Q1

a)

The ones labeled UP, BROADCAST, RUNNING, and MULTICAST will provide the required IP address.

(ipv4) inet 192.168.32.83

(ipv6) inet6 fe80::7eb9:c812:b6a9:f9d8

```
iiitd@iiitd-HP-406-MT:~$ ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.83  netmask 255.255.240.0  broadcast 192.168.47.255
        inet6 fe80::7eb9:c812:b6a9:f9d8  prefixlen 64  scopeid 0x20<link>
        ether ec:8e:b5:14:09:72  txqueuelen 1000  (Ethernet)
        RX packets 23161313  bytes 4004603001 (4.0 GB)
        RX errors 0  dropped 48925  overruns 0  frame 0
        TX packets 749136  bytes 105253413 (105.2 MB)
        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 40025  bytes 4452847 (4.4 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40025  bytes 4452847 (4.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

b)

103.25.231.150

They are different, because the public IP address, also known as the external IP address from your connection, is the Internet Protocol address displayed on the What Is My IP home page.

whereas an internal IP frequently begins with 10.0.0.*, 192.186.1.*, etc and are reserved by IANA, and not assigned as public or external IPs, which is the ip address shown for my local machine.

Q2

a)

```
iiitd@iiitd-HP-406-MT:~$ nslookup -type=soa www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
*** Can't find www.google.com: No answer

Authoritative answers can be found from:
google.com
        origin = ns1.google.com
        mail addr = dns-admin.google.com
        serial = 476050568
        refresh = 900
        retry = 900
        expire = 1800
        minimum = 60
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  has AAAA address 2001:4860:4802:32::a
```

I used the -type=soa option to direct nslookup to display the authoritative name server because in order to receive an authoritative response, the authoritative (primary) name server must be given at the conclusion of the request.

b)

```
iiitd@iiitd-HP-406-MT:~$ nslookup -debug -type=aaaa www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

------------
    QUESTIONS:
        www.google.com, type = AAAA, class = IN
    ANSWERS:
    ->  www.google.com
        has AAAA address 2404:6800:4002:823::2004
        ttl = 122
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
------------
Non-authoritative answer:
Name:   www.google.com
Address: 2404:6800:4002:823::2004
```

```
iiitd@iiitd-HP-406-MT:~$ dig a www.google.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> a www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9856
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         27      IN      A       142.250.194.164

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Sep 23 14:31:37 IST 2022
;; MSG SIZE  rcvd: 59
```

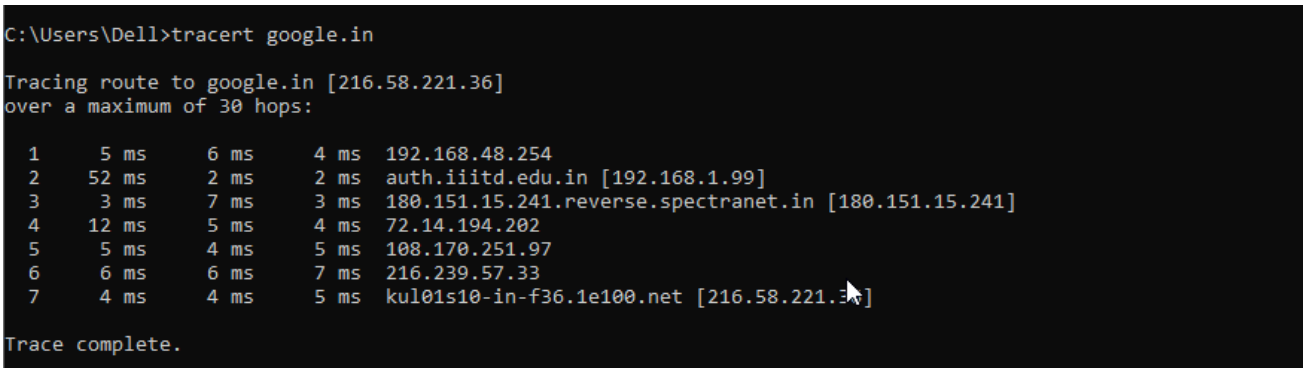
A packet's or data's time-to-live (TTL) number indicates how long it should stay on a computer or network before being deleted. A TTL value is given to each data packet. The TTL value decreases by one each time a data packet completes a hop, therefore

Using the command

dig +nocmd +noall +answer +ttl units A www.google.com

27 sec came out to be the time to live. Hence,this is the time after which ttl value will also expire.

Q3.



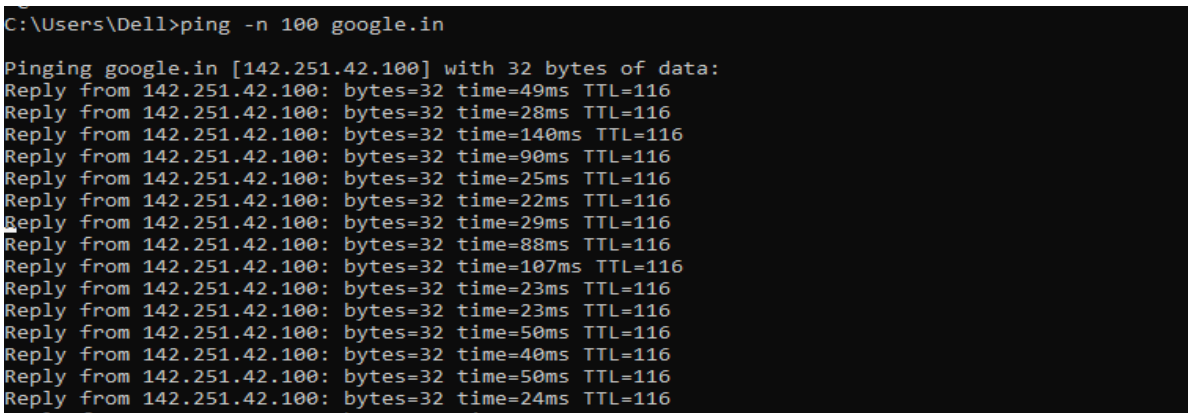
a)

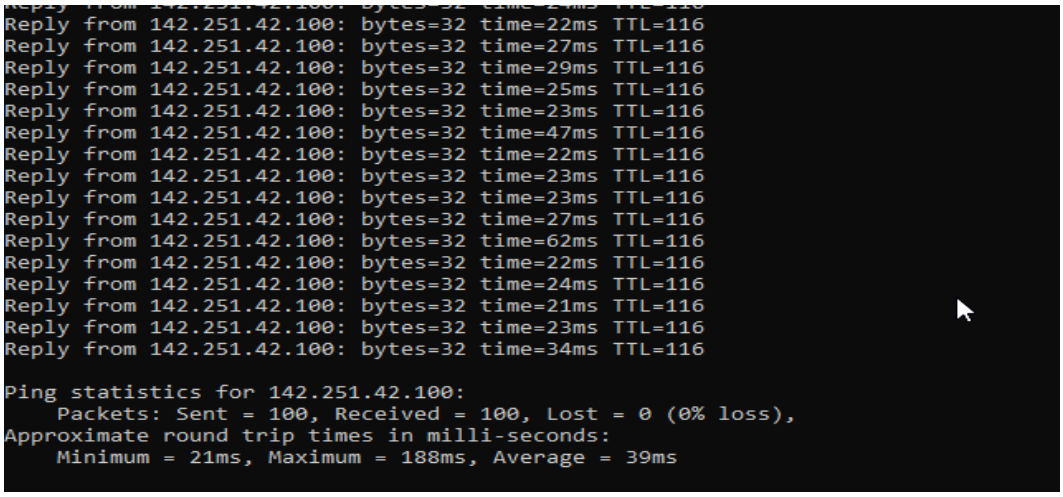
There are 6 intermediates between src and dest

Intermediate Hosts	**Average Latency**
192.168.48.254	(5+6+4)/3 = 5ms
192.168.1.99	(52+2+2)/3 =18.66 ms
180.151.15.241	(3+7+3)/3 = 4.33 ms
72.14.194.202	(12+5+4)/3 = 7 ms
108.170.251.97	(5+4+5)/3 = 4.66 ms
216.239.57.33	(6+6+7)/3 = 6.33 ms

b)

ping -n 100 google.in



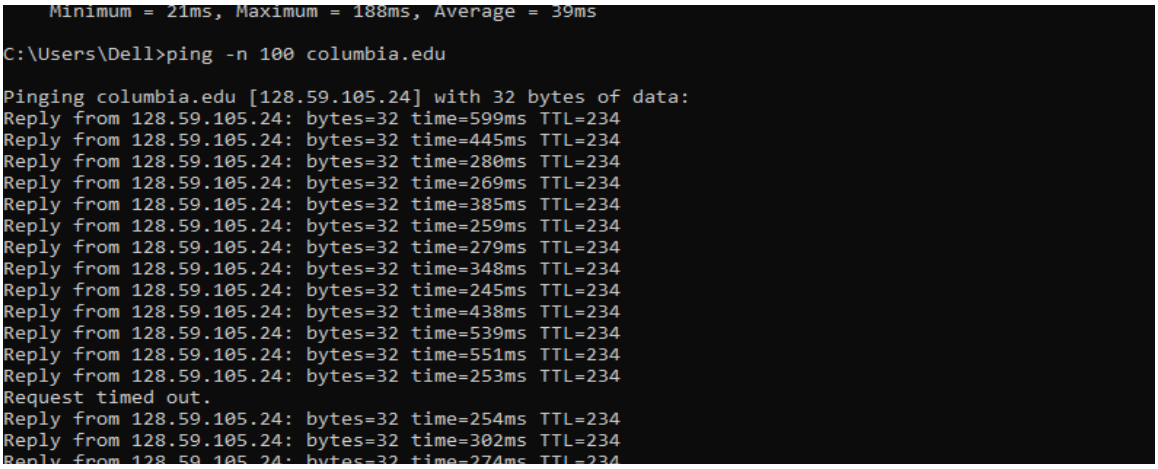


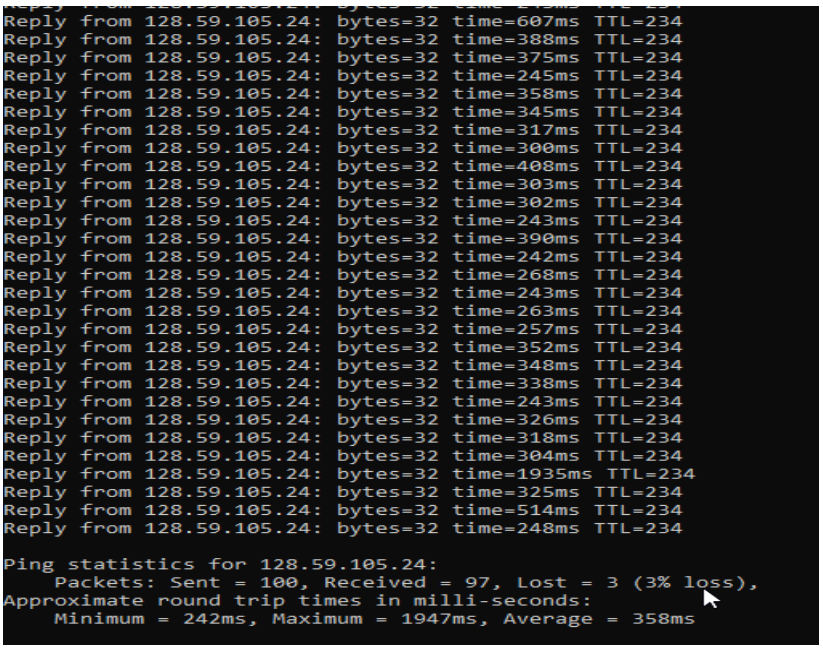
Average One Way Latency will be half of the Average Round Trip Latency.

Average latency=39/2 ms= 19.5 ms

c)

ping -n 100 columbia.edu





Average One Way latency=358/2 ms= 179 ms

d)

No,

Latency measures the entire round trip of that signal, whereas ping only measures one direction.

The Ping Latencies are more or less equal to the Average Latencies calculated in a)

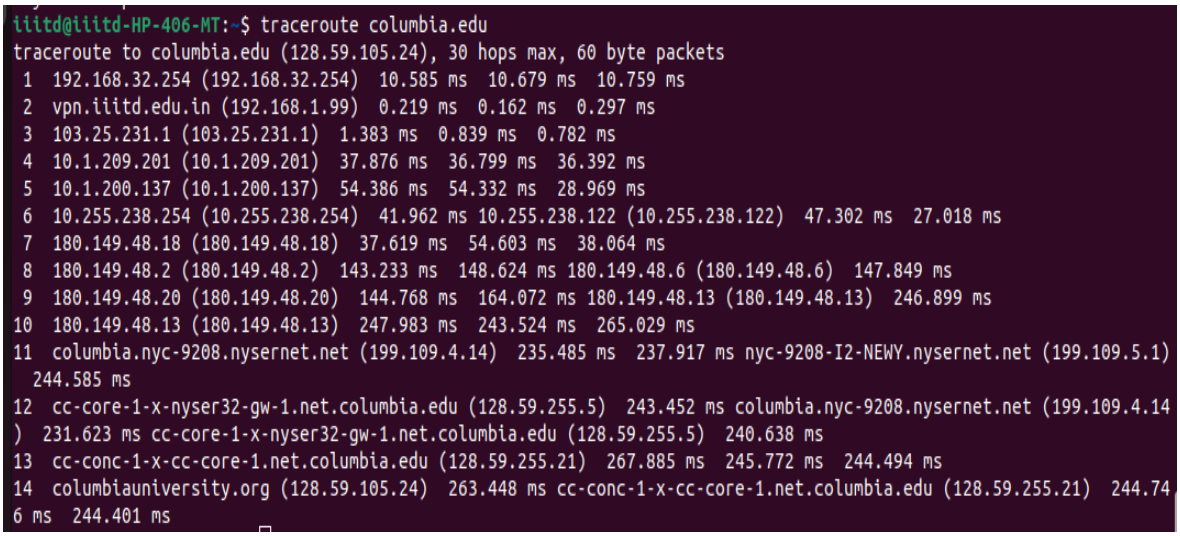
Their sum is 45.98 ms

While the average latency for google.in was 19.5 ms

There is a lot of gap between the two, this is because of the different default intervals used by the two tools. Ping uses a 1 transaction per second interval. There is a lot of overhead in calculation using traceroute, thus the average comes out to be half as much as the ping latencies sum of the intermediates.

e)Yes, 18.66 ms is maximum ping latency for intermediate host, which is close to the answer obtained in b), because the maximum latency for one particular case will be much closer in terms of computation than the overall sum of all the intermediates, which might be because of network congestion or traffic.

f)



The number of intermediate hops between source to dest for columbia.edu are 13, while they were just 6 for google.in

Latency difference between google.in and columbia.edu is because the amount of time it takes for data to move between two points on a network is known as latency.The distance between client devices making requests and the servers responding to those requests, is one of the main causes of network latency.

Columbia.edu is hosted in New York, while google.in is hosted in Delhi, India, thus there is a lot of difference in the average latency mainly due to the difference in number of hops between the source and the destination .

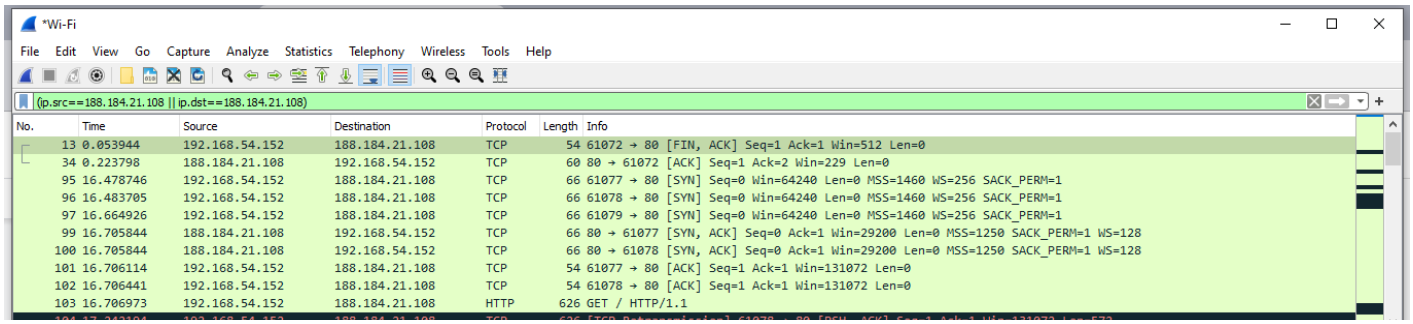
Q4)

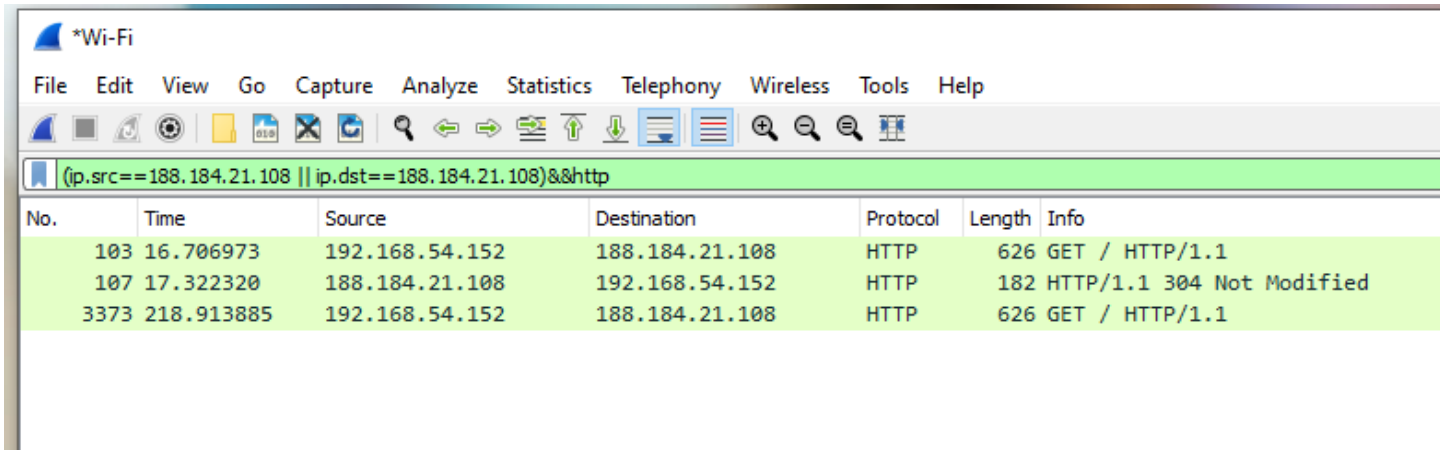
```
iiitd@iiitd-HP-406-MT:~$ sudo ifconfig lo down
[sudo] password for iiitd:
iiitd@iiitd-HP-406-MT:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
^C
--- 127.0.0.1 ping statistics ---
45 packets transmitted, 0 received, 100% packet loss, time 45044ms
```

In the worst case scenario, 100% packet loss, you might even lose access to the Internet. It can be brought on by a variety of things, particularly network congestion.
When no packet you send reaches its destination, 100% packet loss has occurred. 100% packet loss may also be a sign that the host you are attempting to connect to is offline or not connected for some other reason.
I tried the last step, which temporarily disconnected the connection.

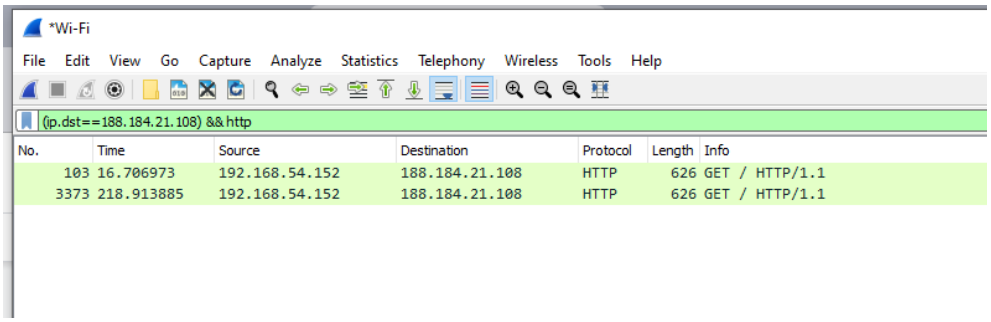
Q5)

```
C:\Users\Dell>nslookup http://info.cern.ch
Server:  ns3.iiitd.edu.in
Address:  192.168.1.8
```





HTTP request packets

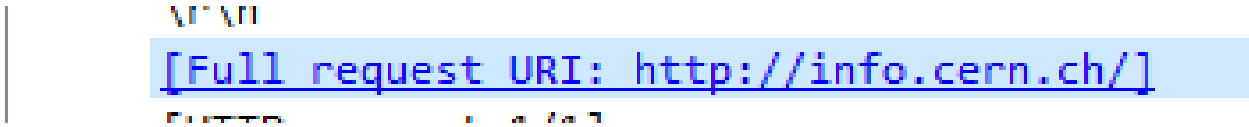


○ HTTP request type- GET

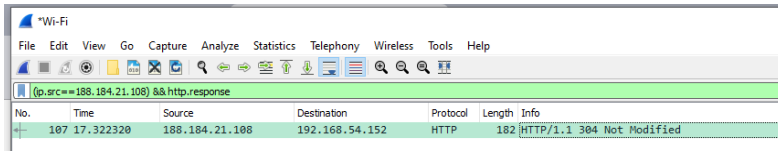
○ User agent type

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36

○ HTTP request packet's URI



b)



HTTP response code: 304

○ HTTP response description - Not Modified

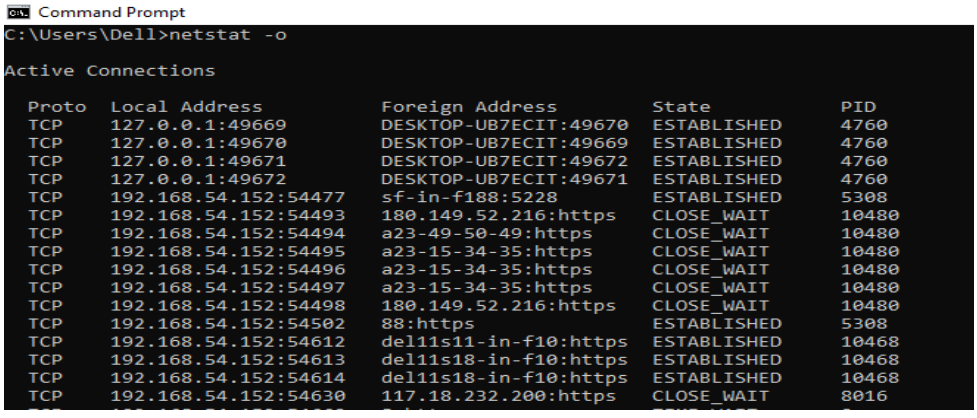
○ Name and version of the web server- Apache HTTP server, HTTP/1.1

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	31				0.0001	100%	0.0100	9.656
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	0				0.0000	0.00%	-	-
???: broken	0				0.0000		-	-
5xx: Server Error	0				0.0000		-	-
4xx: Client Error	0				0.0000		-	-
3xx: Redirection	0				0.0000		-	-
2xx: Success	0				0.0000		-	-
1xx: Informational	0				0.0000		-	-
HTTP Request Packets	31				0.0001	100.00%	0.0100	9.656
SEARCH	20				0.0001	64.52%	0.0100	46.901
GET	11				0.0000	35.48%	0.0100	9.656

Persistent due to the fact that only one TCP connection was used for sending and receiving multiple HTTP requests and responses as opposed to creating separate connections for each request and response pair.

Q6

a) netstat -o



b) Netstat -no -p TCP 188.184.21.108

```
C:\Users\Dell>netstat -no -p TCP 188.184.21.108

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:49669        127.0.0.1:49670        ESTABLISHED     4760
  TCP    127.0.0.1:49670        127.0.0.1:49669        ESTABLISHED     4760
  TCP    127.0.0.1:49671        127.0.0.1:49672        ESTABLISHED     4760
  TCP    127.0.0.1:49672        127.0.0.1:49671        ESTABLISHED     4760
  TCP    192.168.54.152:54477   74.125.24.188:5228     ESTABLISHED     5308
  TCP    192.168.54.152:54494   23.49.50.49:443        CLOSE_WAIT      10480
  TCP    192.168.54.152:54502   35.227.248.88:443      ESTABLISHED     5308
  TCP    192.168.54.152:54630   117.18.232.200:443     CLOSE_WAIT      8016
  TCP    192.168.54.152:54881   180.149.52.216:443     CLOSE_WAIT      10480
  TCP    192.168.54.152:54883   180.149.52.216:443     CLOSE_WAIT      10480
  TCP    192.168.54.152:54884   180.149.52.216:443     CLOSE_WAIT      10480
  TCP    192.168.54.152:54885   23.15.34.35:443        CLOSE_WAIT      10480
  TCP    192.168.54.152:54934   35.241.9.51:443        TIME_WAIT       0
  TCP    192.168.54.152:54936   34.107.254.252:443     TIME_WAIT       0
  TCP    192.168.54.152:54958   199.232.254.114:443    ESTABLISHED     5308
  TCP    192.168.54.152:54973   34.107.148.139:443     TIME_WAIT       0
  TCP    192.168.54.152:54984   34.120.155.137:443     TIME_WAIT       0
  TCP    192.168.54.152:54991   34.98.64.218:443       TIME_WAIT       0
  TCP    192.168.54.152:55016   35.227.252.103:443     TIME_WAIT       0
  TCP    192.168.54.152:60112   142.250.182.170:443    ESTABLISHED     10468
  TCP    192.168.54.152:60116   20.198.118.190:443     ESTABLISHED     4664
  TCP    192.168.54.152:60124   5.9.70.141:443         ESTABLISHED     4288
  TCP    192.168.54.152:60187   34.95.81.168:443       TIME_WAIT       0
  TCP    192.168.54.152:60195   34.102.163.6:443       TIME_WAIT       0
  TCP    192.168.54.152:60274   35.227.202.26:443      TIME_WAIT       0
  TCP    192.168.54.152:60276   185.184.8.90:443       ESTABLISHED     5308
  TCP    192.168.54.152:60352   130.211.23.194:443     TIME_WAIT       0
  TCP    192.168.54.152:60382   35.208.249.213:443     TIME_WAIT       0
  TCP    192.168.54.152:60390   35.190.80.1:443        TIME_WAIT       0
  TCP    192.168.54.152:60417   142.250.192.229:443    ESTABLISHED     5308
```