Indian Institute of Engineering Science and Technology, Shibpur
Department of Computer Science and Technology

Computer Network Lab (CS 3272)

Assignment 1: Networking basic commands

- Name: Dipmay Biswas
- Roll No.: 2021CSB043
- GSuite: 2021csb043.dipmay@students.iiests.ac.in

The aim of this assignment is to make you familiar with few network commands and tools. Prepare a report based on your understating and findings.

Question 1

Read the man pages of ifconfig, ping, traceroute, arp, dig, nslookup, and netstatand write their utilities in brief.

ifconfig

- used to configure network interface controller (NIC)
- if no arguments are given, ifconfig displays active network interfaces.

ping <IP>

- send ICMP ECHO_REQUEST to <IP>
- generally used to check if we can access a URI/IP address or not
- -s flag is used to define the (amount + 8) bytes that will be sent
  - 8 extra bytes also added to the number as header
- -c flag can be used to define how much request to send to the IP, absence of this flag will make the command continuously send request to the IP until we forcefully stop it via Ctrl + C.

traceroute <IP>

- print route packets trace to network host
- sends multiple packets to IP incrementing TTL and listens for ICMP "Time Exceeded" reply from the network devices in the path between the the sender and the destination server.

arp

- manipulate the system ARP (Address Resolution Protocol) cache.
- if run without any specifier, it will print the current content of the table.

dig <URL>

- Domain Information Grouper
- DNS lookup utility
- performs DNS lookup of the <URL> using the DNS IP mentioned in /etc/resolv.conf and returns the IP

nslookup

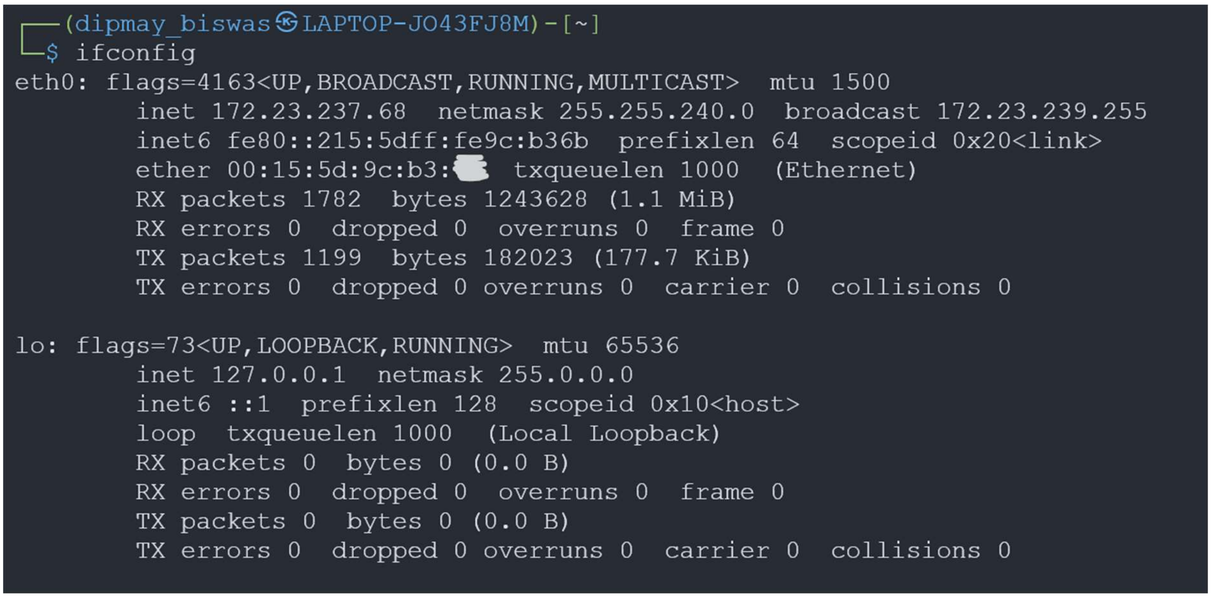
- query Internet name server interactively
- same work as dig but runs interactively
- we can do nslookup <IP> to reverse domain search, i.e find URL from the IP.

netstat

- Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships
- running without any flags displays all active internet connections and connected sockets

Question 2

Find the **IP** and **hardware addresses** of your machine using ifconfig command.



```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.23.237.68  netmask 255.255.240.0  broadcast 172.23.239.255
        inet6 fe80::215:5dff:fe9c:b36b  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:9c:b3:[redacted]  txqueuelen 1000  (Ethernet)
        RX packets 1782  bytes 1243628 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1199  bytes 182023 (177.7 KiB)
        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 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
```

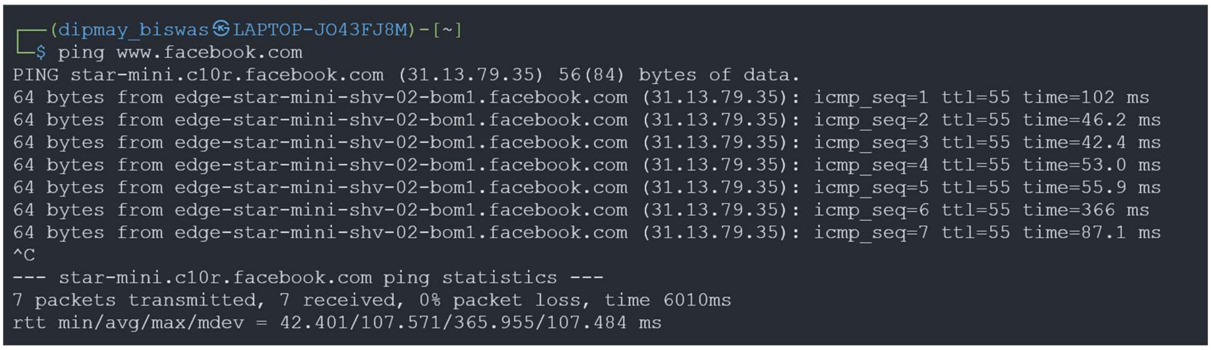
IP addresses -> **172.23.237.68**

hardware addresses -> **00:15:5d:9c:b3:xx** **hiding my hardware addresse in this snapshot for security concerns.*

Question 3

Use “**ping <AnyURL>**” command and find out

i. the average RTT (round trip time).
ii. the %packet loss.
iii. size of packet that is sent to <AnyURL> server.
iv. size of packet that is received by your machine.



```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ ping www.facebook.com
PING star-mini.c10r.facebook.com (31.13.79.35) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=1 ttl=55 time=102 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=2 ttl=55 time=46.2 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=3 ttl=55 time=42.4 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=4 ttl=55 time=53.0 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=5 ttl=55 time=55.9 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=6 ttl=55 time=366 ms
64 bytes from edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35): icmp_seq=7 ttl=55 time=87.1 ms
^C
--- star-mini.c10r.facebook.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 42.401/107.571/365.955/107.484 ms
```

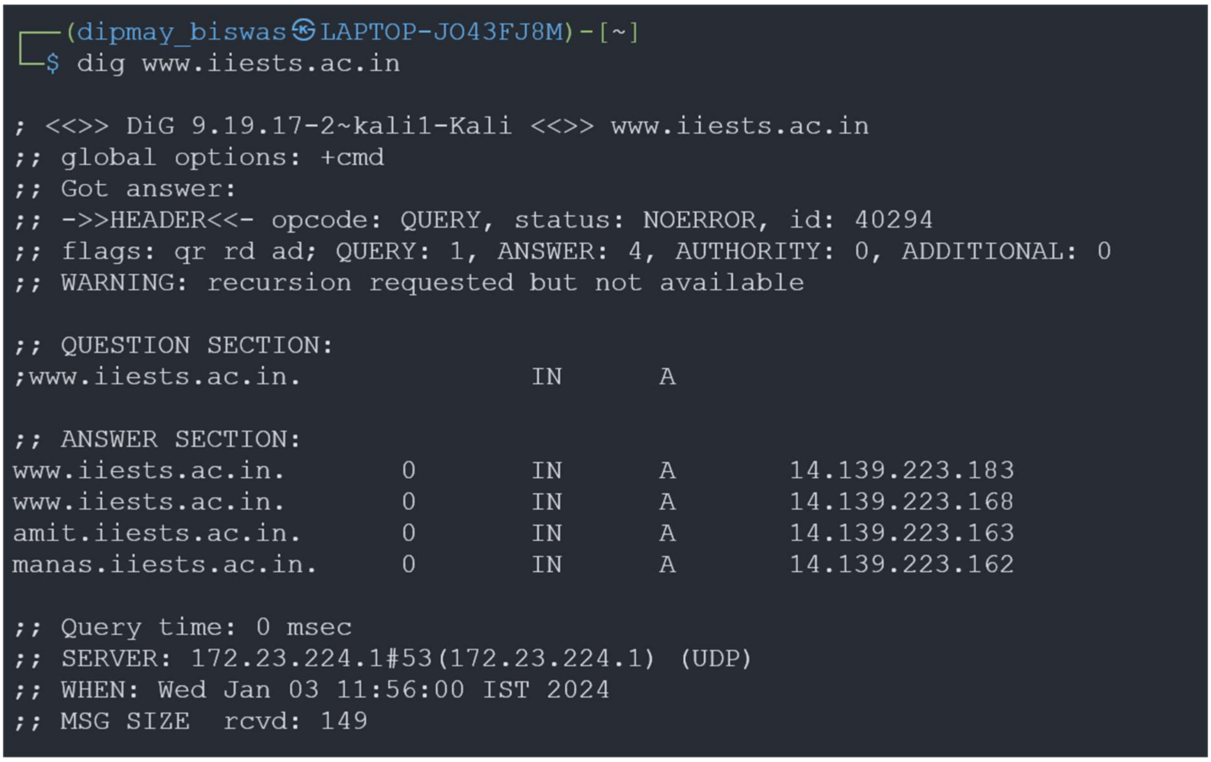
Hence :

i. the average RTT (round trip time) -> **107.571 ms**.
ii. the %packet loss -> **0%**.
iii. size of packet that is sent to www.facebook.com server -> 56 + 8 = **64 bytes**.
iv. size of packet that is received by your machine -> **64 bytes**.

Question 4

Use “**dig <AnyURL>**” command and find out

i. theIP address of <AnyURL>.
ii. theIP addresses of local DNS servers of IIEST.



```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ dig www.iiests.ac.in

; <<>> DiG 9.19.17-2~kali1-Kali <<>> www.iiests.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40294
;; flags: qr rd ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.iiests.ac.in.              IN      A

;; ANSWER SECTION:
www.iiests.ac.in.       0       IN      A       14.139.223.183
www.iiests.ac.in.       0       IN      A       14.139.223.168
amit.iiests.ac.in.      0       IN      A       14.139.223.163
manas.iiests.ac.in.     0       IN      A       14.139.223.162

;; Query time: 0 msec
;; SERVER: 172.23.224.1#53(172.23.224.1) (UDP)
;; WHEN: Wed Jan 03 11:56:00 IST 2024
;; MSG SIZE  rcvd: 149
```

Hence :

i. ip address of
www.iiests.ac.in -> **14.139.223.183**
www.iiests.ac.in ->14.139.223.168
amit.iiests.ac.in -> 14.139.223.163
manas.iiests.ac.in. -> 14.139.223.162

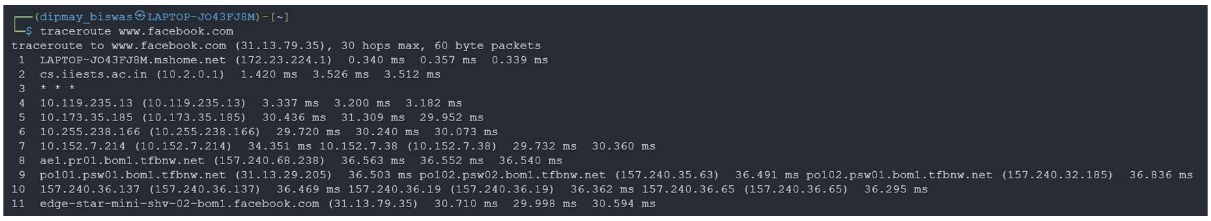
ii. ip address of the DNS server(s) -> **172.23.224.1#53**

Question 5

Use “**traceroute <AnyURL>**” and find out

i. number of hops in between your machine and <AnyURL> server.

ii. the IP address of your network gateway of your subnet.



```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ traceroute www.facebook.com
traceroute to www.facebook.com (31.13.79.35), 30 hops max, 60 byte packets
 1  LAPTOP-JO43FJ8M.mshome.net (172.23.224.1)  0.340 ms  0.357 ms  0.339 ms
 2  cs.iiests.ac.in (10.2.0.1)  1.420 ms  3.526 ms  3.512 ms
 3  * * *
 4  10.119.235.13 (10.119.235.13)  3.337 ms  3.200 ms  3.182 ms
 5  10.173.35.185 (10.173.35.185)  30.436 ms  31.309 ms  29.952 ms
 6  10.255.238.166 (10.255.238.166)  29.720 ms  30.240 ms  30.073 ms
 7  10.152.7.214 (10.152.7.214)  34.351 ms 10.152.7.38 (10.152.7.38)  29.732 ms  30.360 ms
 8  ae1.pr01.bom1.tfbnw.net (157.240.68.238)  36.563 ms  36.552 ms  36.540 ms
 9  po101.psw01.bom1.tfbnw.net (31.13.29.205)  36.503 ms po102.psw02.bom1.tfbnw.net (157.240.35.63)  36.491 ms po102.psw01.bom1.tfbnw.net (157.240.32.185)  36.836 ms
10  157.240.36.137 (157.240.36.137)  36.469 ms 157.240.36.19 (157.240.36.19)  36.362 ms 157.240.36.65 (157.240.36.65)  36.295 ms
11  edge-star-mini-shv-02-bom1.facebook.com (31.13.79.35)  30.710 ms  29.998 ms  30.594 ms
```

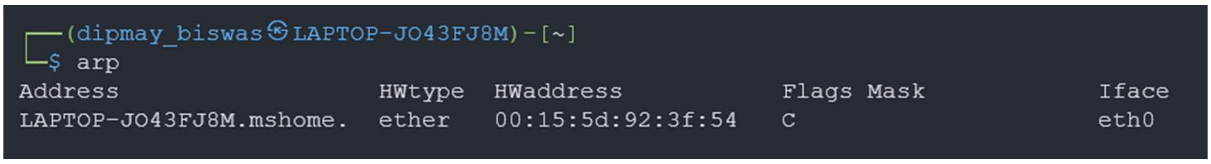
Hence :

i. No. of hops -> **11**

ii. IP address of the network gateway of my subnet: the first traceroute ip address -> **172.23.224.1**

Question 6

Use “**arp**” command to find out the MAC address of the device that is performing as your network gateway.

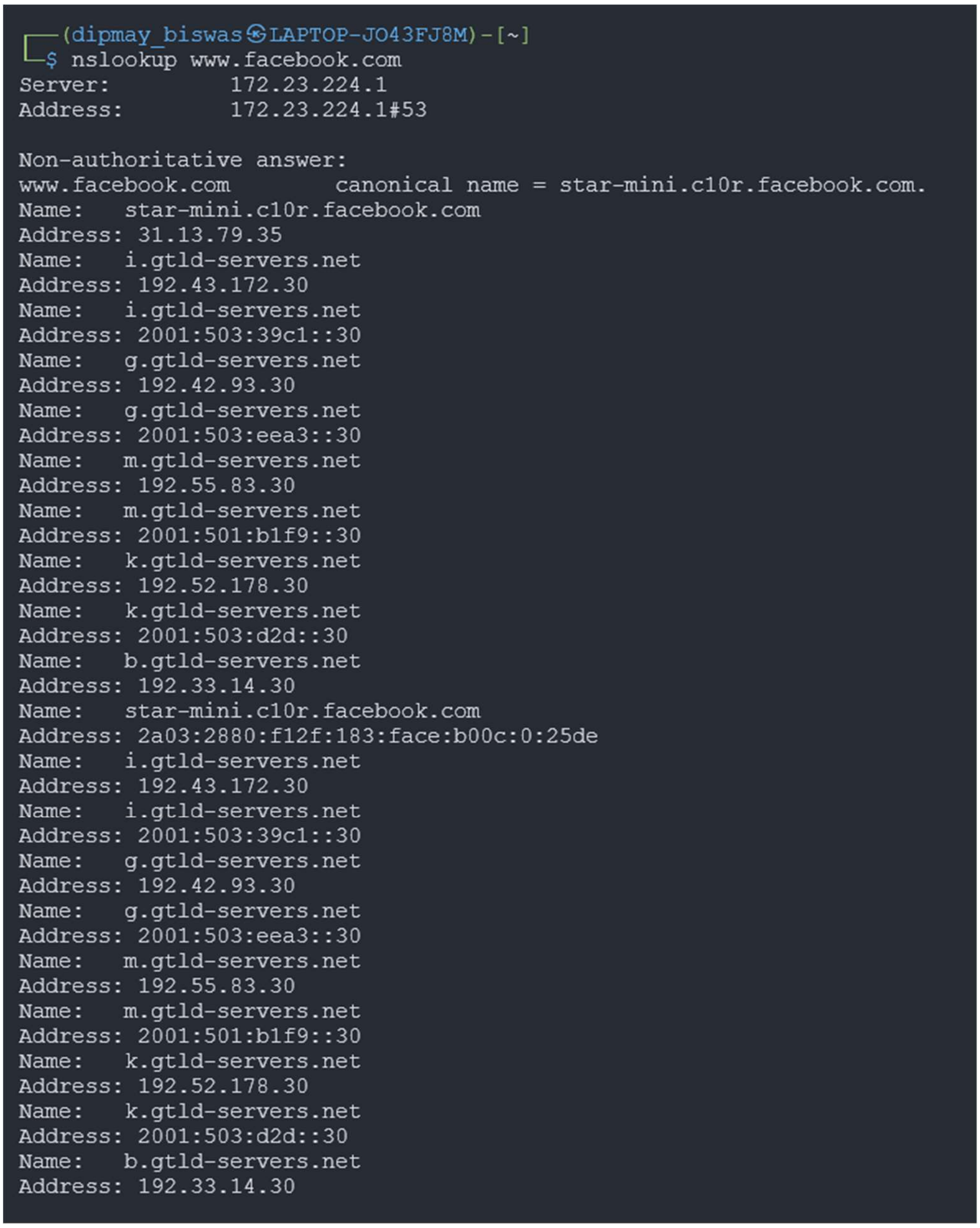


```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
LAPTOP-JO43FJ8M.mshome.  ether   00:15:5d:92:3f:54   C                     eth0
```

Hence MAC address: **00:15:5d:92:3f:54** *(MAC address of other hardware on the network, such as your router)*

Question 7

Use **nslookup** command and find out the IP address of <AnyURL>. Use nslookup command and perform **reverse domain lookup**.

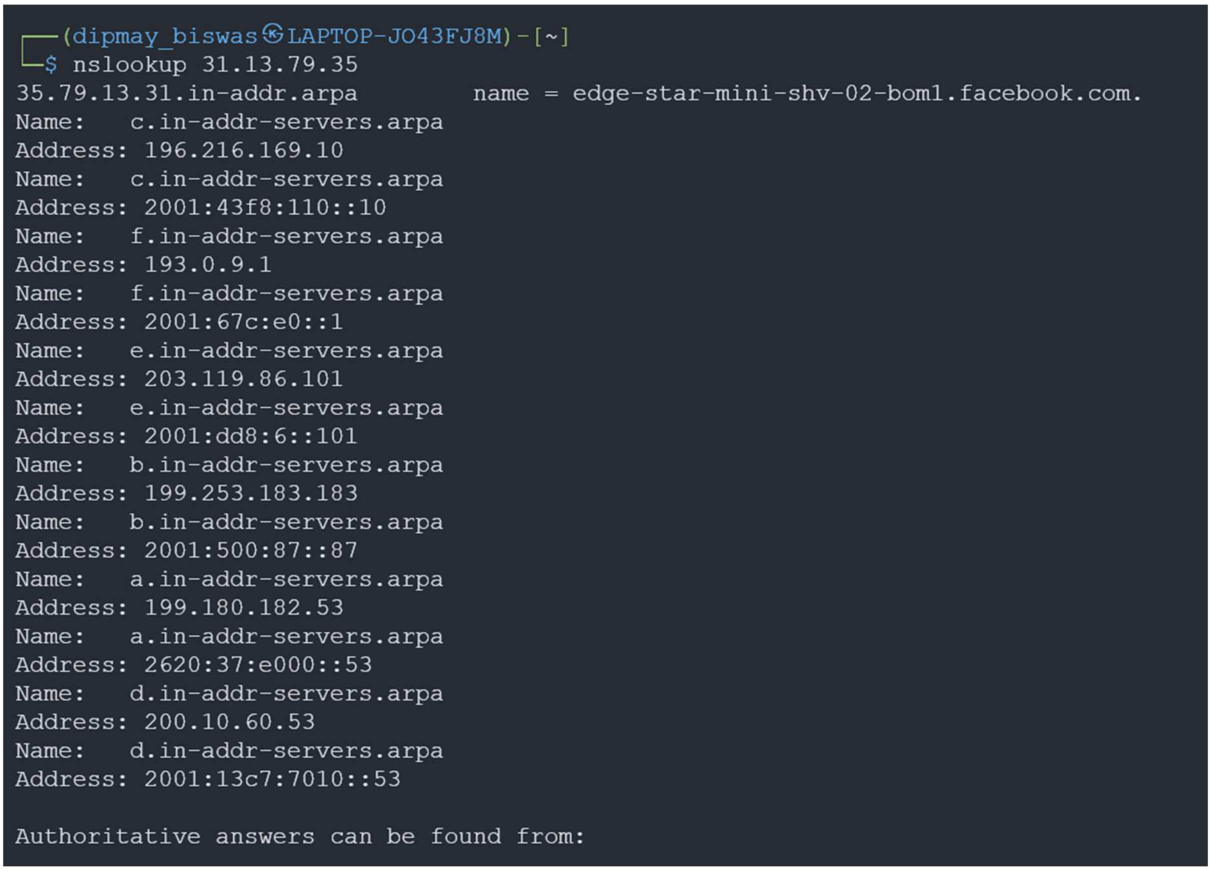


```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ nslookup www.facebook.com
Server:         172.23.224.1
Address:        172.23.224.1#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 31.13.79.35
Name:   i.gtld-servers.net
Address: 192.43.172.30
Name:   i.gtld-servers.net
Address: 2001:503:39c1::30
Name:   g.gtld-servers.net
Address: 192.42.93.30
Name:   g.gtld-servers.net
Address: 2001:503:eea3::30
Name:   m.gtld-servers.net
Address: 192.55.83.30
Name:   m.gtld-servers.net
Address: 2001:501:b1f9::30
Name:   k.gtld-servers.net
Address: 192.52.178.30
Name:   k.gtld-servers.net
Address: 2001:503:d2d::30
Name:   b.gtld-servers.net
Address: 192.33.14.30
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f12f:183:face:b00c:0:25de
Name:   i.gtld-servers.net
Address: 192.43.172.30
Name:   i.gtld-servers.net
Address: 2001:503:39c1::30
Name:   g.gtld-servers.net
Address: 192.42.93.30
Name:   g.gtld-servers.net
Address: 2001:503:eea3::30
Name:   m.gtld-servers.net
Address: 192.55.83.30
Name:   m.gtld-servers.net
Address: 2001:501:b1f9::30
Name:   k.gtld-servers.net
Address: 192.52.178.30
Name:   k.gtld-servers.net
Address: 2001:503:d2d::30
Name:   b.gtld-servers.net
Address: 192.33.14.30
```

hence output IP address of www.facebook.com is **31.13.79.35**

Reverse domain lookup



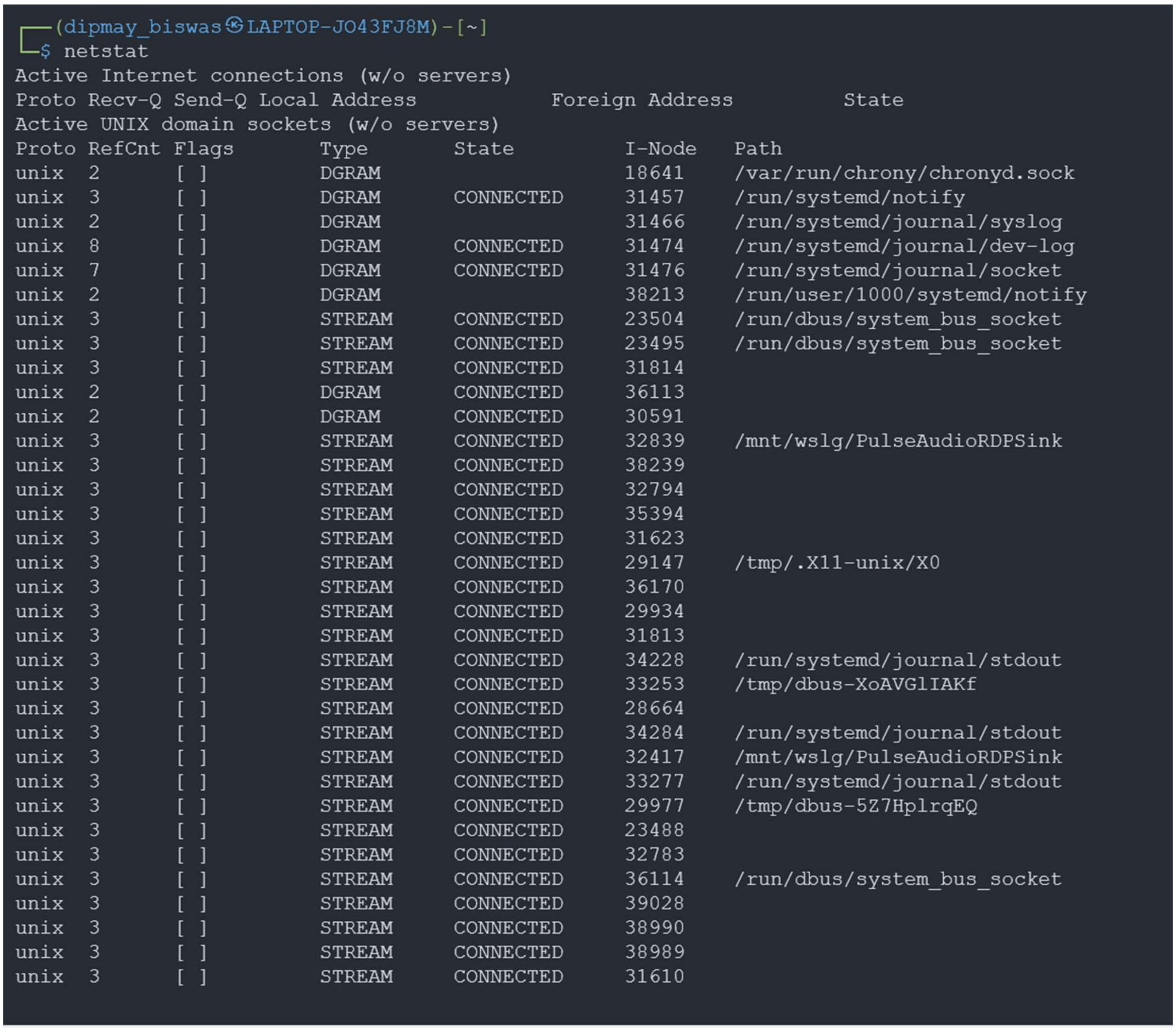
```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ nslookup 31.13.79.35
35.79.13.31.in-addr.arpa        name = edge-star-mini-shv-02-bom1.facebook.com.
Name:   c.in-addr-servers.arpa
Address: 196.216.169.10
Name:   c.in-addr-servers.arpa
Address: 2001:43f8:110::10
Name:   f.in-addr-servers.arpa
Address: 193.0.9.1
Name:   f.in-addr-servers.arpa
Address: 2001:67c:e0::1
Name:   e.in-addr-servers.arpa
Address: 203.119.86.101
Name:   e.in-addr-servers.arpa
Address: 2001:dd8:6::101
Name:   b.in-addr-servers.arpa
Address: 199.253.183.183
Name:   b.in-addr-servers.arpa
Address: 2001:500:87::87
Name:   a.in-addr-servers.arpa
Address: 199.180.182.53
Name:   a.in-addr-servers.arpa
Address: 2620:37:e000::53
Name:   d.in-addr-servers.arpa
Address: 200.10.60.53
Name:   d.in-addr-servers.arpa
Address: 2001:13c7:7010::53

Authoritative answers can be found from:
```

hence the name of the server -> **edge-star-mini-shv-02-bom1.facebook.com.**

Question 8

Use **netstat** command and find out the active connections of your machine.



```
┌──(dipmay_biswas㉿LAPTOP-JO43FJ8M)-[~]
└─$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    18641    /var/run/chrony/chronyd.sock
unix  3      [ ]         DGRAM      CONNECTED     31457    /run/systemd/notify
unix  2      [ ]         DGRAM                    31466    /run/systemd/journal/syslog
unix  8      [ ]         DGRAM      CONNECTED     31474    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM      CONNECTED     31476    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    38213    /run/user/1000/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     23504    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     23495    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     31814
unix  2      [ ]         DGRAM      CONNECTED     36113
unix  2      [ ]         DGRAM      CONNECTED     30591
unix  3      [ ]         STREAM     CONNECTED     32839    /mnt/wslg/PulseAudioRDPSink
unix  3      [ ]         STREAM     CONNECTED     38239
unix  3      [ ]         STREAM     CONNECTED     32794
unix  3      [ ]         STREAM     CONNECTED     35394
unix  3      [ ]         STREAM     CONNECTED     31623
unix  3      [ ]         STREAM     CONNECTED     29147    /tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     36170
unix  3      [ ]         STREAM     CONNECTED     29934
unix  3      [ ]         STREAM     CONNECTED     31813
unix  3      [ ]         STREAM     CONNECTED     34228    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     33253    /tmp/dbus-XoAVGlIAKf
unix  3      [ ]         STREAM     CONNECTED     28664
unix  3      [ ]         STREAM     CONNECTED     34284    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     32417    /mnt/wslg/PulseAudioRDPSink
unix  3      [ ]         STREAM     CONNECTED     33277    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     29977    /tmp/dbus-5Z7HplrqEQ
unix  3      [ ]         STREAM     CONNECTED     23488
unix  3      [ ]         STREAM     CONNECTED     32783
unix  3      [ ]         STREAM     CONNECTED     36114    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     39028
unix  3      [ ]         STREAM     CONNECTED     38990
unix  3      [ ]         STREAM     CONNECTED     38989
unix  3      [ ]         STREAM     CONNECTED     31610
```

Thank you!