CSE 232 : Assignment 1

Command Line Utilities

Ans1. Command Used `ipconfig`

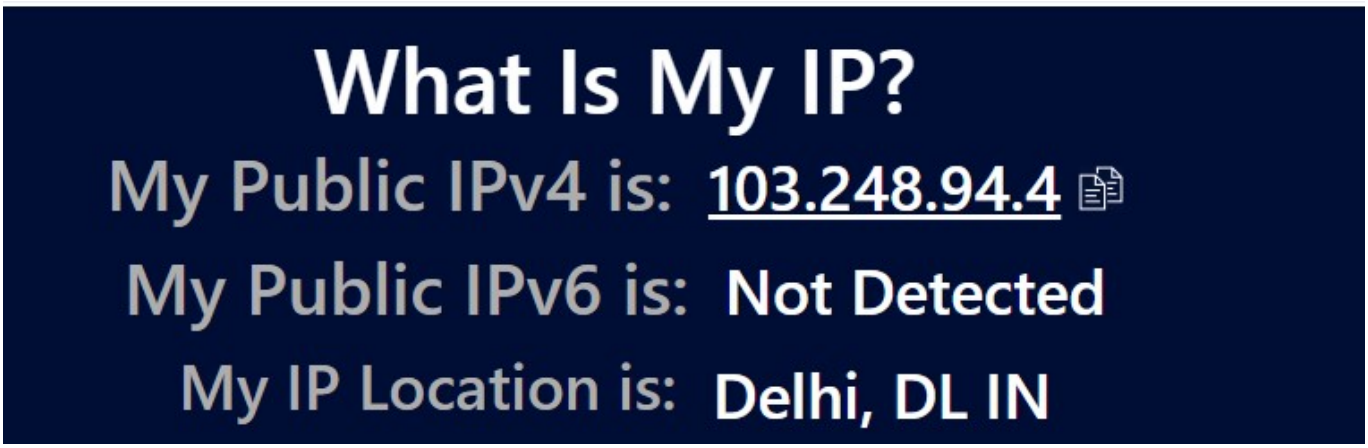
a)

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b2e2:41d9:c27f:188d%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.58
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::1%10
                                       192.168.1.1
```

b) The IP address I see from `ipconfig` is my pc's local IP address. This is assigned by my router and is used for communication within my local network.

The IP address I see on "https://www.whatismyip.com" is my public IP address. This is the address my ISP assigned, and it's used for communication over the Internet.



Ans2.

a) Command Used `nslookup -type=NS google.in`
The above command is used to find the name servers for a domain google.in.

```
PS C:\Users\kitkat> nslookup -type=NS google.in
Server:  one.one.one.one
Address:  1.1.1.1

Non-authoritative answer:
google.in       nameserver = ns4.google.com
google.in       nameserver = ns3.google.com
google.in       nameserver = ns1.google.com
google.in       nameserver = ns2.google.com
```

To find the IP address of a individual name server, we can use the command `nslookup google.in ns1.google.com`. This will give the ipv6 and ipv4 address of the name server ns1.google.com.

```
PS C:\Users\kitkat> nslookup google.in ns1.google.com
Server:  ns1.google.com
Address:  216.239.32.10

Name:    google.in
Addresses:  2404:6800:4002:814::2004
          142.250.77.228

PS C:\Users\kitkat> nslookup google.in ns2.google.com
Server:  ns2.google.com
Address:  216.239.34.10

Name:    google.in
Addresses:  2404:6800:4002:815::2004
          142.250.182.164

PS C:\Users\kitkat>
```

b) Command Used `nslookup -debug google.in`

- The debug mode of nslookup initially performs a reverse DNS lookup to identify the name associated with your DNS server's IP, which is why I see a query for 1.1.1.1.in-addr.arpa and get a result of one.one.one.one.
- For the domain "google.in", the IPv4 address is 142.250.194.164, and time to live is 259 seconds (4 minutes and 19 seconds) before my DNS server will refresh it.
- The IPv6 address for "google.in" is 2404:6800:4002:823::2004, TTL of 300 seconds (5 minutes).

```
PS C:\Users\kitkat> nslookup -debug google.in
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        1.1.1.1.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  1.1.1.1.in-addr.arpa
        name = one.one.one.one
        ttl = 1359 (22 mins 39 secs)

------------
Server:  one.one.one.one
Address:  1.1.1.1

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.in, type = A, class = IN
    ANSWERS:
    ->  google.in
        internet address = 142.250.194.164
        ttl = 259 (4 mins 19 secs)

------------
Non-authoritative answer:
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        google.in, type = AAAA, class = IN
    ANSWERS:
    ->  google.in
        AAAA IPv6 address = 2404:6800:4002:823::2004
        ttl = 300 (5 mins)
```

Ans03.

a) Command used `tracert google.in`

```
PS C:\Users\kitkat> tracert google.in

Tracing route to google.in [142.250.194.132]
over a maximum of 30 hops:

  1    73 ms     1 ms     2 ms  192.168.1.1
  2    95 ms     3 ms     7 ms  10.190.104.1
  3    81 ms     3 ms     6 ms  163.53.87.189
  4    89 ms     4 ms     5 ms  72.14.198.176
  5     9 ms     4 ms     3 ms  142.251.66.169
  6     4 ms     4 ms     3 ms  142.251.52.203
  7     5 ms     2 ms     2 ms  del12s05-in-f4.1e100.net [142.250.194.132]

Trace complete.
```

- I can see a total of 7 hops and the average latency to each intermediate host are 25.33, 35, 30, 32.67, 5.33, 3.67, 3 in milliseconds.

b)

```
PS C:\Users\kitkat> ping -n 50 google.in

Pinging google.in [142.250.194.132] with 32 bytes of data:
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=6ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=2ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=4ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=6ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=5ms TTL=60
Reply from 142.250.194.132: bytes=32 time=6ms TTL=60
Reply from 142.250.194.132: bytes=32 time=3ms TTL=60

Ping statistics for 142.250.194.132:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 6ms, Average = 3ms
```

Average latency to google.in is 3 milliseconds.

c)

Sum of Average Latencies: 25.33 ms + 35 ms + 30 ms + 32.67 ms + 5.33 ms + 3.67 ms + 3 ms = 135 ms
From the ping results: 3ms

- No, The sum of the latencies from tracert is significantly higher than the average latency from ping. This is expected because ping measures the round-trip time (RTT) from my computer to the destination and back, while traceroute measures the time it takes to reach each intermediate host.

d)
Maximum Latency: 35 ms (from Hop 2)
From the ping results: Average Latency: 3ms
Not Matching.

- Although already explained in the above part, the ping and traceroute commands provide different insights into network performance. While ping gives an average round-trip time to a destination, traceroute provides a hop-by-hop breakdown of the path taken by packets.

e) Multiple entries for a single hop in traceroute represent multiple probes sent to the same hop to get a more accurate measurement. Each probe might take a slightly different amount of time, so I see multiple latency values(three in this case). The three round trips time is in milliseconds. it tells us how long it tool packet to get from me to that ipaddress/server and then back to me(latency between two systems)

f)

```
PS C:\Users\kitkat> ping -n 50 stanford.edu

Pinging stanford.edu [171.67.215.200] with 32 bytes of data:
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=275ms TTL=234
Reply from 171.67.215.200: bytes=32 time=275ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=278ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=271ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=278ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=279ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=272ms TTL=234
Reply from 171.67.215.200: bytes=32 time=273ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=274ms TTL=234
Reply from 171.67.215.200: bytes=32 time=275ms TTL=234

Ping statistics for 171.67.215.200:
    Packets: Sent = 50, Received = 50, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 271ms, Maximum = 279ms, Average = 273ms
PS C:\Users\kitkat>
```

Average latency to stanford.edu is 273 milliseconds.

g)

```
PS C:\Users\kitkat> tracert stanford.edu

Tracing route to stanford.edu [171.67.215.200]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2    19 ms    20 ms    18 ms  10.190.104.1
  3     5 ms     2 ms     3 ms  43.248.155.1
  4     6 ms     4 ms     4 ms  122.184.140.109
  5   247 ms   246 ms   245 ms  182.79.146.238
  6     *        *        *     Request timed out.
  7   247 ms   247 ms   246 ms  port-channel8.core2.lax1.he.net [184.104.197.109]
  8     *      259 ms     *     port-channel13.core3.sjc2.he.net [184.104.198.253]
  9     *      253 ms   252 ms  eqix-sv8.hurricaneelectric.com [198.32.176.20]
 10   258 ms   258 ms   257 ms  stanford-university.e0-62.core2.pao1.he.net [184.105.177.238]
 11   269 ms   271 ms   270 ms  woa-west-rtr-vl2.SUNet [171.64.255.132]
 12     *        *        *     Request timed out.
 13   274 ms   274 ms   273 ms  web.stanford.edu [171.67.215.200]

Trace complete.
```

- google.in has 7 hops.
- stanford.edu has 13 hops. Thus, stanford.edu has more hops compared to google.in when traced from my location. The number of hops can vary based on the network path, the location of the servers, and the routing decisions made by intermediate networks. Some hops in stanford took longer than google.in. This might be because of the network path to stanford.edu is longer than the network path to google.in.

h)

> google.in average Latency: 3ms
> stanford.edu average Latency: 273ms

- Physical Distance: One of the primary factors affecting latency is the physical distance between the source and destination server. google.in likely directs me to a server that's geographically closer to me, possibly within India. In contrast, stanford.edu is located in California.

- Network Infrastructure: Google has a vast global network infrastructure with data centers around the world. They use advanced routing and content delivery techniques to ensure low latency and fast access for users. On the other hand, stanford.edu might not have the same level of global infrastructure as Google, leading to higher latencies.

- Number of Hops: As observed from the tracert results, stanford.edu has more intermediate hops compared to google.in. Each hop adds a slight delay, and the cumulative effect can increase the overall latency.

- Server Response Time: The responsiveness of the server itself can also impact latency. Google's servers are optimized for high performance and can handle a large number of requests efficiently. In contrast, specific servers at Stanford University might be under higher load or not as optimized, leading to slightly longer response times.

Ans04. ping command fail for 127.0.0.1 (with 100% packet loss)

- Achieving this in linux environment is pretty easy by adding an entry in iptables for localhost

- Achieving this in Windows is tricky. Adding firewall rules to block ping to 127.0.0.1 using protocol icmpv4 will not achieving our intended result.

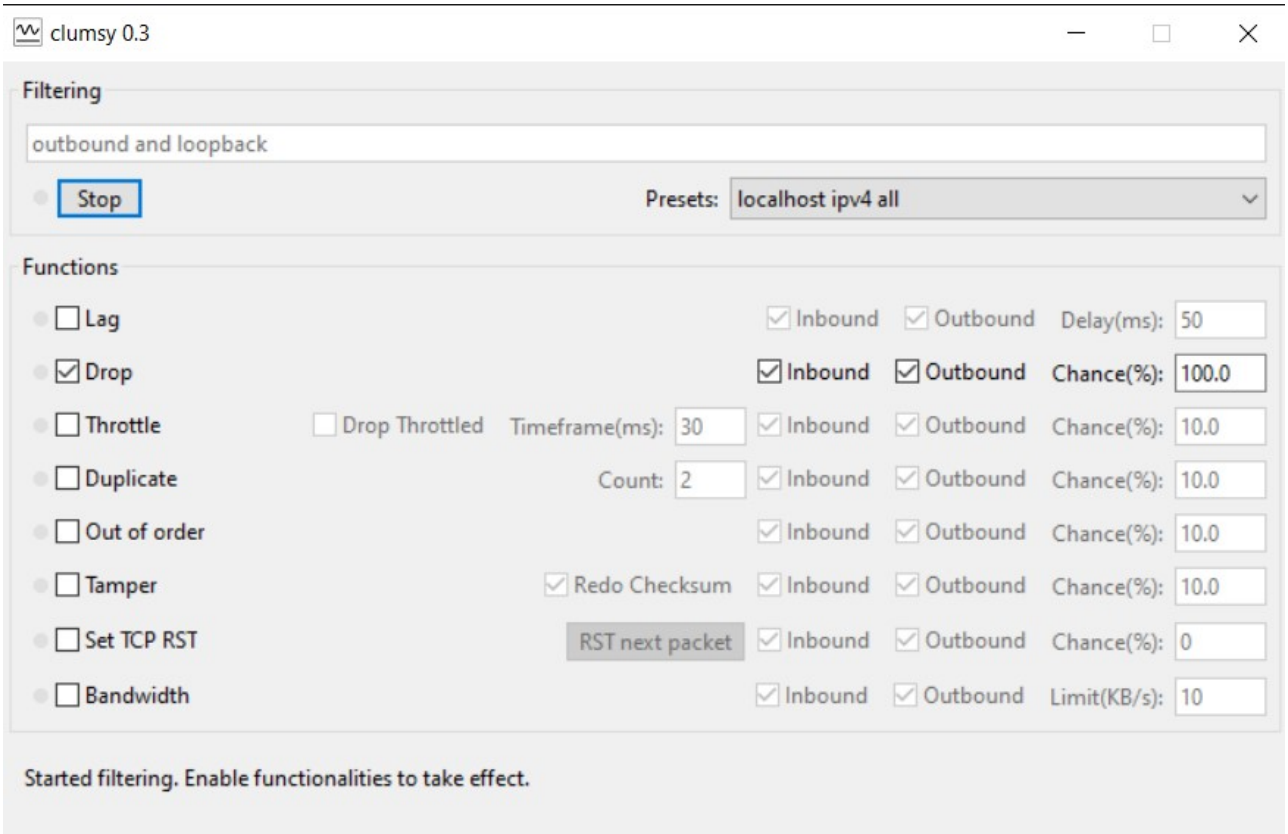
```
PS C:\Windows\system32> netsh advfirewall firewall add rule name="BlockPing127"
dir=in action=block protocol=icmpv4:8,any remoteip=127.0.0.1
Ok.

PS C:\Windows\system32> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
```

- We can block the inbound and outbound traffic for localhost using a freeware `clumsy`



The final result will look like this:

```
PS C:\Windows\system32> ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Windows\system32>
```

Source: Answer on SuperUser by dakkaron

Clumsy: Clumsy

Ans05 Command used:

`telnet 192.168.24.12 9900`

`GET /secret HTTP/1.1 Host: 192.168.24.12`

> secret key: U2FsdGVkX19+x/ug4M1wFYXRji8I6qmUgHOsKtqWGQAeiQ/Xy1Zmg5uKbUbOBO5P

```
telnet 192.168.24.12 9900
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
GET /secret HTTP/1.1
Host: 192.168.24.12

HTTP/1.1 200 OK
Content-Type: text/plain
ip: 192.168.1.99
X-secret: U2FsdGVkX19+x/ug4M1wFYXRji8I6qmUgHOsKtqWGQAeiQ/Xy1Zmg5uKbUbOBO5P
Date: Fri, 25 Aug 2023 16:13:39 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 8

Success
Connection closed by foreign host.
```

Ans06

Command used: `telnet 192.168.24.12 smtp`

My Inputs:

```
telnet 192.168.24.12 smtp
Trying 192.168.24.12...
Connected to 192.168.24.12.
Escape character is '^]'.
220 Welcome to CSE232 Mail Server
helo cse232.com
250 xeon01-rs-iiitd.iiitd.edu.in
MAIL FROM: 21015@cse232.com
250 2.1.0 Ok
RCPT TO: 21031@cse232.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: One piece is real
Like I said, One piece is real
.
250 2.0.0 Ok: queued as D0F1C6F6441E
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

The email was sent successfully and the mail was received in my friend's inbox:

```
From 21015@cse232.com  Fri Aug 25 21:46:41 2023
Return-Path: <21015@cse232.com>
X-Original-To: 21031@cse232.com
Delivered-To: 21031@cse232.com
Received: from cse232.com (vpn.iiitd.edu.in [192.168.1.99])
        by xeon01-rs-iiitd.iiitd.edu.in (Postfix) with SMTP id D0F1C6F6441E
        for <21031@cse232.com>; Fri, 25 Aug 2023 21:45:26 +0530 (IST)
SUBJECT: One piece is real

Like I said, One piece is real
```

> Ankit Kumar, 2021015