Question 1:

(a) The option required to specify the number of echo requests to send with ping command is: **-c**
Example: *ping -c 5 <website/ip>* will send 5 ICMP ECHO_REQUESTS to the specified address.
(b) The option required to set time interval (in seconds), between two successive ping ECHO_REQUESTs is: **-i**
Example: *ping -i 2 <website/ip>* will send ICMP ECHO_REQUESTS to the specified address every 2 seconds. Intervals less than 0.2 seconds require 'sudo' permissions.
(C) The command to send ECHO_REQUEST packets to the destination one after another without waiting for a reply is: **-l**
Example: *ping -l <website/ip>* will shoot the target with ICMP ECHO_REQUESTS without waiting for reply.
3 is the limit of sending such ECHO_REQUEST packets by normal users.
(d) The command to set the ECHO_REQUEST packet size (in bytes) is: **-s**
Example: *ping -s <website/ip>* will send ICMP ECHO_REQUESTS to the specified address with 128bytes of ICMP_DATA.
When Packet Size is set to 64 bytes, then the total packet size will be 72 bytes considering the 8 bytes of ICMP header data and 92 bytes including Internet Protocol version 4 header.

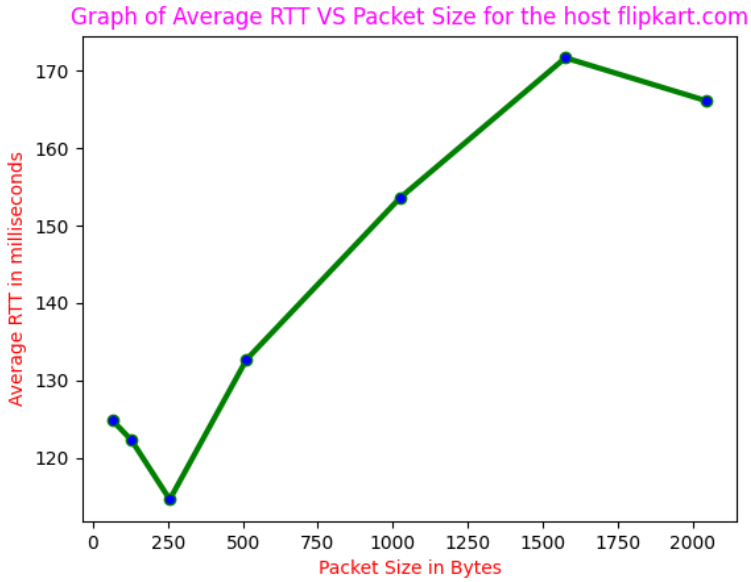
Question 2:

I choose following 5 hosts:
1)google.com 2)youtube.com 3)facebook.com 4)amazon.com 5)flipkart.com

Domain name	IP address	Geolocation	Avg. RT1	Avg. RTT2	Avg. RTT3	Avg RTT
google,com	172.217.174.78	Maharashtra, India	239.776 ms	126.667 ms	128.583 ms	165.009 ms
youtube.com	142.250.67.238	Maharashtra, India	214.689 ms	122.320	129.458 ms	155.489 ms
facebook.com	69.171.250.35	California, US	211.926 ms	133.701 ms	142.173 ms	162.600 ms
amazon.com	176.32.103.205	Virginia, US	594.922 ms	370.194 ms	652.170 ms	522.429 ms
flipkart.com	163.53.78.110	Maharashtra, India	192.596 ms	121.819 ms	156.543 ms	156.986 ms

Packet loss: YES**,** there exist cases, which shows packet loss greater than 0%.

When packets of data travelling across a computer network fail to reach their destination, packet loss occurs, which can be because of firewall blocking. It is mainly caused by network congestion or target IP address might not have any network device connected with it.
Impact of Geolocation: There is a weak correlation between distance and RTT. Mainly it will depend on how many routers/switches come into way, as transmission will not take much time. At each router there may be a delay, so if the packets have to go through more distance, thus more routers, therefore longer the RTT.



Generally, with increase in packet size, RTT increases as shown in the above figure. Time influence on RTT measurements can be understood as different hours correspond to different busy working hours of different continents. Higher RTTs are measured when it is daytime in Asia and Europe. It may be because network traffic is busier, as more users are online.

	64	128	256	512	1024	1576	2048
RTT1(ms)	124.884	122.309	114.643	132.712	153.575	171.667	166.097d
RTT2(ms)	145.436	187.582	607.190	184.615	220.555	352.365	375.261
RTT3(ms)	191.204	171.500	155.049	179.377	259.815	419.323	281.044

Question 3:

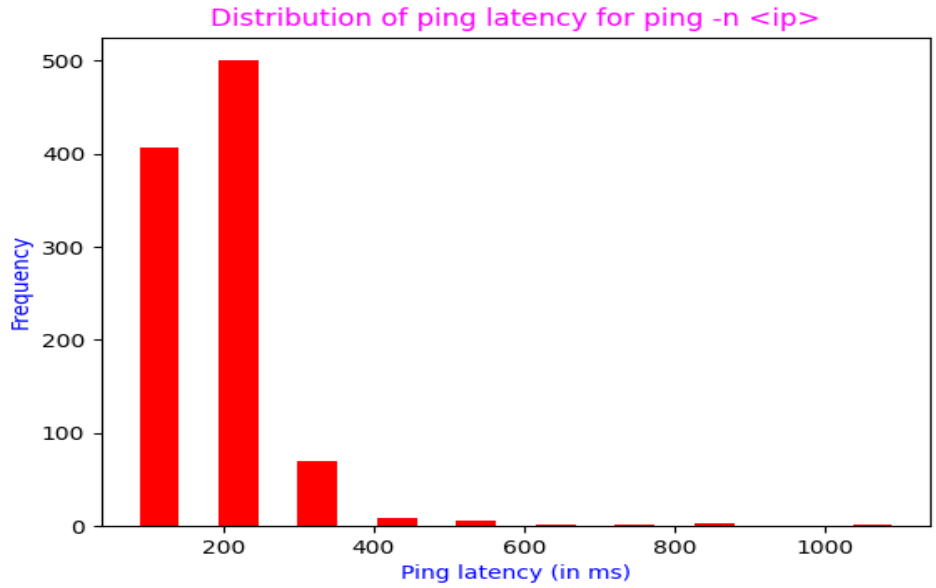
Host: google.com (142.250.192.142)
Command: (1) ping -n -c 1000 142.250.192.142 (2) ping -p ff00 -c 1000 142.250.192.142

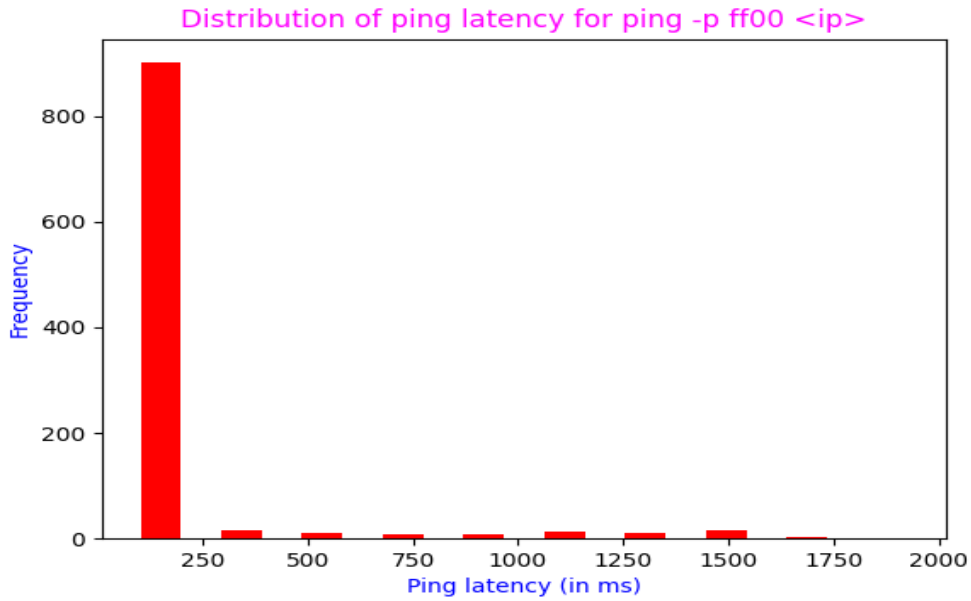
(a) packet loss rate for each command:
Command (1): 0 packet out of 1000 Command (2): 12 packet out of 1000

(b)

Command	Packets sent	Packets received	Packet loss rate	Min. latency	Max. latency	Mean latency	Median latency
(1)	1000	1000	0%	61.690 ms	1117.396ms	187.388 ms	190.0 ms
(2)	1000	988	1.2%	54.384 ms	1974.343ms	180.723 ms	97.3 ms

(c)





(d) No attempt will be made to look up symbolic names/hosts for host addresses leading to less time spent in each request for command (1) and only command (2) goes with dns resolution. Hence it may occur that the command (2) with pattern ff00 may have more ping latency and higher packet loss.
Distribution for command (1): Out of 1000 packets transmitted, all were received and RTT values lied between 61.69 ms and 1117.396 ms. **mdev**(standard deviation) value is 97.618 ms.
Distribution for command (2): Out of 1000 packets transmitted, 988 were received and RTT values lied between 54.384 ms and 19747.343 ms. **mdev**(standard deviation) value is 280.463 ms.

Question 4:

(a) Ifconfig:

It is a utility used to configure the kernel-resident network interfaces. It is used at boot time to set up the interface as necessary. If no arguments are given. Ifconfig displays the status of the currently active interfaces.
Here enp0s3, lo are the names of the active network interfaces on the system.
1) *enp0s3* is the first Ethernet interface. Next Ethernet interfaces would be named enp0s1, enp0s2, etc.
2) *lo* is the loopback interface. This is a special network interface, which the system uses to communicate with itself.
Ifconfig output terminologies explanation:
Link encap:Ethernet : This represents the frame type associated with this interface. In our case it is Ethernet.
HWaddr : the hardware address of the ethernet interface also known as MAC address. It is of 48 bits. First three octets represents the manufacturer id and the last three represents the serial number assigned to the device by the manufacturer.
inet addr : IPv4 address assigned to the interface.
Bcast: denotes the broadcast address for the current network

```
pranav@pranav:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::3eec:6a3a:6c70:d2c0  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:02:af:5d  txqueuelen 1000  (Ethernet)
        RX packets 1605  bytes 1065612 (1.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1429  bytes 166483 (166.4 KB)
        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 343  bytes 30905 (30.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 343  bytes 30905 (30.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Mask : the network mask which decides the potential size of your network
UP : network interface is configured to be enabled.
BROADCAST : Ethernet device supports broadcasting which is a necessary characteristic to obtain IP address via DHCP.

MULTICAST : interface is configured to handle multicast packets. It allows a source to send a packet to multiple machines.
RUNNING : Indicates that the network interface is operational and is ready to accept the data.
MTU : Maximum Transmission Unit is a link layer characteristic which provides a limit on the size of the Ethernet frame. 1500 is the default value for all Ethernet devices.
METRIC : Interface metric is used to compute the cost of a route. It tells the OS which interface a packet should be forwarded to, when multiple interfaces could be used to reach the destination. Lower value means higher priority.
RX packets : the total number of packets received.
1) Errors: Number of damaged packets received.2) Dropped: Number of dropped packets due to reception errors.3) Overruns: Number of received packets that experienced data overruns.4) Frame: Number of received packets that experienced frame errors. Parameter has significance only while routing packets.
TX packets : the total number of packets transmitted.
1) Errors: Number of packets that experienced transmission error.2) Dropped: Number of dropped transmitted packets due to transmission errors.3) Overruns: Number of transmitted packets that experienced data overruns.4) Carrier: Number received packets that experienced loss of carriers. 5) collisions: 0: The value of this field should ideally be 0. If it has a value greater than zero, it could mean that the packets are colliding while traversing your network - sign of network congestion. 6) txqueuelen: 1000: This denotes the length of the transmit queue of the device.
RX/TX bytes : the total amount of data that has passed through the Ethernet interface.(ex. 1.0 MB download and 166.4 KB upload)
Netmasks (or subnet masks): are a shorthand for referring to ranges of consecutive IP addresses in the Internet Protocol. They are used for defining networking rules in e.g. routers and firewalls.

ifconfig options:
1) **-a** to Display information for all network interfaces, even if they are down.
2) **-v** for verbose mode, to display additional information for certain error conditions.
3) **Interface** Its usually a driver name followed by a unit no., e.g. enp7s0 for the first Ethernet interface.
4) **Up**-This flag causes the interface to be activated.
5) **Down**-This flag causes the driver for this interface to be shut down.
6) **metric N** Sets the interface metric, which is used by the interface to make routing decisions.
7) **add address** to add an IPv6 address to an interface.
8) **del address** to remove an IPv6 address from an interface.

(b) route:
Route command is used to view and manipulate the IP routing tables in both UNIX and Windows based systems. This shows us how the system is currently configured and the existing routes table.

```
pranav@pranav:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

Route output terminologies explanation:
Destination: address of the network that the packet is headed to.
Gateway: the gateway address Genmask: The netmask for the destination net.
Flags: U-route is up, G-use gateway, M-modified from routing daemon, C-cache entry, H-target is a host
Metric: The 'distance' to the target (usually counted in hops). It is not used by recent kernels
Ref: Number of references to this route. (Not used in the Linux kernel.)
Use: Count of lookups for the route.
Iface: Interface to which packets for this route will be sent.
Route options:
-F to operate on the kernel's **FIB** (Forwarding Information Base) routing table. This is the default.
-C to operate on the kernel's routing cache. **-v** to select verbose operations. **-n** to show numerical addresses instead of trying to determine symbolic host names. **-e** to use netstat(8)-format for displaying the routing table. **-ee** will generate a very long line with all parameters from the routing table. **del** to delete a route. **add** to add a new route. **target** the destination network or host. You can provide IP addresses in dotted decimal or host/network names. **-net** if the target is a network or **–host** if the target is a host.

Question 5:

Netstat: : This command is capable of producing information related to network connections, routing tables, interface statistics etc. netstat is multi-platform (available on windows also). It lists the network connections that currently exist between your machine and other machines, as well as sockets 'listening' for connections from other machines.
Uses of Netstat:
1) It helps the network administrators to keep an eye on the invalid or suspicious network connections.
2) It can show you which programs are active on your network right now.
3) It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.
Netstat parameters to show all the TCP connections established: Netstat -at

```
pranav@pranav:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
```

Output Explanation:
Proto: The name of the protocol (tcp, udp, raw) used by the socket which is tcp in this case.
Recv-Q: The counts of bytes not copied by the user program connected to this socket.
Send-Q: The count of bytes yet to be acknowledged by the remote host.
Foreign Address: Address and port number of the remote end of the socket.
State: The state of the socket connected in between the Local Address and Foreign Address. These states represent the three-way handshake communication system that TCP uses.
Netstat –r: Display the kernel routing table.

```
pranav@pranav:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp0s3
```

Output: *Destination*: The destination network or destination host. Default IPV4 address for my system. *Gateway*: The gateway to which the routing entry points. *Genmask*: The net mask for the destination net; 255.255.192.0 for a host destination and 0.0.0.0 for the default route. *Flags*: This signifies route is up or to a gateway or host. *MSS*: Default maximum segment size for TCP connection over route. *Windows*: Default windows size over this route. *irtt*: Initial RTT (Round Trip Time). The kernel uses this to guess about the best TCP parameter without waiting on a slow answer. *Iface*: Interface to which packets for this route will be sent.

Option to display network interface status : '*netstat –i*' : In my case there are two interfaces: lo (loopback interface),wlp2s0 (wifi card).

```
pranav@pranav:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500     2761      0      0 0          2632      0      0      0 BMRU
lo       65536      679      0      0 0           679      0      0      0 LRU
```

Loopback interface: It is a logical, virtual interface that your computer uses to communicate with itself. It is used mainly for diagnostics and troubleshooting, and to connect to servers running on the local machine. For example, if you run a web server, you have all your web documents and could examine them file by file. The loopback interface does not represent any actual hardware, but exists so applications running on your computer can always connect to servers on the same machine.

```
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 343  bytes 30905 (30.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 343  bytes 30905 (30.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Question 6:

(a) Hop counts are mentioned in the below table:

	google.com	youtube.com	facebook.com	amazon.com	flipkart.com
Hop count 1	14	14	13	30*	30*
Hop count 2	14(7 common)	14(8 common)	13(5 common)	30*	30*
Hop count 3	14(8 common)	14(7 common)	13(5 common)	30*	30*

*could not find complete path to the server

Common hops(IPs) are: [next-hop is common in all]

1) facebook.com: 172.26.101.72, 172.31.2.71, 157.240.68.136
2) google.com and youtube.com: 172.26.101.72, 72.31.2.71, 10 74.125.51.166

(b) YES, route to the same host changes at different times of the day.
This is because: destination host utilizes multiple Internet servers to handle incoming requests, so it shows different IP addresses. Also packets are sent via the route with less traffic due to presence of load balancers and use of packet switching. So it is possible that at different times there are different paths which leads to the destination in lowest time hence resulting in different no. of hops and different intermediate ip's.
(c) YES, traceroute may not find complete paths in some cases.
This is because: Sometimes we block ICMP/ping packets (due to firewall rules) for security reasons like preventing hackers from getting information about open ports and staving off denial of service attacks. When ping is blocked, the server doesn't respond at all, resulting in "request timed out" messages that prevent traceroute from ever being able to map the path to the final destination. May also occur due to interrupted Internet connection or packets might not reach the destination within fixed max hops.
(b) YES,
Failing ping might be because packet transmission is blocked or packet is discarded, while Traceroute uses an error message from a hop to find the route. Traceroute uses a trick to get the information, which is to manipulate the TTL (Time to Live), so the hop responds with an ICMP error (ICMP TTL exceeded). Also we can find the route to such hosts via traceroute by sending TCP packets instead of default packets to find the route. 'traceroute –T host-ip' will find a route to host-ip via sending TCP probes.

Question 7:

Full arp table for your machine: "arp"
arp or address resolution protocol manipulates/displays the kernel's IPv4 network neighbor cache. ARP comes into play when the sending computer on network wants to know the destination MAC address (of another computer on network). Sending host will send an ARP Request and the destination host will reply with a message ARP Reply containing it's mac address and hence an entry being added.
Table explanation:
1) Address - This column represents IP address of network connections. 2) Hwtype - This represents the hardware type of this machine. 3) Hwaddress - This represents hardware address of the machine of respective rows network connection. 4) Flag - Each complete entry in the ARP cache will be marked with the C flag. Permanent entries are marked with M and published entries have the P flag. 5) Mask - This represents Genmask. 6) Iface - This represents network interface of respective rows connection.
Add and Delete entries to ARP table:
To add entries to the ARP table we can use the command '*arp –s <ip> <mac-addr>'* which binds a particular ip with a given mac_address. Note that entries manually added have flag M. We can also add an entry just by '*pinging*' the required ip address.
To delete any entry, use command '*arp -d <ip>*'

```
pranav@pranav:~$ sudo arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   aa:5e:a4:2d:70:a8   CM                    enp0s3
pranav@pranav:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.43.1             ether   aa:5e:a4:2d:70:a8   CM                    enp0s3
pranav@pranav:~$ sudo arp -s 192.168.43.106 ff:ff:ff:ff:ff:ff
pranav@pranav:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.43.106           ether   ff:ff:ff:ff:ff:ff   CM                    enp0s3
192.168.43.1             ether   aa:5e:a4:2d:70:a8   CM                    enp0s3
pranav@pranav:~$ sudo arp -s 192.168.43.122 ff:ff:ff:ff:ff:ff
pranav@pranav:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.43.122           ether   ff:ff:ff:ff:ff:ff   CM                    enp0s3
192.168.43.106           ether   ff:ff:ff:ff:ff:ff   CM                    enp0s3
192.168.43.1             ether   aa:5e:a4:2d:70:a8   CM                    enp0s3
pranav@pranav:~$ sudo arp -d 192.168.43.122
pranav@pranav:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.43.106           ether   ff:ff:ff:ff:ff:ff   CM                    enp0s3
192.168.43.1             ether   aa:5e:a4:2d:70:a8   CM                    enp0s3
pranav@pranav:~$
```

How long do entries stay cached in ARP table:

We can use command: *cat /proc/sys/net/ipv4/neigh/default/gc_stale_time*

It is 60 seconds on my computer.

What will happen if two IP addresses map to the same Ethernet address:

Having two devices with the same MAC address on the same LAN is bad because they will confuse switches, they will both attempt to respond to the same traffic - it is a mess, devoutly to be avoided. If two devices with the same mac are connected to the router then the DHCP server will assign them only 1 IP. There may be "races" where each computer (say A,B) attempts to register itself with the router and it's mac address. Any traffic coming to machine A can get lost since packet may go to machine B because it registered itself earlier and hence the device which was registered latest in the routing table of router will be UP for receiving and transmitting packets. However, so long as those devices with the same MAC addresses are not connected to the same Ethernet or Wi-Fi network, nothing bad happens because those MAC addresses never leave the network that the NIC is immediately connected to. If the two devices are in different LANs then nothing will happen.

Be specific on how all hosts on the subnet operate: On a subnet, the machines talk to each other with their MAC addresses which uniquely identifies each Ethernet/Wi-Fi card. Machines, a priori, do not know MAC addresses; they just know IP addresses. Therefore, when machine A wants to send a packet to machine B, it sends a broadcast frame following the ARP protocol; the packet asking if anybody knows the MAC address of B. If someone responds with the information (MAC address of B) then A will be able to send its data to B.