NAME - GAUTAM KUMAR MAHAR(2103114) AND AUMKAR LOREKAR(2003108)

PART 1: IP and MAC Addresses and Routing tables

Question 1)

a) ipv4 -> 127.0.0.1/8
ipv6 -> 1/128

b) [WIFI] IPv4 - 10.196.10.13 IPv6 Address - fe80::c323:1927:6307:e475%

c) 1. [Wifi] – IPv4 - 10.196.10.13
IPv6 Address - fe80::c323:1927:6307:e475%

2. Mac Address - c8:94:02:83:1f:25

3. Chongqing Fugui Electronics Co.,ltd.

```
gautamop@gautamop-HP-Pavilion-Laptop-14-ec0xxx:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen
 1000
    link/ether c8:94:02:83:1f:25 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 10.196.10.13/20 brd 10.196.15.255 scope global dynamic noprefixroute wlo1
       valid_lft 86352sec preferred_lft 86352sec
    inet6 fe80::c92a:6b89:cf03:a29e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Question 2)

a) [WIFI] IPv4 - 10.196.10.13 IPv6 Address - fe80::c323:1927:6307:e475%
netmask 255.255.240.0

```
gautamop@gautamop-HP-Pavilion-Laptop-14-ec0xxx:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen
 1000
    link/ether c8:94:02:83:1f:25 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    inet 10.196.10.13/20 brd 10.196.15.255 scope global dynamic noprefixroute wlo1
       valid_lft 86352sec preferred_lft 86352sec
    inet6 fe80::c92a:6b89:cf03:a29e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

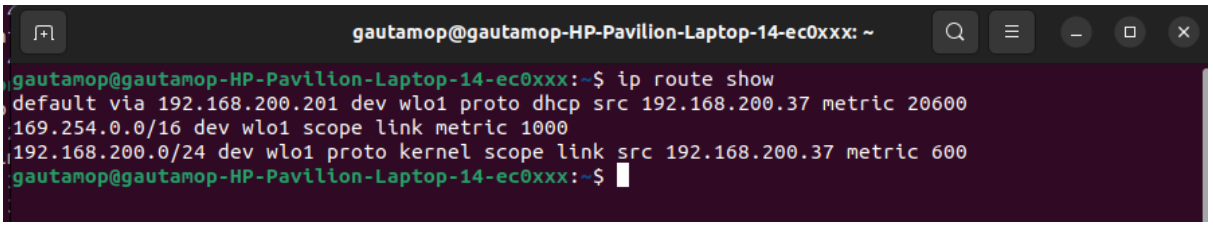
b) 2^12 Hosts

c) 10.196.15.255

d) The Publicly Visible IP Address is 14.139.106.150

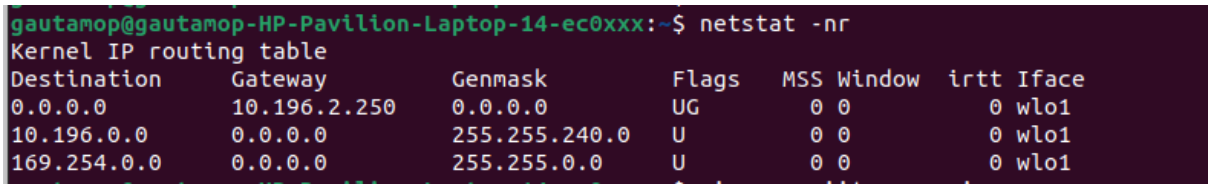
Question 3)

(a) Gateway - We can say its computer sits between different networks or applications. It just serves as an entry and exit for computer networks.
A gateway is a device that connects two different networks together, allowing communication between them.
Gateway ip address - 10.196.2.250



b) Kernel IP routing table -

Destination	Gateway
0.0.0.0	10.196.2.250
10.196.0.0	0.0.0.0
169.254.0.0	0.0.0.0



(c) 0.0.0.0 address is showing the client isn't connected to a TCP/IP network.

(d) 169.254.0.0/16

The inability to connect to or locate a DHCP server for the purpose of receiving an IP address means that you have not given your machine a static IP address.

Part - 2

Question 4)

a) www.iitgoa.ac.in

6.572 ms

```
--- www.iitgoa.ac.in ping statistics ---
110 packets transmitted, 110 received, 0% packet loss, time 109201ms
rtt min/avg/max/mdev = 0.949/6.572/99.752/13.257 ms
```

b) www.celand.is

254.654 ms

```
--- www.iceland.is ping statistics ---
47 packets transmitted, 47 received, 0% packet loss, time 50815ms
rtt min/avg/max/mdev = 195.970/254.654/352.064/34.671 ms
```

Question 5)

A traceroute sends Internet Control Message Protocol (ICMP) packets, which are received by every router participating in the data transmission.
The ICMP packets show whether the routers involved in the transmission can transport the data successfully or not.
Traceroute really uses an IP packet header field that wasn't really intended for delivery but for path or route tracing, making it somewhat of a hack.
According to the IP standard, each IP packet must have a Time-to-live (TTL) value.
This TTL number acts as a self-destruct mechanism to stop undelivered packets from endlessly recirculating the internet.
Every router along a path is supposed to decrease the TTL value by one before delivering a packet farther along the line.

Question 6)

I used the University of Cambridge domain in this question.

a) This is IP address of Cambridge University -> 128.232.132.8

```
gautamop@gautamop-HP-Pavilion-Laptop-14-ec0xxx:~$ dig www.cam.ac.uk

; <<>> DiG 9.18.4-2ubuntu2-Ubuntu <<>> www.cam.ac.uk
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21162
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.cam.ac.uk.                 IN      A

;; ANSWER SECTION:
www.cam.ac.uk.          3600    IN      A       128.232.132.8

;; Query time: 2356 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Jan 19 10:25:32 IST 2023
;; MSG SIZE  rcvd: 58
```

b) Total 23 hops taken to reach the destination.

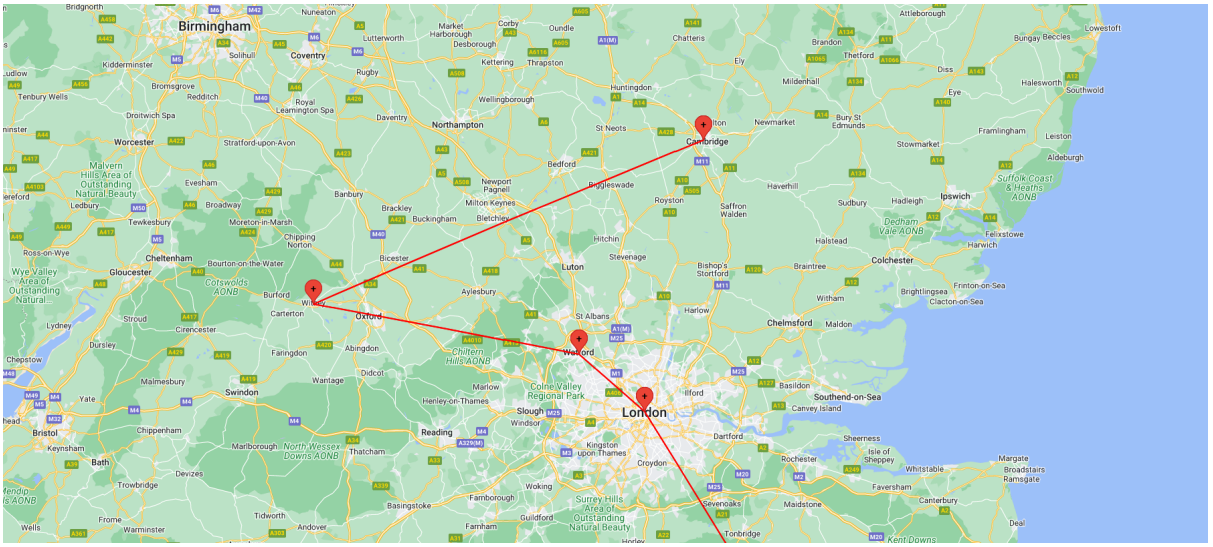
```
gautamop@gautamop-HP-Pavilion-Laptop-14-ec0xxx:~$ traceroute 128.232.132.8
traceroute to 128.232.132.8 (128.232.132.8), 30 hops max, 60 byte packets
 1  _gateway (10.196.2.250)  46.919 ms  46.862 ms  47.279 ms
 2  firewall.iitgoa.ac.in (10.250.209.251)  45.725 ms  46.194 ms  47.216 ms
 3  14.139.106.145 (14.139.106.145)  47.198 ms  47.178 ms  47.153 ms
 4  10.155.103.129 (10.155.103.129)  152.236 ms  150.519 ms  152.191 ms
 5  10.155.103.5 (10.155.103.5)  152.168 ms  152.105 ms *
 6  10.255.234.193 (10.255.234.193)  152.057 ms  106.454 ms  106.080 ms
 7  10.255.232.213 (10.255.232.213)  101.768 ms  101.785 ms aes-static-041.105.144.59.airtel.in (59.14
 8  180.149.48.18 (180.149.48.18)  104.613 ms  103.826 ms  104.361 ms
 9  180.149.48.6 (180.149.48.6)  207.608 ms 180.149.48.2 (180.149.48.2)  196.379 ms  196.574 ms
10  180.149.48.31 (180.149.48.31)  228.847 ms  229.355 ms  229.681 ms
11  nkn.mx1.gen.ch.geant.net (62.40.125.214)  213.849 ms  214.160 ms  214.787 ms
12  ae7.mx1.par.fr.geant.net (62.40.98.239)  206.960 ms nkn.mx1.gen.ch.geant.net (62.40.125.214)  230.
13  ae8.mx1.lon2.uk.geant.net (62.40.98.106)  312.595 ms ae7.mx1.par.fr.geant.net (62.40.98.239)  289.
14  janet-bckp-gw.mx1.lon2.uk.geant.net (62.40.125.58)  289.115 ms  289.095 ms  289.072 ms
15  ae31.erdiss-sbr2.ja.net (146.97.33.22)  289.094 ms janet-bckp-gw.mx1.lon2.uk.geant.net (62.40.125.
16  ae31.erdiss-sbr2.ja.net (146.97.33.22)  289.029 ms ae30.lowdss-sbr1.ja.net (146.97.33.26)  288.999
17  ae30.lowdss-sbr1.ja.net (146.97.33.26)  288.988 ms  288.970 ms  288.945 ms
18  uoc.ja.net (146.97.41.38)  288.828 ms ae26.lowdss-ban1.ja.net (146.97.35.246)  228.575 ms  228.142
19  131.111.6.82 (131.111.6.82)  213.986 ms 146.97.41.38 (146.97.41.38)  228.936 ms  228.698 ms
20  131.111.6.82 (131.111.6.82)  229.147 ms  231.034 ms  231.168 ms
21  193.60.88.2 (193.60.88.2)  238.928 ms  153.250 ms  239.442 ms
22  128.232.128.2 (128.232.128.2)  223.102 ms  223.091 ms 193.60.88.2 (193.60.88.2)  238.908 ms
23  128.232.128.2 (128.232.128.2)  238.674 ms * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

c) The lines appearing as *** mean that the hop is not responding to the message sent by the traceroute command.

d) Traceroute does 3 trials (sends 3 messages) to each hop by default. “traceroute -q” is the command to get traceroute to do 5 trials instead.

e) 285.228ms is the average round-trip delay (in mili-seconds) for reaching the final destination.

f) The geographical location of the last hop is Witney Uk to cambridge UK



PART - 3

Question 7)

a) TCP protocol is being used at the transport layer

b) Source Port: 10.196.10.13
Destination Address: 10.250.200.7

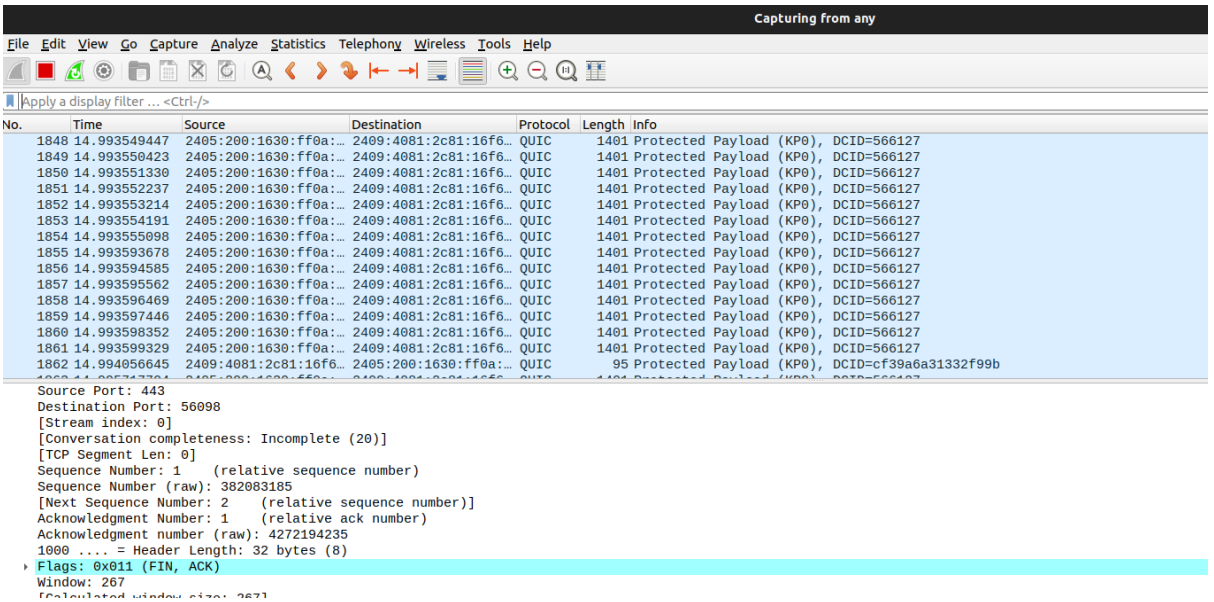
c) Source Port: 39150
Destination Port: 443

```
Header Checksum: 0x9a2b [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.196.10.13
Destination Address: 10.250.200.7
Transmission Control Protocol, Src Port: 39150, Dst Port: 443, Seq: 0, Len: 0
Source Port: 39150
Destination Port: 443
[Stream index: 35]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
```

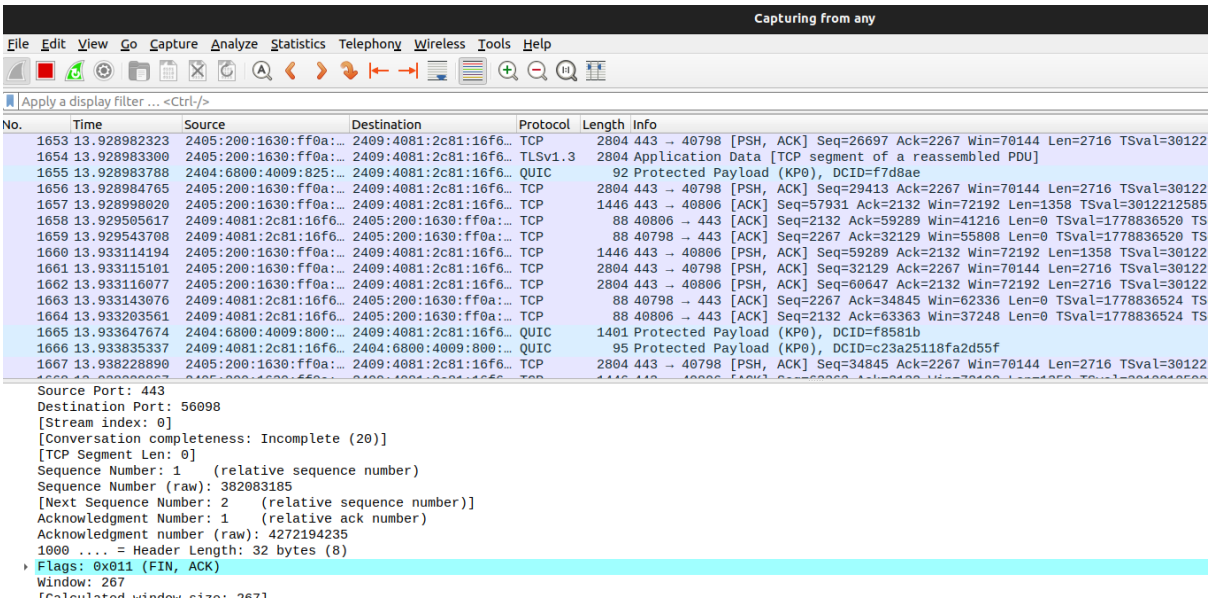
d) The Majority Of Packets are TCP And Most Packets are of Type ACK.

Question 8)

a) www.youtube.com uses **TCP** protocol to open the site and for playing video it uses **QUIC** protocol.



—----------



b) For Google chrome it uses TCP protocol for both reaching the site and playing the video.

Question 9)

> Modern day devices use firewalls and other secure barriers to prevent packet sniffing. Wireshark fails to capture these packet transfers due to heavy encryption. Lack of these safety features will make our data vulnerable to cyber attackers. Wireshark may be able to detect data packets given we disable the software and hardware firewall.