strange happened resulting in a high round trip time for a packet but low round trip time for the other two packets.

First column shows number of hops or steps route took. Next three columns tells the round trip time each data packet took to each point and back to your computer. The last column shows IP address and also the domain name if its available.

Using traceroute we can know whether the problem is with LAN or server. High round trip time doesn't always mean there's a problem with router, it could just mean distance between certain routers are thousands of miles apart. Stars in between indicate that the router wasn't configured to return traceroute replies but still passed on data packets to next router.

TTL : It is a given value of maximum number of hops they can take before getting discarded.

By default it says over a maximum of 30 hops. So if datapackets don't reach destination after 30 hops, data packets are dropped. The reason for keeping a limit is to prevent data packets from travelling endlessly around internet trying to figure out its destination. This could happen, if certain routers in internet are misconfigured and the data packets could be caught in an endless loop.
In windows it is tracert not traceroute.



Traceroute

Traceroute commands:

1. traceroute domainname or IP address
   Prints all the path travelled by the data packets to reach the given destination

2. traceroute -m 40 www.wikipedia.com
   Limits traceroute to 40 hops

3. $traceroute -f 10 wikipedia.com
   This diplays only from hop_count 10

4. $traceroute -n www.wikipedia.com
   This prints ip addresses instead of domain names

5. $traceroute -I www.wikipedia.com
   This try to print complete details instead of stars

6. $traceroute -q 2 www.wikipedia.com

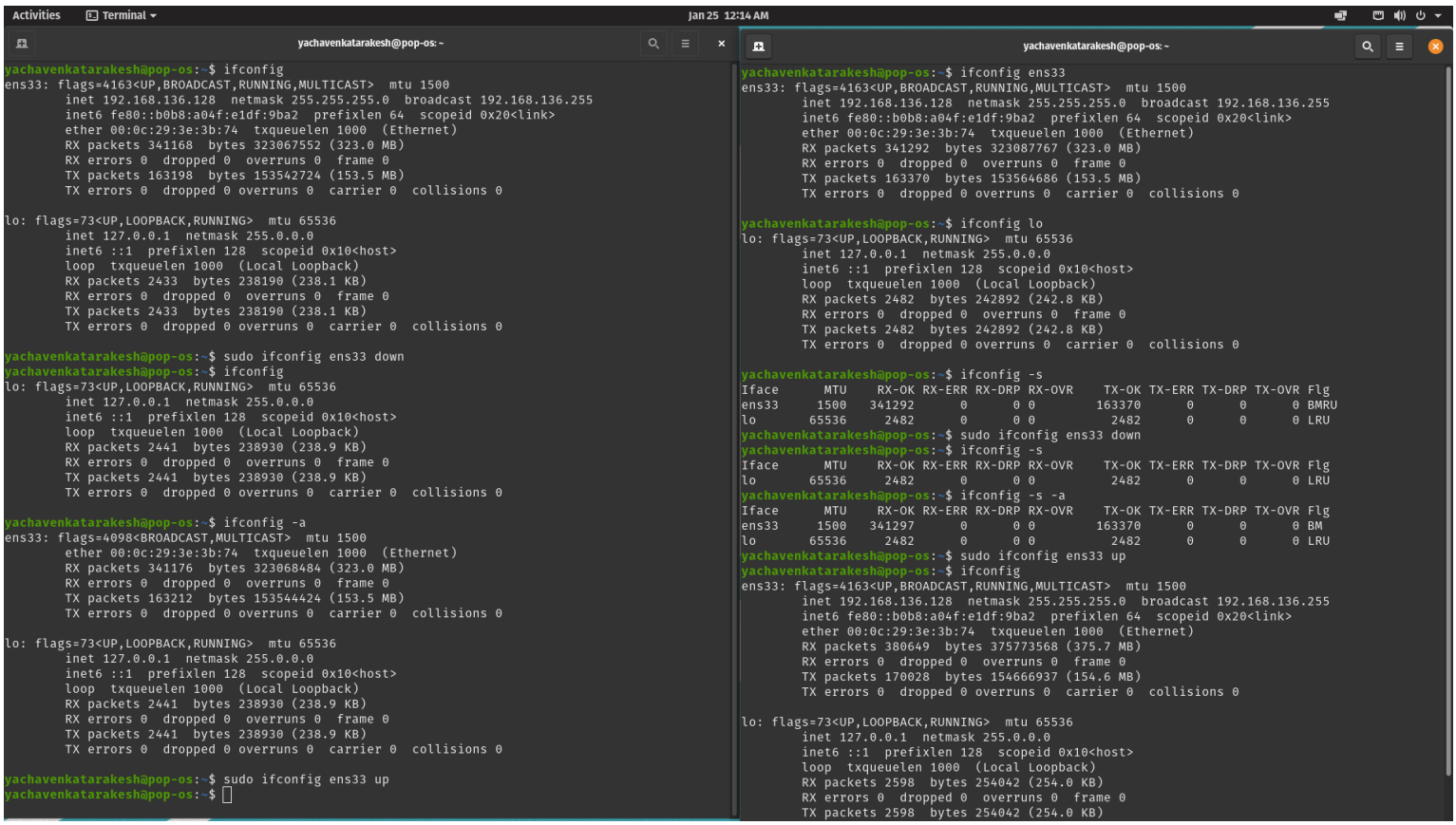
This limits number of datapackets per hop to 2

7. $traceroute -g www.wikipedia.com www.google.com

To route a packet through this gate

8. $traceroute -F www.wikipedia.com

To not fragment the packet



Ifconfig

Ifconfig stands for interface configuration. It is used to view and change the configuration of network interface on system.

“ens0” -> Connected to wired (Ethernet)

“wlan0” -> Connected to wireless (router)

“lo” -> loop back interface, which system uses to communicate to itself.

Each of the network interface contains

1. Hwaddr (Mac address of the computer)
2. inet addr (Local IP address given to the computer) (LAN address)
3. Bcast (Broadcast address)
4. Mask (Subnet mask)
5. inet6 addr (IPv6 address)

6. Rx packets -> Received packets
7. Tx packets -> Transmitted packets
   At the time of execution of the command
8. mtu (Maximum Transmission Unit)
   Size of each packet received by the ethernet card. Loop back interface will have larger packet size
9. txqueuelen this denotes the length of that transmitted queue of your device.
   You can set it to smaller values for slower devices with high latency.
10. Collision (>0 indicate that the packets are colliding while transferring your network which is sure sign of network congnition)

ifconfig commands:

1. $ifconfig
   Shows all the network interfaces which are active in the device

2. $ifconfig interface_name
   Shows details of only that particular interface

3. $sudo ifconfig ens33 down
   This disables the ens33 interface

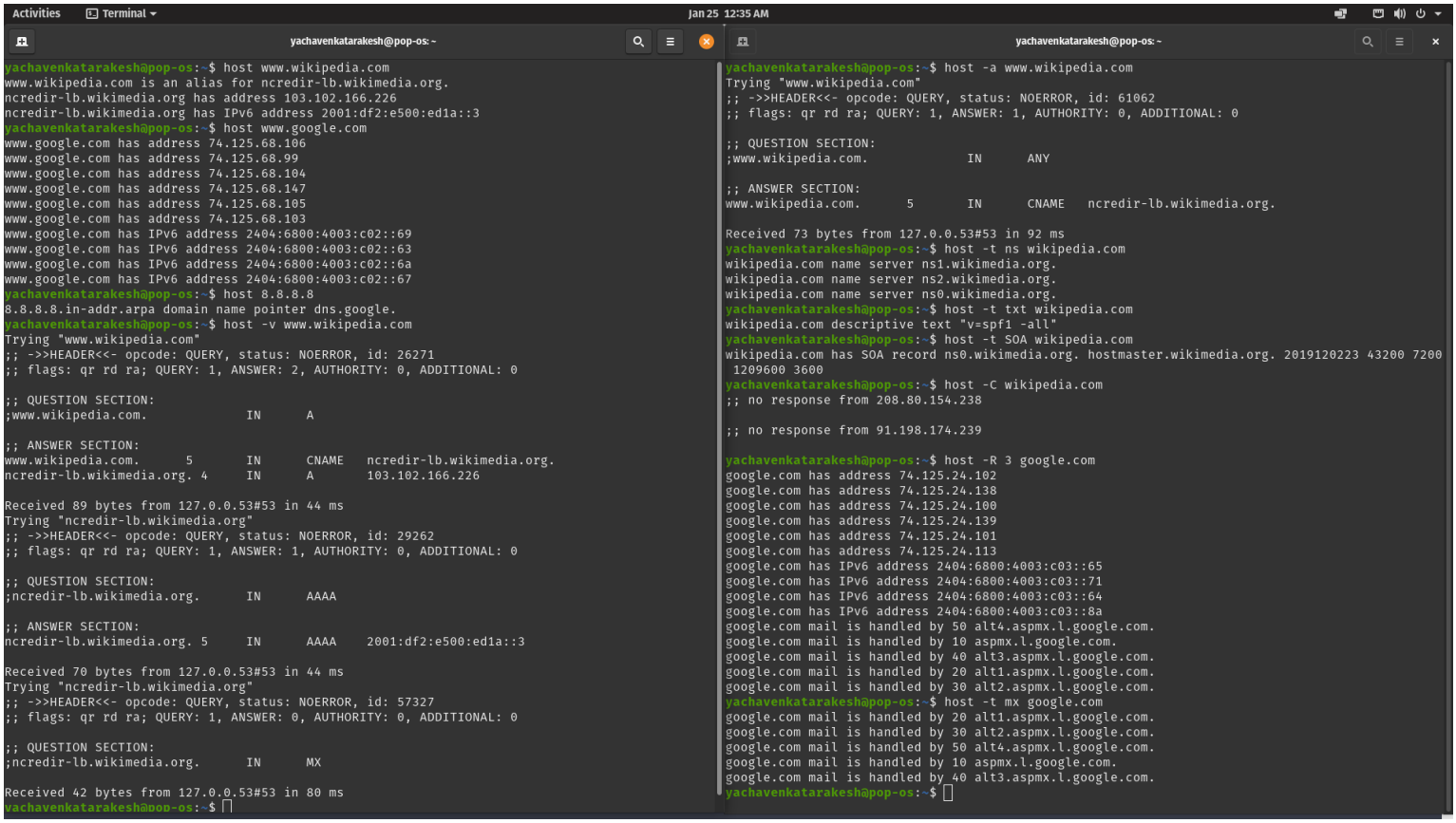
4. $sudo ifconfig ens33 up
   This enables the ens33 interface

5. $ifconfig -a
   Shows all network interfaces even if they are disabled.

6. $ifconfig ens33 netmask some_value
   By this way we can edit the netmask values of that particular interface
7. $ifconfig ens33 broadcast some_value

8. $ifconfig -s
   Shows short list of all active network interfaces.

9. $ifconfig interface add IPv6_address
   To add an IPv6 address



Host is used to determine what domain a particular IP address resolves to. It gives information about domain servers IPv4, IPv6 addresses and mail server that domain uses.

Host commands:

1. $host www.wikipedia.com or $host 8.8.8.8

   Host some domain name or its IP address.

2. $host -t ns www.wikipedia.com

   Gives the appropriate name servers associated with the domain (i.e. they're the site's DNS providers)

3. $host -t mx www.wikipedia.com

   Gives the list of mail servers and their priorities. They can also be used for reverse lookup.

4. $host -a www.wikipedia.com

   It is used to specify the query type or enables the verbose output.

5. $host -t txt www.wikipedia.com

   It is used to print the txt record

6. $host -t SOA www.wikipedia.com

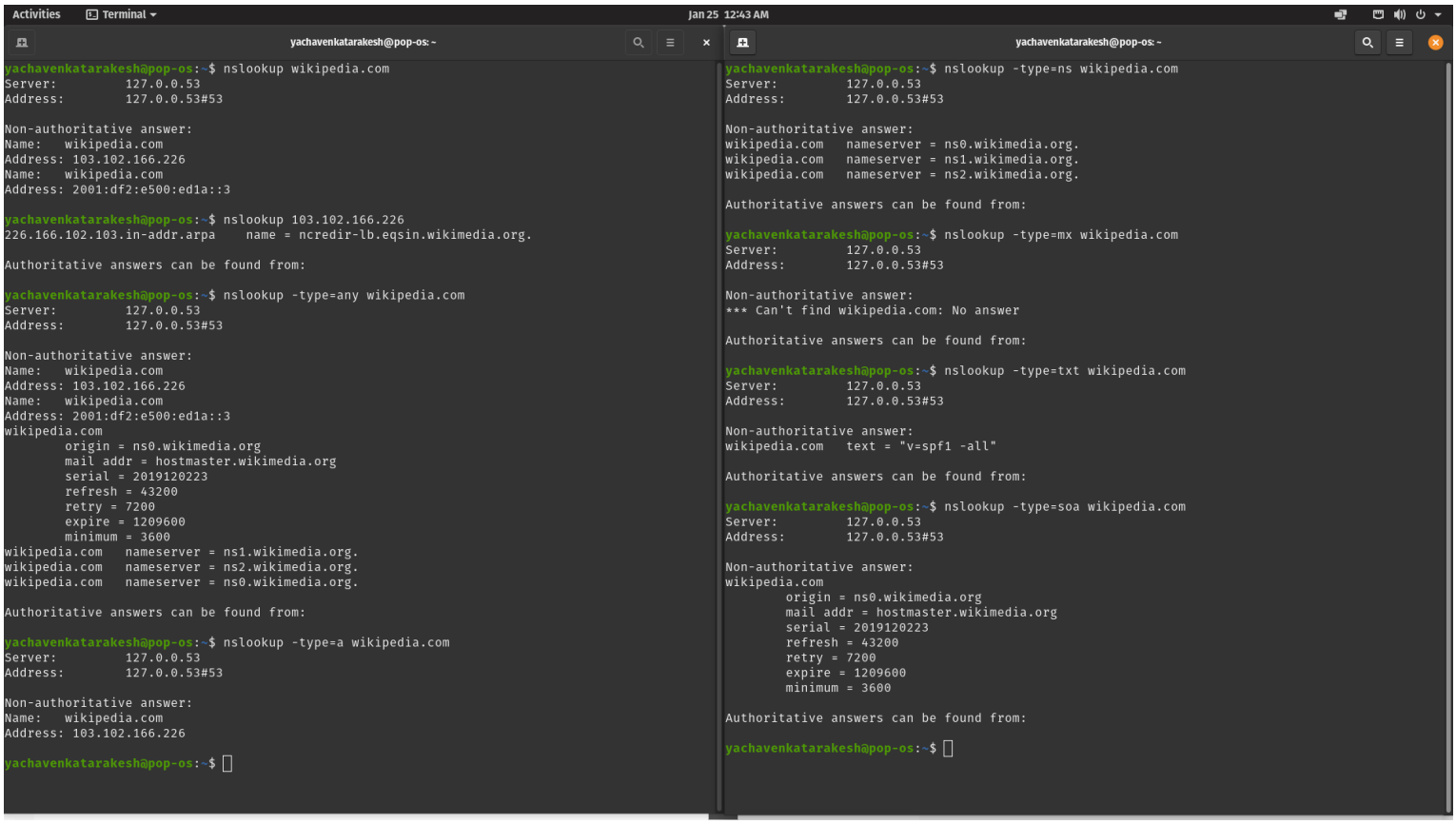
It is used to print SOA record

7. $host -R 3 www.wikipedia.com

Number of retries you can do in case of one try fails.

8. host -l www.wikipedia.com

To list all the hosts in that domain



nslookup

Nslookup is a network administrarion tool for querying the Domain Name system(DNS) to obtain domain name or iP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

Nslookup Commands:

1. $nslookup www.wikipedia.com

It will give server IP address (DNS server). Obviously they're found on port 53 and the domain names and their addresses will be displayed.

2. $nslookup 192.168.4.40

You can also do the reverse DNS lookup by providing the IP Address as argument

3. nslookup -type=any www.wikipedia.com

Look up for any record

4 nslookup -type=a www.wikipedia.com

Lookup for an ‘a’ record

5. nslookup -type=ns www.wikipedia.com

Lookup for an ‘ns(name server)’ record

6. nslookup -type=SOA www.wikipedia.com

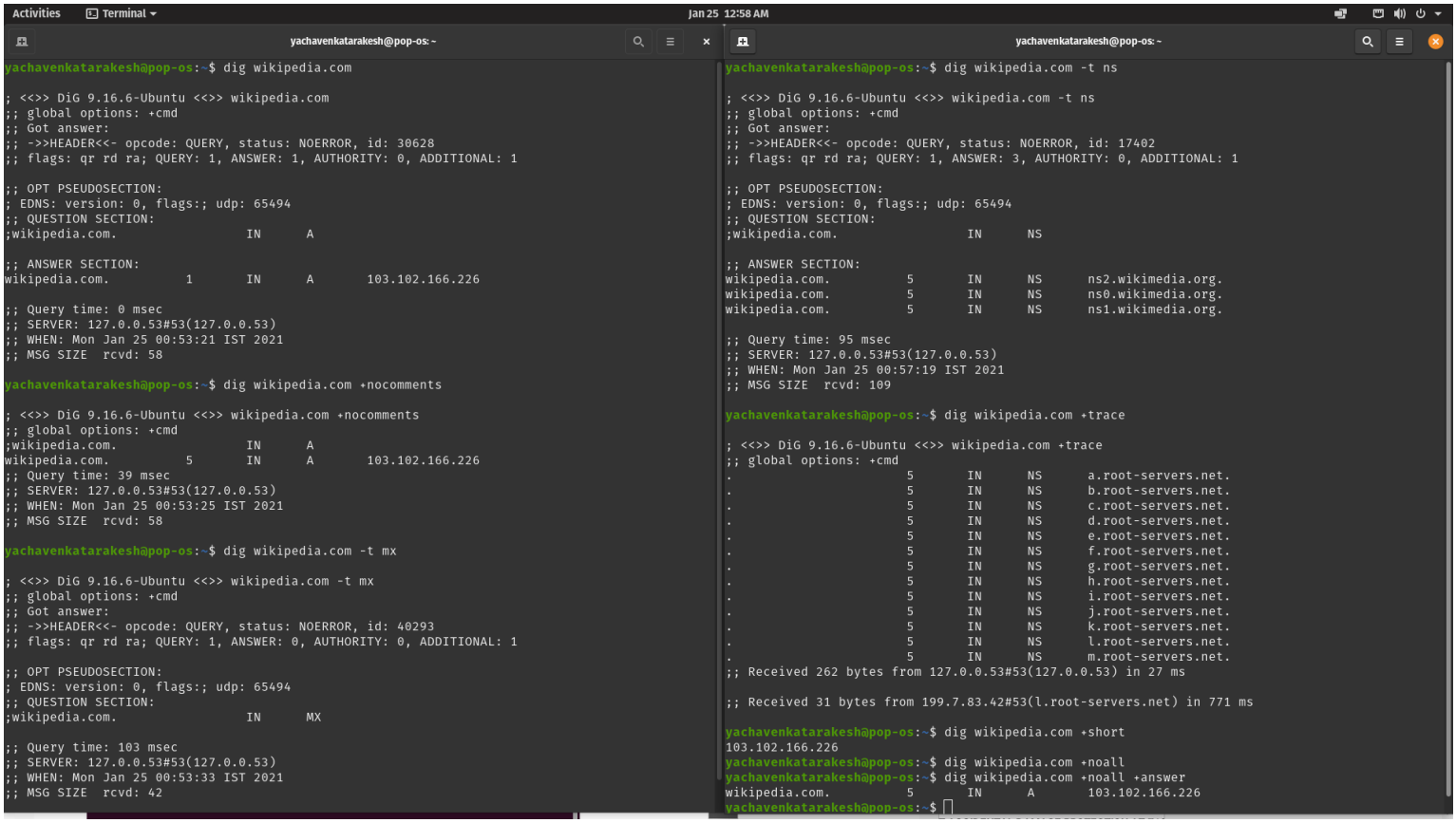
Lookup for ‘soa’ record

7. nslookup -type=mx www.wikipedia.com

Lookup for mail servers record

8. nslookup -type=txt www.wikipedia.com

Lookup for txt record



dig

Resource ‘A’ means computer’s IP address

‘NS’ means DNS name server for the named zone

‘MX’ means mail server

It displays domain name, TTL and then ‘A’ record and its IP address

Dig command gives IP addresses of servers hosted by that domain

dig commands:

1. dig www.wikipedia.com

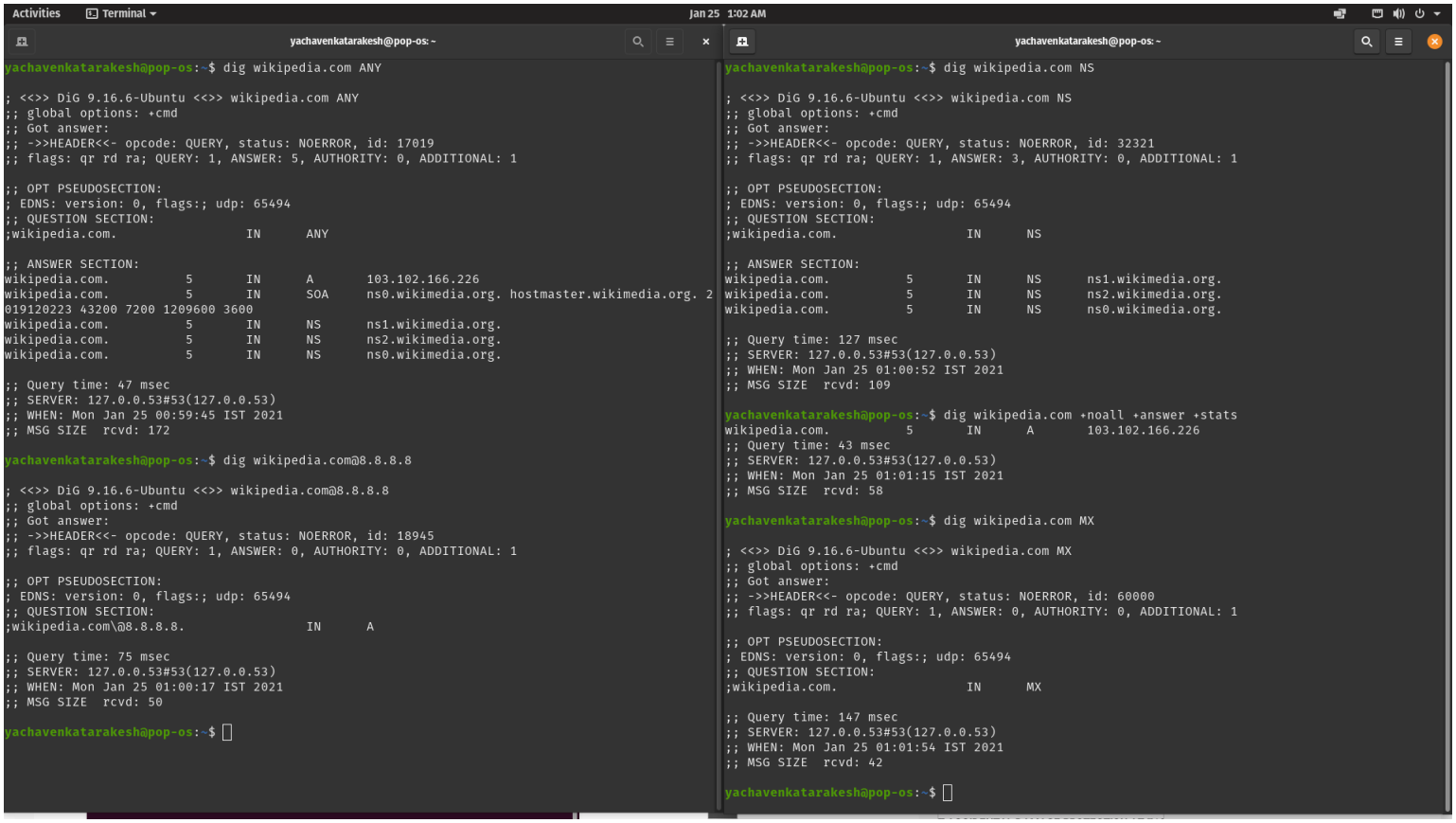
Returns domain name, TTL and then ‘A’ record and its IP address

2. dig www.wikipedia.com -t mx

For Mail servers

3. dig www.wikipedia.com -t ns

For name servers



4. dig www.wikipedia.com +short

To get only the relevant matter

5. dig www.wikipedia.com +nocomments

To get comment lines out

6. dig www.wikipedia.com +noall

To set or clear all display flags

7. dig www.wikipedia.com +noall +answer

To get detailed answer

8. dig www.wikipedia.com ANY

To get all DNS record types

9. dig www.wikipedia.com +trace

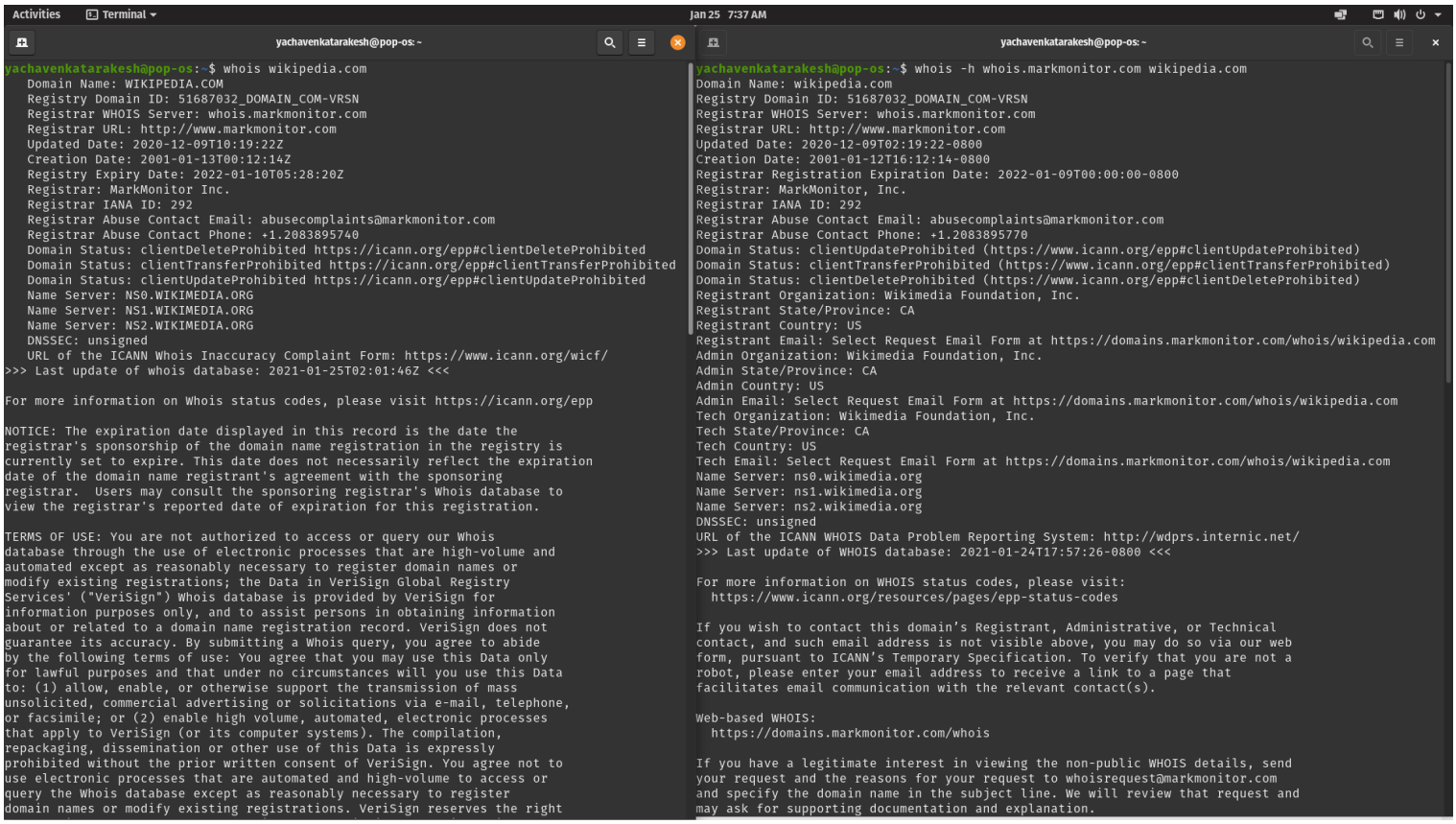
To trace the DNS path

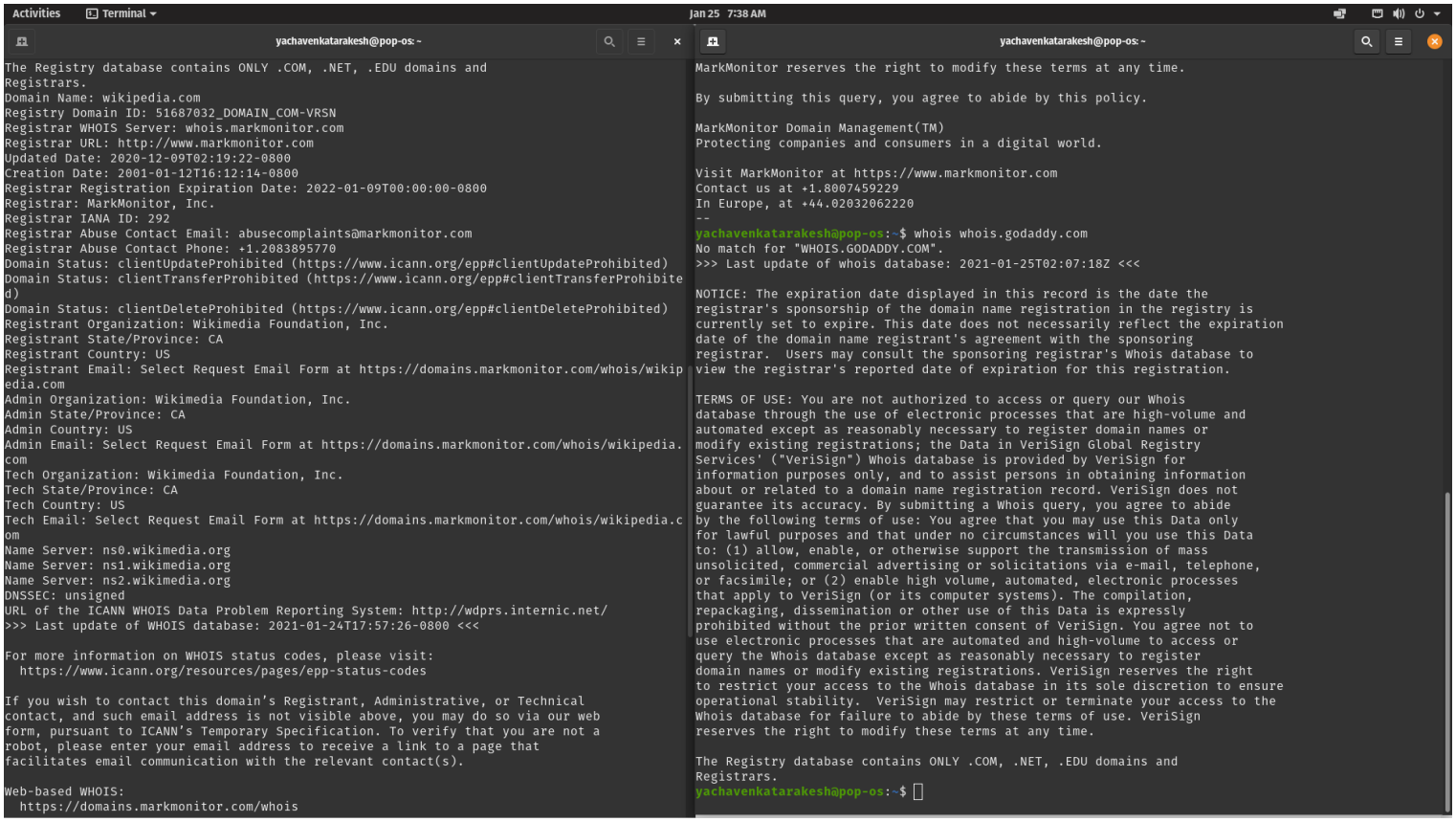
10. dig www.wikipedia.com @ 8.8.8.8

To specify name servers

11. dig www.wikipedia.com +noall +answer +stats

To query the statistics section





whois

whois is a query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as domain name, an IP address block, or an autonomous system, but is also used for wider range of other information. The protocol stores and delivers db content in human readable format.

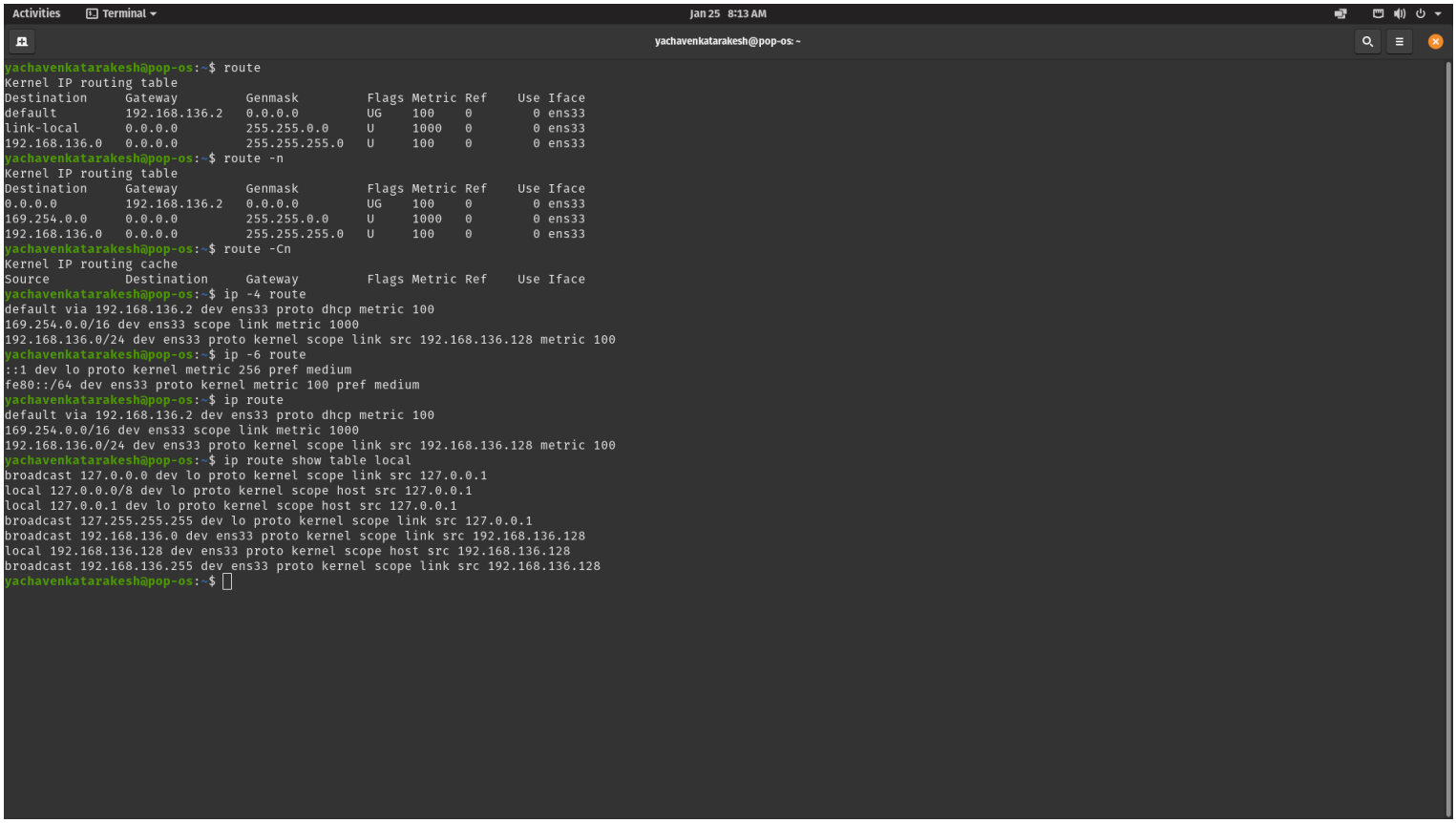
Whois method is used for checking information about ownership of a domain name like owner name, email, phone, address, domain created date, expire date, modification date, hosting server detail, domain IP. This protocol had its origin in ARPANET NICNAME protocol and was based on Name/Finger protocol. This is widely used by hackers for social engineering attacks and this also has a sister protocol Rwhois

There are two entities here Registries and Registrars. There are only few registries (Verisign) and thousands of registrars(eg : Godaddy, Tucows etc.,) and site owners has to buy it from registrars.

Why didn't we get full whois record for a website?

There are 2 types of whois while registries maintain thin records (only registrar's information) and registrars maintain thick record (registrant info in addition to registrar info).

If nothing about whois server mentioned, it returns whois information from registry database which is responsible for managing TLD(Top level domain). Some registrars explicitly block whois lookup from command line to prevent DOS attack.

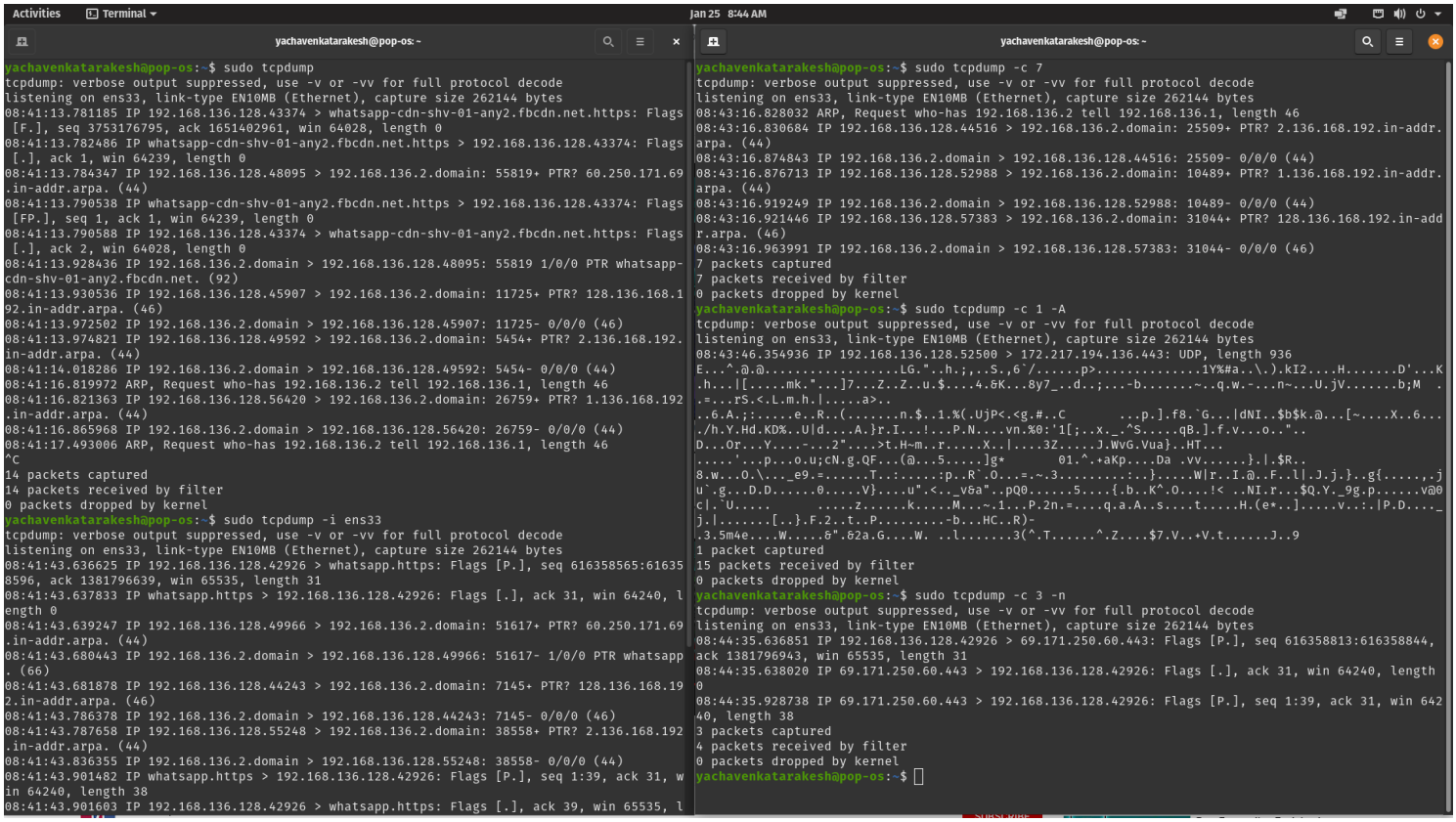


route

Route is used when required to work with IP/Kernel routing tables. Mainly used to setup static routes to specific hosts/networks via interface. Route is used for showing or updating IP/Kernel routing table. It contains details of destination IP address of server you're trying to connect, gateway IP address of router, then subnet mask, flags(probably two most common flags are U meaning router is up and running, G meaning gateway so this router uses a gateway, Iface is interface.

When there is no gateway it means that device is on same network as my own computer.

If final IP address matches for more than one rule then it chooses the one with longest subnet mask.



tcpdump

It is a common packet analyzer runs under command line, it allows user to display tcp packets transmitted or received over a network to which the computer is attached.

tcpdump commands:

1. $sudo tcpdump

Shows all the network packets moving from that device.

2. $sudo tcpdump -i ens33

Shows only those packets moving via ens33 network interface

3. $sudo tcpdump -c n

To capture only n packets

4. $sudo tcpdump -c 10 -A

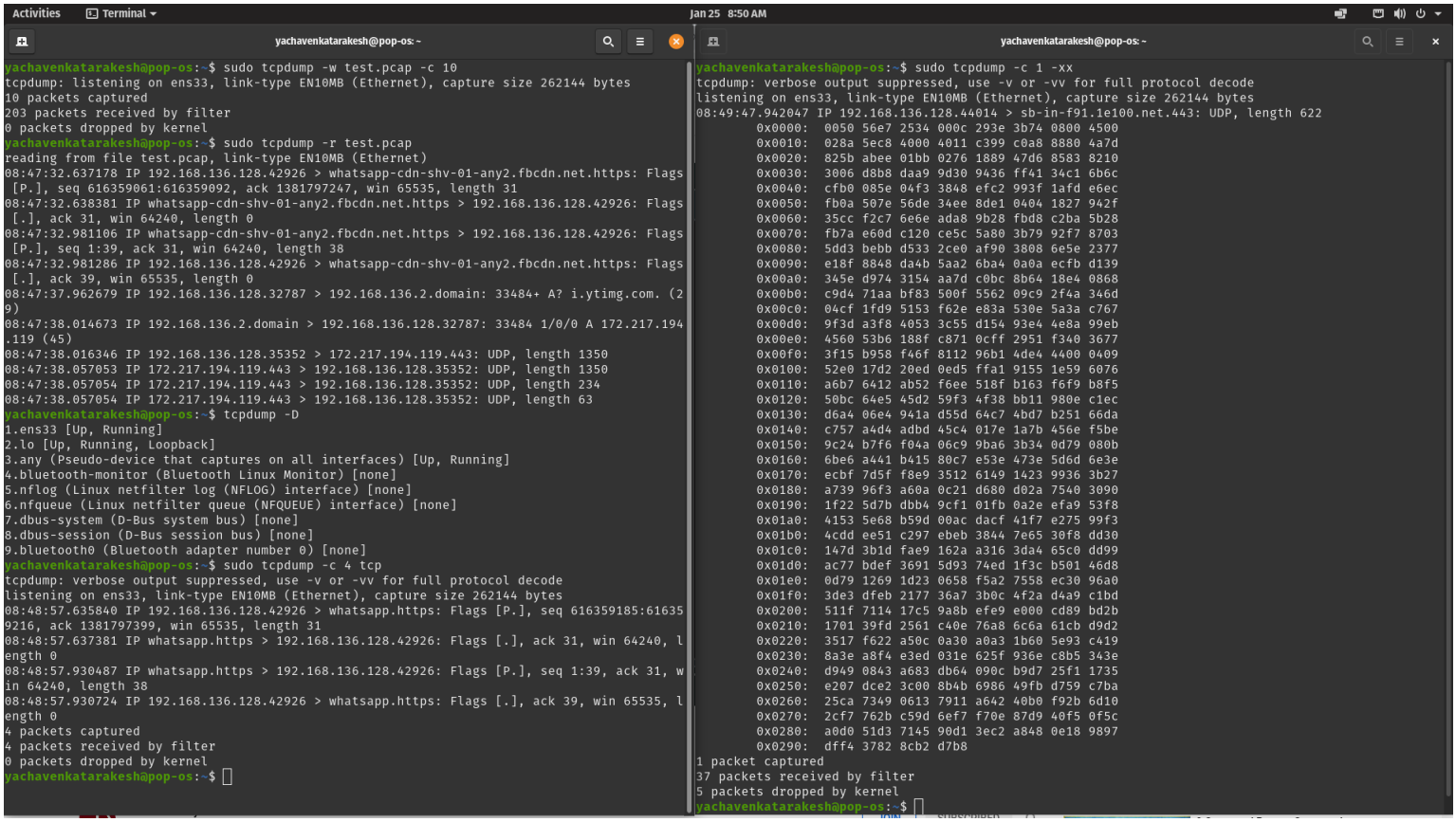
To get in ASCII format

5. $sudo tcpdump -D

To get list of all available interfaces

6. $sudo tcpdump -n

To get packet transferring in IP address.



7. $tcpdump -w test.pcap

Save packets into the file test.pacp

8. $tcpdump -r test.pcap

View saved packets from the file test.pcap

9. $sudo tcpdump -c 10 -xx

To get in both ASCII and Hexa decimal format

10. $sudo tcpdump tcp

To capture only based on some protocol

11. $ sudo tcpdump port 2201

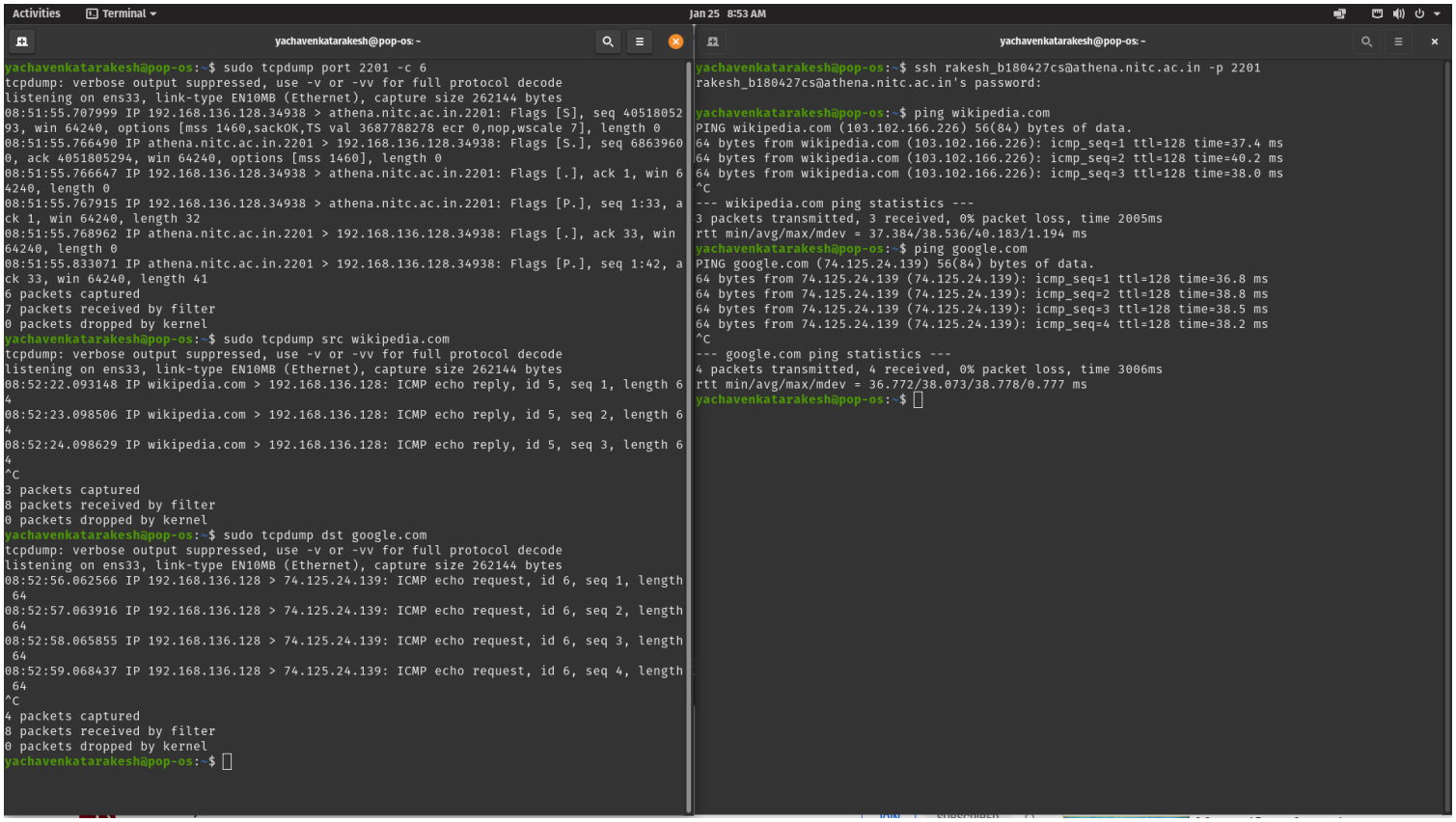
ping ssh rakesh_b180427cs@athena.nitc.ac.in -p 2201

This is used to capture those packets via port 2201

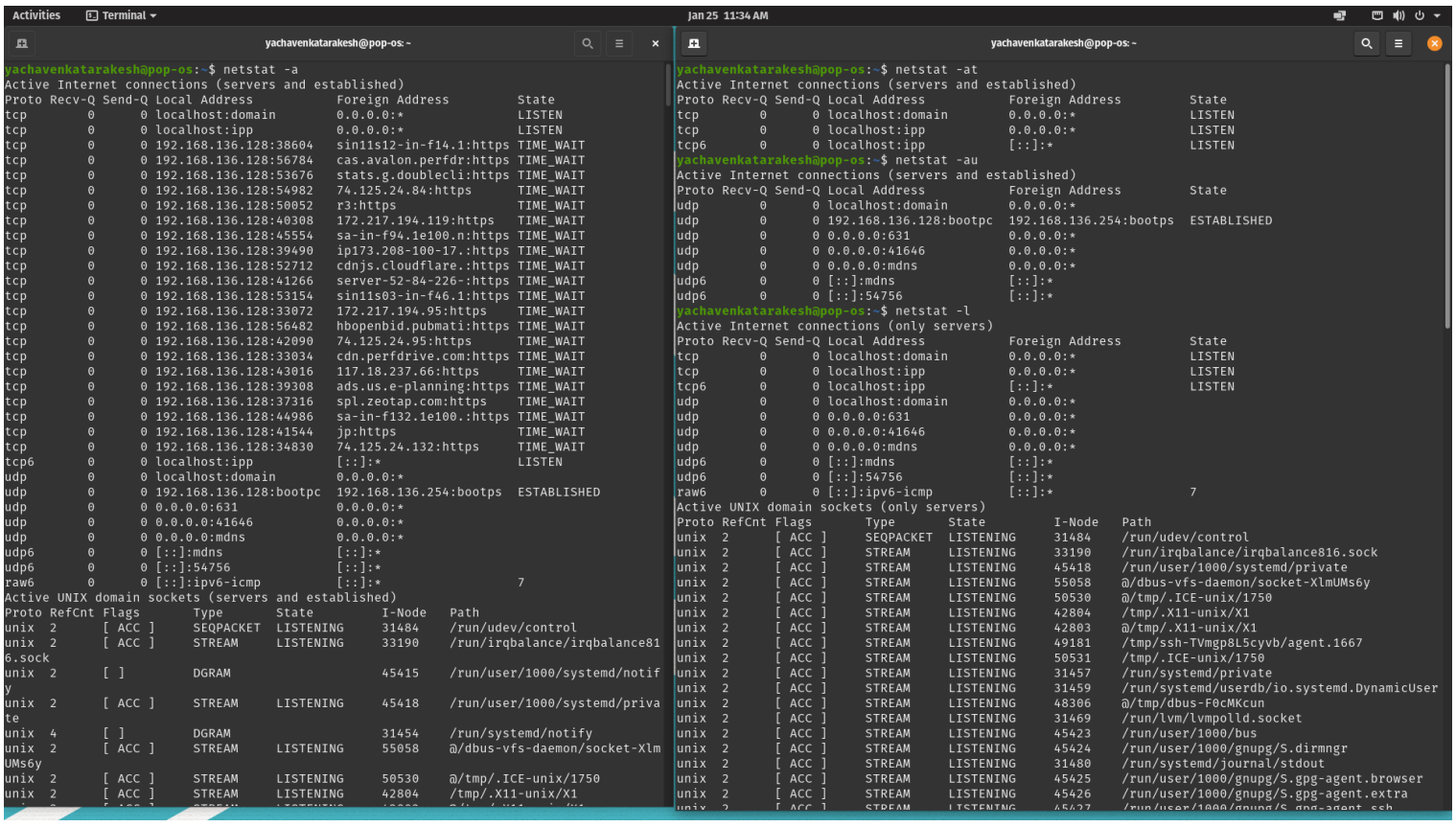
12. $sudo tcpdump src www.wikipedia.com

$sudo tcpdump dst www.wikipedia.com

This is used to capture those packets via that domain name similarly ip addresses could also be given.



tcpdump



netstat

It is used for network and system management. It is a command line network utility tool that display network connections for DCP protocol, routing tables and number of other network interfaces and protocol statistics. It is also used to find out number of active connections in a computer and what connections/ services running

netstat commands:

1. $netstat -a

   To show list of both listening and non-listening sockets

2. $netstat -at

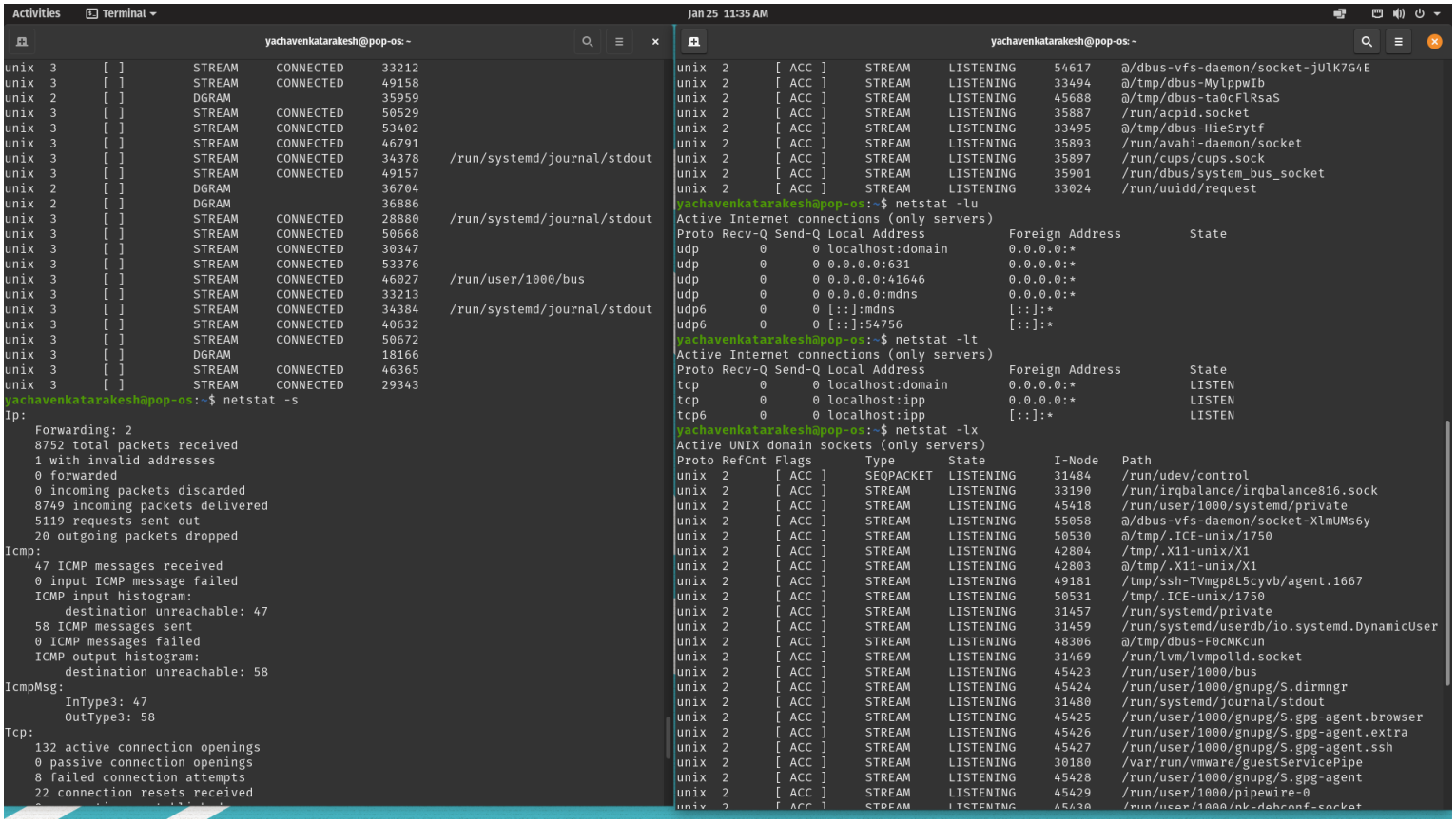
   To list all tcp ports

3. $netstat -au

   To list all udp ports

4. $netstat -l

   To list only the listening sockets



5. $netstat -lu

   To list only listening udp packets

6. $netstar -lt

   To list only listening TCP packets

7. $netstat -lx

To list only the listening UNIX ports

8. $netstat -s

To list the statistics from all the ports

9. $netstat -pt

To display the PID and program names

10. $nestat -c

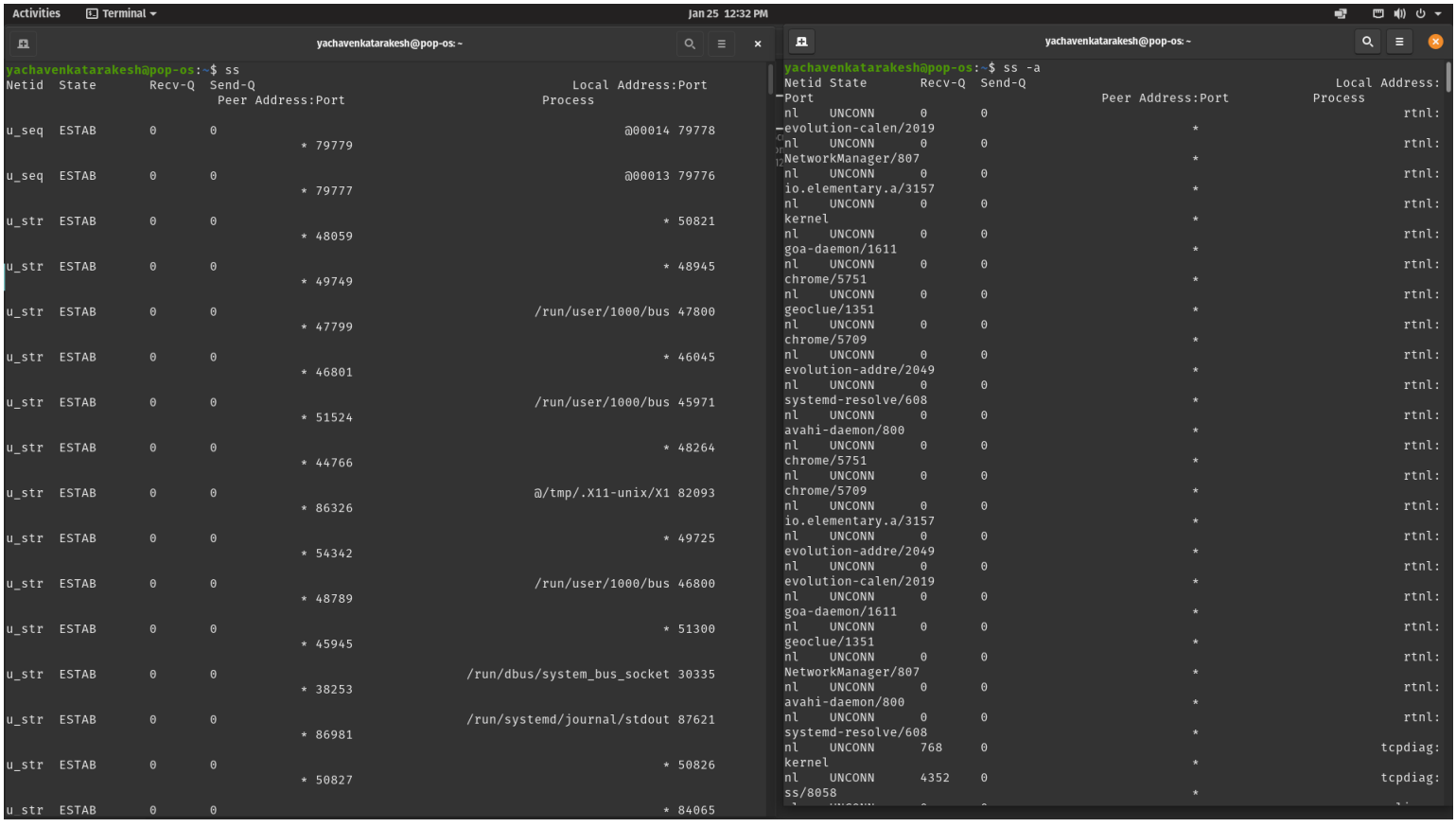
To print the netstat information continuously

11. $netstat -r

To get kernel routing information

12. $netstat -i

To get the list of network interfaces.



ss

ss tool is similar to the netstat command so it is also used for displaying network socket related information on a linux system. It displays more detailed information compared to that of netstat tool.

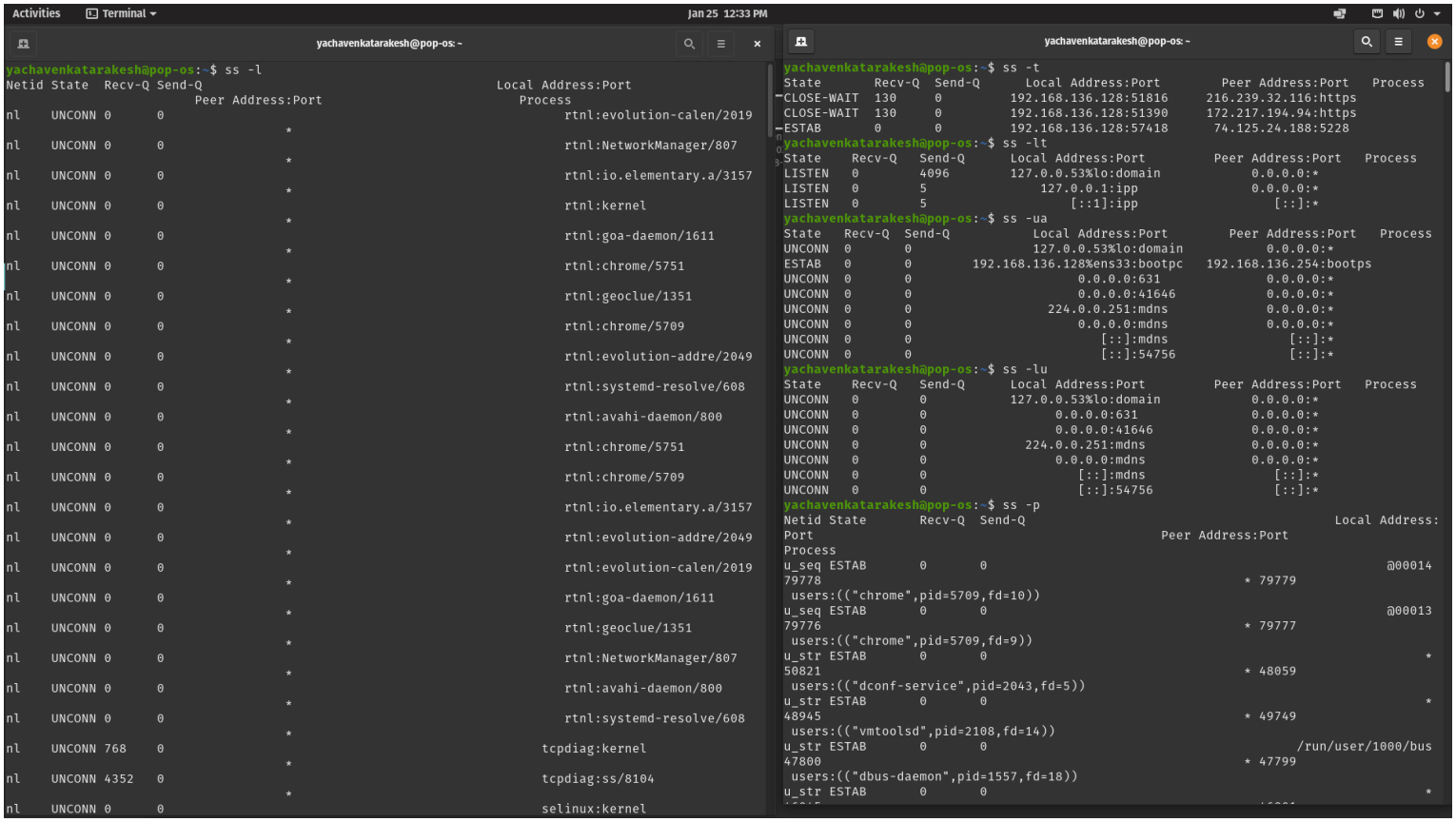
ss commands:

1. ss

ss without any options simply lists all the connections regardless of the state they are in.

2. ss -a

This is used to retrieve both listening and non-listening ports



3. ss -l

To display only listening sockets

4. $ss -t

To display all tcp connections

5. $ss -lt

To display all listening tcp connections

6.$ss -ua

To display all udp connections

7.$ss -lu

To display all listening udp connections

8.$ss -p

To display PID’s of all sockets

9.$ss -s

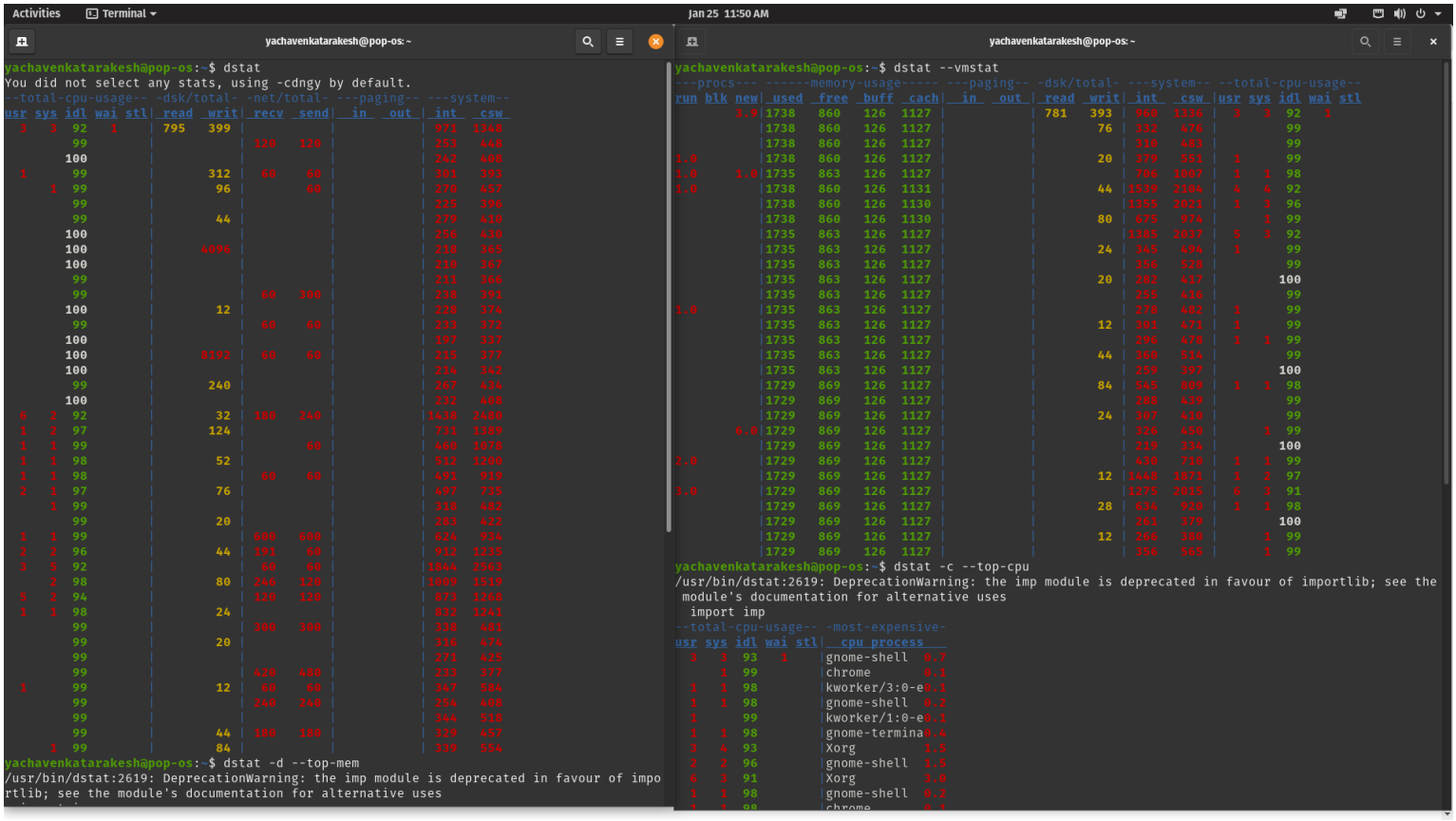
To list the summary statistics

10.$ss -4

To list all IPv4 socket connections

11.$ss -6

To list all IPv6 socket connections



dstat

dstat is used to retireve information or statistics of the components of the system such as network connections, IO devices, CPU etc., It is generally used to retrieve a handful of information about the above mentioned components. Using this tool one can even see the throughput for block devices that makeup a single filesystem or storage system.

dstat commands:

1. dstat

Display statistics of the major OS components

2. dstat –vmstat

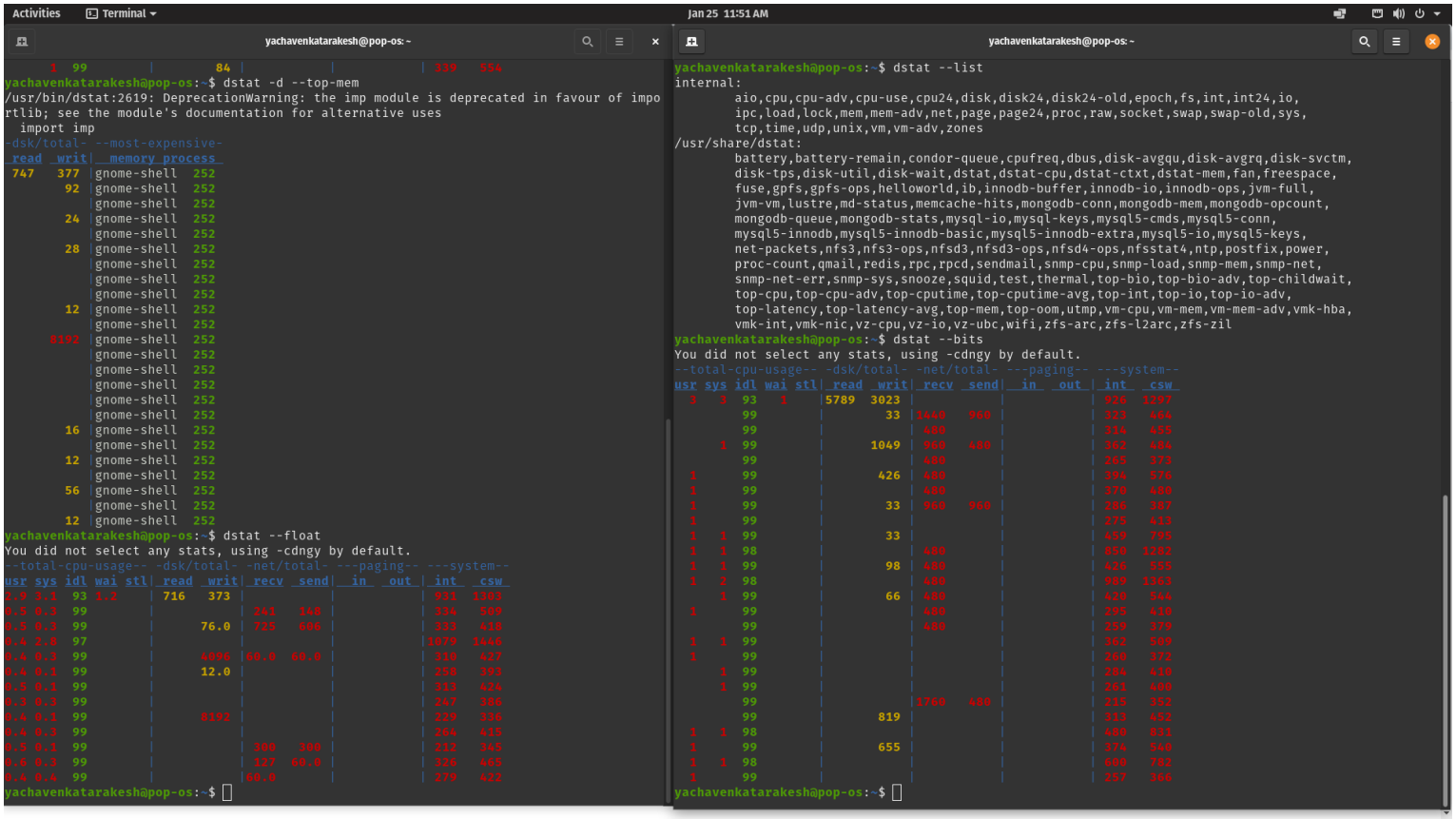
Display information which is displayed by the vmstat tool

3. dstat –netstat

Display information which is displayed by the vmstat tool

4. dstat -c –top-cpu

Display stats of all process which are using most of the CPU



5. dstat -d –top-mem

Display stats of all process using most of the memory

6. dstat –list

Display list of all plugins

7. dstat –float

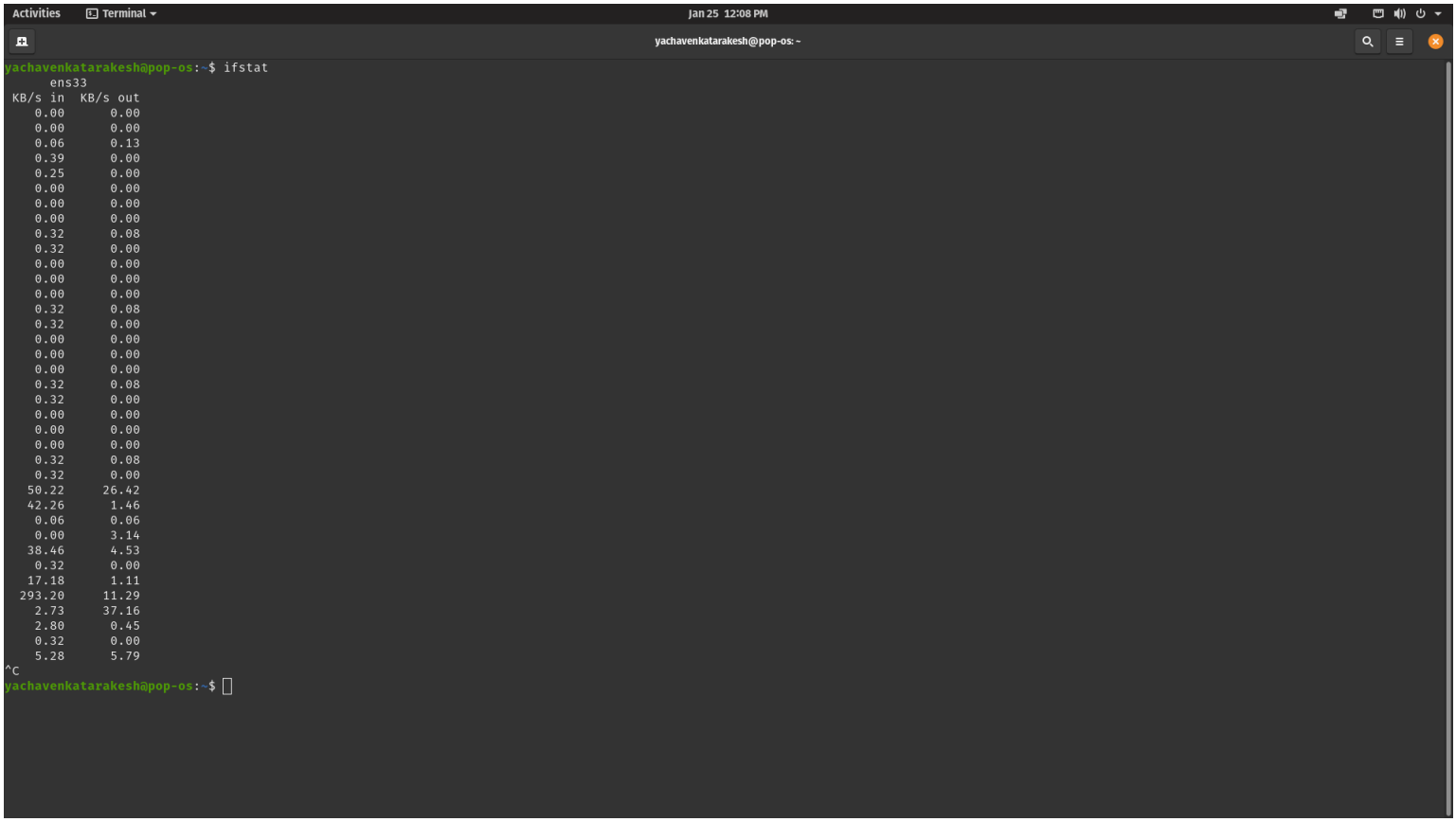
Will display accurate values instead of rounded

8. dstat –bits

Prints in bits

9. dstat –nocolor

Will not display any color



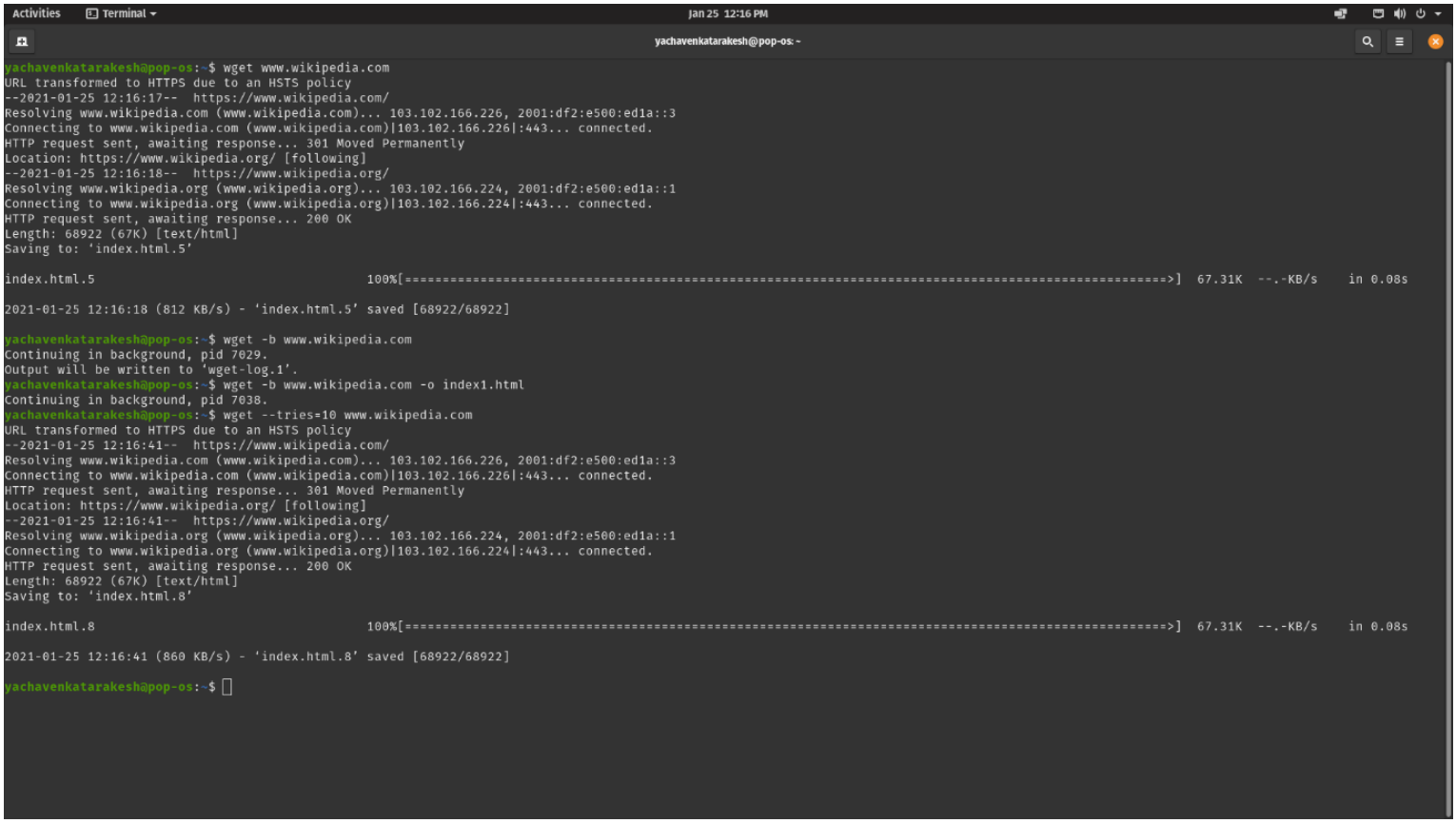
Ifstat

It is used to report network interface statistics and displays in and out speeds of network's bandwidth consumption and speed at regular intervals of time. Also helpful in finding the network's bandwidth as we could find the average of all. It is similar to that of vmstat or iostat which reports io and virtual memory statistics respectively.

Ifstat commands:

1. $ifstat

   Displays network bandwidth consumption for various time intervals.



This is a very useful command to download the files from the server even when the user hasn't logged onto the system and can work in without use of any browser and also can work in background without hindering current process. It can also be used to get links in HTML, XHTML pages or can convert links to downloadable HTML files for offline viewing. This can be used to resume the download if it stopped due to network failure. Hence it is best useful for slow or unstable networks. It will keep retrying until the whole file is downloaded.

wget commands:

1. wget www.wikipedia.com

Downloads the page into some default file. i.e. downloads the html file

2. wget file_Link

Downloads the file at this link

3. $wget -b www.wikipedia.com

Downloads in background, so we neednot resume our work until it gets downloaded.

4.$wget -b www.wikipedia.com -o file.html

Saves the text to our required file instead of some default files

5. $wget –tries=10 www.wikipedia.com

To try a given number of times in case of failures due to network issues

6.$wget -c www.wikipedia.com

To resume a partially downloaded file so that user need not again start from first if download failed due to some connectivity issues

YACHA VENKATA RAKESH

B180427CS

NETWORKS LAB

WEEK 1 SUBMISSION

CSE 3RD YEAR A BATCH