# CSE232: Programming Assignment 1

Submission by: Swapnil Panigrahi (2022522)

## Q1

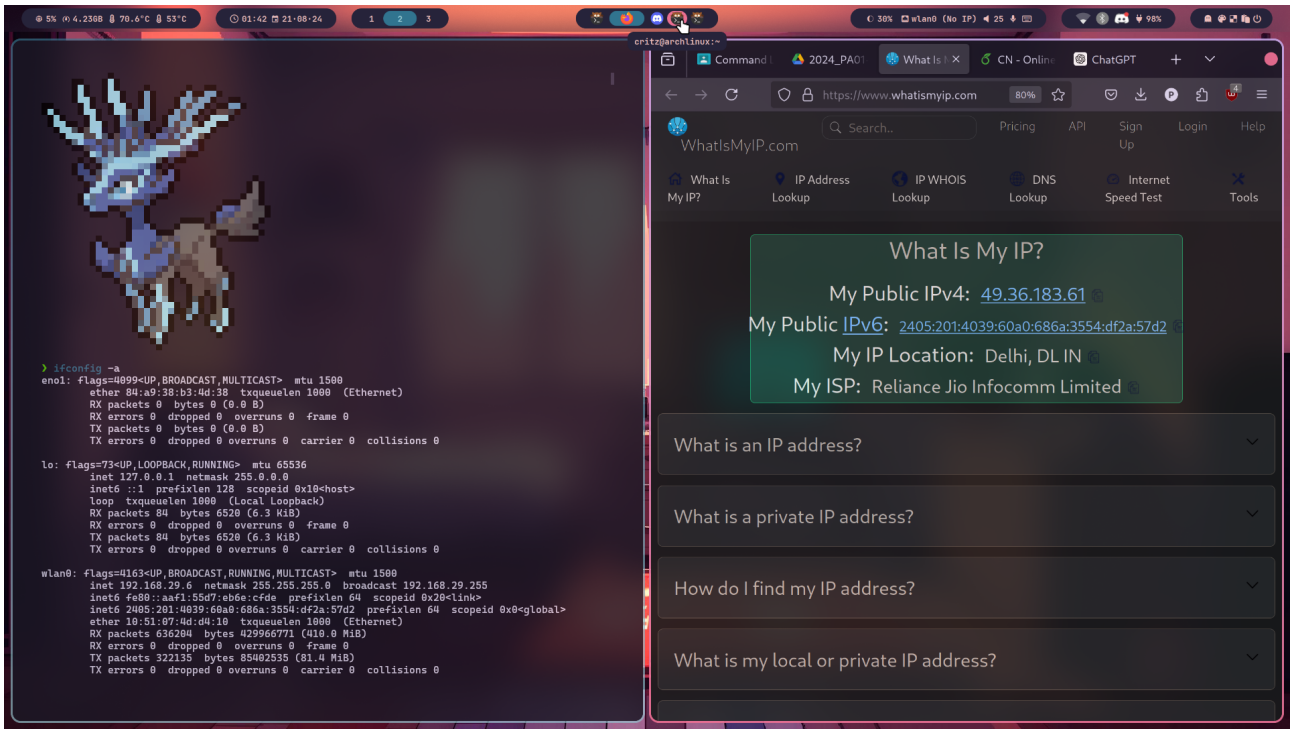


Figure 1: WhatIsMyIP vs. `ifconfig` command

### Commands

```
1 ifconfig -a
```

- Clearly, private IP shown by `ifconfig` is `192.168.29.6` but public IP shown by the website `49.36.183.61`
- They aren't identical because the public IP is assigned by the ISP and which is seen as the sender's address by the servers when packets reach them

## Q2


Figure 2: Change IP address to `192.168.22.12`

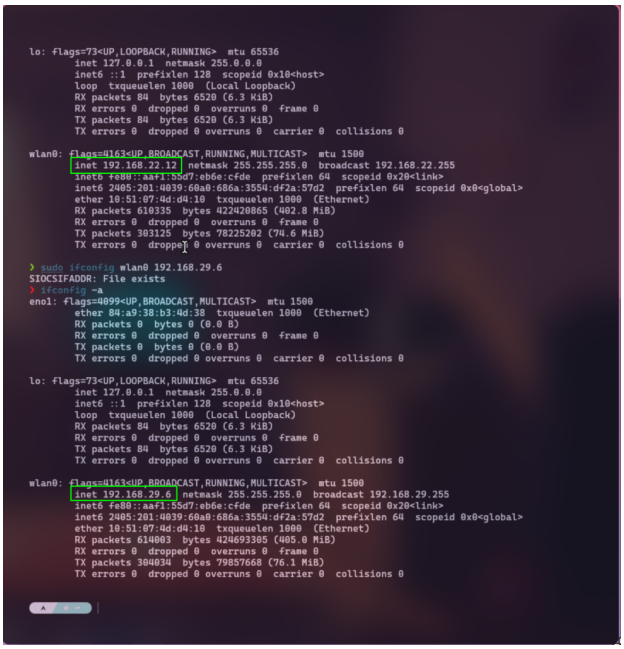


Figure 3: Change IP address back to `192.168.29.6`

### Commands

```
ifconfig -a
sudo ifconfig wlan0 192.168.22.12
ifconfig -a
sudo ifconfig wlan0 192.168.29.6
```

## Q3

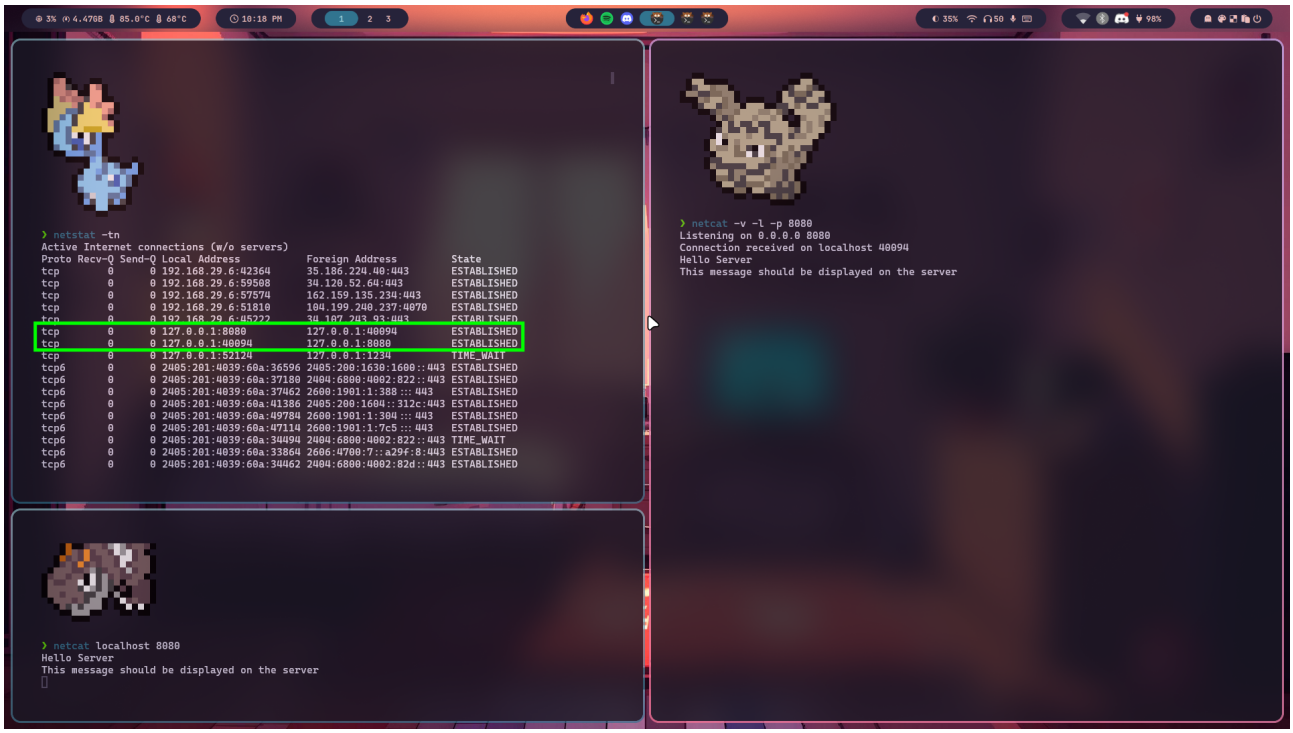


Figure 4: Setting up connection with localhost, and checking state of TCP connection

### Commands

```
# Open server terminal
netcat -v -l -p 8080
```

```
# Open client terminal
netcat localhost 8080
Hello Server
This message should be displayed on server
```

```
# Open monitor terminal
netstat -tn
```

## Q4

- References: ServerFault Article


Figure 5: Authoritative answer for `google.in` & TTL for `alibaba.in`

### Commands

```
nslookup
google.in
set type=ns
google.in
server ns1.google.com
google.in
```

```
nslookup -debug alibaba.com
```

1. `nslookup` starts an interactive version of the nslookup
2. `google.in` gives the non-authoritative answer from local DNS server
3. `set type=ns` helps us lookup the "name servers" for `google.in`
4. `server ns1.google.com` changes the DNS server to an authoritative server for `google.in`
5. Querying `google.in` again returns an authoritative answer from server `ns1.google.com`

1. TTL for `alibaba.com` on local DNS server is 84 seconds
2. TTL for the same on the authoritative server is 231 seconds

## Q5


Figure 6: `traceroute` to `google.in`

### Commands

```
traceroute google.in
ping -c 50 google.in
ping -c 50 stanford.edu
traceroute stanford.edu
```

a. There are 15 intermediate hosts with the following IP addresses (taking the first host at each hop):

| IP Address | Average Latency (ms) |
|---|---|
| 192.168.29.1 | 1.668 |
| 10.232.136.1 | 7.721 |
| 172.16.18.29 | 7.665 |
| 192.168.96.236 | 10.495 |
| 172.26.111.117 | 10.441 |
| 172.26.111.131 | 7.221 |
| 192.168.44.44 | 5.059 |
| 142.250.169.176 | 10.070 |
| 142.251.71.163 | 7.839 |
| 142.251.49.120 | 7.808 |
| 192.178.82.236 | 7.732 |
| 209.85.250.56 | 12.299 |
| 142.250.46.171 | 30.849 |
| 142.250.209.71 | 33.144 |
| 142.250.66.4 | 29.690 |
| **Total Latency** | **189.701 ms** |

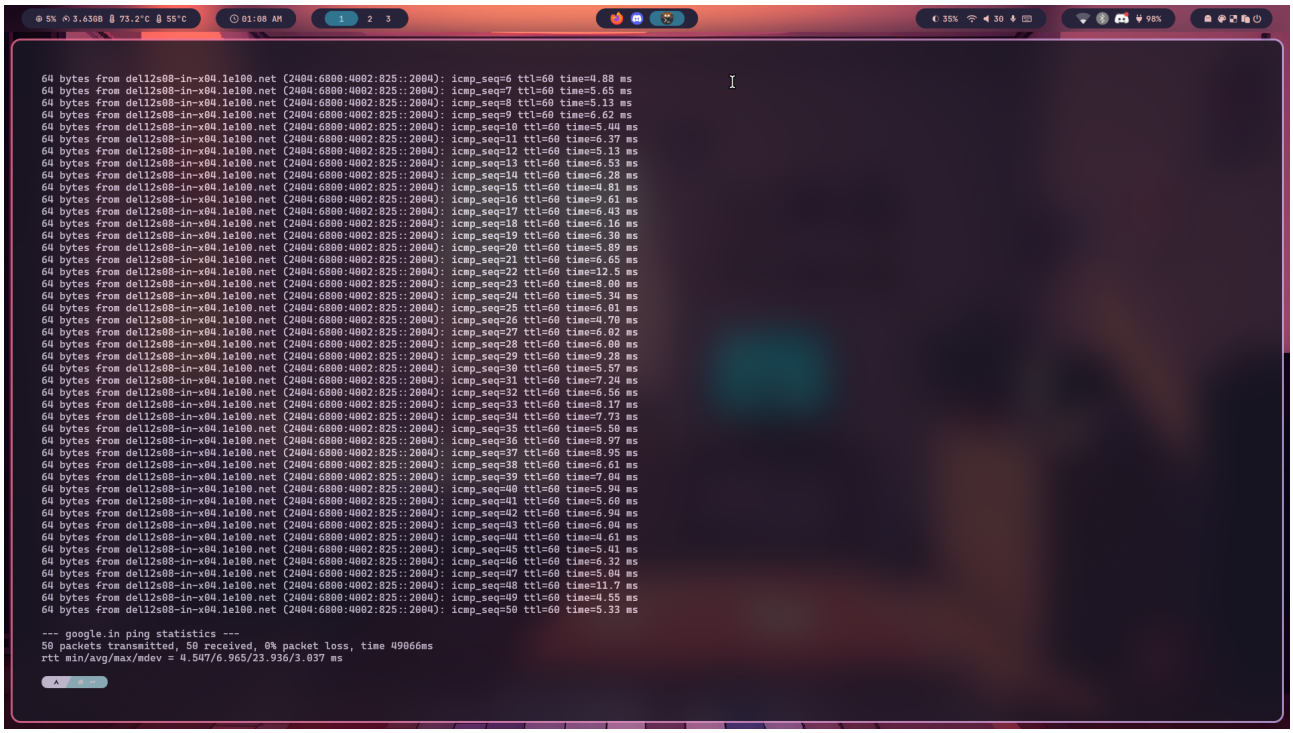


Figure 7: `ping` command to `google.in`

b. The average latency is 6.965 ms

c. i. The average latency for `ping` command is 6.965 (RTT) while the total latency for `traceroute` command is 189.7 ms

   ii. `traceroute` command gives us the latency to ping each hop, which adding up won't necessarily give us the correct RTT to our final hop `ping`

d. i. The highest latency for `traceroute` is 34.812 ms while the average for `ping` command is 6.965 ms.

   ii. The highest latency of `traceroute` is the latency to that host and not to the destination address i.e. the slowest hop, while for `ping` command, the latency is to the destination address.

e. We see multiple IPs for each hop as routers distribute traffic across multiple paths to next hop for load balancing purposes

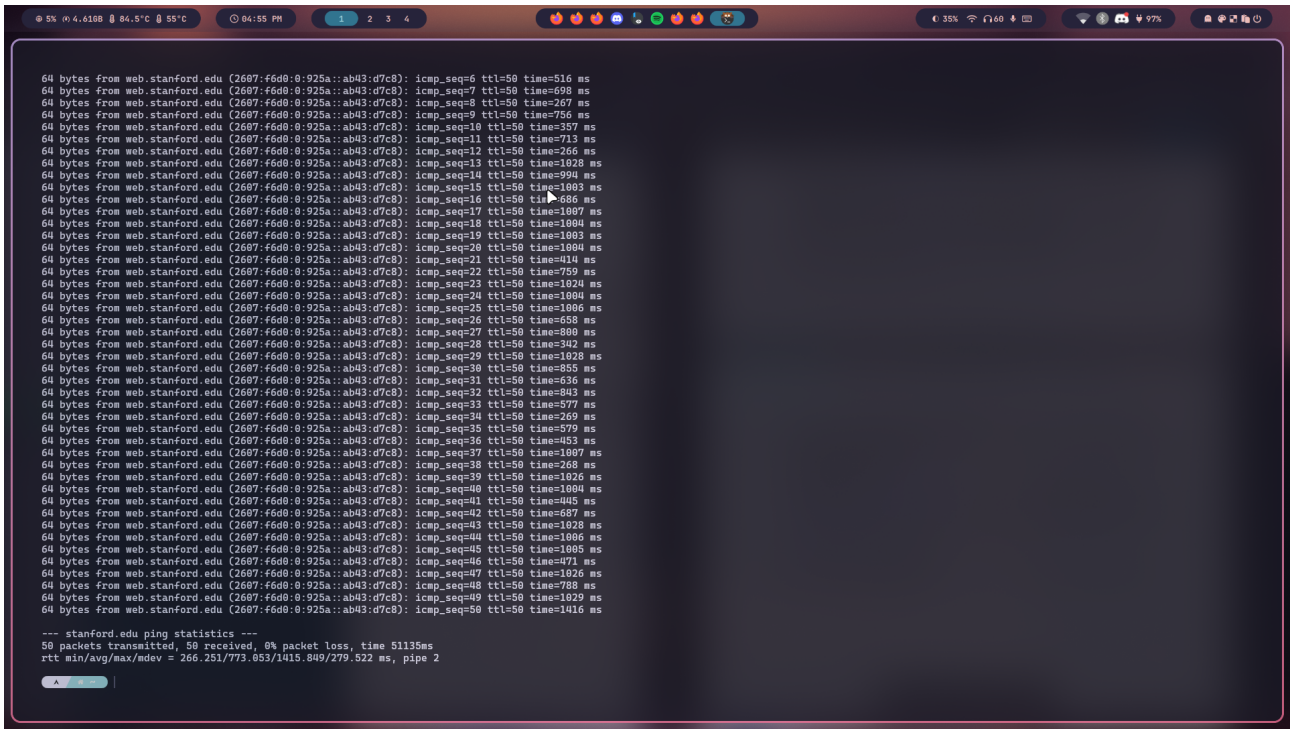


Figure 8: `ping` command to `stanford.edu`

f. The average latency is 773.053 ms


Figure 9: `traceroute` command to `stanford.edu`

g. The number of hops (ignoring "* * *") is 16, compared to 15 hops for google.in

h. Latency is different for both which could be due to geographical difference in the server locations. A part of the reason could also be network congestion.

## Q6

- References: AskUbuntu Article

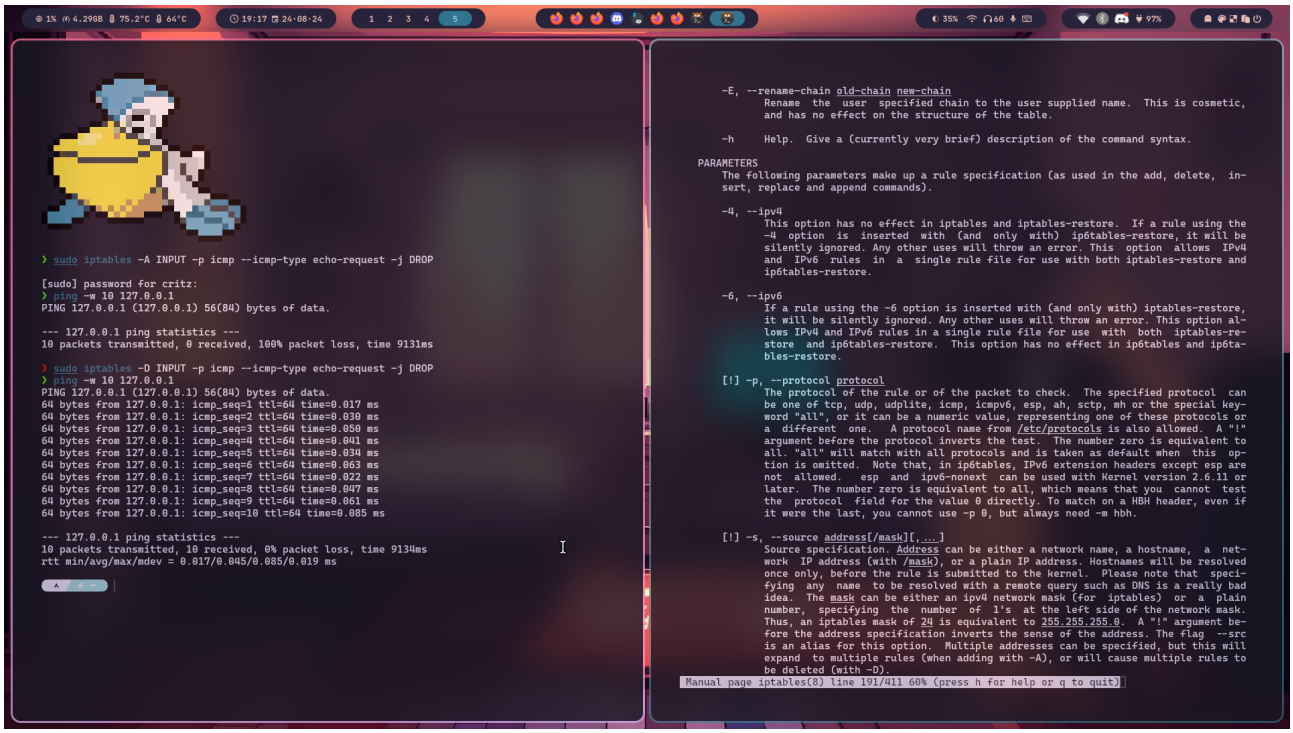


Figure 10: `ping` command with 100% packet loss

### Commands

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
ping -w 10 127.0.0.1
sudo iptables -D INPUT -p icmp --icmp-type echo-request -j DROP
ping -w 10 127.0.0.1
```

1. `iptables` is the command-line utility that allows us to configure the firewall
2. `-A INPUT` appends a rule to the incoming traffic to the machine1
3. Since `ping` command uses ICMP protocol, we silently discard ICMP echo requests, without sending anything back
4. Simply running the command with `-D` instead, deletes the rule and we can ping `localhost` again