

CSE-232: COMPUTER NETWORKS

ASSIGNMENT 1

-Ritika Nagar

Q1):

```
ritika@ritika-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.147.128 netmask 255.255.255.0 broadcast 192.168.147.255
    inet6 fe80::17a2:9235:2add:6819 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:36:d2:ae txqueuelen 1000 (Ethernet)
    RX packets 402873 bytes 598175358 (598.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24097 bytes 3067128 (3.0 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 1135 bytes 324560 (324.5 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1135 bytes 324560 (324.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IP address shown on WhatIsMyIP is a public IP address, which can also be called an external IP address. Moreover, an internal IP address starts with 192.168.1.*, 172.16.*.*, or 10.0.0.*. These IPv4 internal blocks are reserved via (IANA) and not assigned as public or external IPs.

Q2):

```
C:\Users\ritik>nslookup -type=soa www.google.com
Server:  ns3.iiitd.edu.in
Address: 192.168.1.8

google.com
    primary name server = ns1.google.com
    responsible mail addr = dns-admin.google.com
    serial   = 475109091
    refresh  = 900 (15 mins)
    retry    = 900 (15 mins)
    expire   = 1800 (30 mins)
    default TTL = 60 (1 min)
ns1.google.com internet address = 216.239.32.10
ns1.google.com AAAA IPv6 address = 2001:4860:4802:32::a
```

- a) Typically, most of the responses to our nslookup queries are non-authoritative, which means they are from a cached copy from a third party and not from the primary DNS server holding the master copy. To get an authoritative answer, we need to specify the authoritative name server as part of the request. To do this include the -type=soa switch and nslookup will respond back with the name of the authoritative name server.

```
ritika@ritika-virtual-machine:~$ dig A www.google.com

; <<>> DiG 9.16.1-Ubuntu <<>> A www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32139
;; 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.                5        IN      A      142.250.207.228

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Sep 19 10:30:17 IST 2022
;; MSG SIZE rcvd: 59
```

- b) This entry would expire in 5s since TTL is a value that implies how long the data should be kept before discarding by DNS.

Q3):

a)

```
C:\Users\ritik>tracert google.in

Tracing route to google.in [142.250.193.68]
over a maximum of 30 hops:

  0  2 ms    2 ms    1 ms  MYGROUP [192.168.1.1]
  1  3 ms    3 ms    3 ms  103.212.157.12
  2  6 ms    *       10 ms  103.212.157.1
  3  *       *       *      Request timed out.
  4  5 ms    5 ms    4 ms  142.250.160.212
  5  7 ms    7 ms    8 ms  142.251.78.139
  6  5 ms    6 ms    6 ms  142.251.54.85
  7  6 ms    7 ms    9 ms  del11s16-in-f4.1e100.net [142.250.193.68]

Trace complete.
```

There are 8 intermediate hosts in total.

Their average latencies are

Table 1

IP Address	Average Latency	Ping Latency
103.212.157.12	3ms	4ms
142.250.160.212	4.66ms	6ms
142.251.78.139	7.33ms	7ms
142.251.54.85	5.66ms	6ms
142.250.193.68	7.33ms	7ms

b)

```
ritika@ritika-virtual-machine:~$ ping -c 100 google.in
PING google.in (142.250.194.228) 56(84) bytes of data.
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=1 ttl=128 time=9.67 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=2 ttl=128 time=7.32 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=3 ttl=128 time=8.08 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=4 ttl=128 time=7.71 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=5 ttl=128 time=6.64 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=6 ttl=128 time=7.03 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=7 ttl=128 time=8.07 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=8 ttl=128 time=6.35 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=9 ttl=128 time=7.03 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=10 ttl=128 time=12.1 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=11 ttl=128 time=9.12 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=12 ttl=128 time=7.33 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=13 ttl=128 time=7.30 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=14 ttl=128 time=6.70 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=15 ttl=128 time=6.97 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=16 ttl=128 time=6.44 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=17 ttl=128 time=8.00 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=18 ttl=128 time=8.27 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=19 ttl=128 time=7.55 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=20 ttl=128 time=6.01 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=21 ttl=128 time=7.01 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=22 ttl=128 time=5.67 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=23 ttl=128 time=8.18 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=24 ttl=128 time=10.8 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=25 ttl=128 time=6.95 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=26 ttl=128 time=6.68 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=27 ttl=128 time=6.91 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=28 ttl=128 time=6.29 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=29 ttl=128 time=7.20 ms
64 bytes from del12s08-in-f4.1e100.net (142.250.194.228): icmp_seq=30 ttl=128 time=8.26 ms
```

Average Latency: 7.369 ms

c)

```
ritika@ritika-virtual-machine:~$ ping -c 100 columbia.edu
PING columbia.edu (128.59.105.24) 56(84) bytes of data.
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=1 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=2 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=3 ttl=128 time=246 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=4 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=5 ttl=128 time=247 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=6 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=7 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=8 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=9 ttl=128 time=246 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=10 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=11 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=12 ttl=128 time=249 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=13 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=14 ttl=128 time=243 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=15 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=16 ttl=128 time=246 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=17 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=18 ttl=128 time=247 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=19 ttl=128 time=253 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=20 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=21 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=22 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=23 ttl=128 time=244 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=24 ttl=128 time=245 ms
64 bytes from www-ltm.cc.columbia.edu (128.59.105.24): icmp_seq=25 ttl=128 time=245 ms
```

Average Latency: 254.180 ms

d) From table 1 on page4: Adding up the ping latencies of all intermediate hosts is 30ms which is not equal to the average latency which is 7.39 ms. This can be concluded by the fact that ping gives a direct path from source to destination. ping is essentially point-to-point traffic. Whereas, tracert is the time taken for a packet to get to each point in its route from point to point.

e) Maximum ping latency amongst the intermediate hosts is 7 ms which is somehow equal to the average latency. Here also we have the same reasons from the above point. These both are not exactly equal because we can take into account network congestion and noises in the case of tracert command.

f)

```
C:\Users\ritik>tracert columbia.edu

Tracing route to columbia.edu [128.59.105.24]
over a maximum of 30 hops:

  1    2 ms    2 ms    1 ms  MYGROUP [192.168.1.1]
  2   11 ms    3 ms    4 ms  103.212.157.12
  3    *      *      *      Request timed out.
  4    5 ms    6 ms    7 ms  115.113.240.105.static-delhi.vsnl.net.in [115.113.240.105]
  5   28 ms   27 ms   29 ms  172.23.183.134
  6   30 ms   27 ms   27 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7    *    150 ms    *    if-be-6-2.ecore1.emrs2-marseille.as6453.net [195.219.174.16]
  8    *      *      *      Request timed out.
  9   150 ms  147 ms  160 ms  if-ae-55-4.tcore1.pvu-paris.as6453.net [80.231.153.168]
 10   149 ms  149 ms  149 ms  be6453.agr21.par04.atlas.cogentco.com [130.117.15.69]
 11   151 ms  150 ms  147 ms  be2151.ccr32.par04.atlas.cogentco.com [154.54.61.33]
 12   144 ms  145 ms  145 ms  be2103.ccr42.par01.atlas.cogentco.com [154.54.61.21]
 13   249 ms  256 ms  244 ms  be3628.ccr42.jfk02.atlas.cogentco.com [154.54.27.169]
 14   247 ms  244 ms  243 ms  be2897.rcr24.jfk01.atlas.cogentco.com [154.54.84.214]
 15   244 ms  282 ms  241 ms  38.122.8.210
 16   242 ms  243 ms  243 ms  cc-core-1-x-nyser32-gw-1.net.columbia.edu [128.59.255.5]
 17   244 ms  244 ms  243 ms  cc-conc-1-x-cc-core-1.net.columbia.edu [128.59.255.21]
 18   249 ms  246 ms  242 ms  neurotheory.columbia.edu [128.59.105.24]
```

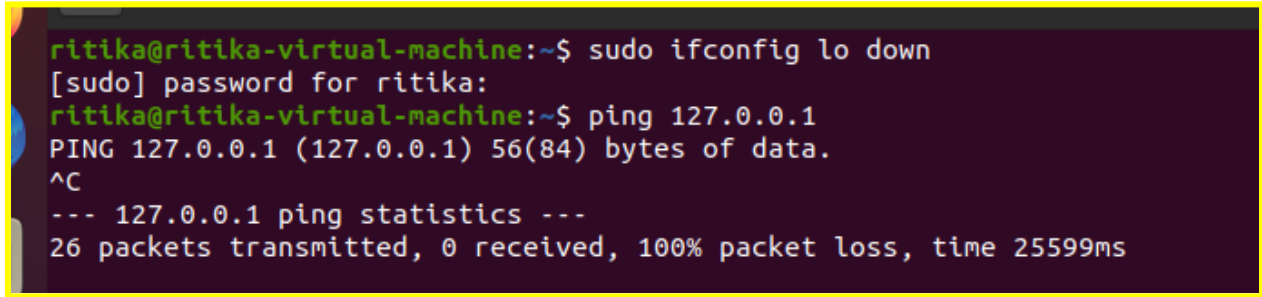
Number of hops in google.in: 8

Number of hops in columbia.edu: 18

Every domain name on the internet contains a top-level domain label, known as a TLD. (.in) is TLD which belongs to India and (.edu) is TLD which is associated with an American institution.

We know our latency depends upon the distance; in the case of columbia.edu there are more hops that data need to make to reach its destination. Every hop introduces extra latency. The greater the distance, the greater latency.

Q4)

A terminal window with a dark purple background and yellow border. It shows a user named 'ritika' at a 'ritika-virtual-machine' prompt. The user runs 'sudo ifconfig lo down', followed by a password prompt. Then they run 'ping 127.0.0.1', which shows a single successful ping. After pressing Ctrl-C, it displays ping statistics for 127.0.0.1, showing 26 packets transmitted, 0 received, and 100% packet loss.

```
ritika@ritika-virtual-machine:~$ sudo ifconfig lo down
[sudo] password for ritika:
ritika@ritika-virtual-machine:~$ 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 ---
26 packets transmitted, 0 received, 100% packet loss, time 25599ms
```

We can make the ping command fail, by making out interface down using the command [ifconfig lo down](#). If a system's only network interface is down, we will not be able to access it except on the console. The ping command will report 100% lost packers and all other network commands will fail. Because of this, the ping command will not be able to send requests over the network to a specific device.

Q5):

- For HTTP request packets

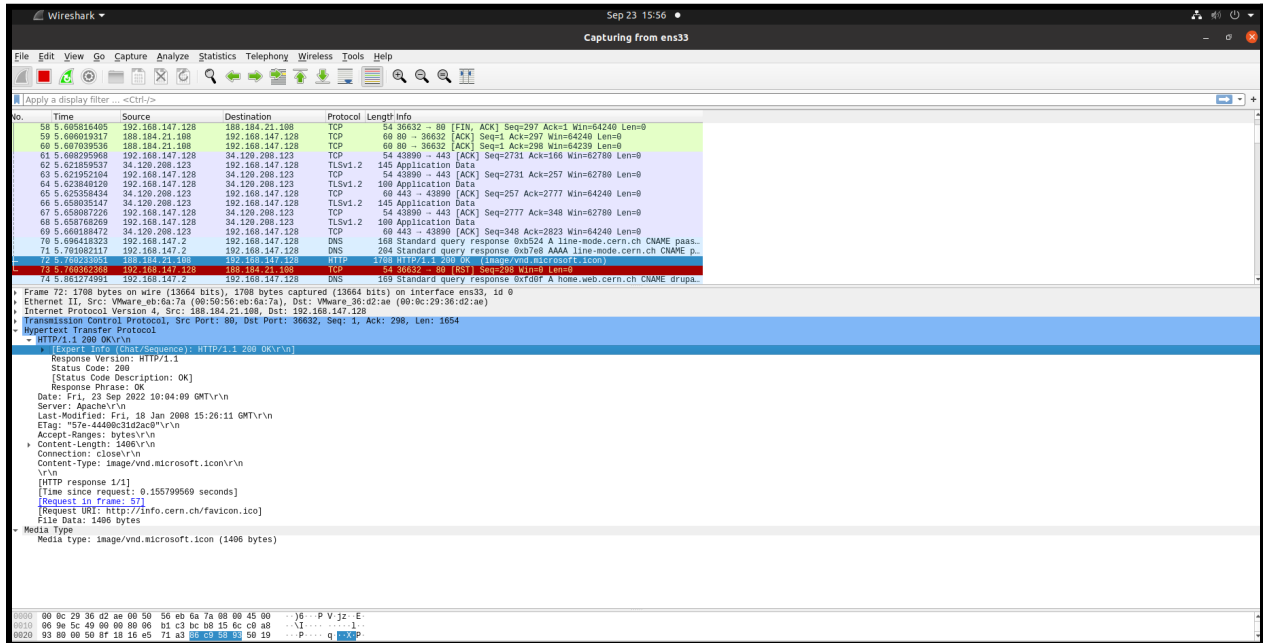
The image shows a Wireshark packet capture of an HTTP GET request. The packet list on the left shows a sequence of packets, with packet 58 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request for 'http://info.cern.ch/favicon.ico'. The packet bytes pane at the bottom shows the raw data of the packet, including the Ethernet II header, Internet Protocol Version 4 header, Transmission Control Protocol header, and the Hypertext Transfer Protocol (HTTP) request.

No.	Time	Source	Destination	Protocol	Length	Info
52	5.537251574	192.168.147.128	192.168.147.2	DNS	87	Standard query 0x80f3 AAAA home.web.cern.ch OPT
53	5.564379516	34.129.208.123	192.168.147.128	TLsv1.2	145	Application Data
54	5.565599893	192.168.147.128	34.129.208.123	TLsv1.2	100	Application Data
55	5.565732065	34.129.208.123	192.168.147.128	TLsv1.2	128	Application Data
56	5.566190391	34.129.208.123	192.168.147.128	TCP	60	443 → 43890 [ACK] Seq=166 Ack=2731 Win=64240 Len=0
58	5.605816405	192.168.147.128	188.184.21.108	TCP	54	36632 → 80 [FIN, ACK] Seq=297 Ack=1 Win=64240 Len=0
59	5.606019317	188.184.21.108	192.168.147.128	TCP	60	80 → 36632 [ACK] Seq=1 Ack=297 Win=64240 Len=0
60	5.607039536	188.184.21.108	192.168.147.128	TCP	60	80 → 36632 [ACK] Seq=1 Ack=298 Win=64239 Len=0
61	5.608295968	192.168.147.128	34.129.208.123	TCP	54	43890 → 443 [ACK] Seq=2731 Ack=166 Win=62780 Len=0
62	5.621859537	34.129.208.123	192.168.147.128	TLsv1.2	145	Application Data
63	5.621952104	192.168.147.128	34.129.208.123	TCP	54	43890 → 443 [ACK] Seq=2731 Ack=257 Win=62780 Len=0
64	5.623840120	192.168.147.128	34.129.208.123	TLsv1.2	100	Application Data
65	5.623558434	34.129.208.123	192.168.147.128	TCP	60	443 → 43890 [ACK] Seq=257 Ack=2777 Win=64240 Len=0
66	5.658083547	34.129.208.123	192.168.147.128	TLsv1.2	145	Application Data
67	5.658087226	192.168.147.128	34.129.208.123	TCP	54	43890 → 443 [ACK] Seq=2777 Ack=348 Win=62780 Len=0
68	5.658768269	192.168.147.128	34.129.208.123	TLsv1.2	100	Application Data

Frame 57: 350 bytes on wire (2800 bits), 350 bytes captured (2800 bits) on interface ens33, id 0
Ethernet II, Src: VMware_38:02:ae (08:0c:29:36:d2:ae), Dst: VMware_eb:6a:7a (08:50:56:eb:6a:7a)
Internet Protocol Version 4, Src: 192.168.147.128, Dst: 188.184.21.108
Transmission Control Protocol, Src Port: 36632, Dst Port: 80, Seq: 1, Ack: 1, Len: 296
Hypertext Transfer Protocol
GET /favicon.ico HTTP/1.1
[Expert Info (Chat/Sequence): GET /favicon.ico HTTP/1.1
[Severity Level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /favicon.ico
Request Version: HTTP/1.1
Host: info.cern.ch
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://info.cern.ch/
[Full request URI: http://info.cern.ch/favicon.ico]
[HTTP request 1/1]
[Response in frame 72]
0000 00 50 56 eb 6a 7a 08 0c 29 36 d2 ae 08 00 45 00 PV jz }8...E
0010 01 50 71 8d 40 90 40 06 a1 cd c0 a8 93 80 bc b8 Pq 0 0
0020 15 6c 8f 18 00 50 86 c9 57 6a 16 e5 71 a3 50 18 1...P Wj q P
0030 7a f0 27 00 00 00 47 45 54 20 2f 66 61 76 69 63 GE T /favico
0040 6f 6e 2e 69 63 8f 20 48 54 54 50 2f 31 2e 31 8d on.ico H TTP/1.1
0050 0a 48 6f 73 74 3a 20 69 6e 66 0f 2e 63 65 72 6e Host: i nfo.cern
0060 2e 63 68 0d 6a 55 73 65 72 2d 41 67 65 6e 74 3a .ch Use r-Agent:
0070 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 Mozilla /5.0 (X1
0080 31 3b 20 55 62 75 6e 74 75 3b 29 4c 69 6e 75 78 1; Ubuntu; Linux
0090 20 78 38 36 6f 76 34 2b 20 72 76 5a 31 30 34 2e x86_64; rv:104.
00a0 30 29 20 47 05 83 0b 0f 2f 32 30 31 30 30 31 30 0) Gecko /2010010
00b0 31 20 46 69 72 65 66 6f 78 2f 31 30 34 2e 30 8d 1 Firefo x/104.0

- HTTP Request Type: Get
- User-agent Type: Mozilla Firefox
- HTTP request packet's URL: http://info.cern.ch/favicon.ico

- For HTTP response packets



- HTTP response code: 200
- HTTP response description: OK
- Name and version of the web server: Apache\r\n\r\n

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
▼ Total HTTP Packets	51				0.0001	100%	0.0300	50.989
Other HTTP Packets	0				0.0000	0.00%	-	-
▼ HTTP Response Packets	9				0.0000	17.65%	0.0200	51.041
??? : broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
▼ 2xx: Success	9				0.0000	100.00%	0.0200	51.041
204 No Content	6				0.0000	66.67%	0.0100	138.998
200 OK	3				0.0000	33.33%	0.0200	51.041
1xx: Informational	0				0.0000	0.00%	-	-
▼ HTTP Request Packets	42				0.0001	82.35%	0.0200	50.989
SEARCH	32				0.0001	76.19%	0.0100	43.127
GET	10				0.0000	23.81%	0.0200	50.989

There have 3 web objects downloaded over the same TCP connection. Therefore this is a persistent HTTP connection. Also, we can verify this, since HTTP/1.1 connections are persistent.

Q6):

a) netstat -no -p TCP

b) State for all TCP connection(s) is LISTEN.

```
ritika@ritika-virtual-machine:~$ netstat -at info.cern.ch
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:domain       0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
```