

CSE 232: Assignment 2

Kesar Shrivastava

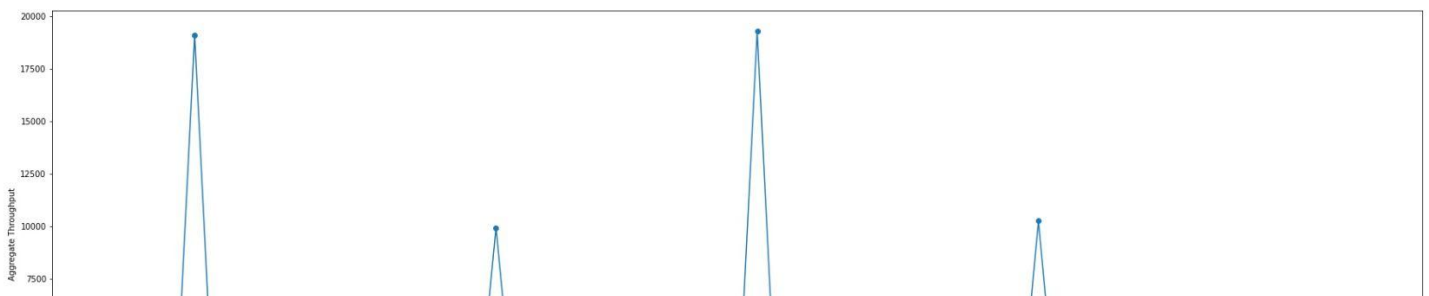
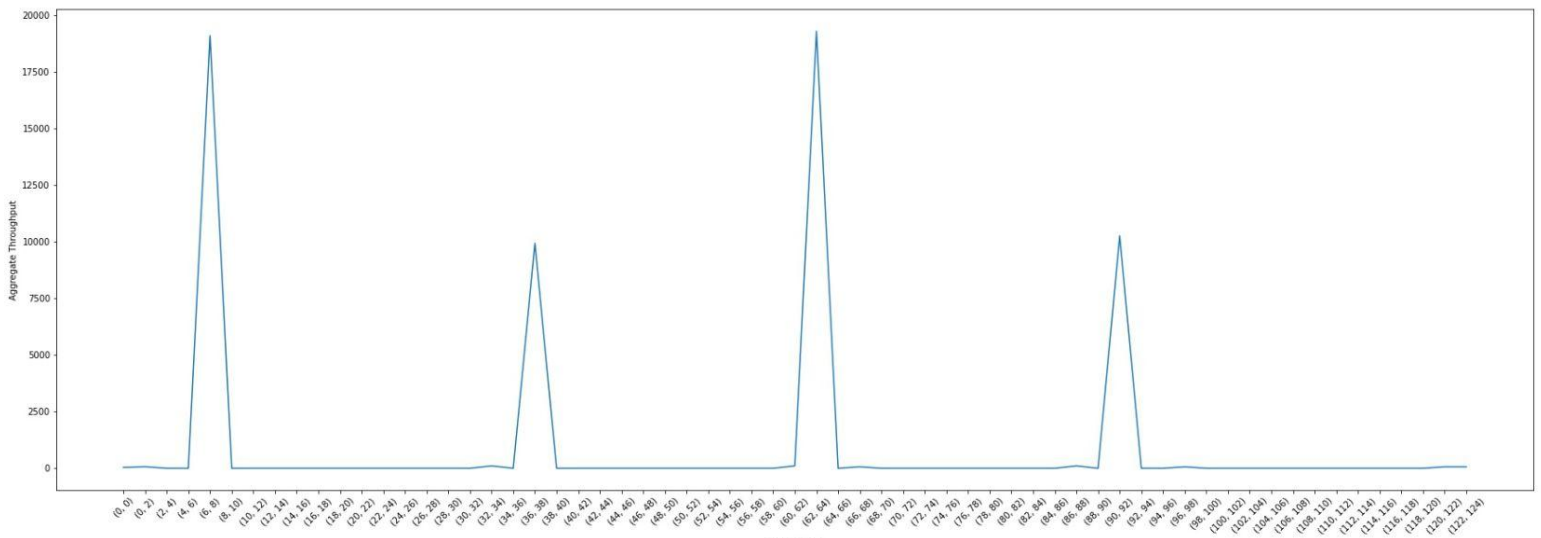
2019051

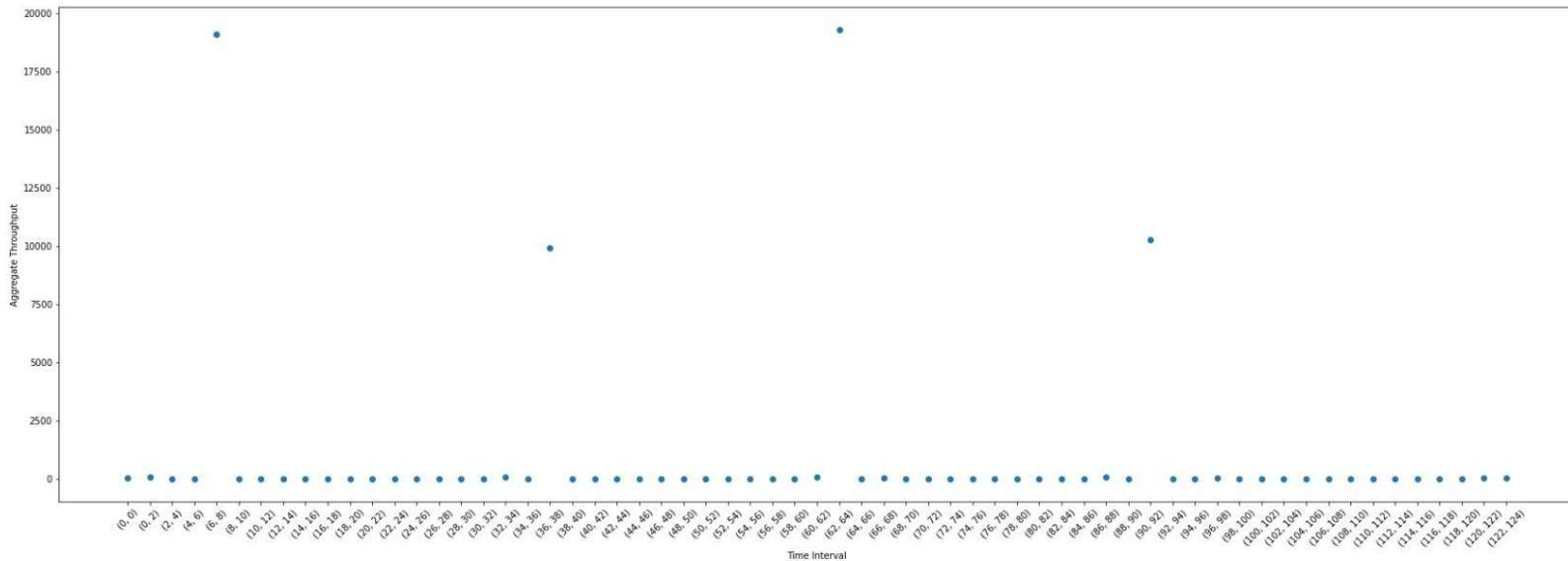
Q1

Packet capture: The packets are captured from the loopback interface since both the client and the server are running on the same machine. From the display filter of Wireshark, the packets are filtered using tcp.port (according to the port number in the program). It is then exported into csv format and using a python script the plot is made.

Analysis: Since there are three to four clients running in parallel which communicate with the server we see spikes when the packets are sent in between both. There are also some bumps in between due to input output.

The plots: They are provided as pdf in the zip file too.





Q2

Capture filter: host info.cern.ch

The packets are captured from the ethernet interface.

The complete packet capture:

Wireshark interface showing packet capture details. The selected packet (Frame 7) is an HTTP GET request to /favicon.ico from 10.0.2.15 to 188.184.21.108. The details pane shows the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers.

Frame 7: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_21:e7:f7 (08:00:27:21:e7:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 188.184.21.108
 Transmission Control Protocol, Src Port: 51018, Dst Port: 80, Seq: 1, Ack: 1, Len: 331
 Hypertext Transfer Protocol

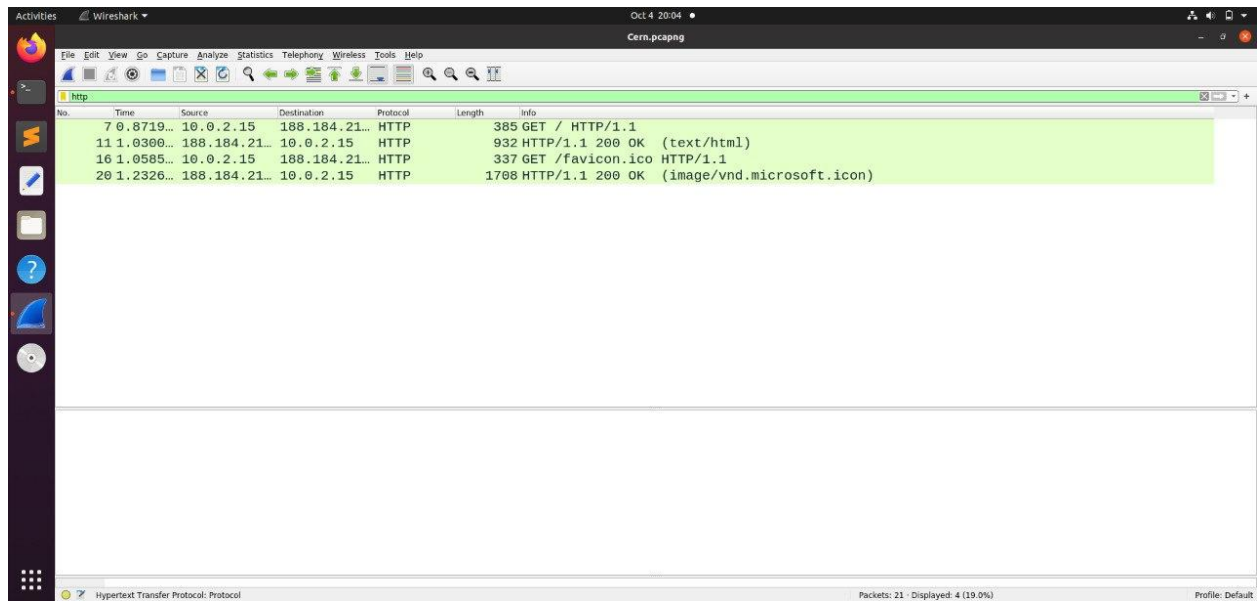
Raw packet data (hex and ASCII):

```

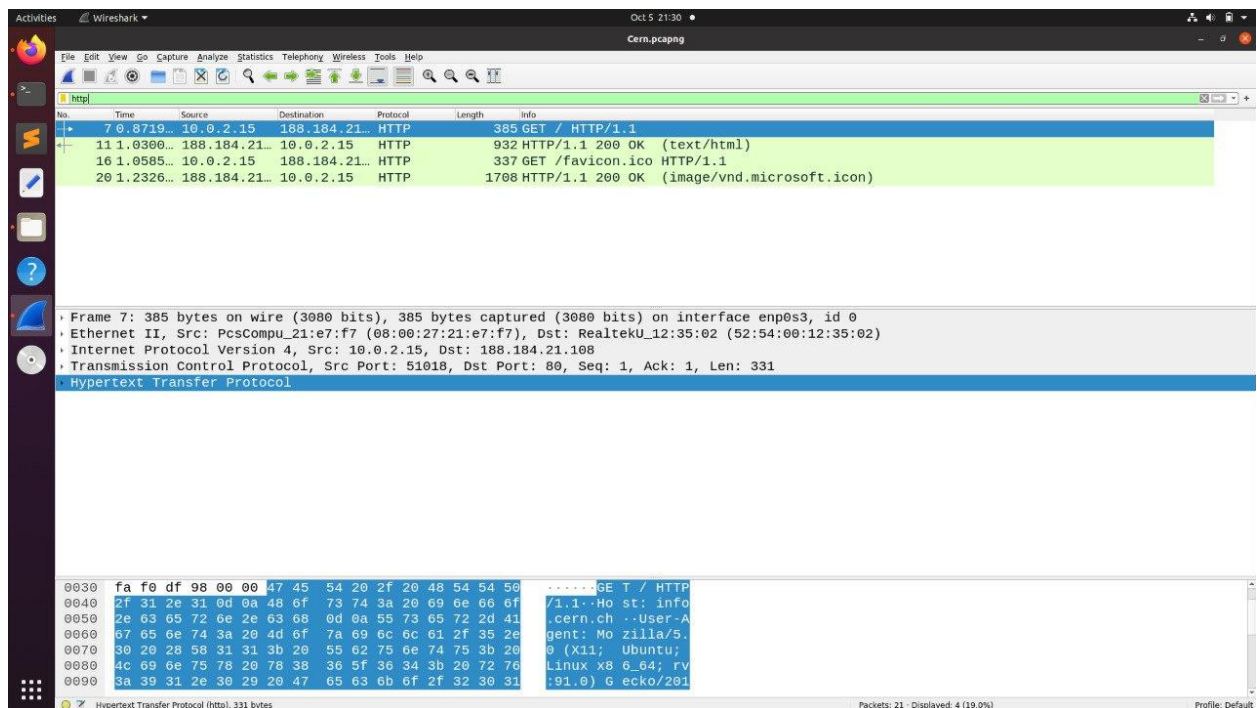
0000 52 54 00 12 35 02 08 00 27 21 e7 f7 08 00 45 00 RT..5...!....E:
01 73 64 fe 40 00 40 06 f6 53 9a 00 02 0f bc b8 -sd@0:~S....
0020 15 6c c7 4a 00 50 d7 eb 35 56 0e ca 22 02 50 18 .LJP...SV/"p.
0030 fa f0 df 98 00 00 47 45 54 20 2f 20 48 54 50 .....GET / HTTP
0040 2f 31 2e 31 0d 9a 48 6f 73 74 3a 20 69 6e 66 6f /1.1..Ho st: info
0050 2e 63 65 72 0e 2e 63 68 0d 0a 55 73 65 72 2d 41 .cern.ch -User-A
0060 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.

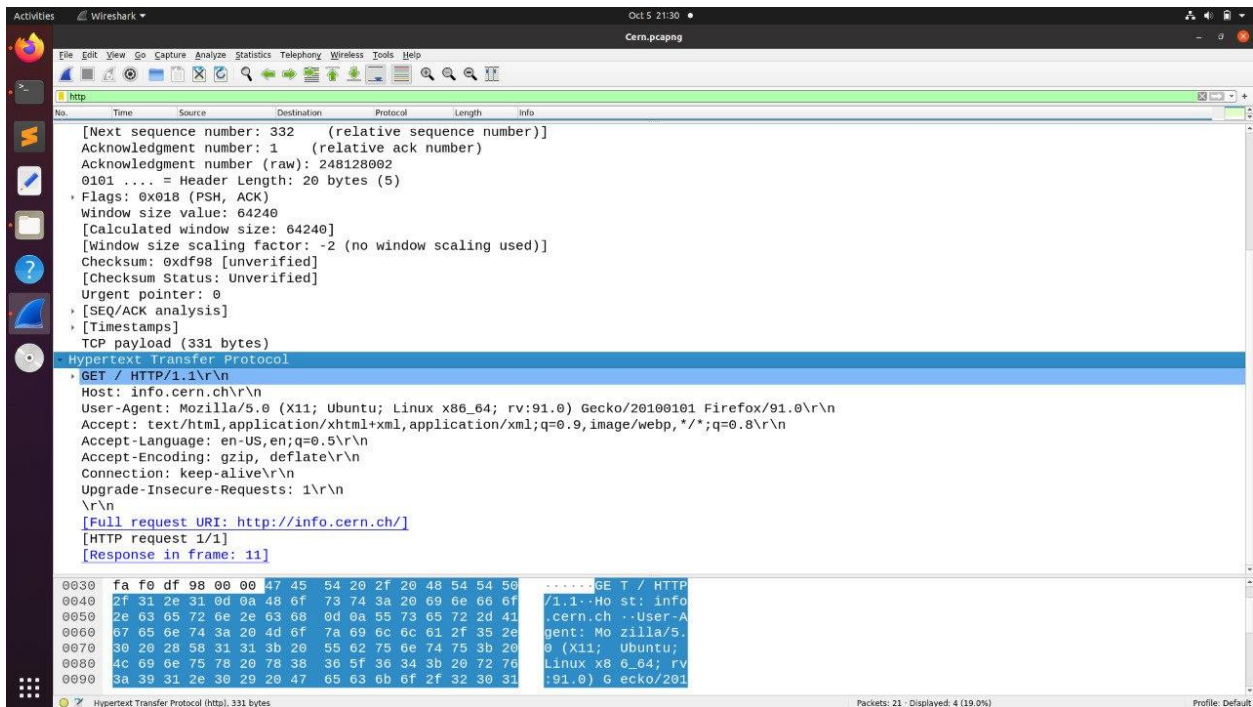
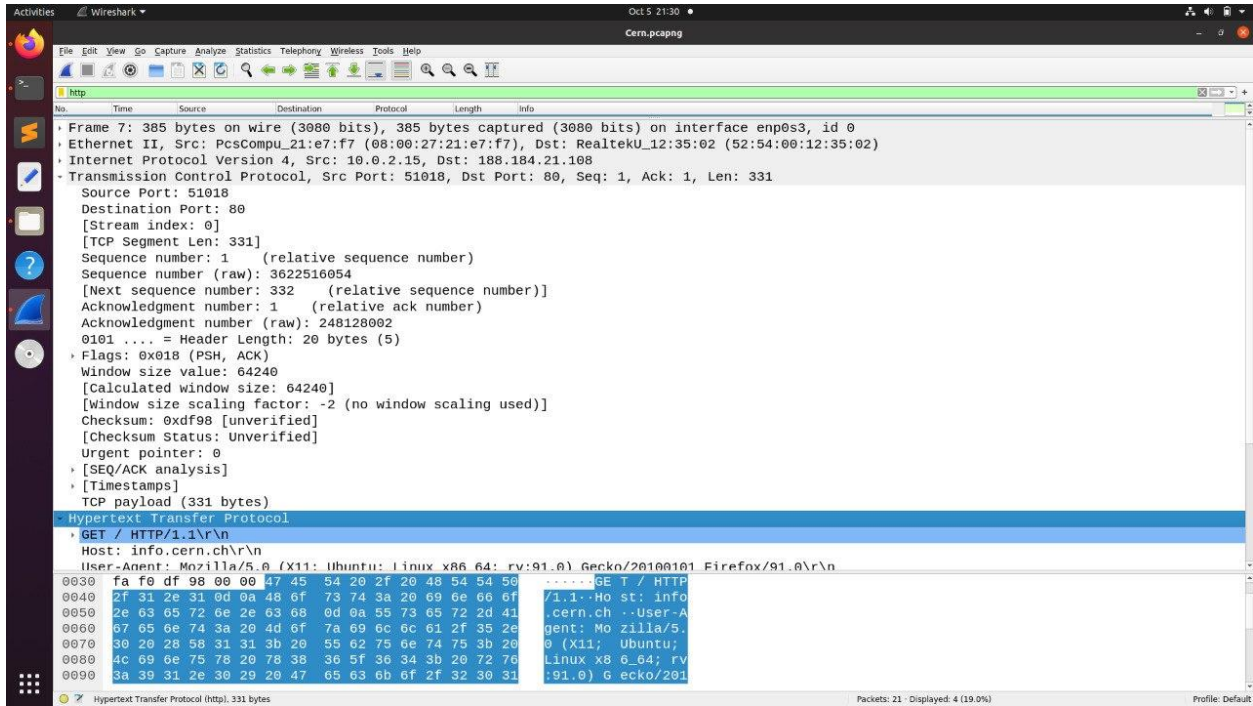
```

HTTP filter is applied:



The HTTP request messages:





Wireshark - Cern.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
7	0.8719...	10.0.2.15	188.184.21...	HTTP	385	GET / HTTP/1.1
11	1.0300...	188.184.21...	10.0.2.15	HTTP	932	HTTP/1.1 200 OK (text/html)
16	1.0585...	10.0.2.15	188.184.21...	HTTP	337	GET /favicon.ico HTTP/1.1
20	1.2326...	188.184.21...	10.0.2.15	HTTP	1708	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

Frame 16: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) on interface enp0s3, id 0

- Ethernet II, Src: PcsCompu_21:e7:f7 (08:00:27:21:e7:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 188.184.21.108
- Transmission Control Protocol, Src Port: 51020, Dst Port: 80, Seq: 1, Ack: 1, Len: 283
- Hypertext Transfer Protocol

0030 fa f0 df 68 00 00 47 45 54 20 2f 66 61 76 09 63 ...h..GET /favico

0040 6f 6e 2e 09 03 6f 20 48 54 54 50 2f 31 2e 31 0d ...n.ico M TTP/1.1

0050 9a 48 6f 73 74 3a 20 09 6e 66 6f 2e 63 65 72 6e ...Host: i nfo.cern

0060 2e 63 68 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a ...ch..Use r-Agent:

0070 20 4d 6f 7a 09 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 20 4c 69 6e 75 78 ...i; Ubunt u; Linux

0090 20 78 38 36 5f 36 34 3b 20 72 76 3a 39 31 2e 36 ...x86_64; rv:91.0

Hypertext Transfer Protocol (http), 283 bytes

Packets: 21 · Displayed: 4 (19.0%)

Profile: Default

Wireshark - Cern.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

Frame 16: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) on interface enp0s3, id 0

- Ethernet II, Src: PcsCompu_21:e7:f7 (08:00:27:21:e7:f7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15, Dst: 188.184.21.108
- Transmission Control Protocol, Src Port: 51020, Dst Port: 80, Seq: 1, Ack: 1, Len: 283
- Source Port: 51020
- Destination Port: 80
- [Stream index: 1]
- [TCP Segment Len: 283]
- Sequence number: 1 (relative sequence number)
- Sequence number (raw): 1264322761
- [Next sequence number: 284 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Acknowledgment number (raw): 248384002
- 0101 ... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window size value: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0xdf68 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (283 bytes)
- Hypertext Transfer Protocol
- GET /favicon.ico HTTP/1.1\r\n
- Host: info.cern.ch\r\n
- User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n

0030 fa f0 df 68 00 00 47 45 54 20 2f 66 61 76 09 63 ...h..GET /favico

0040 6f 6e 2e 09 03 6f 20 48 54 54 50 2f 31 2e 31 0d ...n.ico M TTP/1.1

0050 9a 48 6f 73 74 3a 20 09 6e 66 6f 2e 63 65 72 6e ...Host: i nfo.cern

0060 2e 63 68 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a ...ch..Use r-Agent:

0070 20 4d 6f 7a 09 6c 6c 61 2f 35 2e 30 20 28 58 31 ...Mozilla /5.0 (X1

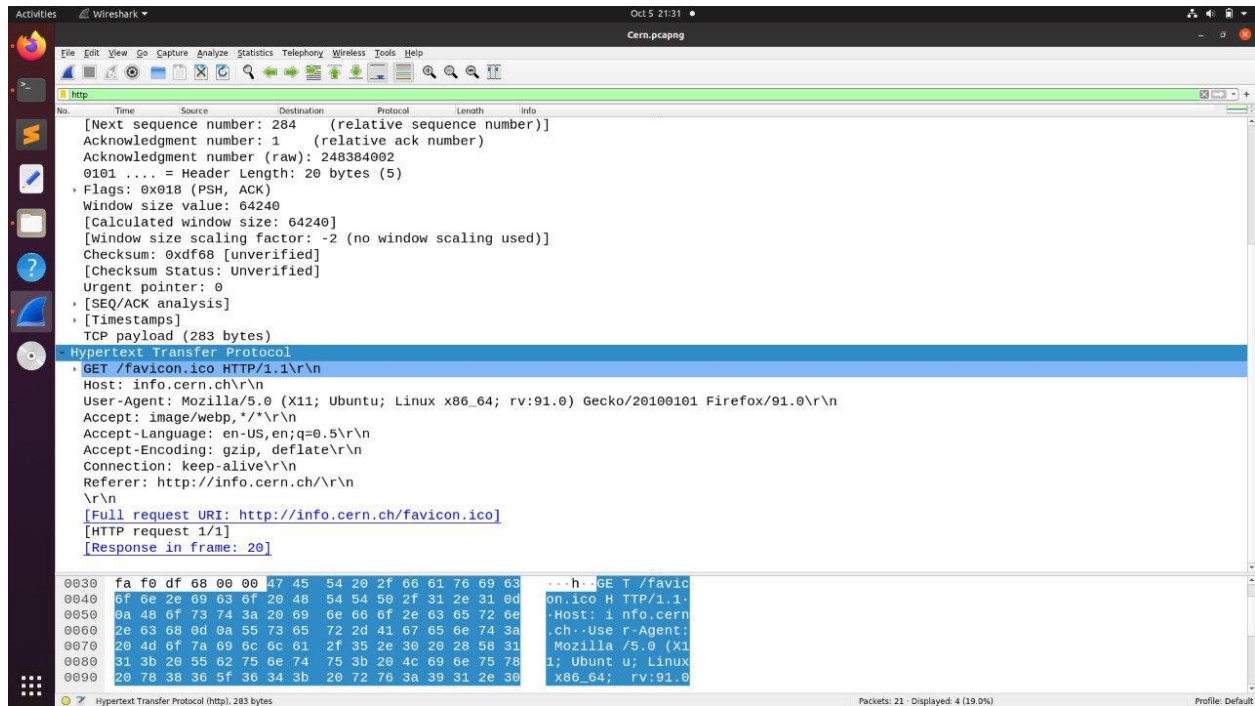
0080 31 3b 20 55 62 75 6e 74 75 3b 20 4c 69 6e 75 78 ...i; Ubunt u; Linux

0090 20 78 38 36 5f 36 34 3b 20 72 76 3a 39 31 2e 36 ...x86_64; rv:91.0

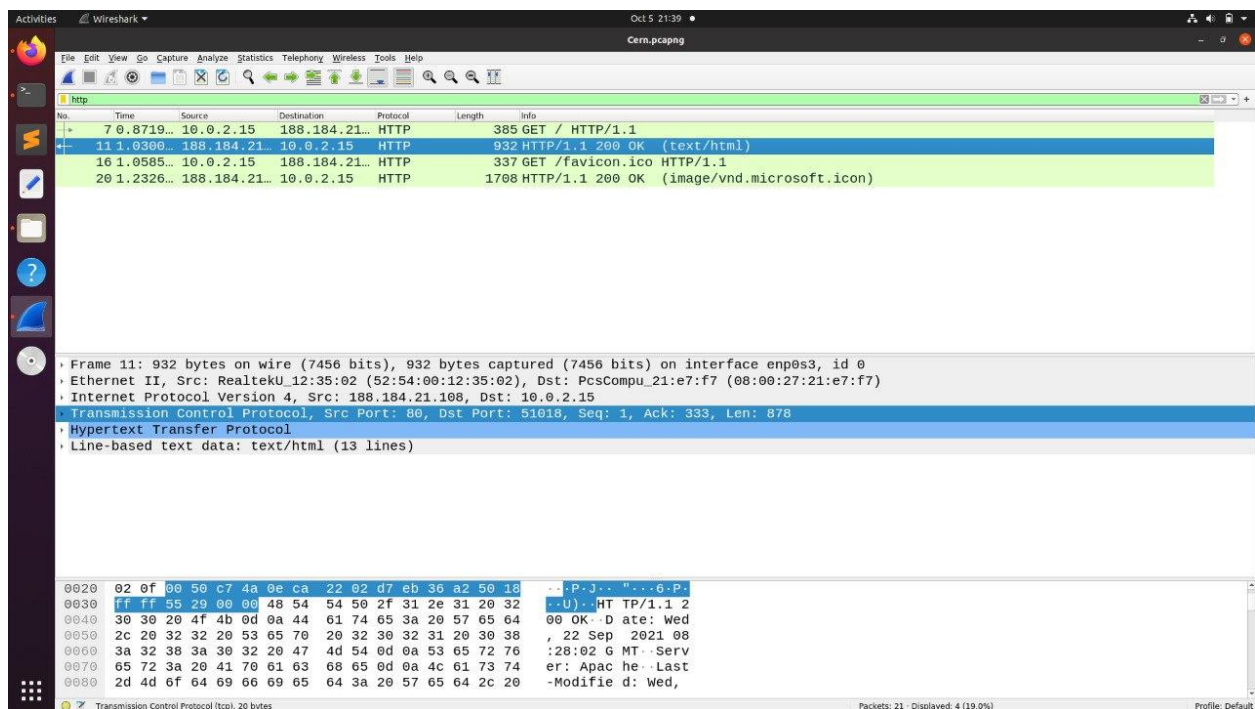
Hypertext Transfer Protocol (http), 283 bytes

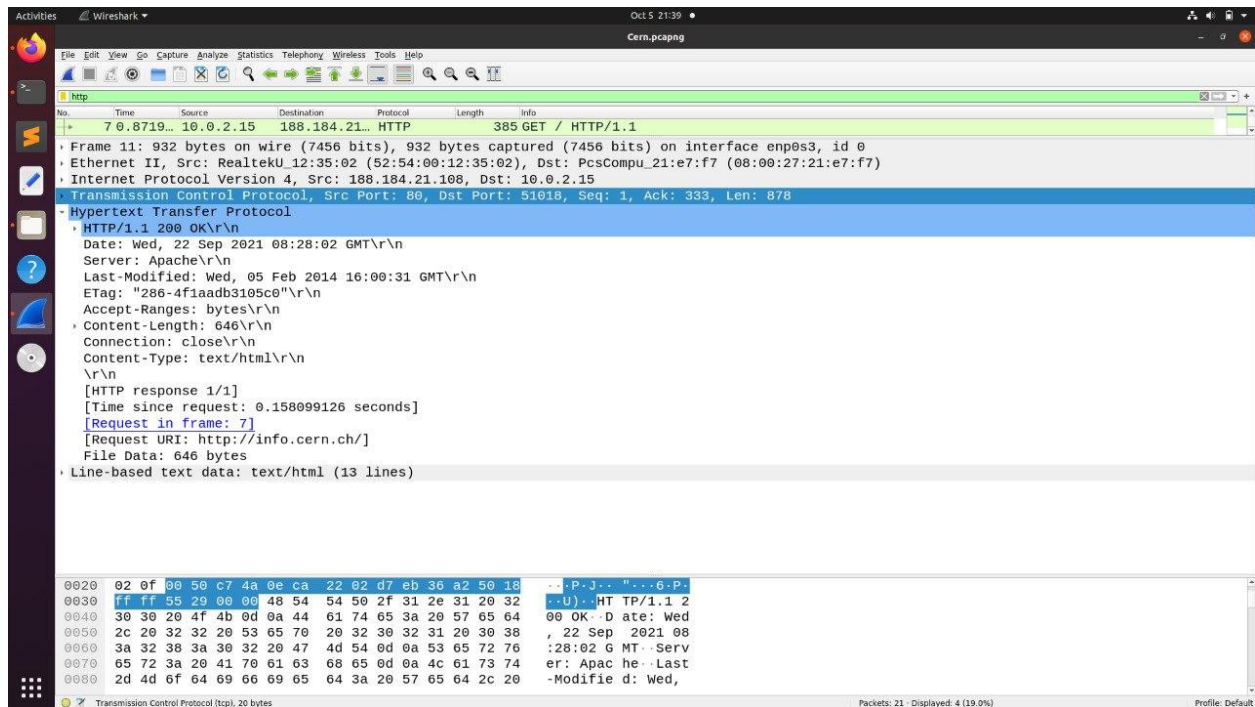
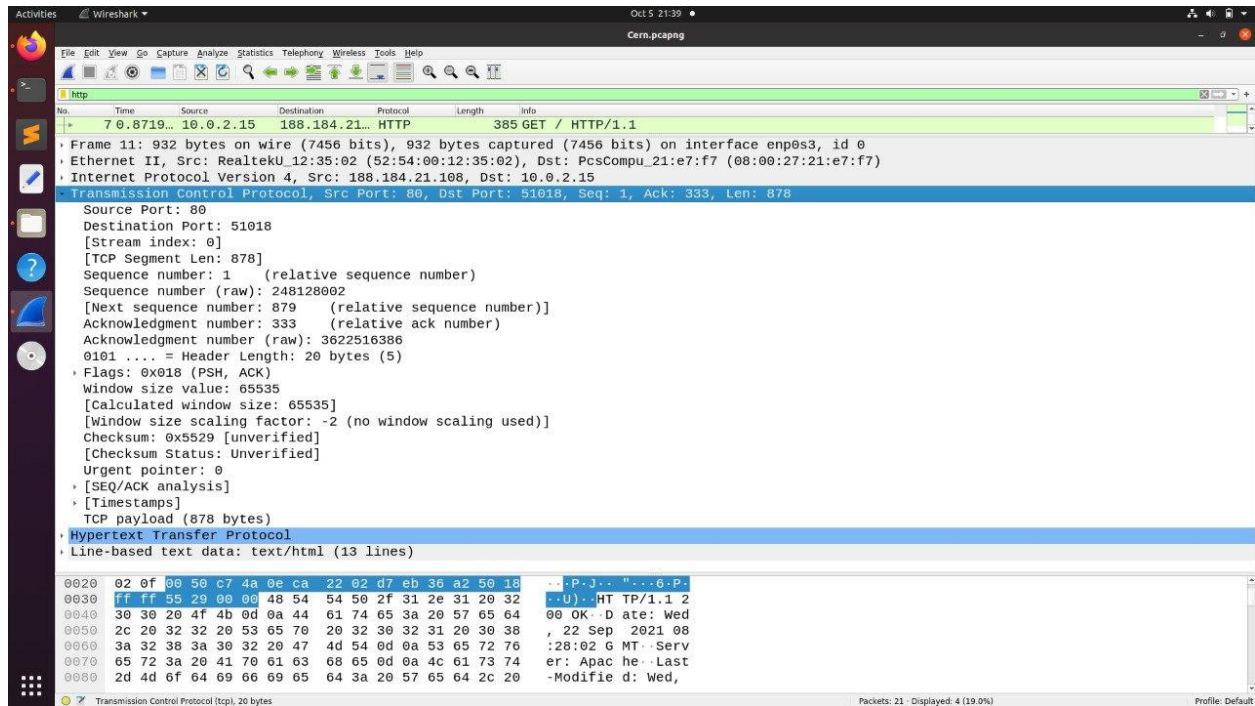
Packets: 21 · Displayed: 4 (19.0%)

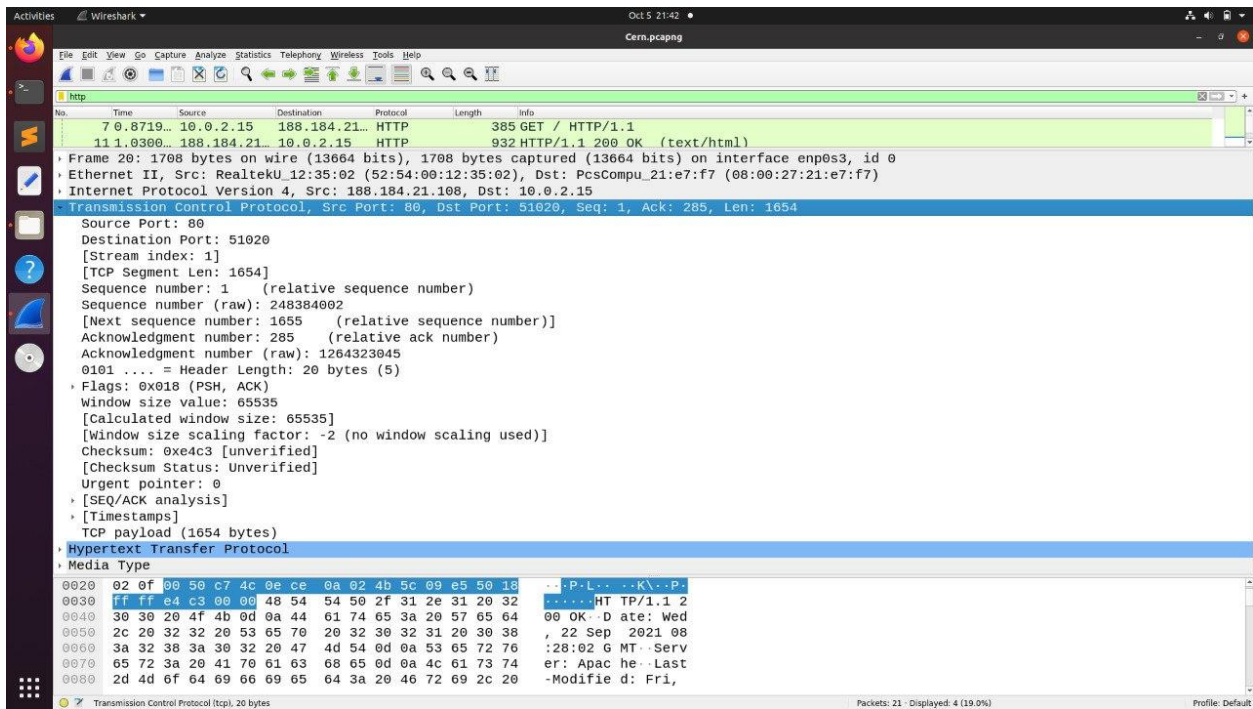
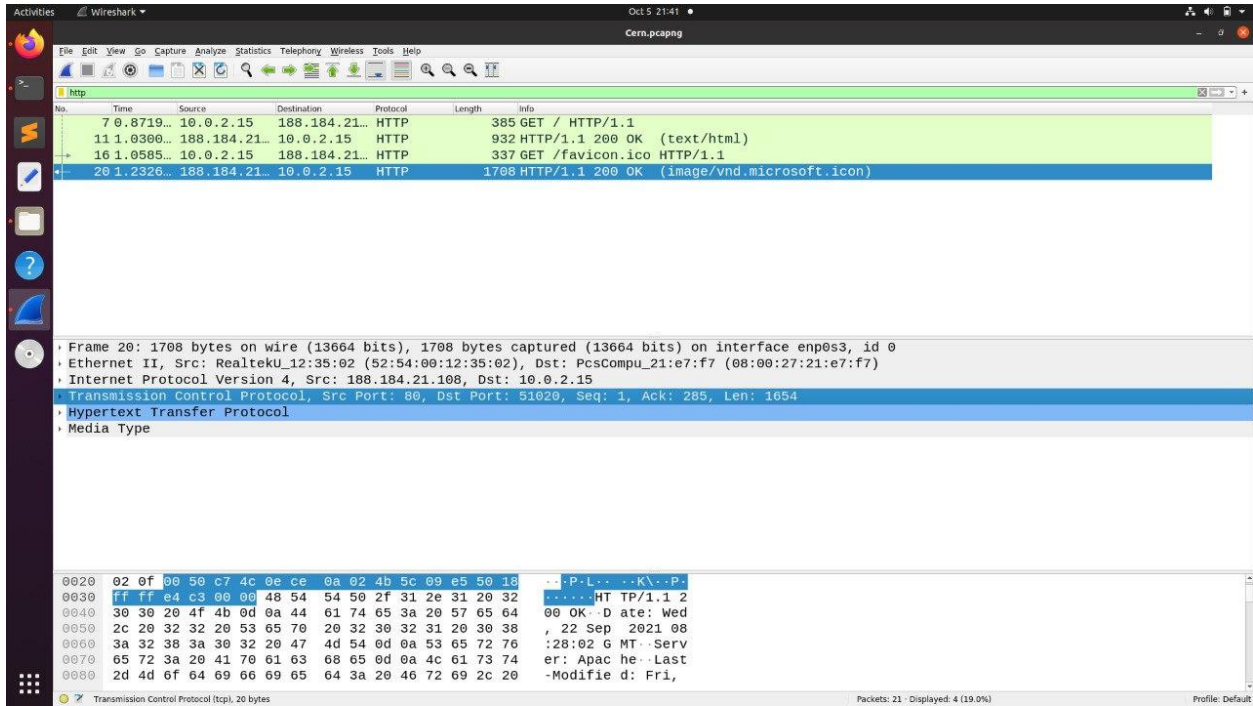
Profile: Default

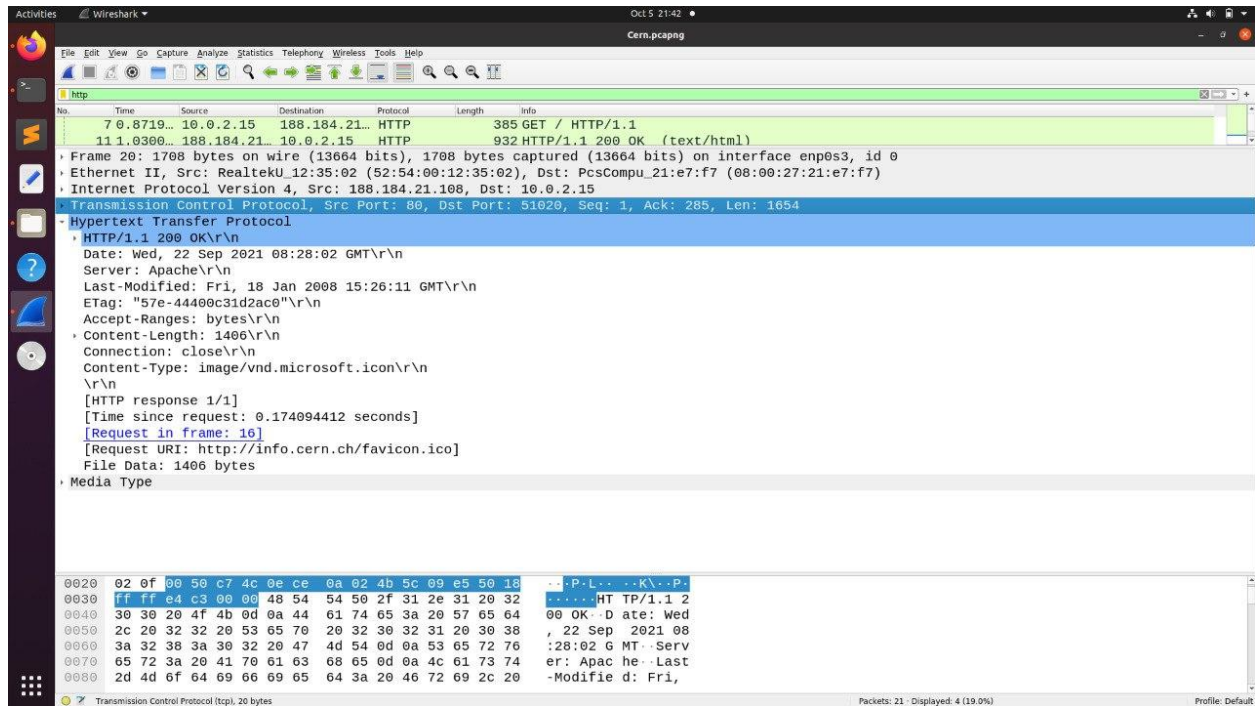


The HTTP response messages:









Packet by frame number:

Frame 7:

HTTP packet type: Request

HTTP Request type: GET

User Agent Type: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101

Firefox/91.0\r\n

HTTP request packet's URL: <http://info.cern.ch/>

Frame 11:

HTTP packet type: Response

HTTP response code: 200

HTTP response description: OK

Name and version of the webserver: Apache\r\n

Frame 16:

HTTP packet type: Request

HTTP Request type: GET

User Agent Type: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0\r\n

HTTP request packet's URL: <http://info.cern.ch/favicon.ico>

Frame 20:

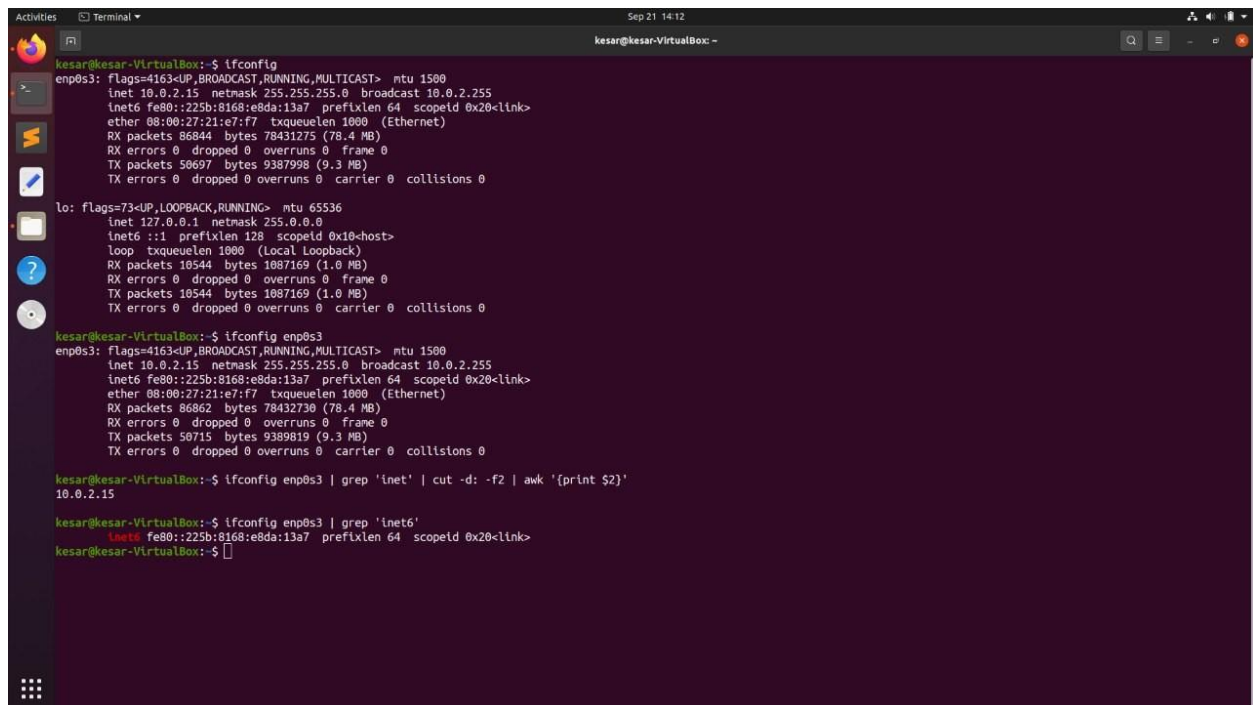
HTTP packet type: Response

HTTP response code: 200

HTTP response description: OK

Name and version of the webserver: Apache\r\n

Q3 (a)



```
kesar@kesar-VirtualBox:~$ 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::225b:8168:e8da:13a7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:e7:f7 txqueuelen 1000 (Ethernet)
    RX packets 86844 bytes 78431275 (78.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50697 bytes 9387998 (9.3 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 10544 bytes 1087169 (1.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10544 bytes 1087169 (1.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kesar@kesar-VirtualBox:~$ ifconfig enp0s3
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::225b:8168:e8da:13a7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:e7:f7 txqueuelen 1000 (Ethernet)
    RX packets 86862 bytes 78432730 (78.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 50715 bytes 9389819 (9.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kesar@kesar-VirtualBox:~$ ifconfig enp0s3 | grep 'inet' | cut -d: -f2 | awk '{print $2}'
10.0.2.15

kesar@kesar-VirtualBox:~$ ifconfig enp0s3 | grep 'inet6'
inet6 fe80::225b:8168:e8da:13a7 prefixlen 64 scopeid 0x20<link>
kesar@kesar-VirtualBox:~$
```

ifconfig command is used to configure the kernel-resident network interfaces. It shows two interfaces: enp0s3 and lo. enp0s3 represents the active network interface. The inet and inet6 represent IPv4 and IPv6 addressing respectively.

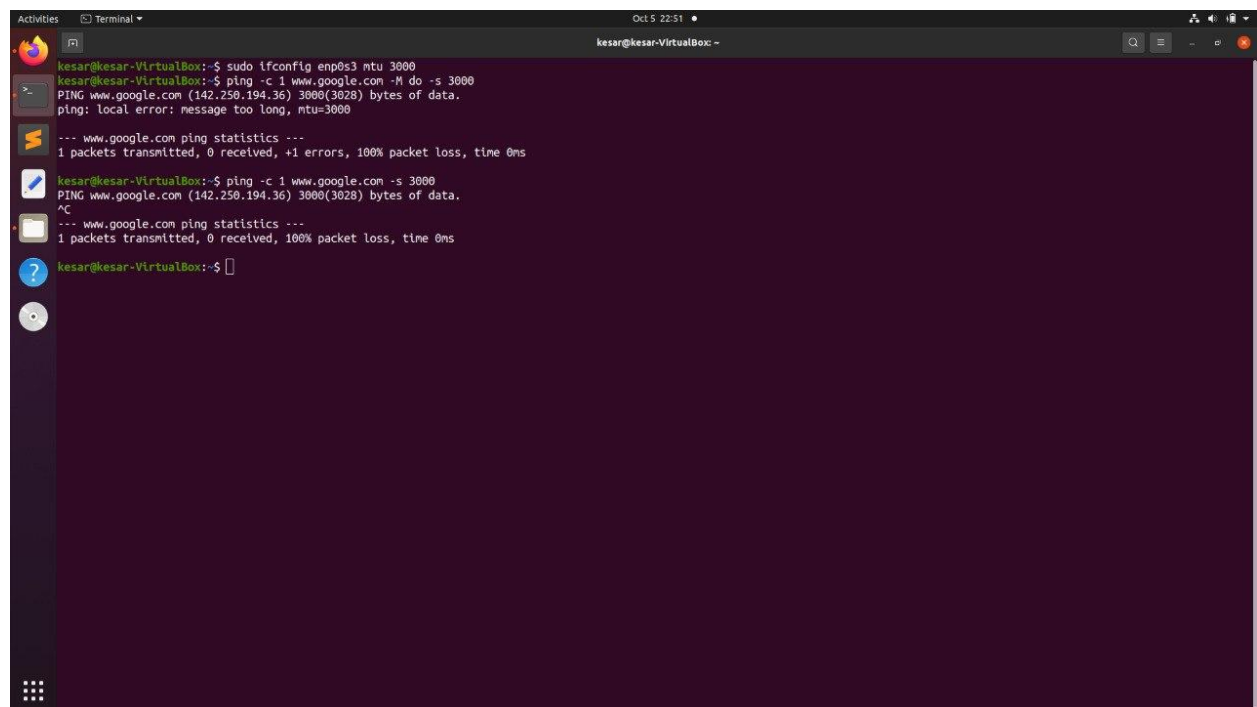
Q3 (b)



The IP address figured out in (a) is different from what is shown on the given webpage. This happens due to the categorization of the IP addresses into public and private.

A private IP address is used to communicate within the same network while the public IP address which used to communicate outside the network. Ifconfig gives us the private IP address.

Q4 (a)



MTU(Maximum Transmission Unit) is the largest packet or frame size specified in bytes that can be sent over a network connection.

MTU 3000 means that we are sending a packet of size 3000 bytes over the network.

Command to test whether we can send a packet of size 3000 bytes to www.google.com:

ping www.google.com -M do -s 3000

First we change the mtu of the ethernet interface using the ifconfig command. Ping command sends ICMP echo request to network hosts. It takes URL or the ip address of the host and sends it a data packet. Using different options we can modify the packet size to be sent.

-s: specifies the number of data bytes to be sent.

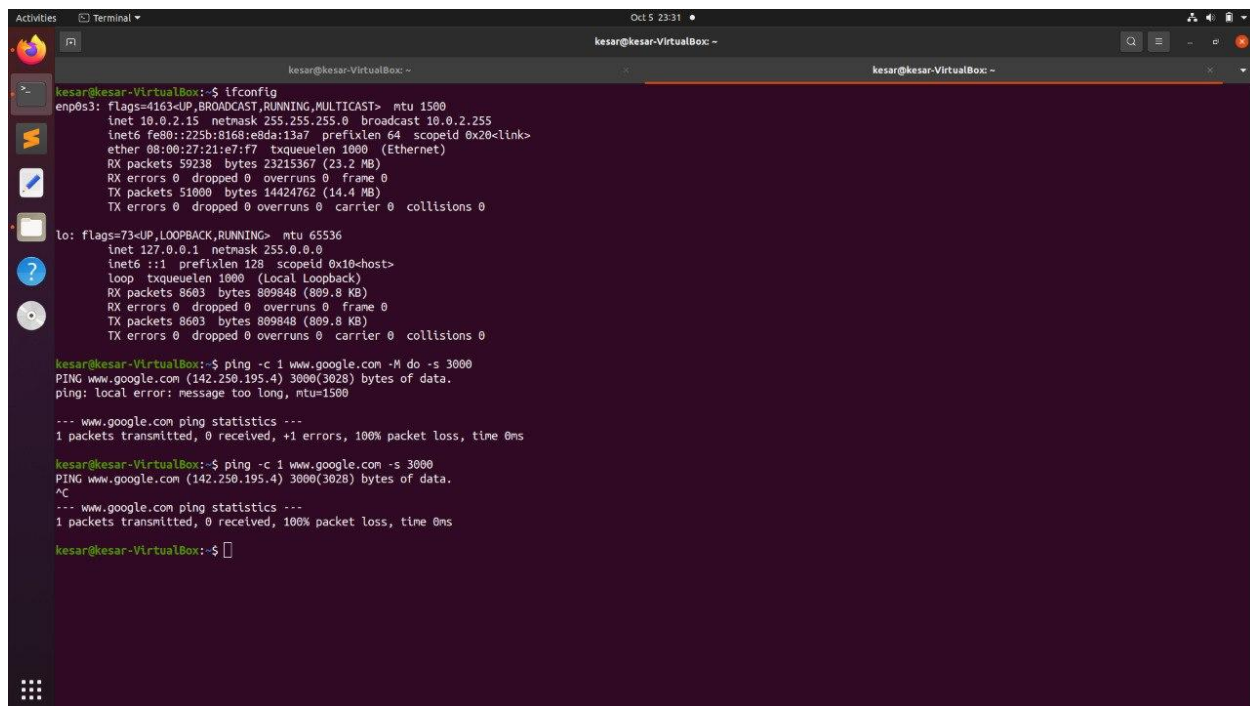
-M do: prohibits the fragmentation of the data packet.

-c: specifies the number of packets to be sent.

Since the packet cannot be fragmented any router that receives the packet will analyze the header and check for the Don't Fragment flag. Since the flag is on and the packet exceeds the MTU (due to the addition of 28 bytes extra header), the router then drops the packet instead of fragmenting it.

Also, a command is run when we are not mentioning the -M do option. But after this too we see a 100% packet loss. This is because even after fragmentation the packet size is too big to be transmitted.

The maximum transmission unit is 552 bytes. $3000 > 552$, and hence we see 100% packet loss.



```
kesar@kesar-VirtualBox:~$ 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::225b:8168:e8da:13a7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:e7:f7 txqueuelen 1000 (Ethernet)
    RX packets 59238 bytes 23215367 (23.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 51000 bytes 14424762 (14.4 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 8603 bytes 809848 (809.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8603 bytes 809848 (809.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kesar@kesar-VirtualBox:~$ ping -c 1 www.google.com -M do -s 3000
PING www.google.com (142.250.195.4) 3000(3028) bytes of data.
ping: local error: message too long, mtu=1500

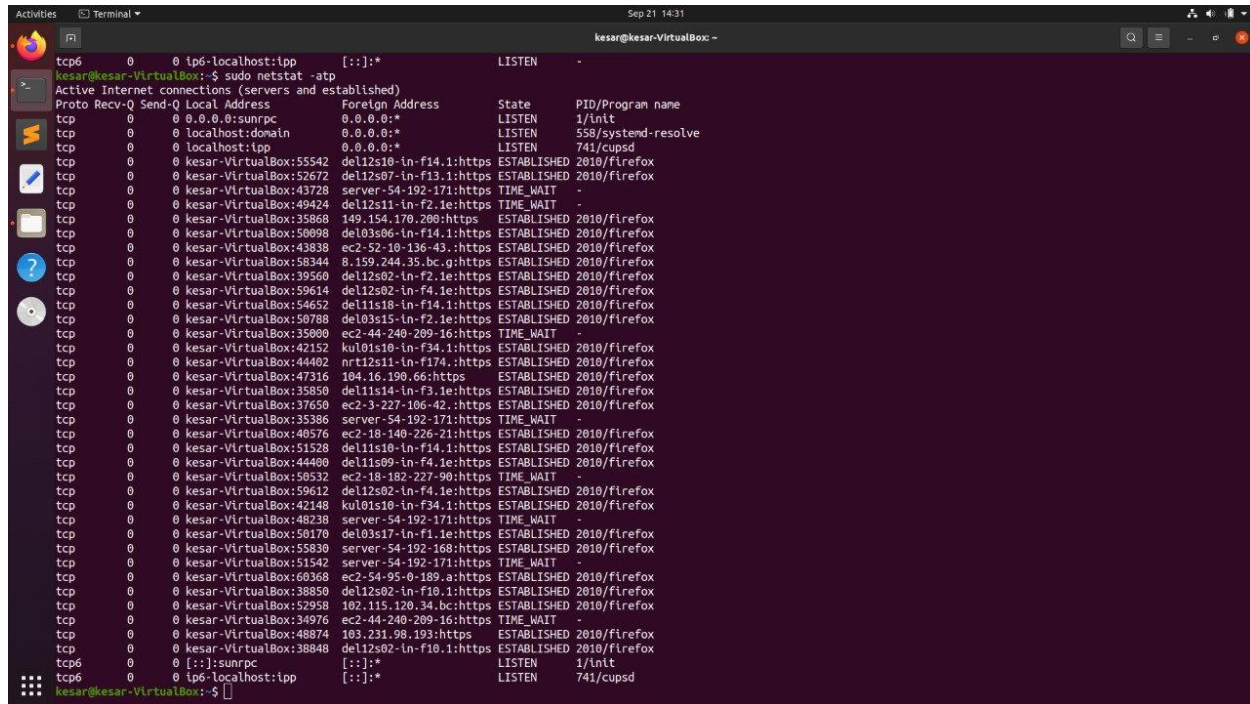
--- www.google.com ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

kesar@kesar-VirtualBox:~$ ping -c 1 www.google.com -s 3000
PING www.google.com (142.250.195.4) 3000(3028) bytes of data.
^C
--- www.google.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

kesar@kesar-VirtualBox:~$
```


In the above screenshot we are not changing the mtu and the reason why we see packet loss is similar to the first case: the packet size is greater than the mtu.

Q4 (b)

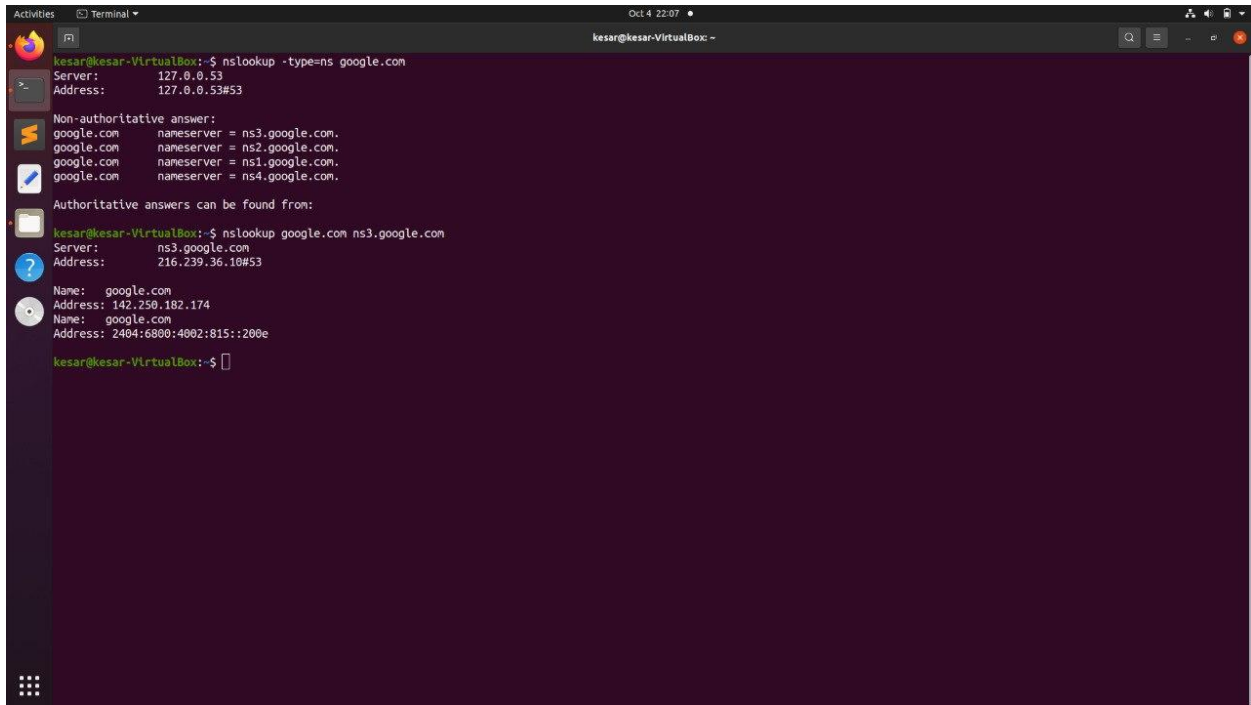


```
Activities Terminal Sep 21 14:31
kesar@kesar-VirtualBox: ~$ sudo netstat -atp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:sunrpc 0.0.0.0:* LISTEN 1/init
tcp 0 0 localhost:domain 0.0.0.0:* LISTEN 558/systemd-resolve
tcp 0 0 localhost:ipp 0.0.0.0:* LISTEN 741/cupsd
tcp 0 0 kesar-VirtualBox:55542 del12s10-ln-f14.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:52672 del12s07-ln-f13.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:43728 server-54-192-171:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:49424 del12s11-ln-f2.1e:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:35868 149.154.170.200:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:50098 del03s06-ln-f14.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:43838 ec2-52-10-136-43:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:58344 8.159.244.35.bc.gs:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:39560 del12s02-ln-f2.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:59614 del12s02-ln-f4.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:54652 del11s18-ln-f14.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:50788 del03s15-ln-f2.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:35000 ec2-44-240-209-16:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:42152 kul01s10-ln-f34.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:44402 nrt12s11-ln-f174:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:47316 104.16.190.66:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:35050 del11s14-ln-f3.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:37650 ec2-3-227-106-42:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:35386 server-54-192-171:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:40576 ec2-18-140-226-21:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:51528 del11s10-ln-f14.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:44400 del11s09-ln-f4.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:50532 ec2-18-182-227-90:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:59612 del12s02-ln-f4.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:42148 kul01s10-ln-f34.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:48238 server-54-192-171:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:50170 del03s17-ln-f1.1e:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:55830 server-54-192-168:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:51542 server-54-192-171:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:60368 ec2-54-95-0-189.a:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:38850 del12s02-ln-f10.1:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:52958 102.115.120.34.bc:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:34976 ec2-44-240-209-16:https TIME_WAIT -
tcp 0 0 kesar-VirtualBox:48874 103.231.98.193:https ESTABLISHED 2010/firefox
tcp 0 0 kesar-VirtualBox:38848 del12s02-ln-f10.1:https ESTABLISHED 2010/firefox
tcp6 0 0 :::sunrpc :::* LISTEN 1/init
tcp6 0 0 ip6:localhost:ipp :::* LISTEN 741/cupsd
kesar@kesar-VirtualBox: ~$
```

netstat command prints information about the Linux networking subsystem. The required command is 'netstat -atp'.

-a lists all the currently active connections. -t filters out all the tcp connections and -p shows the pid of the program to which each socket belongs. We use sudo so that we get the root privileges and all the connections are shown.

Q5 (a)

A screenshot of a Linux terminal window titled 'kesar@kesar-VirtualBox: ~'. The terminal shows the output of the command 'nslookup -type=ns google.com'. The output includes the server address (127.0.0.53), a list of non-authoritative name servers for google.com (ns3.google.com, ns2.google.com, ns1.google.com, ns4.google.com), and a list of authoritative name servers (ns3.google.com) with their IP addresses (142.250.182.174 and 2404:6800:4002:815::200e). The terminal prompt is 'kesar@kesar-VirtualBox:~\$'.

nslookup is the command that queries the name servers interactively. Using this command we can get the authoritative result. The option `-type=ns` helps get all name servers that are authoritative for that domain.

Thus, in the screenshot attached '`nslookup -type=ns google.com`' gives all its name servers. By default, nslookup queries the same DNS the system is configured to use for all network operations. We can specify a custom DNS to query. The command '`nslookup google.com ns3.google.com`' provides us with the authoritative answer to our previous query of google.com

Q5 (b)

```
Select kesar@LAPTOP-T2VER417: /mnt/c/Users/KESAR SHRIVASTAVA

kesar@LAPTOP-T2VER417:/mnt/c/Users/KESAR SHRIVASTAVA$ nslookup -debug www.google.com
Server:      202.56.215.55
Address:     202.56.215.55#53

-----
QUESTIONS:
  www.google.com, type = A, class = IN
ANSWERS:
-> www.google.com
   internet address = 216.58.196.196
   ttl = 40
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Non-authoritative answer:
Name:   www.google.com
Address: 216.58.196.196
-----
QUESTIONS:
  www.google.com, type = AAAA, class = IN
ANSWERS:
-> www.google.com
   has AAAA address 2404:6800:4007:806::2004
   ttl = 40
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Name:   www.google.com
Address: 2404:6800:4007:806::2004
```

As seen from the screenshot, the TTL(time to live) is **40 seconds** so the entry would expire by 40 Seconds. Time to live (TTL) refers to the amount of time that a packet is set to exist inside a network before being discarded by a router.

Below screenshot shows TTL for www.google.com using authoritative DNS server

```
Select kesar@LAPTOP-T2VER417: /mnt/c/Users/KESAR SHRIVASTAVA

kesar@LAPTOP-T2VER417:/mnt/c/Users/KESAR SHRIVASTAVA$ nslookup -debug www.google.com ns1.google.com
Server:      ns1.google.com
Address:     216.239.32.10#53

-----
QUESTIONS:
  www.google.com, type = A, class = IN
ANSWERS:
-> www.google.com
   internet address = 216.58.221.36
   ttl = 300
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Name:   www.google.com
Address: 216.58.221.36
-----
QUESTIONS:
  www.google.com, type = AAAA, class = IN
ANSWERS:
-> www.google.com
   has AAAA address 2404:6800:4002:806::2004
   ttl = 300
AUTHORITY RECORDS:
ADDITIONAL RECORDS:
-----
Name:   www.google.com
Address: 2404:6800:4002:806::2004

kesar@LAPTOP-T2VER417:/mnt/c/Users/KESAR SHRIVASTAVA$
```

TTL: 300 seconds

Q6 (a)

```
C:\Users\KESAR SHRIVASTAVA>tracert www.iiith.ac.in

Tracing route to www.iiit.ac.in [196.12.53.50]
over a maximum of 30 hops:

  1    2 ms    2 ms    <1 ms  192.168.1.1
  2    5 ms    6 ms    5 ms  182.78.219.41
  3   48 ms   46 ms   47 ms  116.119.61.117
  4   46 ms   53 ms   46 ms  49.44.220.188
  5    *      *      *      Request timed out.
  6   56 ms   57 ms   56 ms  115.242.184.26.static.jio.com [115.242.184.26]
  7   62 ms   62 ms   62 ms  196.12.34.76
  8   63 ms   63 ms   65 ms  196.12.53.50

Trace complete.
```

There are 8 intermediate hosts. 7 intermediate hosts if we ignore the Asterix host.

The IP address and average latency to each intermediate hosts is:

1. 192.168.1.1 $(2+2+1)/3$ ms = 1.67 ms
2. 182.78.219.41 $(5+6+5)/3$ ms = 5.33 ms
3. 116.119.61.117 $(48+46+47)/3$ ms = 47 ms
4. 49.44.220.188 $(46+53+46)/3$ ms = 48.33 ms
6. 115.242.184.26 $(56+57+56)/3$ ms = 56.33 ms
7. 196.12.34.76 $(62+62+62)/3$ ms = 62 ms
8. 196.12.53.50 $(63+63+65)/3$ ms = 63.67 ms

Q6 (b)

The image shows a terminal window with a dark background. The title bar at the top reads "Activities" on the left, "Terminal" in the center, and "Oct 5 19:06" on the right. The terminal content shows a user named "kesar" at a prompt "kesar@kesar-VirtualBox: ~" executing a series of ping commands to the IP address 196.12.53.50. The first command is "ping -c 100 www.iitih.ac.in". The output consists of 100 lines, each showing the result of a single ping. Each line starts with "64 bytes from 196.12.53.50 (196.12.53.50):" followed by the sequence number, TTL, and time. The times vary slightly, ranging from approximately 64.0 ms to 74.2 ms. The terminal window has a sidebar on the left with icons for various applications, and a top bar with search, window management, and system status icons.

```
kesar@kesar-VirtualBox: ~$ ping -c 100 www.iitih.ac.in
PING www.iitih.ac.in (196.12.53.50) 56(84) bytes of data:
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=1 ttl=58 time=66.5 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=2 ttl=58 time=65.0 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=3 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=4 ttl=58 time=65.2 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=5 ttl=58 time=64.0 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=6 ttl=58 time=64.5 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=7 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=8 ttl=58 time=74.2 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=9 ttl=58 time=107 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=10 ttl=58 time=64.9 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=11 ttl=58 time=66.0 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=12 ttl=58 time=74.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=13 ttl=58 time=70.0 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=14 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=15 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=16 ttl=58 time=65.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=17 ttl=58 time=64.6 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=18 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=19 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=20 ttl=58 time=64.6 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=21 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=22 ttl=58 time=68.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=23 ttl=58 time=65.0 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=24 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=25 ttl=58 time=65.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=26 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=27 ttl=58 time=72.3 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=28 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=29 ttl=58 time=65.3 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=30 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=31 ttl=58 time=64.9 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=32 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=33 ttl=58 time=69.6 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=34 ttl=58 time=64.5 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=35 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=36 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=37 ttl=58 time=66.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=38 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=39 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=40 ttl=58 time=68.7 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=41 ttl=58 time=65.7 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=42 ttl=58 time=67.7 ms
64 bytes from 196.12.53.50 (196.12.53.50): icmp_seq=43 ttl=58 time=64.5 ms
```

The screenshot shows a terminal window titled "Terminal" with the command prompt "kesar@kesar-VirtualBox: ~". The terminal output displays a series of network statistics for a connection to 196.12.53.50, followed by a ping test to www.lit.ac.in.

```
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=61 ttl=58 time=63.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=62 ttl=58 time=71.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=63 ttl=58 time=64.9 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=64 ttl=58 time=63.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=65 ttl=58 time=65.0 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=66 ttl=58 time=63.9 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=67 ttl=58 time=64.5 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=68 ttl=58 time=63.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=69 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=70 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=71 ttl=58 time=64.9 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=72 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=73 ttl=58 time=65.6 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=74 ttl=58 time=65.5 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=75 ttl=58 time=64.2 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=76 ttl=58 time=64.9 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=77 ttl=58 time=65.4 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=78 ttl=58 time=70.0 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=79 ttl=58 time=89.0 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=80 ttl=58 time=64.2 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=81 ttl=58 time=64.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=82 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=83 ttl=58 time=64.8 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=84 ttl=58 time=64.3 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=85 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=86 ttl=58 time=64.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=87 ttl=58 time=66.1 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=88 ttl=58 time=65.0 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=89 ttl=58 time=66.8 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=90 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=91 ttl=58 time=65.5 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=92 ttl=58 time=64.7 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=93 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=94 ttl=58 time=64.1 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=95 ttl=58 time=65.8 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=96 ttl=58 time=67.9 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=97 ttl=58 time=64.6 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=98 ttl=58 time=64.4 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=99 ttl=58 time=64.5 ms
64 bytes from 196.12.53.50: (196.12.53.50): icmp_seq=100 ttl=58 time=64.6 ms

--- www.lit.ac.in ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 10161ms
rtt min/avg/max/ndev = 63.576/66.129/106.897/5.180 ms
kesar@kesar-VirtualBox: ~
```

The average latency is 66.129 ms

Q6 (c)

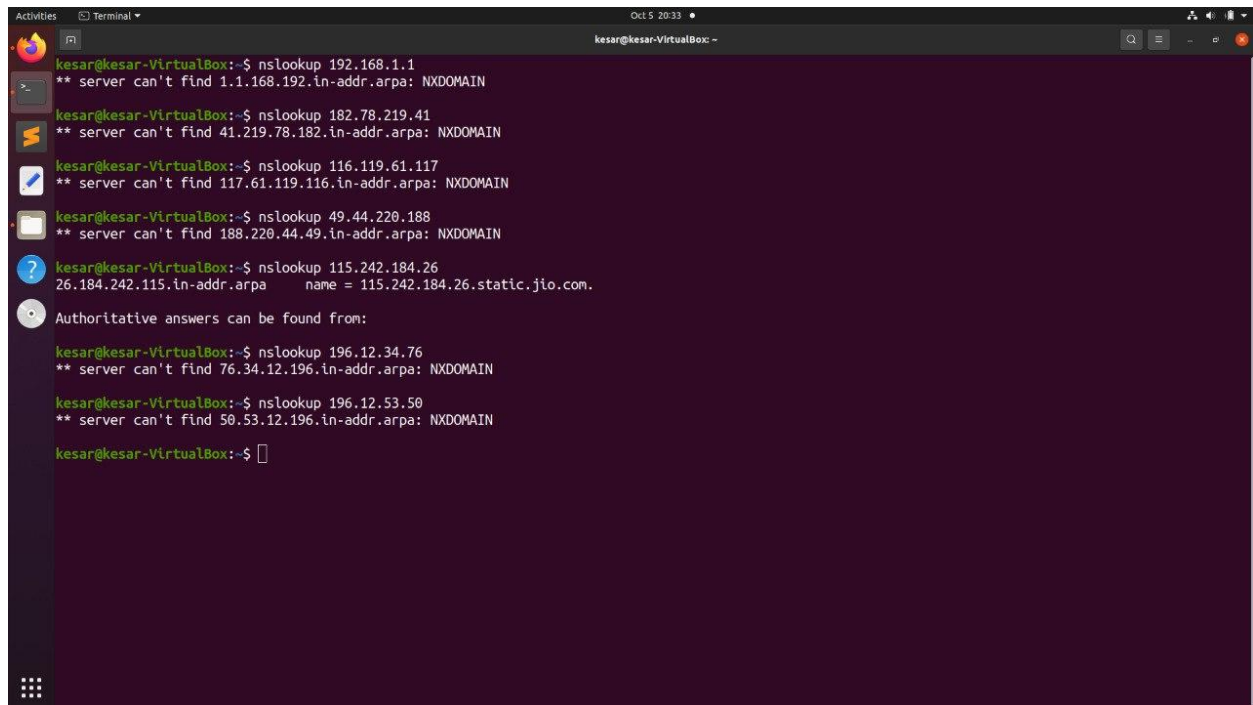
After adding up all the average ping latency of the intermediate hosts, we get: 284.33 ms = (1.67+5.33+47+48.33+56.33+62+63.67) ms. This is greater than the (b) that is 66.129 ms.

We see a greater number here because during traceroute we wait for the timeout response of each of the intermediate host and the average latency we get is the round trip time between our machine and the intermediate host as seen in the traceroute output. It thus doubles up the time. However, ping is just forwarded where we just forward a single packet and hence it is less than the addition.

Q6 (d)

The maximum average latency in (a) part is from the 8th host that is 63.67ms is comparable to (b) part (66.129 ms). The variation in the latency is due to the fact that packet traverses through different nodes for different times. The variation arises because the traffic in the network varies from time to time. This matches to the maximum latency in the traceroute output because the average latency for ping will be dominated by the slowest node in between.

Q6 (e)



```
kesar@kesar-VirtualBox:~$ nslookup 192.168.1.1
** server can't find 1.1.168.192.in-addr.arpa: NXDOMAIN

kesar@kesar-VirtualBox:~$ nslookup 182.78.219.41
** server can't find 41.219.78.182.in-addr.arpa: NXDOMAIN

kesar@kesar-VirtualBox:~$ nslookup 116.119.61.117
** server can't find 117.61.119.116.in-addr.arpa: NXDOMAIN

kesar@kesar-VirtualBox:~$ nslookup 49.44.220.188
** server can't find 188.220.44.49.in-addr.arpa: NXDOMAIN

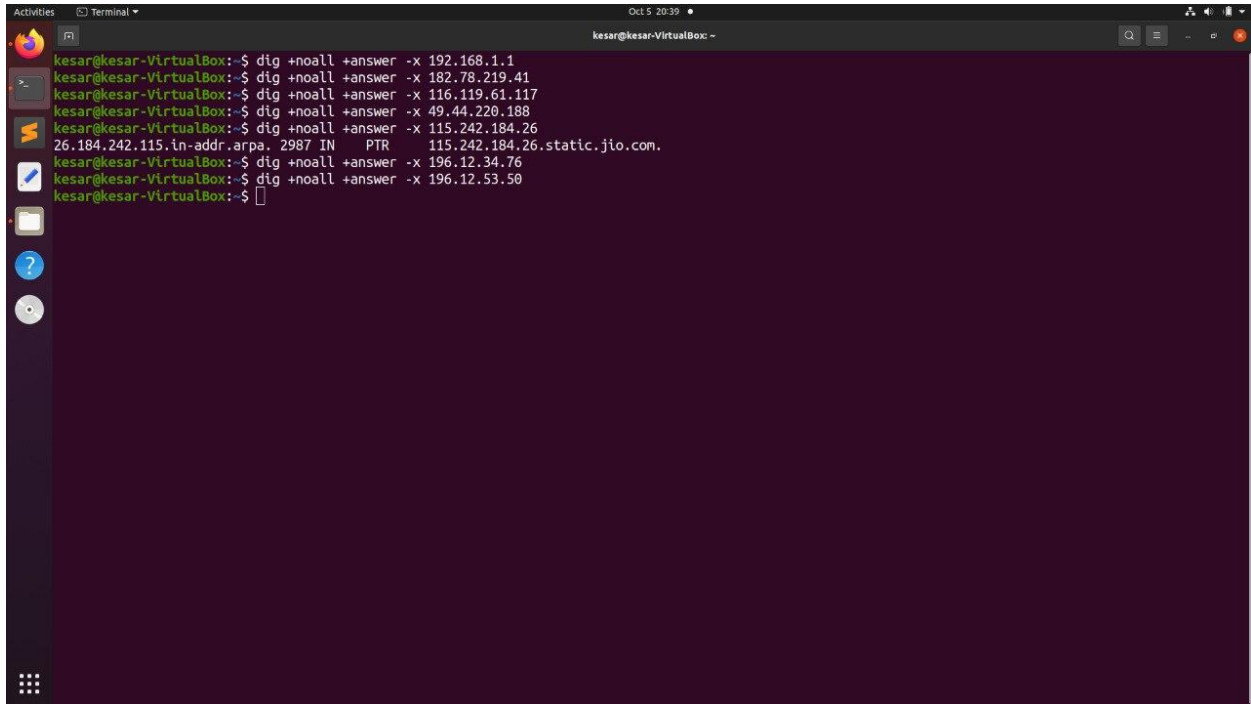
kesar@kesar-VirtualBox:~$ nslookup 115.242.184.26
26.184.242.115.in-addr.arpa      name = 115.242.184.26.static.jio.com.

Authoritative answers can be found from:

kesar@kesar-VirtualBox:~$ nslookup 196.12.34.76
** server can't find 76.34.12.196.in-addr.arpa: NXDOMAIN

kesar@kesar-VirtualBox:~$ nslookup 196.12.53.50
** server can't find 50.53.12.196.in-addr.arpa: NXDOMAIN

kesar@kesar-VirtualBox:~$
```

A screenshot of a terminal window titled 'Terminal' with a dark background. The terminal shows a series of commands and their outputs. The user is logged in as 'kesar' on a machine named 'kesar-VirtualBox'. The commands are: 1. 'dig +noall +answer -x 192.168.1.1' resulting in '192.168.1.1.static.jio.com.'. 2. 'dig +noall +answer -x 182.78.219.41' resulting in '182.78.219.41.static.jio.com.'. 3. 'dig +noall +answer -x 116.119.61.117' resulting in '116.119.61.117.static.jio.com.'. 4. 'dig +noall +answer -x 49.44.220.188' resulting in '49.44.220.188.static.jio.com.'. 5. 'dig +noall +answer -x 115.242.184.26' resulting in '115.242.184.26.static.jio.com.'. 6. 'dig +noall +answer -x 196.12.34.76' resulting in '196.12.34.76.static.jio.com.'. 7. 'dig +noall +answer -x 196.12.53.50' resulting in '196.12.53.50.static.jio.com.'. The terminal window has a sidebar on the left with icons for applications and a top bar showing the date 'Oct 5 20:39'.

Nslookup and dig both can be used to perform the reverse DNS lookups. dig -x is used to perform reverse DNS lookup for dig command.

The hostname in the screenshots comes only for one intermediate IP address that is 115.242.184.26.

In nslookup screenshot the name field gives the hostname of this IP address and in the dig screenshot too 115.242.184.26.static.jio.com is the hostname.

There are not any aliases.

Q7

Ifconfig is a command used to configure kernel-resident network interfaces. 127.0.0.1 is the IP address of one such interface called loopback. It is a virtual network device used to access network services locally.

Ifconfig has an option down that is used to deactivate the driver for the given interface.

Hence the command: sudo ifconfig lo down would deactivate loopback making it unreachable.

Thus, the ping command on this IP address would fail with 100% packet loss.

sudo needs to be added as it lets us have the root user privileges. Without this, the loopback would not get deactivated.

```
Activities Terminal Sep 21 13:54 kesar@kesar-VirtualBox: -
kesar@kesar-VirtualBox:~$ 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::225b:8168:e8da:13a7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:21:e7:f7 txqueuelen 1000 (Ethernet)
    RX packets 66741 bytes 58979011 (58.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39473 bytes 7275011 (7.2 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 8850 bytes 913260 (913.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8850 bytes 913260 (913.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kesar@kesar-VirtualBox:~$ sudo ifconfig lo down
[sudo] password for kesar:
kesar@kesar-VirtualBox:~$ 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 ---
19 packets transmitted, 0 received, 100% packet loss, time 18419ms

kesar@kesar-VirtualBox:~$
```