

CSE 232: Assignment 1

Due date: September 23, 2022

Read the following instructions carefully

- For all the observations and explanations create a single report.
- Attach screenshots in the report.
- Naming Convention: <Roll_No>-Assignment1.zip

Q1. [1+2]

- a) Learn to use the ifconfig command, and figure out the IP address of your network interface. Put a screenshot.



```
ritvikpendyala - zsh - 81x52
ether 76:8f:3c:c4:41:fb
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=6463<RXCSUM, TXCSUM, TSO4, TSO6, CHANNEL_IO, PARTIAL_CSUM, ZEROINVERT_C
SUM>
ether 74:8f:3c:c4:41:fb
inet6 fe80::c26:222c:2ee7:419c%en0 prefixlen 64 secured scopeid 0xb
inet 192.168.53.69 netmask 0xfffff000 broadcast 192.168.63.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
awd10: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether ea:b0:ce:ca:75:a6
inet6 fe80::e8b0:ceff:feca:75a6%awd10 prefixlen 64 scopeid 0xc
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether ea:b0:ce:ca:75:a6
inet6 fe80::e8b0:ceff:feca:75a6%llw0 prefixlen 64 scopeid 0xd
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=63<RXCSUM, TXCSUM, TSO4, TSO6>
ether 36:1b:4f:f5:a5:00
Configuration:
id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
ipfilter disabled flags 0x0
member: en1 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 8 priority 0 path cost 0
member: en2 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 9 priority 0 path cost 0
nd6 options=201<PERFORMNUD,DAD>
media: <unknown type>
status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1300
inet6 fe80::4c2a:d9a2:d204:97d2%utun0 prefixlen 64 scopeid 0xf
nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
inet6 fe80::5f18:977d:6c3e:3f91%utun1 prefixlen 64 scopeid 0x10
nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
inet6 fe80::ca01:b1c:bd2c:69%utun2 prefixlen 64 scopeid 0x11
nd6 options=201<PERFORMNUD,DAD>
ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

- b) Go to the webpage <https://www.whatismyip.com> and find out what IP is shown for your machine. Are they identical or different? Why?

What Is My IP?

My Public IPv4 is: 180.151.15.242 

My Public IPv6 is: Not Detected

My IP Location is: Ludhiana, PB IN

My ISP is: Shyam Spectra Pvt Ltd

My IP Information

Hide My IP Address

Answer : (a) My device IP address after typing in the command "ifconfig": 192.168.53.69

(b) On the website, my network IP address is: 180.151.15.242

Different, The reason the two of them are different is that the network on which we are assigned public IPs to our devices which are visible to everyone but the device IP is something that is kept private, and only the router would know it as the device IP is used as a medium which the router identifies the device and the router assigns a dynamic IP address to the device is what is our public IP address. Essentially the IP address that the website detects is the proxy server's IP address which the ISP provides you with.

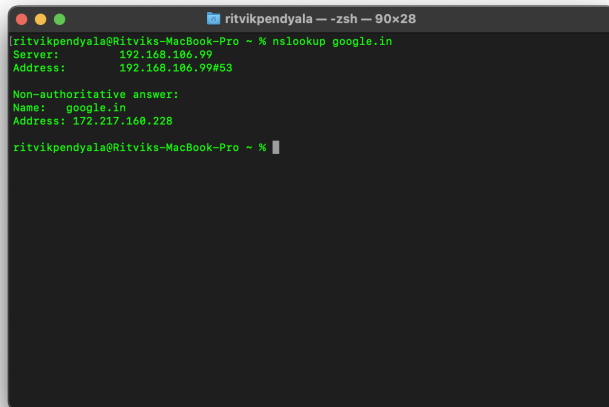
Q2. nslookup [[2+1] + [2 +1]]

a) Get an authoritative result in nslookup. Put a screenshot. Explain how you did it.

Answer: Nslookup is essentially a tool that allows you to find the IP address or the DNS record of any website. When we just use the command of nslookup and a website's name, we have the non-authoritative answer being given on the terminal. To get the authoritative answer we need to add in -type=soa(Search of Authority) in between nslookup and the websites name and this would give us the actual IP address of the website and the information would be exact and not cached info as in

non authoritative answer. On adding the command “-type=soa” we get the option of getting an authoritative answer which would contain the actual IP Address of the website we’re looking for! Here as we can see from the screenshots provided the non authoritative answer is quite different from the authoritative one which would be the actual endpoint IP.

Eg: Below PFA the non authoritative answer from the nslookup command

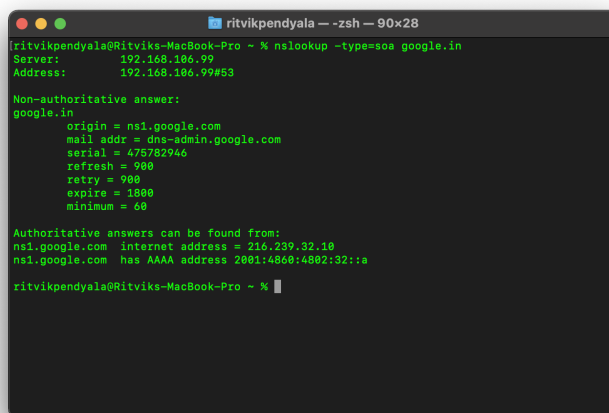


```
ritvikpendyala -- zsh -- 90x28
[ritvikpendyala@Ritviks-MacBook-Pro ~ % nslookup google.in
Server:      192.168.186.99
Address:     192.168.186.99#53

Non-authoritative answer:
Name:   google.in
Address: 172.217.160.228

ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

Find below the authoritative answer options for google.in



```
ritvikpendyala -- zsh -- 90x28
[ritvikpendyala@Ritviks-MacBook-Pro ~ % nslookup -type=soa google.in
Server:      192.168.186.99
Address:     192.168.186.99#53

Non-authoritative answer:
google.in
  origin = nsl.google.com
  mail addr = dns-admin.google.com
  serial = 470702946
  refresh = 900
  retry = 900
  expire = 1800
  minimum = 60

Authoritative answers can be found from:
nsl.google.com internet address = 216.239.32.10
nsl.google.com has AAAA address 2001:4860:4802:32::a

ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

Looking into any of the 2 options given for the authoritative answer we can use one to find the endpoint IP address of google.in which we can see from the below ss.

```
ritvikpendyala — zsh — 90x28
ritvikpendyala@Ritviks-MacBook-Pro ~ % nslookup google.in ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

Name:   google.in
Address: 142.250.194.164

ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

b) Find out time to live for any website on the local dns. Put a screenshot. Explain in words (with unit) that after how much time this entry would expire.

Answer: TTL is the amount of time the packet would exist in the network before being discarded that is in this case it would be the system you're using as we're checking the local dns which is the localhost. So we're finding the amount of time the packet (from google.in) would exist inside your localhost. Using the command "nslookup -debug google.in" we can find the TTL of the packets coming from google.in. TTL = 92 which means after 92 seconds the packet would be discarded. Unit of TTL is seconds.

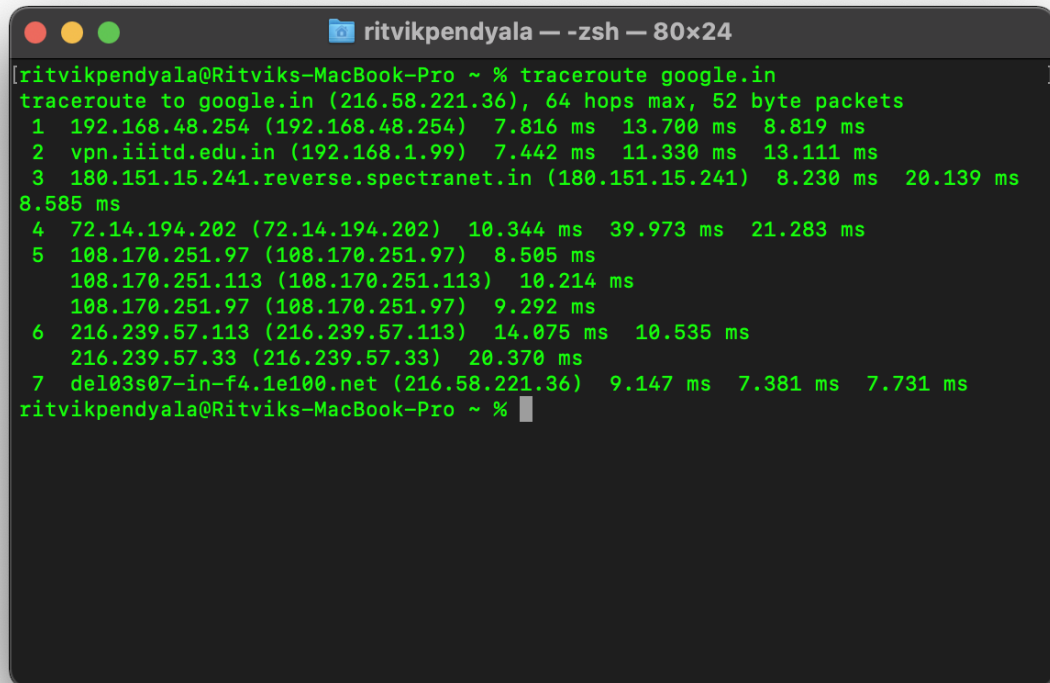
```
ritvikpendyala — zsh — 80x24
Last login: Fri Sep 23 01:53:18 on ttys004
ritvikpendyala@Ritviks-MacBook-Pro ~ % nslookup -debug google.in
Server:      192.168.1.8
Address:     192.168.1.8#53

-----
QUESTIONS:
  google.in, type = A, class = IN
ANSWERS:
-> google.in
  internet address = 172.217.160.228
  ttl = 92
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer:
Name:   google.in
Address: 172.217.160.228

ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

Q3. Run the command, `traceroute google.in`

- a) How many intermediate hosts do you see, what are the IP addresses, compute the average latency to each intermediate host. Put a screenshot. [2+2]



```
ritvikpendyala@Ritviks-MacBook-Pro ~ % traceroute google.in
traceroute to google.in (216.58.221.36), 64 hops max, 52 byte packets
 1 192.168.48.254 (192.168.48.254) 7.816 ms 13.700 ms 8.819 ms
 2 vpn.iiitd.edu.in (192.168.1.99) 7.442 ms 11.330 ms 13.111 ms
 3 180.151.15.241.reverse.spectranet.in (180.151.15.241) 8.230 ms 20.139 ms
 8.585 ms
 4 72.14.194.202 (72.14.194.202) 10.344 ms 39.973 ms 21.283 ms
 5 108.170.251.97 (108.170.251.97) 8.505 ms
 108.170.251.113 (108.170.251.113) 10.214 ms
 108.170.251.97 (108.170.251.97) 9.292 ms
 6 216.239.57.113 (216.239.57.113) 14.075 ms 10.535 ms
 216.239.57.33 (216.239.57.33) 20.370 ms
 7 del03s07-in-f4.1e100.net (216.58.221.36) 9.147 ms 7.381 ms 7.731 ms
ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

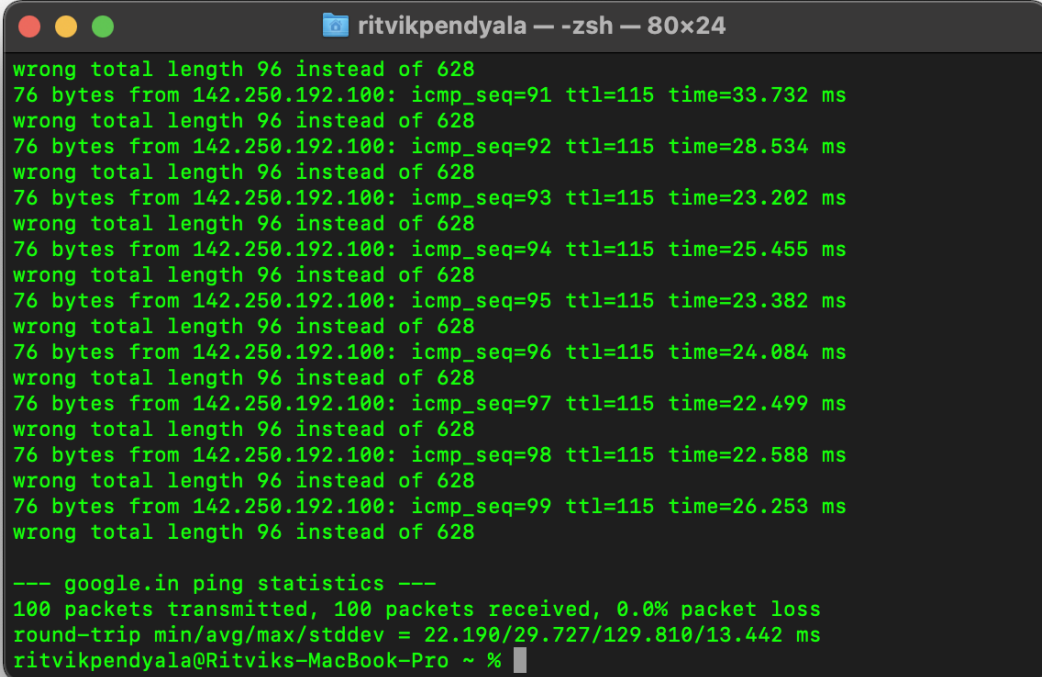
1 192.168.48.254 (192.168.48.254) 7.816 ms 13.700 ms 8.819 ms = **10.11166666667ms**
2 vpn.iiitd.edu.in (192.168.1.99) 7.442 ms 11.330 ms 13.111 ms = **10.62766666667ms**
3 180.151.15.241.reverse.spectranet.in (180.151.15.241) 8.230 ms 20.139 ms 8.585 ms = **12.378ms**
4 72.14.194.202 (72.14.194.202) 10.344 ms 39.973 ms 21.283 ms = **23.866666667ms**
5 108.170.251.97 (108.170.251.97) 8.505 ms
108.170.251.113 (108.170.251.113) 10.214 ms
108.170.251.97 (108.170.251.97) 9.292 ms = **9.337ms**
6 216.239.57.113 (216.239.57.113) 14.075 ms 10.535 ms
216.239.57.33 (216.239.57.33) 20.370 ms = **14.9933333ms**
7 del03s07-in-f4.1e100.net (216.58.221.36) 9.147 ms 7.381 ms 7.731 ms = **8.08633333ms**

As you can see from the above there are 7 intermediate hosts. The average latency is calculated right next to them, that is the average of the 3 RTTS by default.

Note that some of the intermediate hosts might not be visible, their IP addresses will come as “**”, ignore those hosts for this assignment.**

b) Send 100 ping messages to [google.in](https://www.google.in), Determine the average latency. Put a screenshot.[2]

Command used: ping -s 600 -c 100 google.in

A screenshot of a terminal window titled "ritvikpendyala — -zsh — 80x24". The terminal displays the output of a ping command to google.in. It shows 100 individual ping results, each consisting of a line indicating a failure ("wrong total length 96 instead of 628") and a line showing the received data ("76 bytes from 142.250.192.100: icmp_seq=91 ttl=115 time=33.732 ms"). The sequence numbers range from 91 to 99. At the bottom, a summary line reads: "--- google.in ping statistics --- 100 packets transmitted, 100 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 22.190/29.727/129.810/13.442 ms". The prompt "ritvikpendyala@Ritviks-MacBook-Pro ~ %" is visible at the end of the line.

```
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=91 ttl=115 time=33.732 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=92 ttl=115 time=28.534 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=93 ttl=115 time=23.202 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=94 ttl=115 time=25.455 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=95 ttl=115 time=23.382 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=96 ttl=115 time=24.084 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=97 ttl=115 time=22.499 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=98 ttl=115 time=22.588 ms
wrong total length 96 instead of 628
76 bytes from 142.250.192.100: icmp_seq=99 ttl=115 time=26.253 ms
wrong total length 96 instead of 628

--- google.in ping statistics ---
100 packets transmitted, 100 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.190/29.727/129.810/13.442 ms
ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

--- google.in ping statistics ---

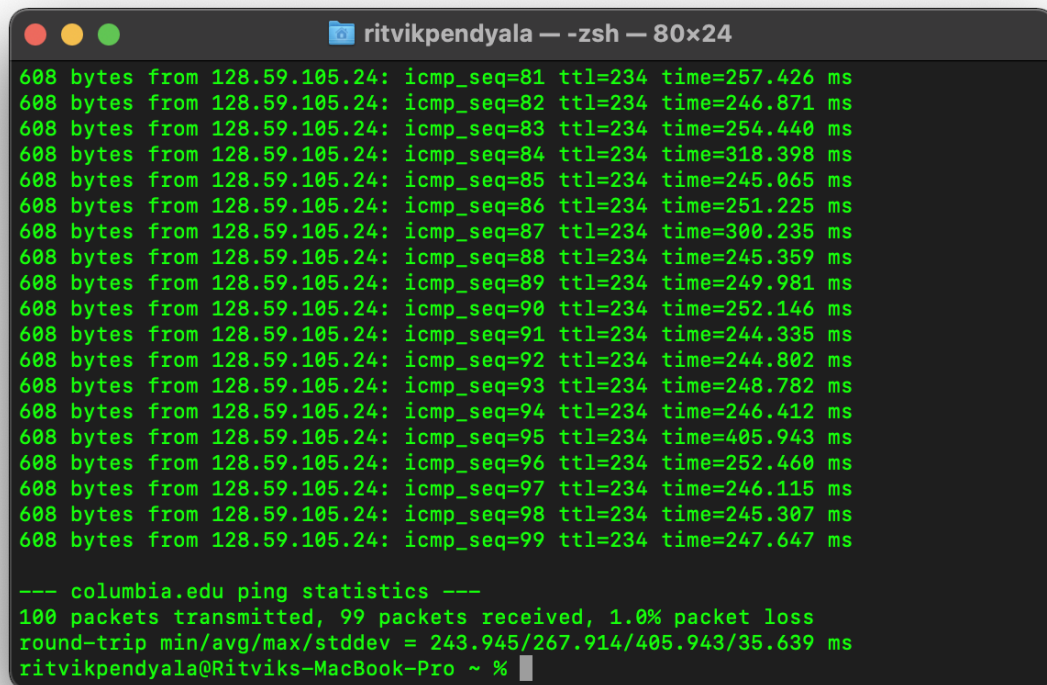
100 packets transmitted, 100 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 22.190/29.727/129.810/13.442 ms

Average latency = 29.727ms

c) Send 100 ping messages to columbia.edu, Determine the average latency. Put a screenshot.[2]

Command used: `ping -s 600 -c 100 columbia.edu`

A screenshot of a terminal window titled "ritvikpendyala — -zsh — 80x24". The terminal displays the output of a ping command. It shows 100 ping attempts, each with a response of "608 bytes from 128.59.105.24: icmp_seq=81 to icmp_seq=99, ttl=234, and various times in milliseconds. At the bottom, it shows the "columbia.edu ping statistics" summary: 100 packets transmitted, 99 packets received, 1.0% packet loss, and round-trip statistics: min/avg/max/stddev = 243.945/267.914/405.943/35.639 ms. The prompt is "ritvikpendyala@Ritviks-MacBook-Pro ~ %".

```
608 bytes from 128.59.105.24: icmp_seq=81 ttl=234 time=257.426 ms
608 bytes from 128.59.105.24: icmp_seq=82 ttl=234 time=246.871 ms
608 bytes from 128.59.105.24: icmp_seq=83 ttl=234 time=254.440 ms
608 bytes from 128.59.105.24: icmp_seq=84 ttl=234 time=318.398 ms
608 bytes from 128.59.105.24: icmp_seq=85 ttl=234 time=245.065 ms
608 bytes from 128.59.105.24: icmp_seq=86 ttl=234 time=251.225 ms
608 bytes from 128.59.105.24: icmp_seq=87 ttl=234 time=300.235 ms
608 bytes from 128.59.105.24: icmp_seq=88 ttl=234 time=245.359 ms
608 bytes from 128.59.105.24: icmp_seq=89 ttl=234 time=249.981 ms
608 bytes from 128.59.105.24: icmp_seq=90 ttl=234 time=252.146 ms
608 bytes from 128.59.105.24: icmp_seq=91 ttl=234 time=244.335 ms
608 bytes from 128.59.105.24: icmp_seq=92 ttl=234 time=244.802 ms
608 bytes from 128.59.105.24: icmp_seq=93 ttl=234 time=248.782 ms
608 bytes from 128.59.105.24: icmp_seq=94 ttl=234 time=246.412 ms
608 bytes from 128.59.105.24: icmp_seq=95 ttl=234 time=405.943 ms
608 bytes from 128.59.105.24: icmp_seq=96 ttl=234 time=252.460 ms
608 bytes from 128.59.105.24: icmp_seq=97 ttl=234 time=246.115 ms
608 bytes from 128.59.105.24: icmp_seq=98 ttl=234 time=245.307 ms
608 bytes from 128.59.105.24: icmp_seq=99 ttl=234 time=247.647 ms

--- columbia.edu ping statistics ---
100 packets transmitted, 99 packets received, 1.0% packet loss
round-trip min/avg/max/stddev = 243.945/267.914/405.943/35.639 ms
ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

--- columbia.edu ping statistics ---

100 packets transmitted, 99 packets received, 1.0% packet loss

round-trip min/avg/max/stddev = 243.945/267.914/405.943/35.639 ms

Average latency is 267.914ms =

d) Add up the ping latency of all the intermediate hosts and compare with (b). Are they matching, explain?[1+1]

On adding up the latency of the intermediate hosts = 89.04006633034ms

Here the traceroute is the total sum from the source to each network source in the traceroute hop till we get to the destination last server. So the sum would obviously be much larger than the ping as in the ping the latency is from the source directly to the destination so hence the avg ping doesn't match with the sum of the latency of the intermediate sources.

e) Take the maximum of ping latency amongst the intermediate hosts and compare with (b). Are they matching, explain? [1+1]

Here the maximum ping latency is : 23.86666667ms and the average latency from part b is The max of the average ping latency is 29.727ms and in theory these two should be more or less the same as the max traceroute from the source to destination would be equal to the max ping latency. Although in practical applications they would be very near to each other value wise as theres always room for error as well as there would be the processing time at each port which would account for the latency gap between the theoretically similar values.

- f) Traceroute columbia.edu. Compare the number of hops between google.in and columbia.edu (between the traceroute result of google.in and columbia.edu). Can you explain the reason for the latency difference between google.in and columbia.edu? [1+1]

```

ritvikpendyala — -zsh — 97x28

--- google.in ping statistics ---
100 packets transmitted, 100 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.190/29.727/129.810/13.442 ms
ritvikpendyala@Ritviks-MacBook-Pro ~ % clear

ritvikpendyala@Ritviks-MacBook-Pro ~ % traceroute columbia.edu
traceroute to columbia.edu (128.59.105.24), 64 hops max, 52 byte packets
 1 192.168.48.254 (192.168.48.254) 20.827 ms 5.599 ms 14.817 ms
 2 vpn.iiitd.edu.in (192.168.1.99) 4.234 ms 5.844 ms 4.405 ms
 3 180.151.15.241.reverse.spectranet.in (180.151.15.241) 6.611 ms 7.375 ms 7.215 ms
 4 219.65.112.205.static-delhi.vsnl.net.in (219.65.112.205) 16.919 ms 11.687 ms 9.959 ms
 5 172.23.183.134 (172.23.183.134) 30.835 ms 38.787 ms 41.198 ms
 6 ix-ae-0-100.tcore1.mlv-mumbai.as6453.net (180.87.38.5) 44.302 ms 37.283 ms 37.850 ms
 7 * * *
 8 * if-ae-7-2.tcore1.pye-paris.as6453.net (195.219.174.9) 162.465 ms *
 9 * * *
10 be6453.agr21.par04.atlas.cogentco.com (130.117.15.69) 158.603 ms 152.007 ms 149.152 ms
11 be3169.ccr31.par04.atlas.cogentco.com (154.54.37.237) 157.155 ms
   be2151.ccr32.par04.atlas.cogentco.com (154.54.61.33) 156.003 ms 183.657 ms
12 be2103.ccr42.par01.atlas.cogentco.com (154.54.61.21) 172.715 ms 155.636 ms
   be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157) 156.865 ms
13 be3628.ccr42.jfk02.atlas.cogentco.com (154.54.27.169) 364.279 ms 374.383 ms 307.151 ms
14 be2897.rcr24.jfk01.atlas.cogentco.com (154.54.84.214) 309.228 ms 305.905 ms 304.738 ms
15 38.122.8.210 (38.122.8.210) 310.140 ms 290.831 ms 307.328 ms
16 cc-core-1-x-nyser32-gw-1.net.columbia.edu (128.59.255.5) 308.899 ms 253.517 ms 248.581 ms
17 cc-conc-1-x-cc-core-1.net.columbia.edu (128.59.255.21) 261.248 ms 253.134 ms 387.656 ms
18 www.neurotheory.columbia.edu (128.59.105.24) 287.374 ms 251.570 ms 314.438 ms
ritvikpendyala@Ritviks-MacBook-Pro ~ %

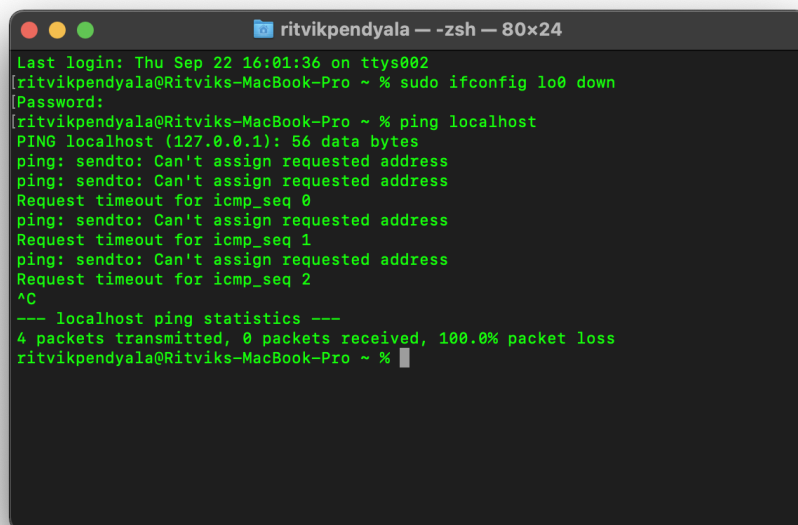
```

As we can see from part a and after performing the traceroute for columbia.edu theres a substantial difference between the number of hops between the two traceroutes! The reason in my opinion is that google.in has peered with some of the ISPs in between when we try to access such that we can access the Google domains much quicker as the hops present the evidence that is its only 7 hops away unlike columbia's internal edu network which doesn't need the requirement of peering with ISP in between so to access it we have to go all the way to the top that is to the Top of the ISP's and then go down the hierarchy, so from the ss as we can see we go from delhi to mumbai to paris to jfk to new york then to columbia's internal network so due to the lack of the requirement of peering and them not having done that we take around 18 hops to reach the network unlike in google's case where we reach it in 7 hops. The latency gap

between the two would result because of the number of ports that google and columbia.edu has as more the number of ports higher the latency gap! In addition to that Google is more of a public server and needs to maintain lower hops such that users can access when compared columbia as its more of a private network so as to google would have more number of ports resulting in a much lower latency than the columbia uni's latency!

Q4. [2+1] Make your ping command fail for 127.0.0.1 (with 100% packet loss). Explain how you do it. Put a screenshot that it failed.

Here in we're pinging the localhost and we'll get a ping as long as the connection is stable and running! So we can use the command "sudo ifconfig lo0 down" to stop localhost responsiveness and make the localhost down.



```
ritvikpendyala — zsh — 80x24
Last login: Thu Sep 22 16:01:36 on ttys002
[ritvikpendyala@Ritviks-MacBook-Pro ~ % sudo ifconfig lo0 down
[Password:
[ritvikpendyala@Ritviks-MacBook-Pro ~ % ping localhost
PING localhost (127.0.0.1): 56 data bytes
ping: sendto: Can't assign requested address
ping: sendto: Can't assign requested address
Request timeout for icmp_seq 0
ping: sendto: Can't assign requested address
Request timeout for icmp_seq 1
ping: sendto: Can't assign requested address
Request timeout for icmp_seq 2
^C
--- localhost ping statistics ---
4 packets transmitted, 0 packets received, 100.0% packet loss
ritvikpendyala@Ritviks-MacBook-Pro ~ %
```

This results in a 100% packet loss as the connection is useless as we've rendered the localhost useless by turning it down. Although this is just temporary and we can rectify the same by running the command "sudo ifconfig lo0 up".

Q5. [2+2+2+1] Use your web browser to retrieve the <http://info.cern.ch> web page. While retrieving the web page, use wireshark/tshark/tcpdump at your machine to capture the communication between your machine and the web server. You may need to filter the required packets. Put the screenshot of HTTP request and response messages. Explain the following

details for each captured packet.

- For HTTP request packets
 - HTTP request type
 - User agent type
 - HTTP request packet's URL
 - Name and version of the web server
- For HTTP response packets
 - HTTP response code
 - HTTP response description
- How many web objects get downloaded? Were they over the same TCP connection or different connections?

Answer:

2 different sets of objects are downloaded from 2 different TCP connections. - 4 objects in total - 2 Get and 2 response frome

- From this tell if it is HTTP persistent or non-persistent?

Answer:

They aren't persistent as the packets are received on 2 different ports hence they aren't persistent.

Total Packets received :

***ens33**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
609	27.967786048	23.63.111.227	192.168.152.129	OCSP	943	Response
613	27.973258265	23.63.111.227	192.168.152.129	OCSP	943	Response
813	31.503431029	192.168.152.129	117.18.237.29	OCSP	470	Request
817	31.510323506	117.18.237.29	192.168.152.129	OCSP	793	Response
980	40.694478539	192.168.152.129	172.217.160.195	OCSP	473	Request
982	40.784402741	172.217.160.195	192.168.152.129	OCSP	756	Response
1009	41.065507298	192.168.152.129	188.184.21.108	HTTP	390	GET / HTTP/1.1
1018	41.225784982	188.184.21.108	192.168.152.129	HTTP	932	HTTP/1.1 200 OK (text/html)
1024	41.240508393	192.168.152.129	172.217.160.195	OCSP	473	Request
1031	41.328295911	172.217.160.195	192.168.152.129	OCSP	756	Response
1169	41.990188042	192.168.152.129	188.184.21.108	HTTP	342	GET /favicon.ico HTTP/1.1
1176	42.165802540	188.184.21.108	192.168.152.129	HTTP	458	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

Frame 23: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface ens33, id 0
 Ethernet II, Src: VMware_ef:24:f0 (00:50:56:ef:24:f0), Dst: VMware_fe:29:31 (00:0c:29:fe:29:31)
 Internet Protocol Version 4, Src: 188.185.87.101, Dst: 192.168.152.129
 Transmission Control Protocol, Src Port: 80, Dst Port: 47300, Seq: 1, Ack: 2, Len: 207
 Hypertext Transfer Protocol
 Line-based text data: text/html (3 lines)

```

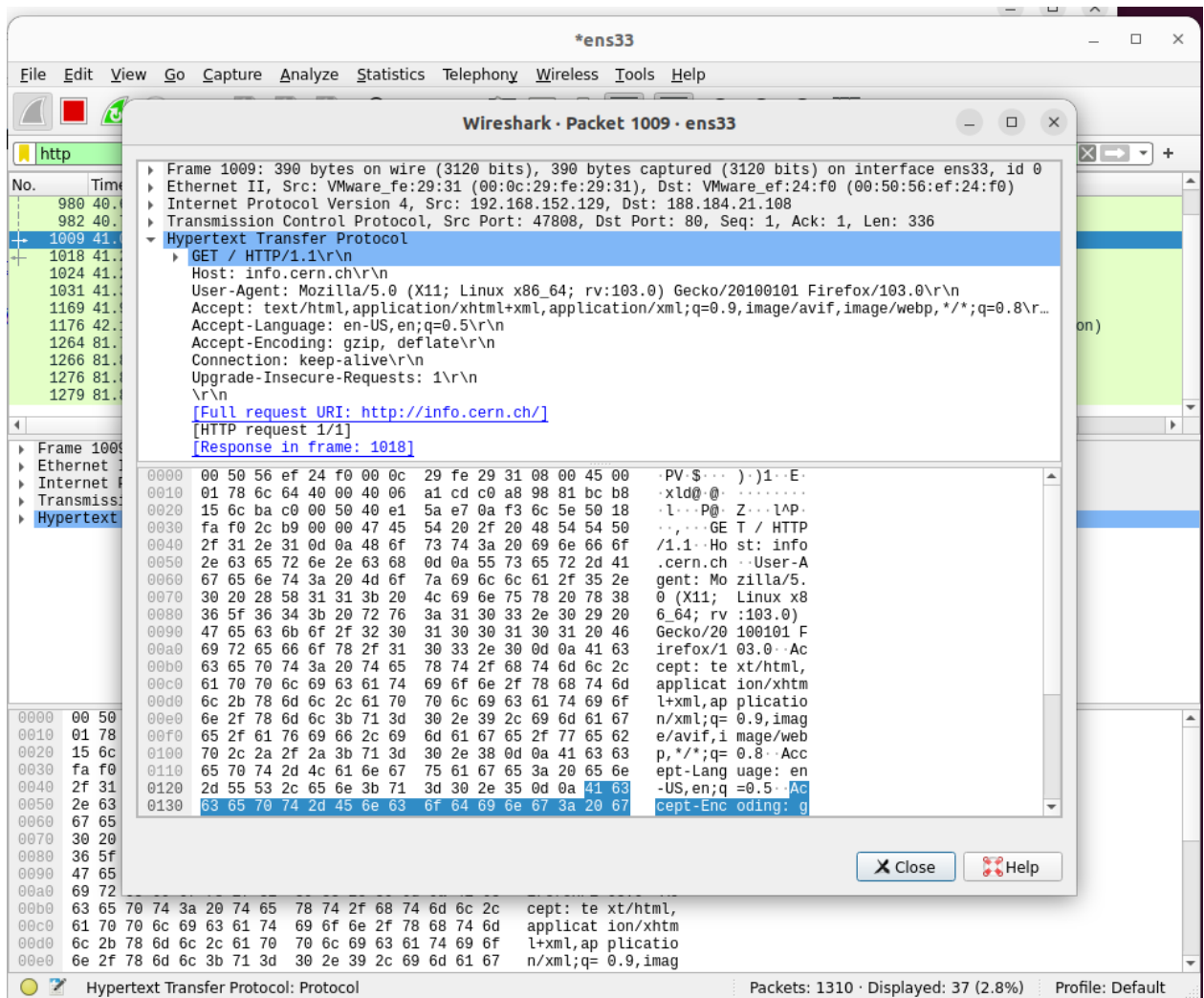
0000  00 0c 29 fe 29 31 00 50 56 ef 24 f0 08 00 45 00  ...).1P V.$...E.
0010  00 f7 a8 5f 00 00 80 06 24 59 bc b9 57 65 c0 a8  ..._....$Y..We..
0020  98 81 00 50 b8 c4 07 a6 55 ea b2 f2 cb ad 50 19  ...P....U../..P.
0030  fa ef c1 8f 00 00 48 54 54 50 2f 31 2e 31 20 34  ....HT TP/1.1 4
0040  30 30 20 42 61 64 20 72 65 71 75 65 73 74 0d 0a  00 Bad r equest..
0050  63 6f 6e 74 65 6e 74 2d 6c 65 6e 67 74 68 3a 20  content- length:
0060  39 30 0d 0a 63 61 63 68 65 2d 63 6f 6e 74 72 6f  90 ..cach e-contro
0070  6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 63 6f 6e  l: no-ca che ..con
0080  74 65 6e 74 2d 74 79 70 65 3a 20 74 65 78 74 2f  tent-typ e: text/
0090  68 74 6d 6c 0d 0a 63 6f 6e 6e 65 63 74 69 6f 6e  html..co nnection
00a0  3a 20 63 6c 6f 73 65 0d 0a 0d 0a 3c 68 74 6d 6c  : close- ...<html
00b0  3e 3c 62 6f 64 79 3e 3c 68 31 3e 34 30 30 20 42  ><body>< h1>400 B
00c0  61 64 20 72 65 71 75 65 73 74 3c 2f 68 31 3e 0a  ad reques t</h1>..
00d0  59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e  Your bro wser sen
00e0  74 20 61 6e 20 69 6e 76 61 6c 69 64 20 72 65 71  t an inv alid req
  
```

Hypertext Transfer Protocol: Protocol Packets: 1256 · Displayed: 33 (2.6%) Profile: Default

Request SS-1: Request type : GET

User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0\r\n

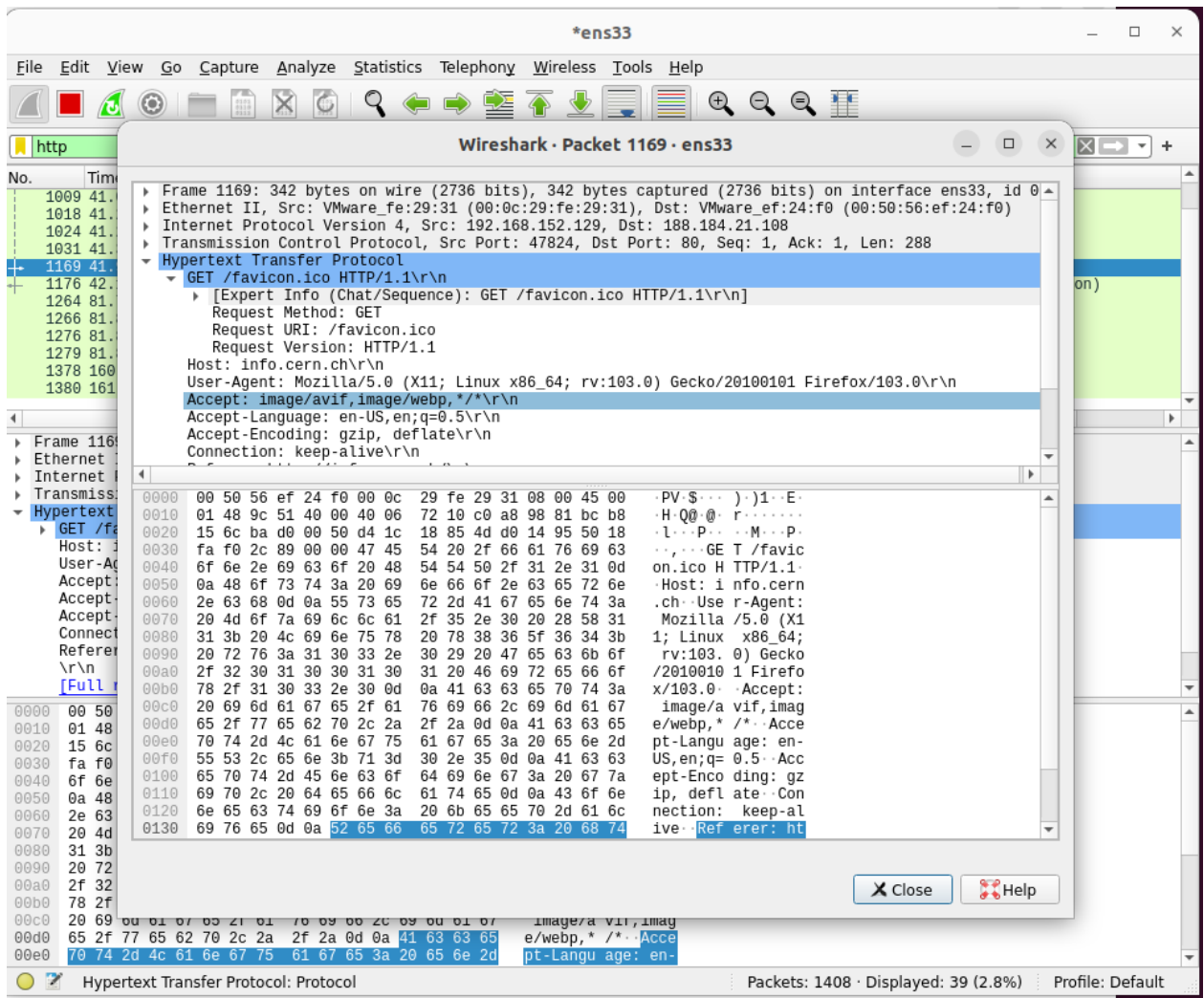
HTTP request packet's URL :[Full request URI: http://info.cern.ch/]



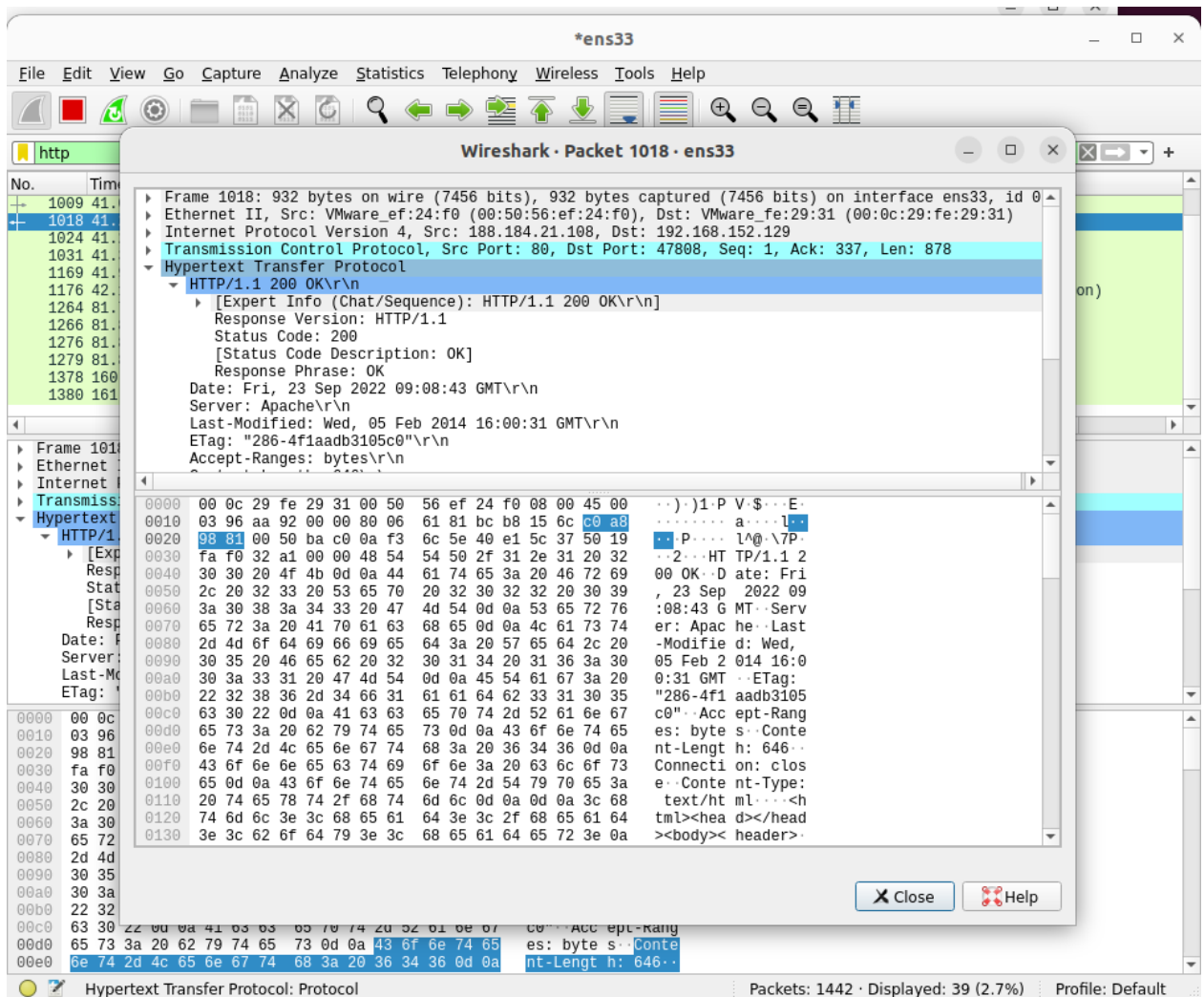
Request SS-1: Request type : GET

User Agent: Mozilla/5.0 (X11; Linux x86_64; rv:103.0) Gecko/20100101 Firefox/103.0\r\n

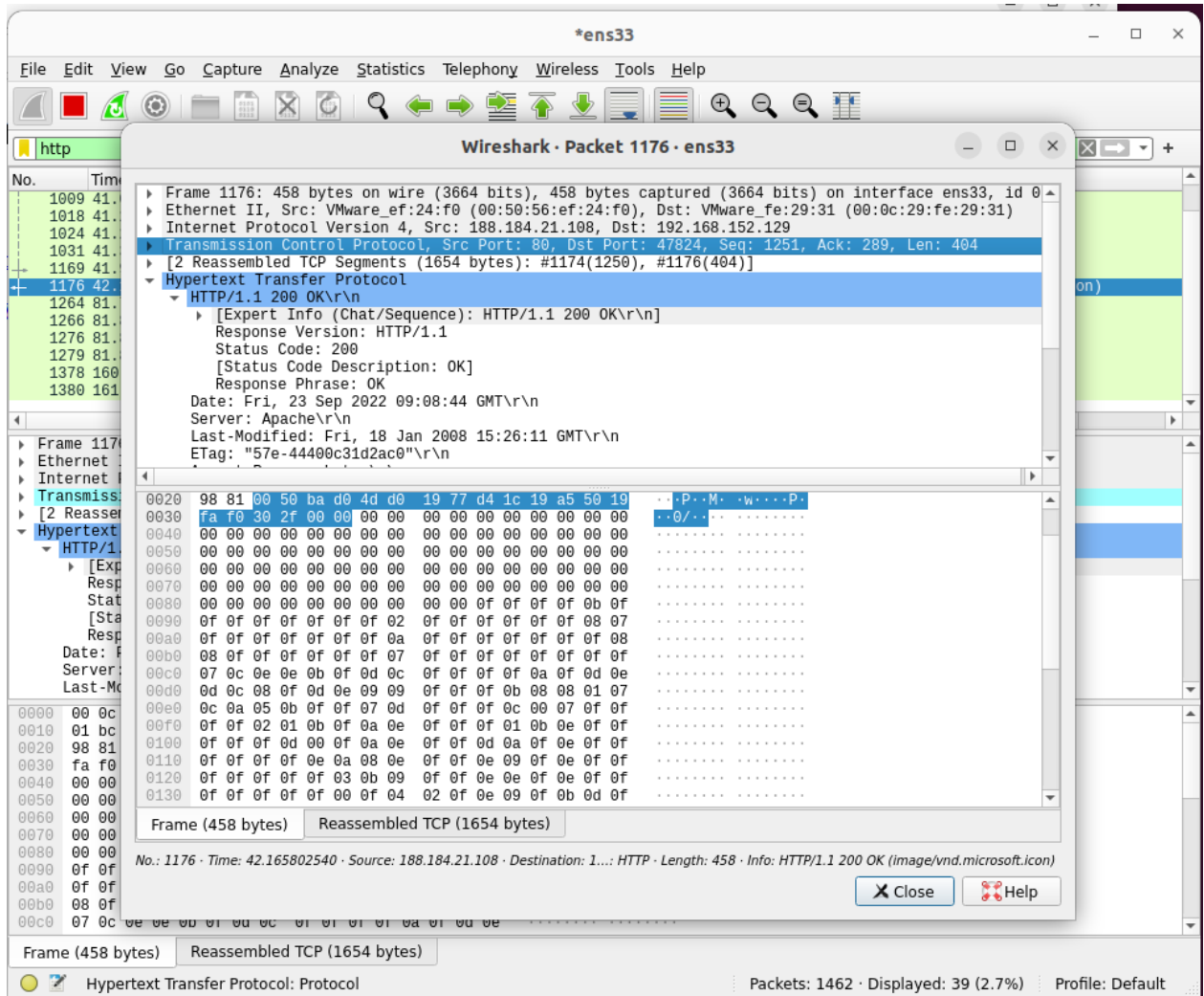
HTTP request packet's URL :[Full request URI: http://info.cern.ch/]



Response Packets below:
 HTTP response code - 200
 HTTP response description - OK
 Name and version of the web server - Apache



Response Packets below:
 HTTP response code - 200
 HTTP response description - OK
 Name and version of the web server - Apache



Q6. [1+1] Note: perform this test after Q5

a) Write the command to display all active tcp connections with pids

Command used to display all the active tcp connections with pids

: netstat -at -tp


```

pendi@pendi-virtual-machine:~/Desktop$ netstat -at -tp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN      -
tcp        0      0 pendi-virtual-mac:54830 ec2-34-208-34-131:https ESTABLISHED 3974/firefox
tcp        0      0 pendi-virtual-mac:33816 239.237.117.34.bc:https ESTABLISHED 3974/firefox
tcp        0      0 pendi-virtual-mac:51858 82.221.107.34.bc.g:http ESTABLISHED 3974/firefox
tcp        0      0 pendi-virtual-mac:34674 221.5.120.34.bc.g:https ESTABLISHED 3974/firefox
tcp        0      0 pendi-virtual-mac:59788 123.208.120.34.bc:https ESTABLISHED 3974/firefox
tcp        0      0 pendi-virtual-mac:51846 82.221.107.34.bc.g:http ESTABLISHED 3974/firefox
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      -
pendi@pendi-virtual-machine:~/Desktop$

```

b) Determine the state of the TCP connection(s) to this server <http://info.cern.ch>

Command: netstat -t info.cern.ch

```

pendi@pendi-virtual-machine:~/Desktop$ netstat -t info.cern.ch
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 pendi-virtual-mac:49434 a23-63-111-217.dep:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:49440 a23-63-111-217.dep:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:49448 a23-63-111-217.dep:http TIME_WAIT
tcp        0      0 pendi-virtual-mac:37926 bom07s29-in-f4.1e:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:49292 bom07s32-in-f3.1e1:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:49288 bom07s32-in-f3.1e1:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:41230 123.208.120.34.bc:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:48126 bom12s21-in-f10.1:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:44972 82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:33272 82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:53224 server-99-86-47-1:https ESTABLISHED
tcp        0      0 pendi-virtual-mac:49410 a23-63-111-217.dep:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:52416 102.115.120.34.bc:https ESTABLISHED
tcp        0      0 pendi-virtual-mac:50014 ec2-52-43-58-150.:https ESTABLISHED
tcp        0      0 pendi-virtual-mac:53488 76.237.120.34.bc.:https ESTABLISHED
tcp        0      0 pendi-virtual-mac:52806 123.208.120.34.bc:https ESTABLISHED
tcp        0      0 pendi-virtual-mac:56846 117.18.237.29:http      ESTABLISHED
tcp        0      0 pendi-virtual-mac:53452 76.237.120.34.bc.:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:51442 123.208.120.34.bc:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:53502 76.237.120.34.bc.:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:49418 a23-63-111-217.dep:http ESTABLISHED
tcp        0      0 pendi-virtual-mac:51428 123.208.120.34.bc:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:53468 76.237.120.34.bc.:https TIME_WAIT
tcp        0      0 pendi-virtual-mac:36774 239.237.117.34.bc:https ESTABLISHED
pendi@pendi-virtual-machine:~/Desktop$

```