SUDHIR **SHARMA**

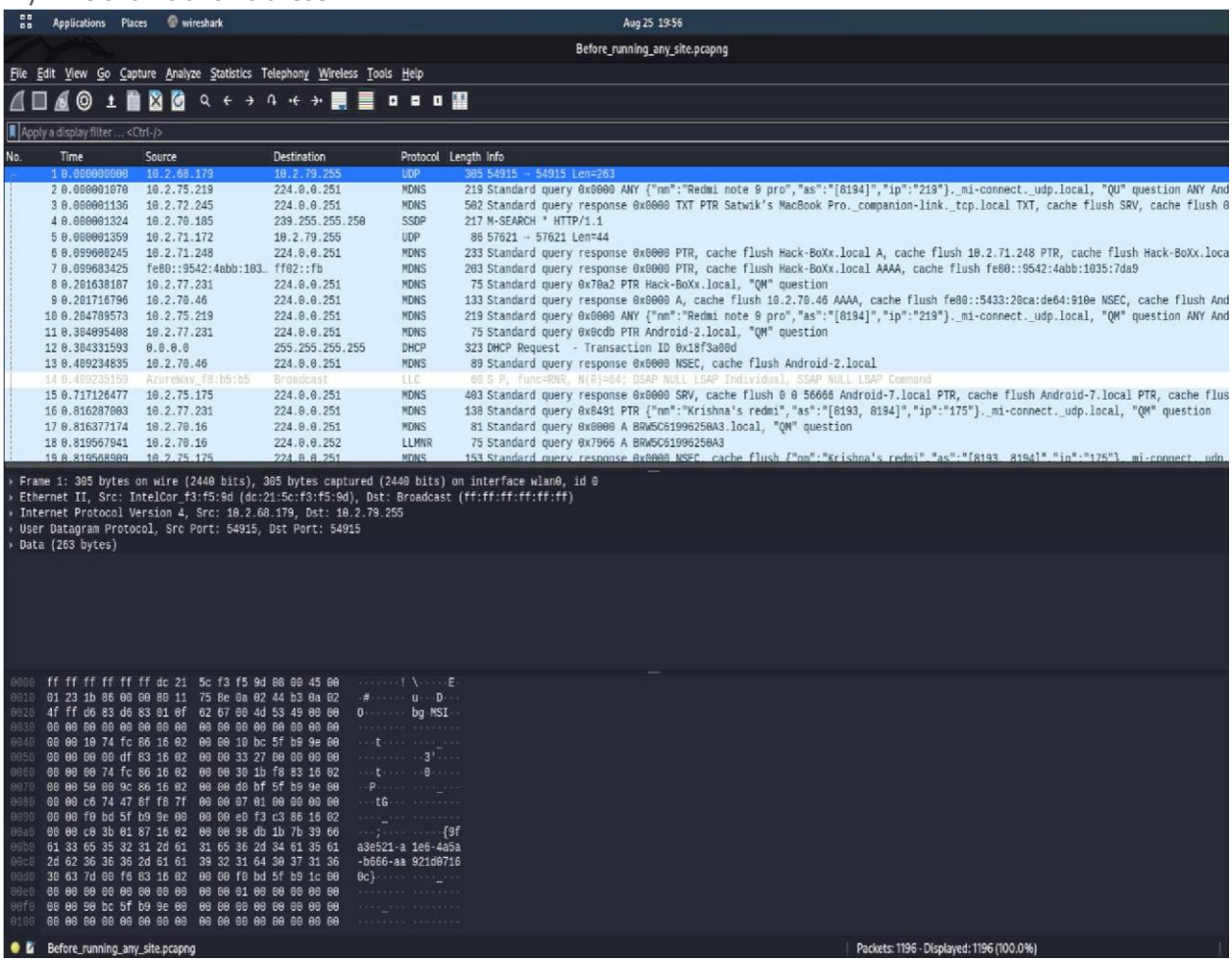
CS301: Computer Networks

12041500

ASSIGNMENT 1: APPLICATION LAYER PROTOCOLS (HTTP &DNS)

Before Running Any Thing

My wire sharks shows these



The Complete file [Link]

Filtering http request shows no information.

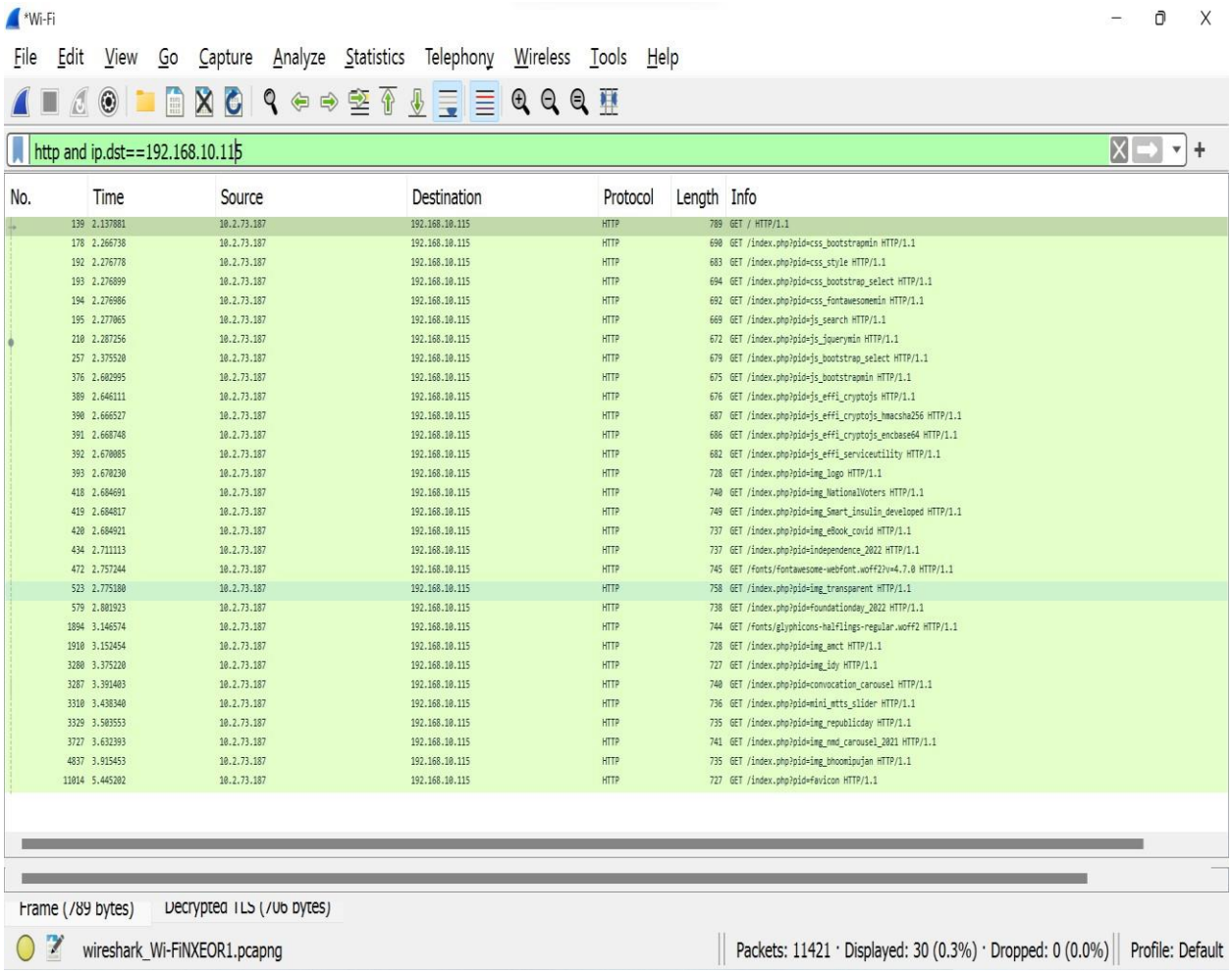


Fig 1- GET Request

Solution of Question 1

To find Number of get request we can also use “http.request.method == "GET"and ip.dst==192.168.10.115”

1 The pcap file name Is given as [12041500_get_request]

2 For filtering of packets we used the ip address of www.iitbhilai.ac.in which we found using the ping command.

```
Microsoft Windows [Version 10.0.22000.856]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sudhir Sharma>ping iitbhilai.ac.in

Pinging iitbhilai.ac.in [192.168.10.115] with 32 bytes of data:
Reply from 192.168.10.115: bytes=32 time=4ms TTL=63
Reply from 192.168.10.115: bytes=32 time=7ms TTL=63
Reply from 192.168.10.115: bytes=32 time=2ms TTL=63
Reply from 192.168.10.115: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.10.115:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 7ms, Average = 4ms

C:\Users\sudhir Sharma>
```

3 From figure 1, we can see that a total of 30 get requests were sent.

4 From figure 1.2, we can see that a total of 30 packets were received out of which the embedded contents are as follows:

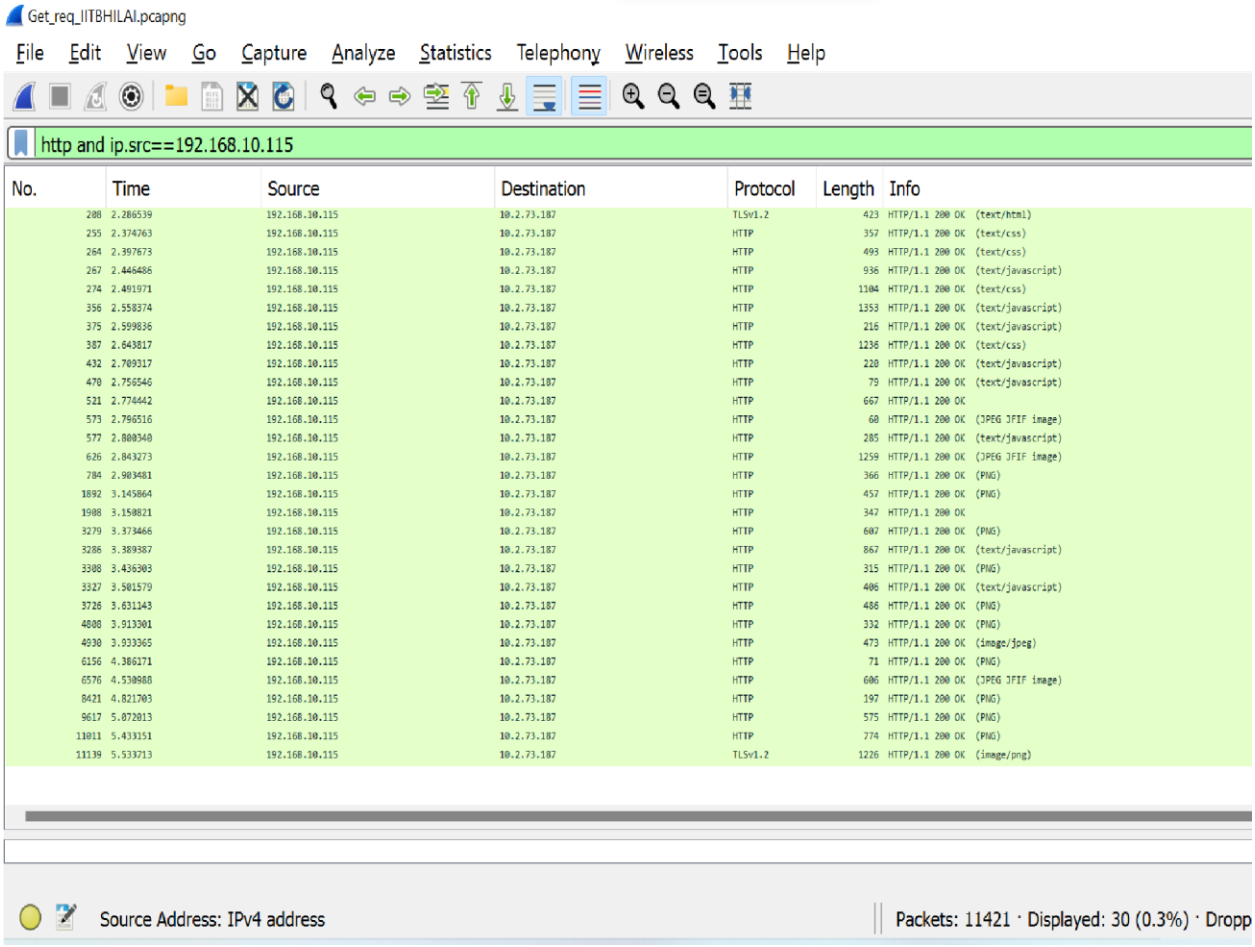


Fig 1.2 Packets received

Out of which

--- 8 text/JavaScript
--- 10 PNG
--- 1 img/png
--- 3 JPEG JFIF image
--- 4 text/css
--- 1 text/html
--- 2 unknown

IO GRAPHS

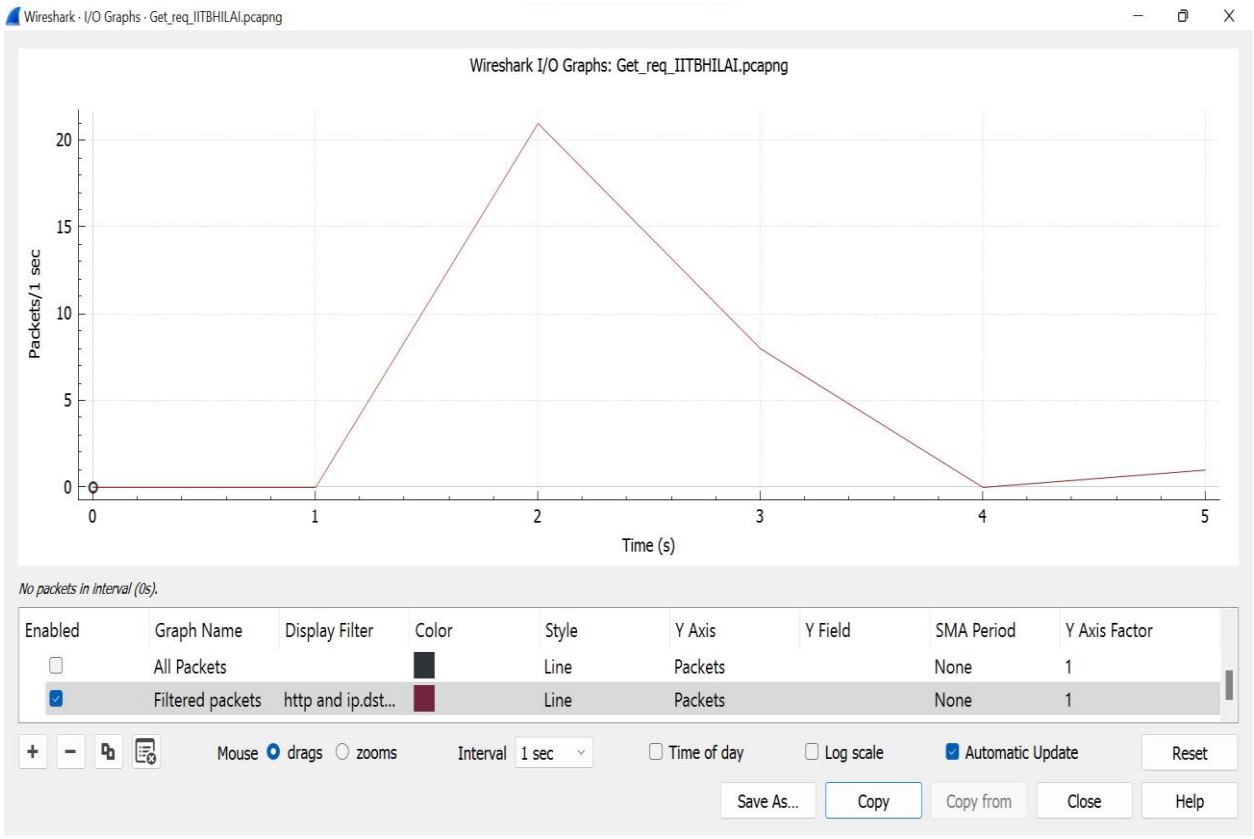


Fig 1.3 Packets Sent

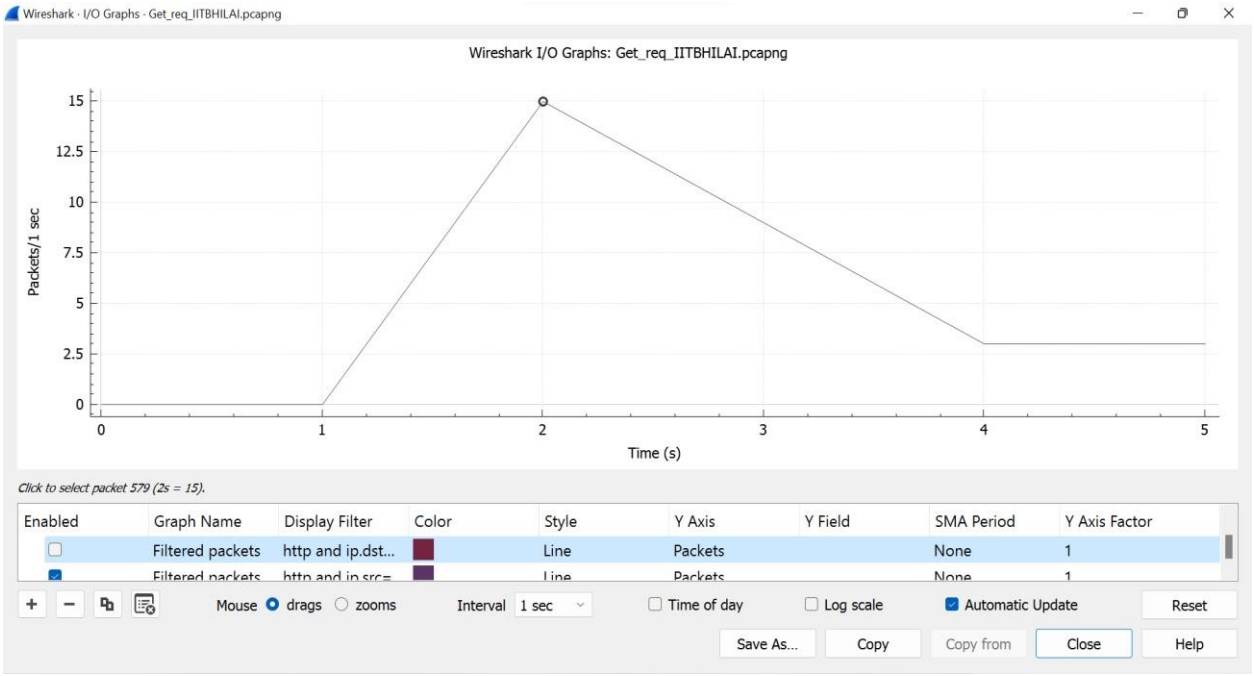


Fig 1.4 Packets Received

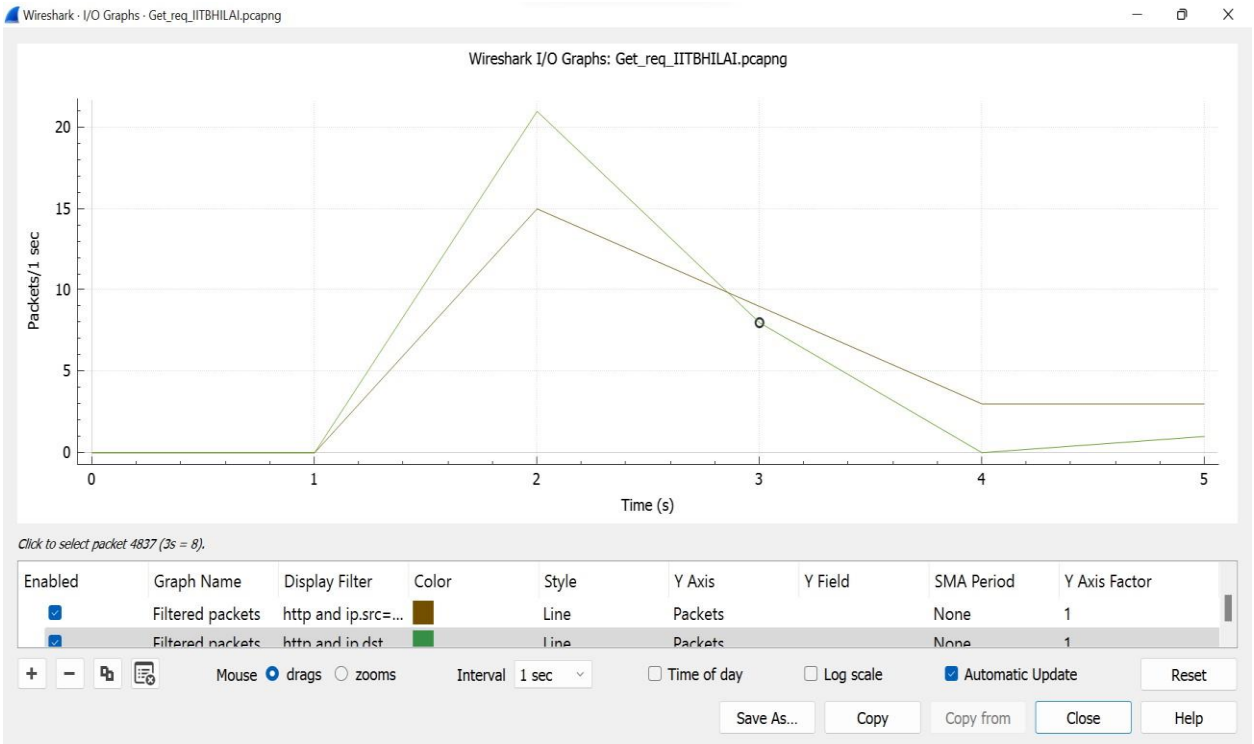


Fig 1.5 Packets Sent VS Packets Received

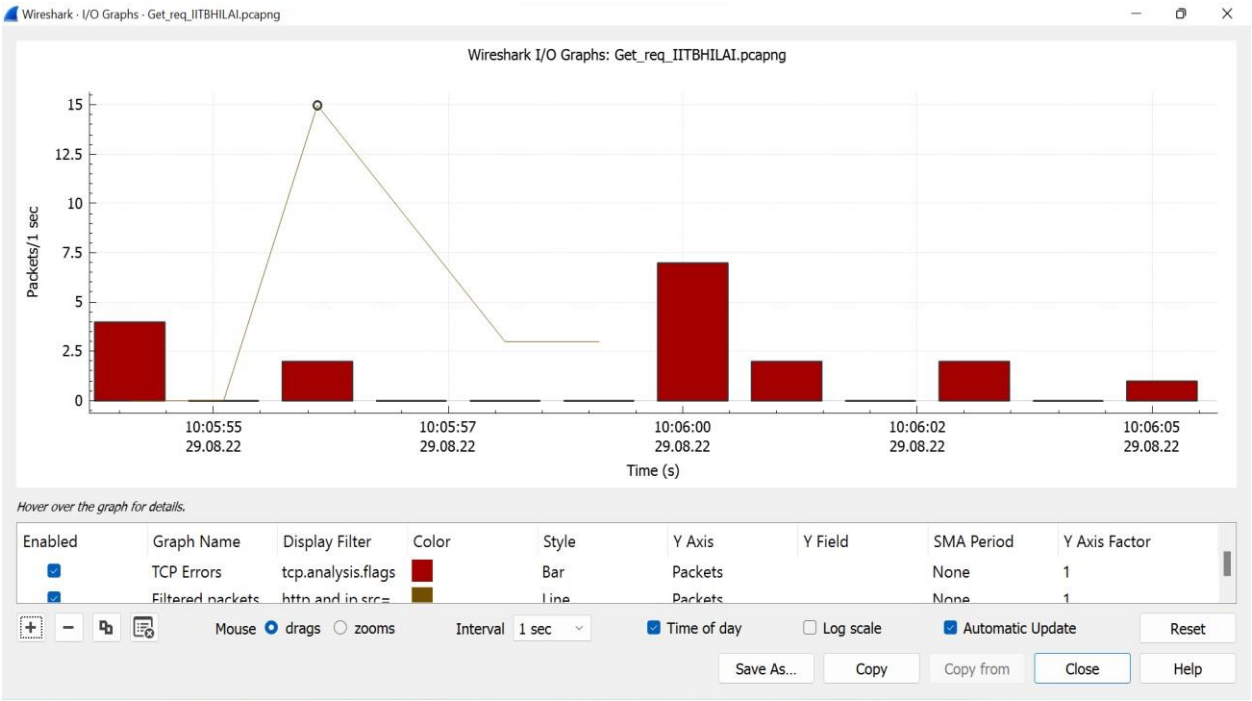
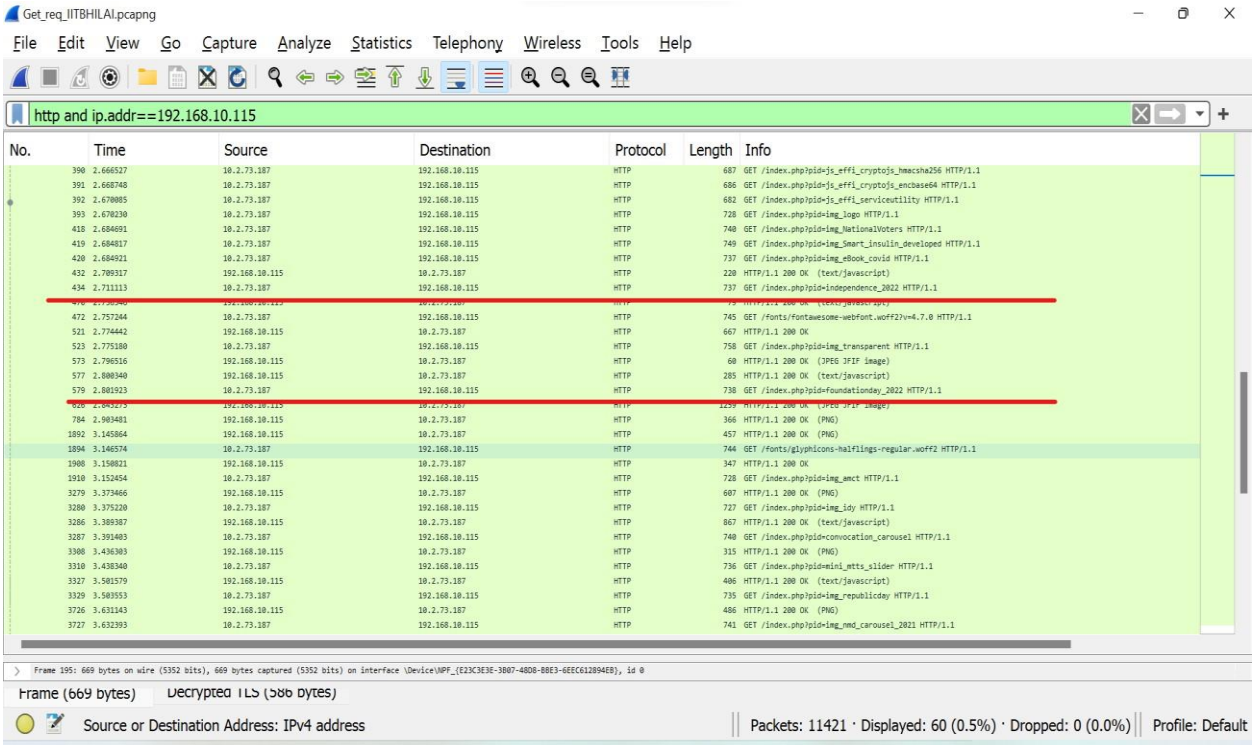


Fig 1.6 TCP Errors vs Packets Received

Using Filter "http and ip.addr==192.168.10.115 " we get 60 Packets

We get different images some of which were shown below



Solution of Question 2

the total amount of data being received in the corresponding HTTP response message is .

10.2.73.187	192.168.10.115	HTTP	789	GET / HTTP/1.1
10.2.73.187	192.168.10.115	HTTP	690	GET /index.php?pid=cs
10.2.73.187	192.168.10.115	HTTP	683	GET /index.php?pid=cs
10.2.73.187	192.168.10.115	HTTP	694	GET /index.php?pid=cs
10.2.73.187	192.168.10.115	HTTP	692	GET /index.php?pid=cs
10.2.73.187	192.168.10.115	HTTP	669	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	672	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	679	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	675	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	676	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	687	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	686	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	682	GET /index.php?pid=js
10.2.73.187	192.168.10.115	HTTP	728	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	740	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	749	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	737	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	737	GET /index.php?pid=in
10.2.73.187	192.168.10.115	HTTP	745	GET /fonts/fontawesom
10.2.73.187	192.168.10.115	HTTP	758	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	738	GET /index.php?pid=fo
10.2.73.187	192.168.10.115	HTTP	744	GET /fonts/glyphicons
10.2.73.187	192.168.10.115	HTTP	728	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	727	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	740	GET /index.php?pid=co
10.2.73.187	192.168.10.115	HTTP	736	GET /index.php?pid=mi
10.2.73.187	192.168.10.115	HTTP	735	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	741	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	735	GET /index.php?pid=im
10.2.73.187	192.168.10.115	HTTP	727	GET /index.php?pid=fa

Total data = 21k

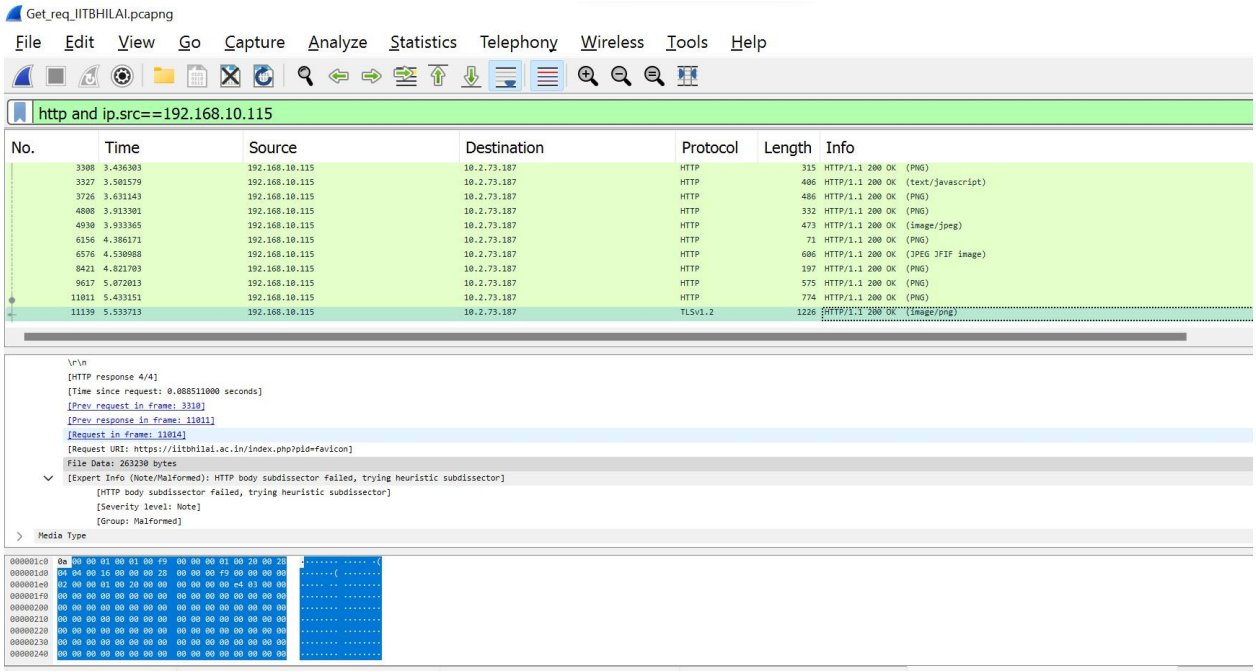
Wireshark · Conversations · Get_req_IITBHILAI.pcapng

Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 9 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.2.73.187	192.168.10.115	30	21 k	30	21 k	0	0	2.137881	3.3073	52 k	0

SOLUTION OF QUESTION 3

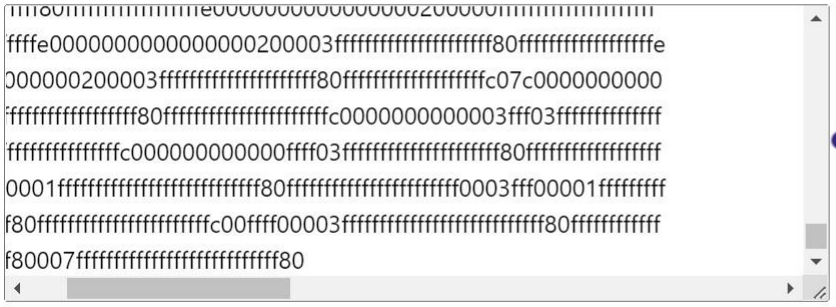
FOR RECONSTRUCTING IMAGE FROM HEX, THE HEX SHOWN IN FIGURE 1.7 IS USED AND THE RECONSTRUCTED IMAGE WE USE HEX EDITOR



HEX DATA

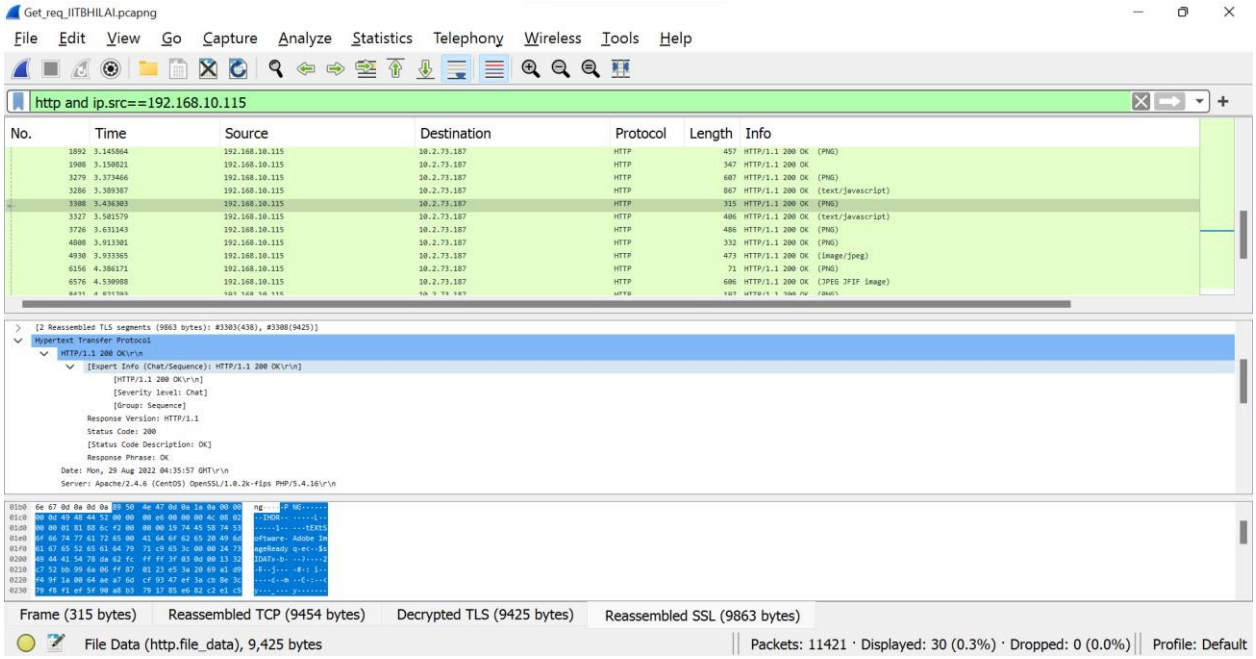
Hexadecimal -> image

Hex string:



Convert

CORRESPONDING IMAGE



HEX DATA

Hexadecimal -> image

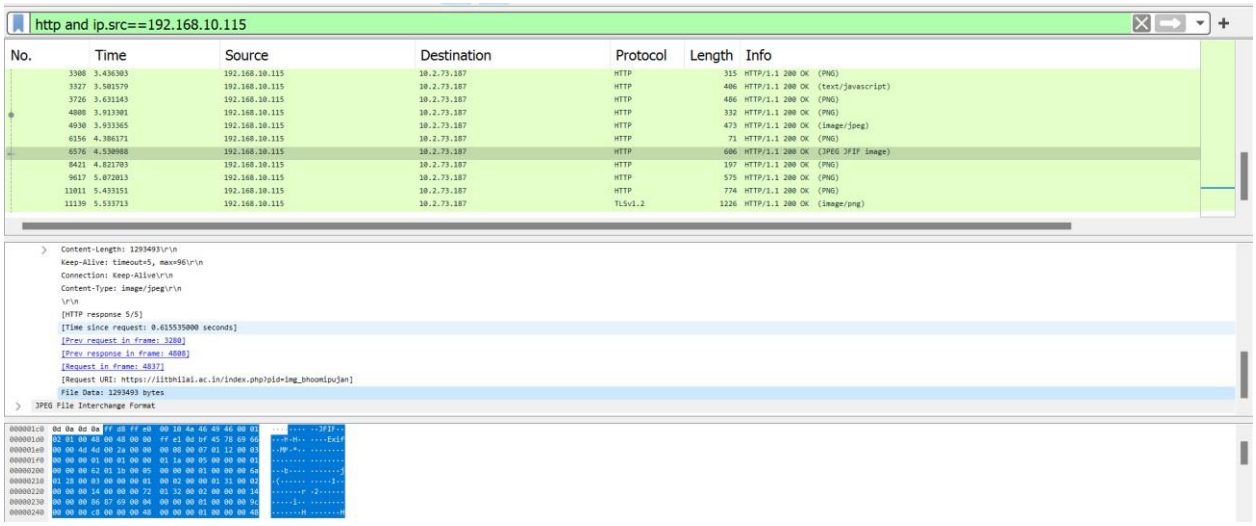
Hex string:

IIT BHILAI

```
2976cd1a0f1db52f6a1d07b2ebd64ff9eec82bc5aa5ab787e52d8cc79a38386
bbf6f66059174abefb2afbe7fc5a2767c9bcc4d0390b438346b832e835de347
e5fcada8061785951cbf1230599e9c5dd5d3a268b193cca1572a6b048156d2
047e3c9f1f4878a381c942f606bd47a0e1b7573971b0d265daf892018f27b15
8969d07856a22ceca9f05add3f76655cb95c090405e29a0982c5645908467b
9b562064af5815b5f8d588bec2763468fcee94c54d447d5da75e87518bc809
bbf92c2c2653af376106dc6d985c26a3f32d1acf9296a54183a62c0d1af7f11f
8e4005706d411cc70000000049454e44ae426082
```

Convert

CORRESPONDING IMAGE



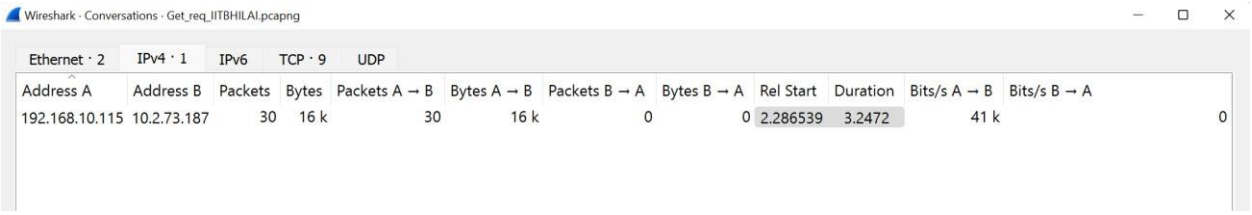
HEX DATA

CORRESPONDING IMAGE

Solution of Question 4

the total amount of data being received when I access https://www.iitbhilai.ac.in is 16k

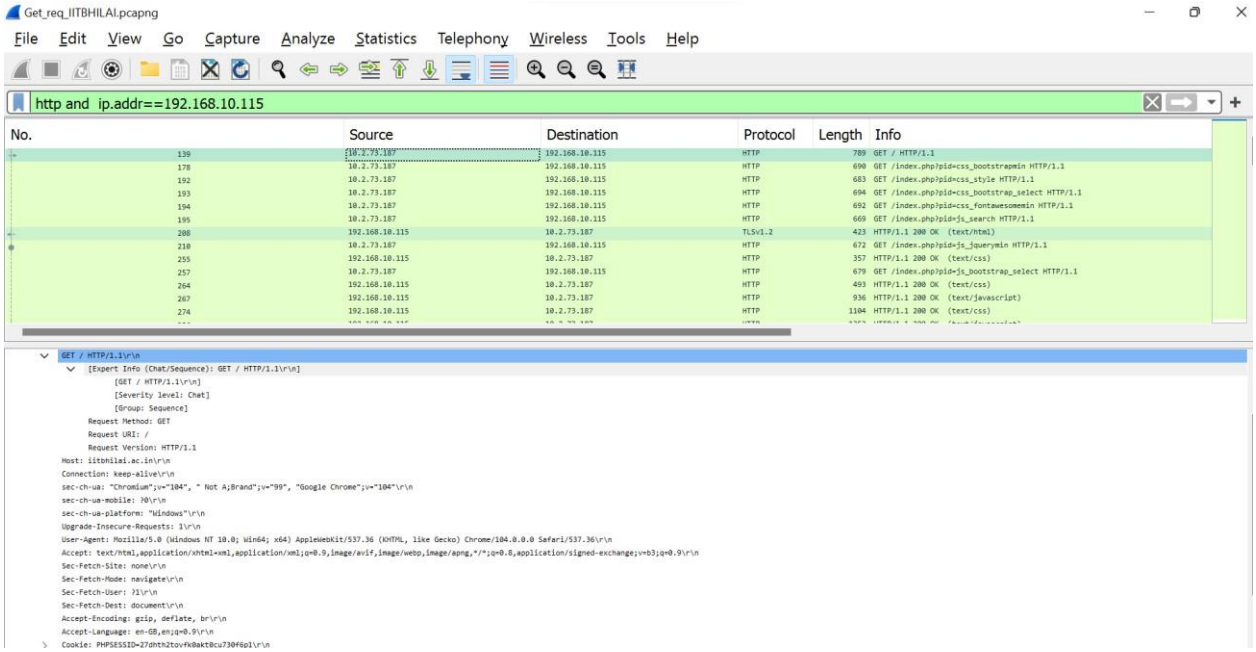
	Source	Destination	Protocol	Length	Info
	192.168.10.115	10.2.73.187	HTTP	493	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	936	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	1104	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	1353	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	216	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	1236	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	220	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	79	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	667	HTTP/1.1 200 OK
	192.168.10.115	10.2.73.187	HTTP	60	HTTP/1.1 200 OK (JP
	192.168.10.115	10.2.73.187	HTTP	285	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	1259	HTTP/1.1 200 OK (JP
	192.168.10.115	10.2.73.187	HTTP	366	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	457	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	347	HTTP/1.1 200 OK
	192.168.10.115	10.2.73.187	HTTP	607	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	867	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	315	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	406	HTTP/1.1 200 OK (te
	192.168.10.115	10.2.73.187	HTTP	486	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	332	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	473	HTTP/1.1 200 OK (im
	192.168.10.115	10.2.73.187	HTTP	71	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	606	HTTP/1.1 200 OK (JP
	192.168.10.115	10.2.73.187	HTTP	197	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	575	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	HTTP	774	HTTP/1.1 200 OK (PN
	192.168.10.115	10.2.73.187	TLSv1.2	1226	HTTP/1.1 200 OK (im



Total data receive = 16k

SOLUTUON OF PROBLEM 5

a) No there is no IF-MODIFIED-SINCE line in the GET message.

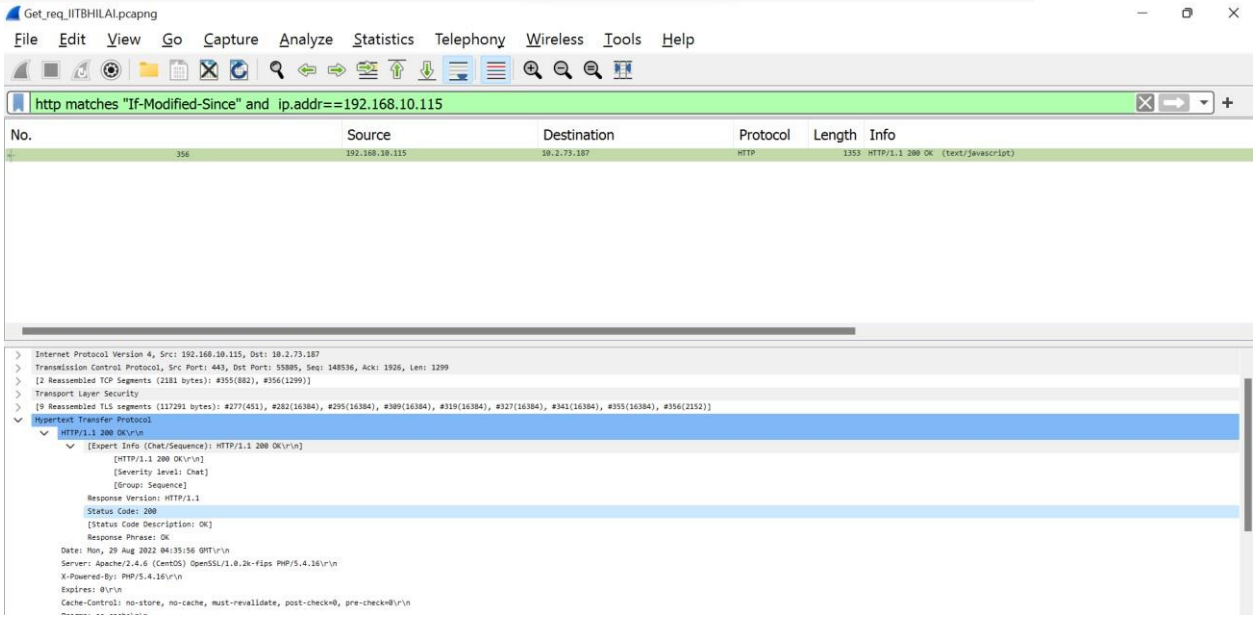


b) The server did explicitly return the contests of the file. Wireshark includes a section titled As “Line-Based Text Data” which shows the server sent back to my browser which is specially What the website showed when I brought it up on my browser.

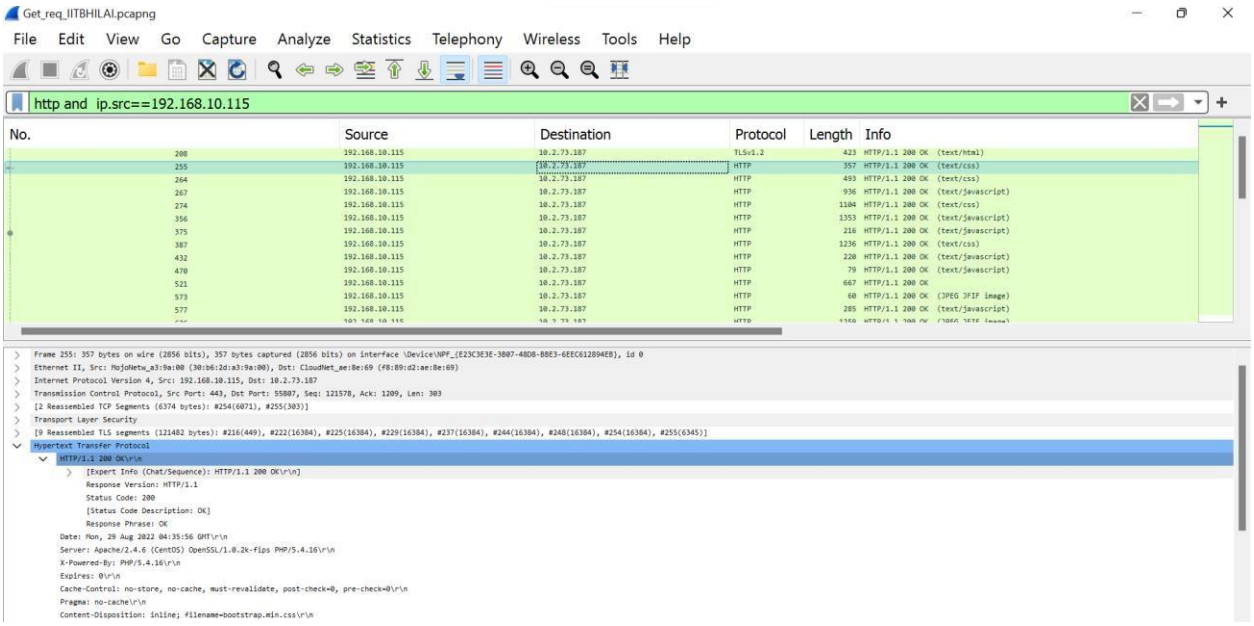
c) The **If-Modified-Since header** is a request-header that is sent to a server as a conditional request. If the contents have changed, the server responds with a 200 status code and the entire requested document is updated.

Yes in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the date and time that I last accessed the webpage

It shows *Status code =200 (ok)* we can just use filter to see the if modified since frame.



Or we can also see that the second HTTP GET it shows the same as shown above.



d) The HTTP status code is “200:Modified” Mon 29 Aug 2022 04:35:56 GMT\r\n

The server did return the contents of the file because the browser simply retrieved the contents from its cache. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead, it simply told my browser to retrieve the old file from its cached memory.

Solution of question 6

I) Throughput when no other traffic in the background is 52k bps (figure 1.10)

File

Name:	C:\Users\sudhir Sharma\Desktop\Get_req_IITBHILAI.pcapng
Length:	27 MB
Hash (SHA256):	174388b83c7eee6a3820983d62b9f1725592ff32352146f4a4d77847237cfe18
Hash (RIPEMD160):	d95fbf8e85d52f6ff08ae042e2267ea7f16369b7
Hash (SHA1):	cb39b98e504b77cf011d6041e8999c6f33ce0be2
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2022-08-29 10:05:54
Last packet:	2022-08-29 10:06:06
Elapsed:	00:00:12

Capture

Hardware:	11th Gen Intel(R) Core(TM) i5-1155G7 @ 2.50GHz (with SSE4.2)
OS:	64-bit Windows 10 (21H2), build 22000
Application:	Dumpcap (Wireshark) 3.6.7 (v3.6.7-0-g4e304d7ec222)

Interfaces

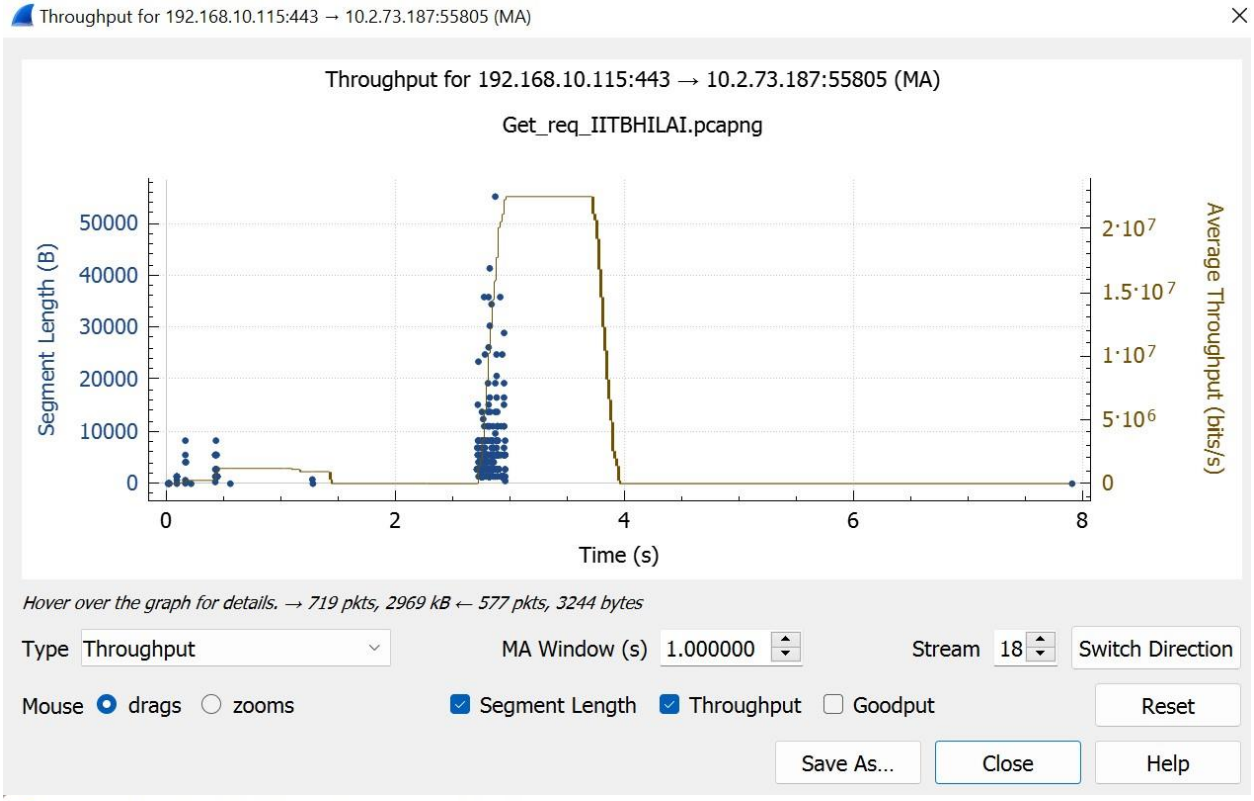
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

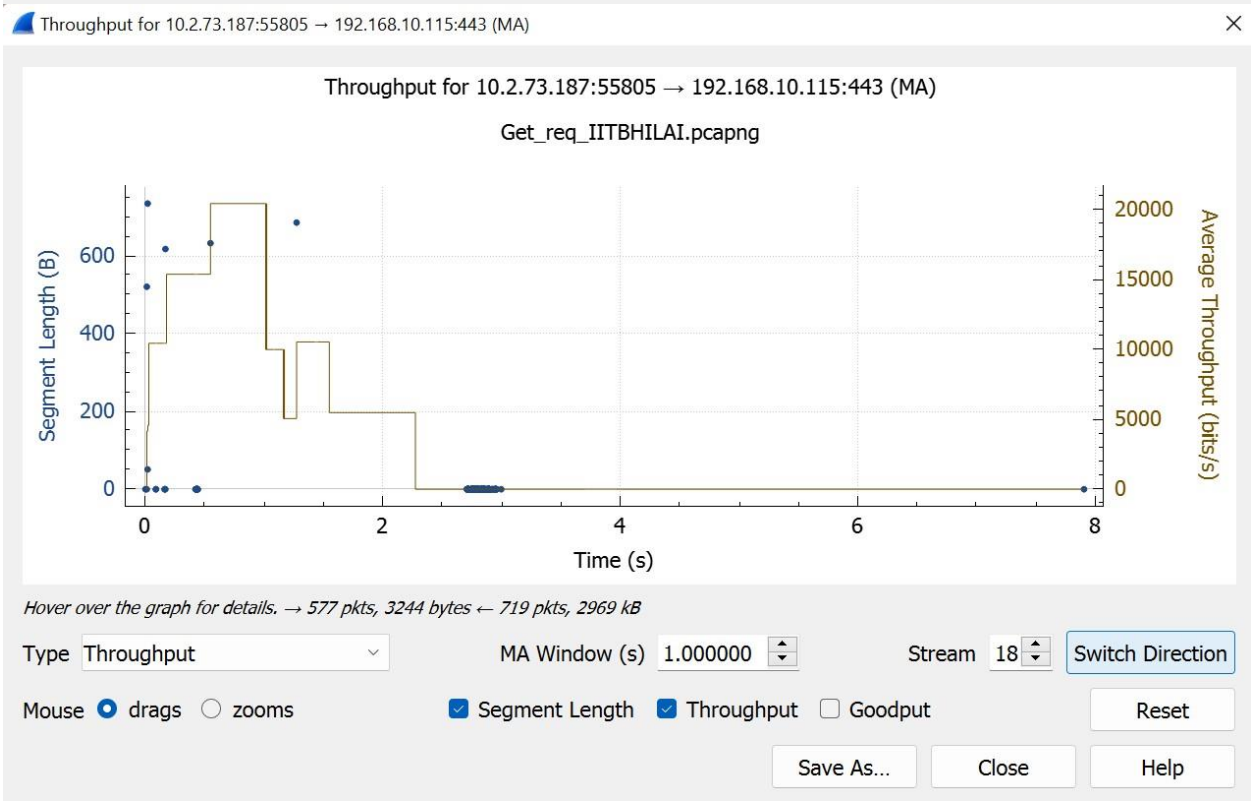
Statistics

Measurement	Captured	Displayed	Marked
Packets	11421	30 (0.3%)	—
Time span, s	12.392	3.307	—
Average pps	921.6	9.1	—
Average packet size, B	2391	717	—
Bytes	27302588	21519 (0.1%)	0
Average bytes/s	2203 k	6506	—
Average bits/s	17 M	52 k	—

Fig 1.10 throughput – no traffic

GRAPHICALLY REPRESENTATION





II) CREATING TRAFFIC (DOWNLOADING LARGE FILES) THROUGHPUT , WHEN LARGE FILE IS DOWNLOADING IN BACKGROUND, IS 20K BPS (THROUGHPUT DECREASES) (FIGURE 1.11)

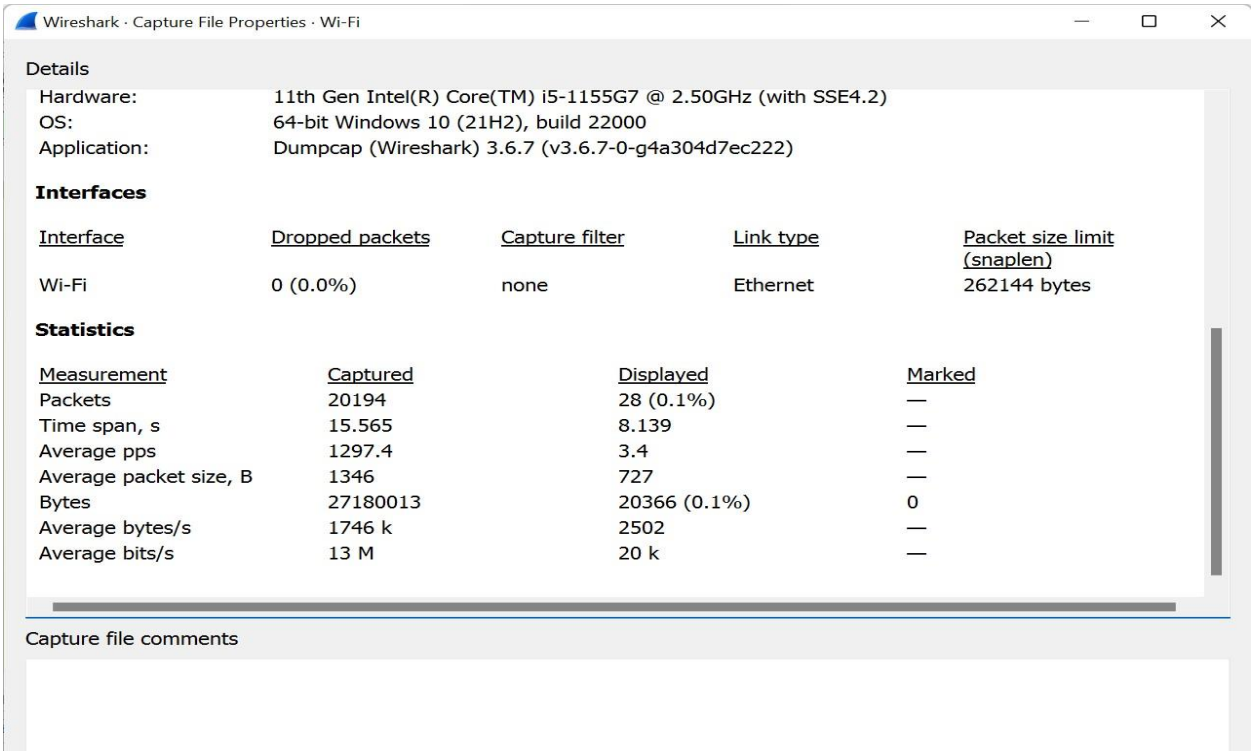
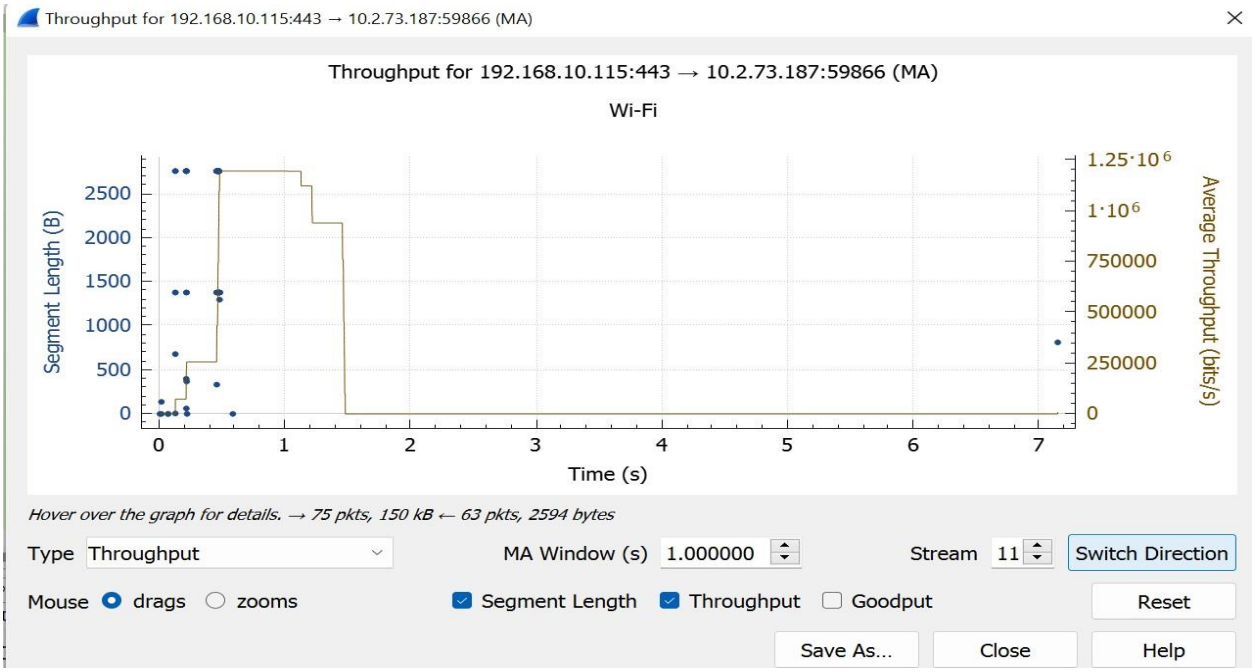


Fig 1.11 throughput –traffic

GRAPHICALLY REPRESENTATION

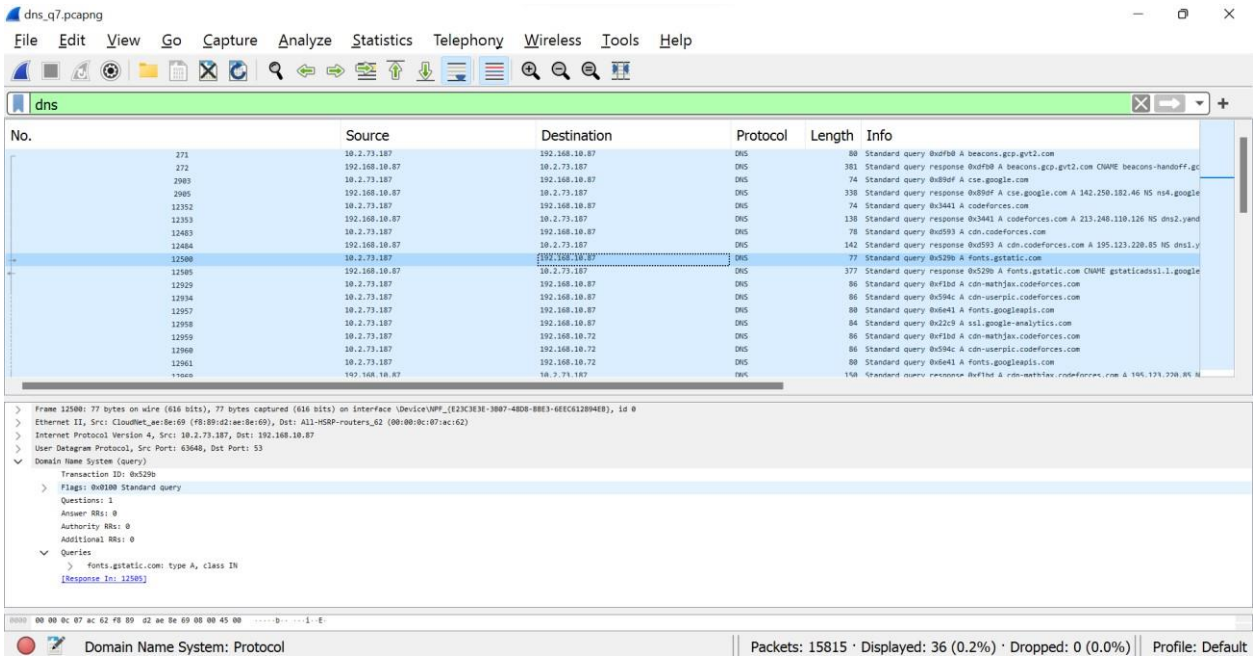


THROUGHPUT FOR 192.168.10.115->10.2.73.187

IN THE ABOVE FIGURES, WE CONSIDER AVERAGE BITS/S AS THROUGHPUT AND THE DISPLAYED COLUMN SHOWS THE THROUGHPUT FOR PACKETS FILTERED FOR WWW.IITBHILAI.AC.IN.

SOLUTION OF PROBLEM 7

I have opened www.codeforces.com for these test.



36 DNS packets have you observed in total.
Domain Name IP table of some of the dns is shown below.
Complete file is named as dns_q7

Domain Name	IP Address
beacons-handoff.gcp.gvt2.com	172.217.160.131
codeforces.com	213.248.110.126
gstaticadssl.l.google.com	142.250.196.35
cdn-mathjax.codeforces.com	195.123.220.85
195.123.220.85	172.217.166.106
ns2.google.com i.ytimg.com	216.239.34.10
.	142.250.67.86
.	.
.	.
.	.
	.

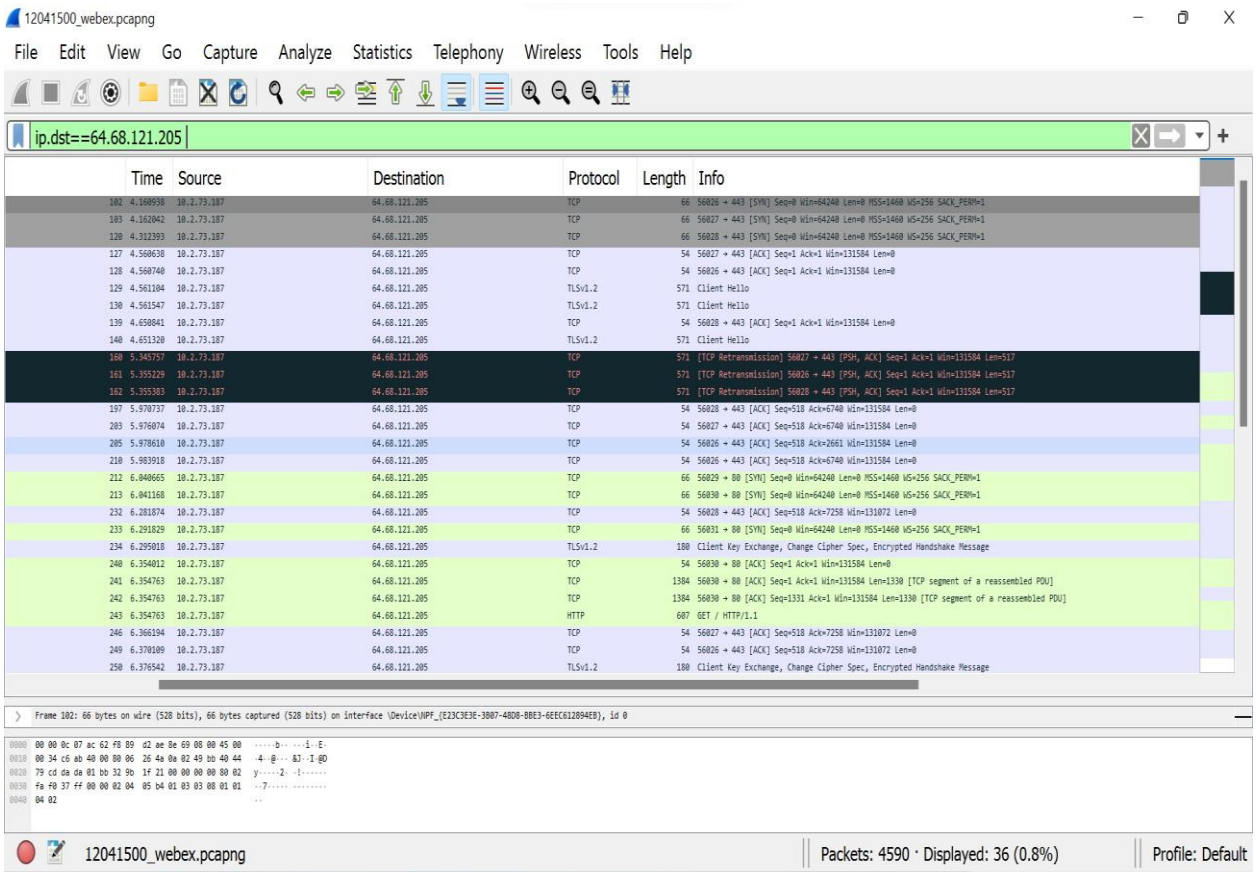
b) yes I can find out the IP of the DNS servers by exploring the DNS packets.

PART B

1)

The website we surf is www.webex.com. The pacp file name is 12041500_webex. To find the loading time of the webpage we look at the arrival time of the first and the last packet and take their difference.

To add time column goto edit -> preferences -> appearance -> column
To display arrival time of packets goto view -> Time Display Format -> Seconds Since Beginning of Capture.



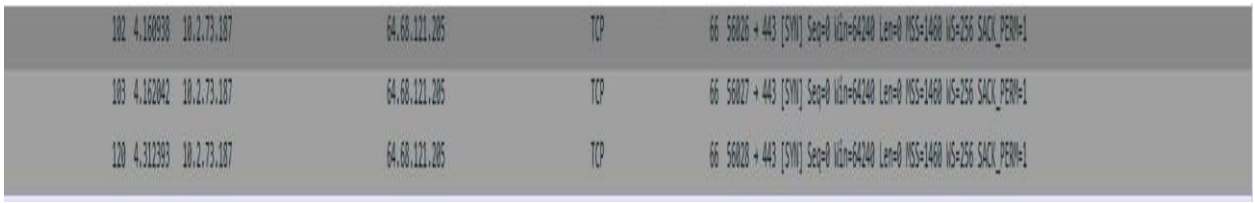


Figure 1.12: Arrival time of first packet

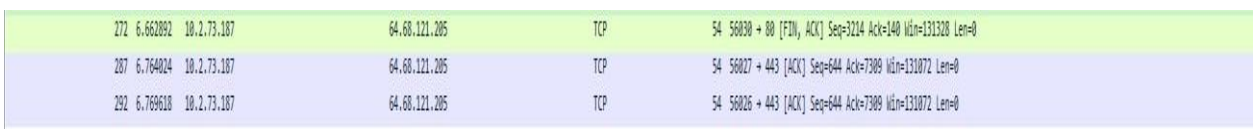
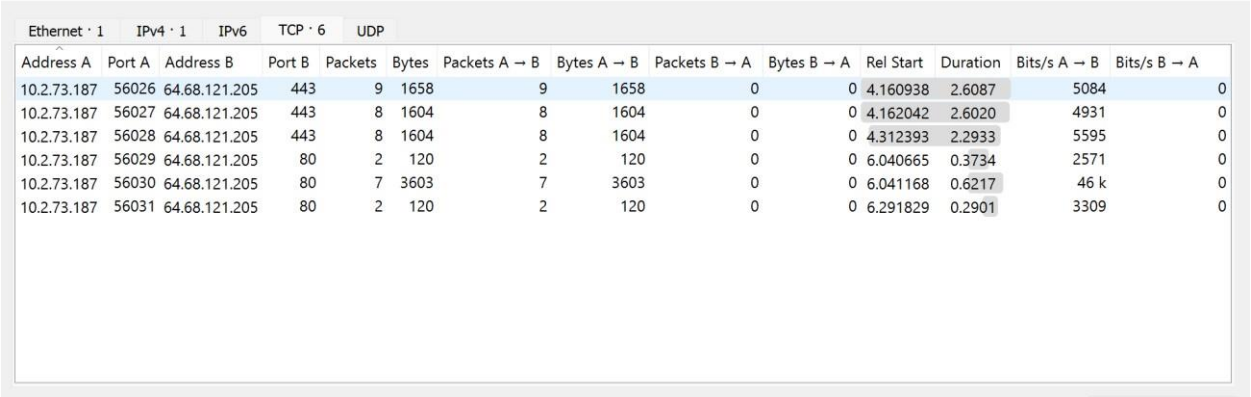


Figure 1.13: Arrival time of last packet

Therefore the loading time= 6.769618-4.160938

= 2.60868 second

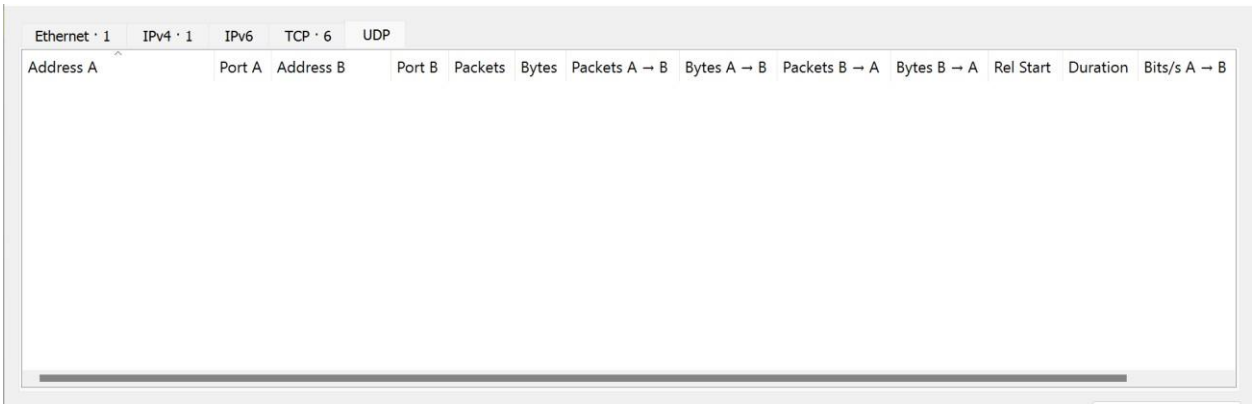
For finding the number of connections that were used to download this webpage we look at statistics → endpoints. There are 6 TCP connections (figure 1.14) and 0 UDP connections (figure 1.15)



Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 6 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
10.2.73.187	56026	64.68.121.205	443	9	1658	9	1658	0	0	4.160938	2.6087	5084	0
10.2.73.187	56027	64.68.121.205	443	8	1604	8	1604	0	0	4.162042	2.6020	4931	0
10.2.73.187	56028	64.68.121.205	443	8	1604	8	1604	0	0	4.312393	2.2933	5595	0
10.2.73.187	56029	64.68.121.205	80	2	120	2	120	0	0	6.040665	0.3734	2571	0
10.2.73.187	56030	64.68.121.205	80	7	3603	7	3603	0	0	6.041168	0.6217	46 k	0
10.2.73.187	56031	64.68.121.205	80	2	120	2	120	0	0	6.291829	0.2901	3309	0

Fig 1.14 TCP connections



Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 6 | UDP

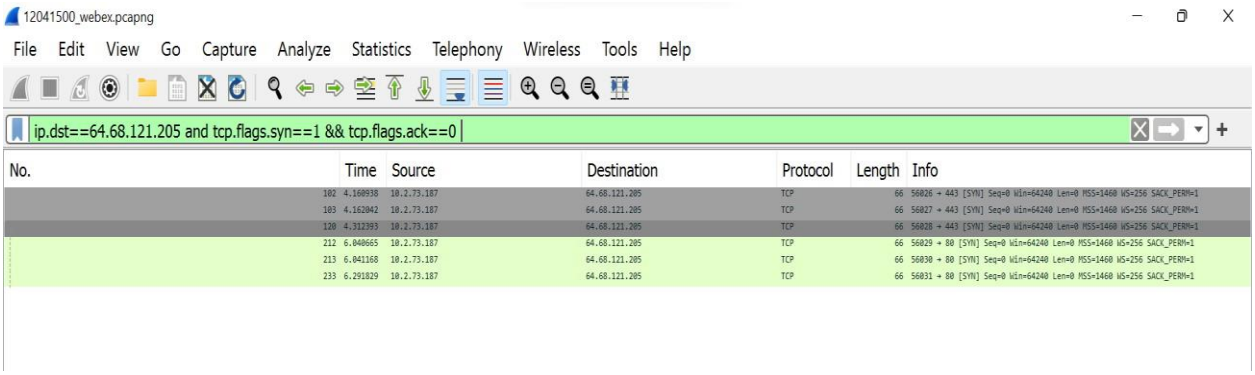
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B

Fig 1.15 UDP Connections

All the connections are persistent.

Using Filter

I did some research and used display filter: tcp.flags.syn==1 && tcp.flags.ack==0 and it found only 6 TCP Connections as shown manually above.



For finding the number of objects that have been transferred on these connections, we look at statistics → Protocol Hierarchy (figure 1.16). 36 packets are transferred over TCP.

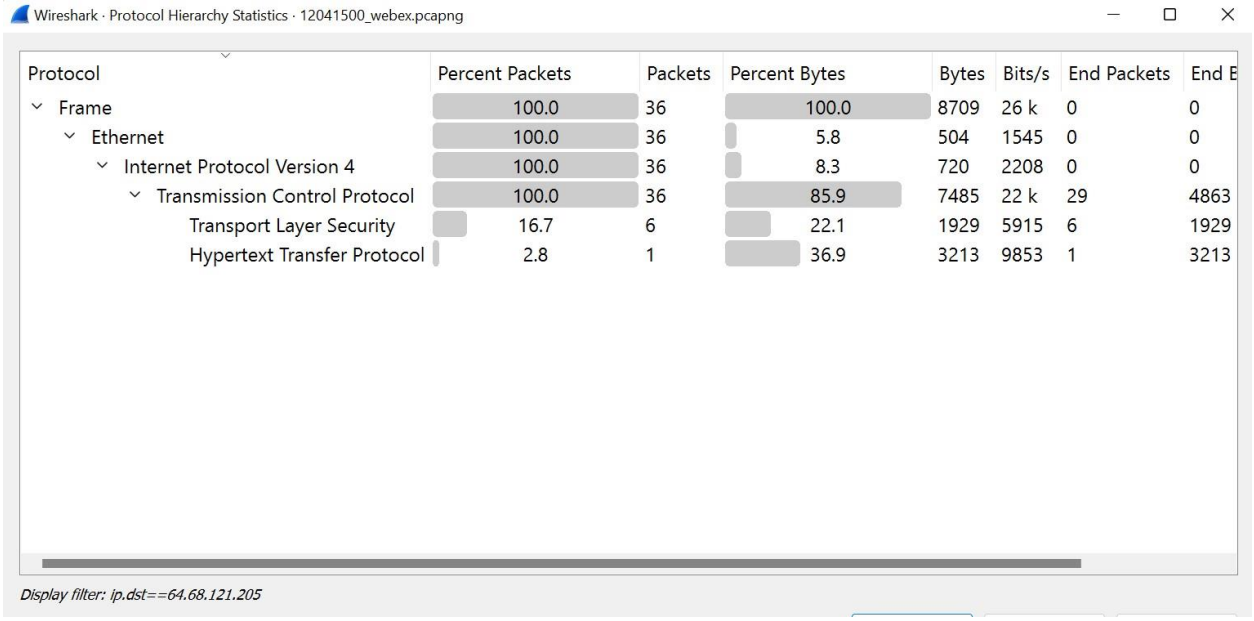


Figure 1.16: Transferred packets

To find which object took the longest time to download, we look at the max inter-packet interval (figure 1.17) shown in highlighted

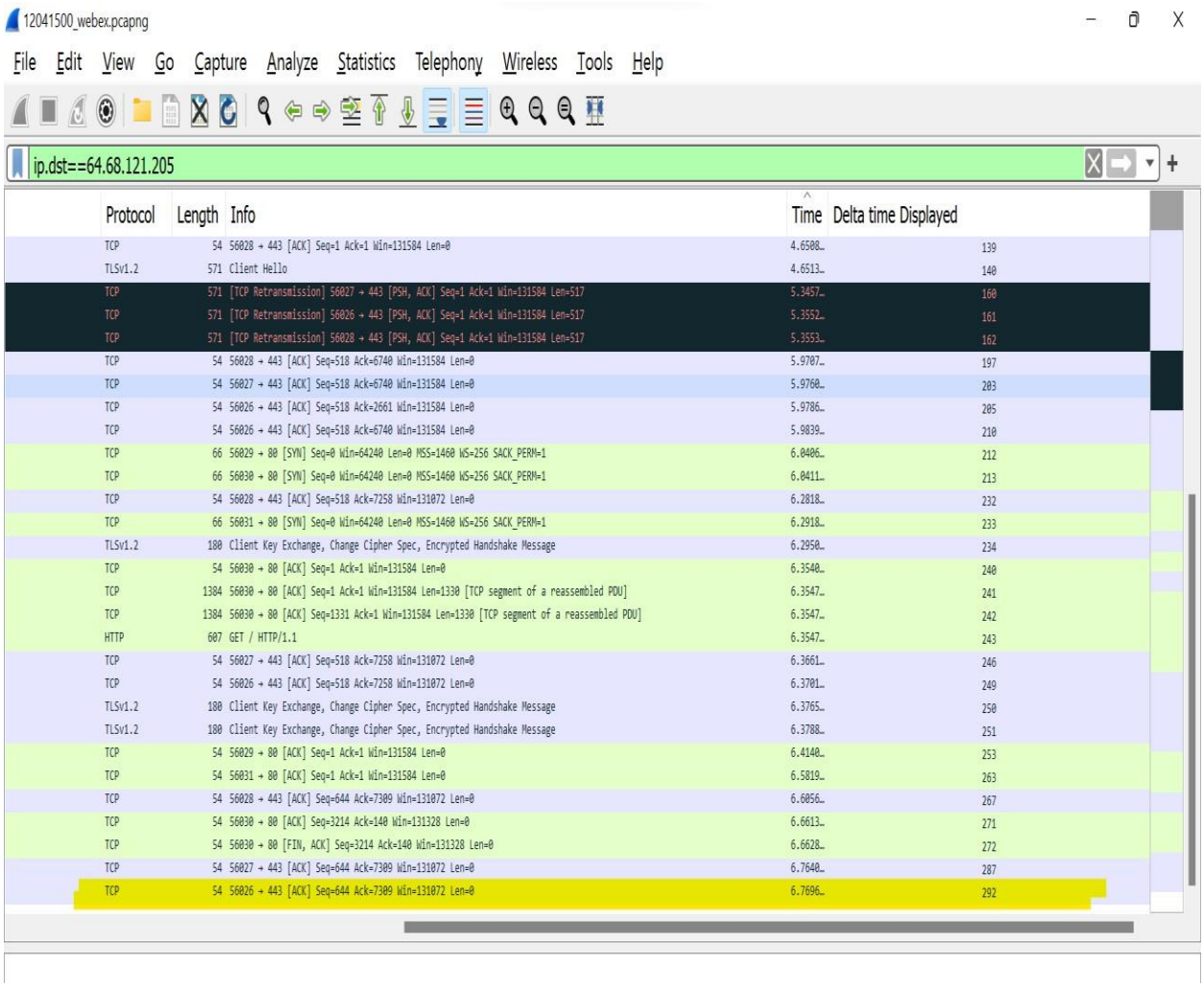


Figure 1.17: Packet that took the longest time to download (highlighted)

2

The command we use is **dig @a.root-servers.net www.iitbhilai.ac.in +norecurse.**

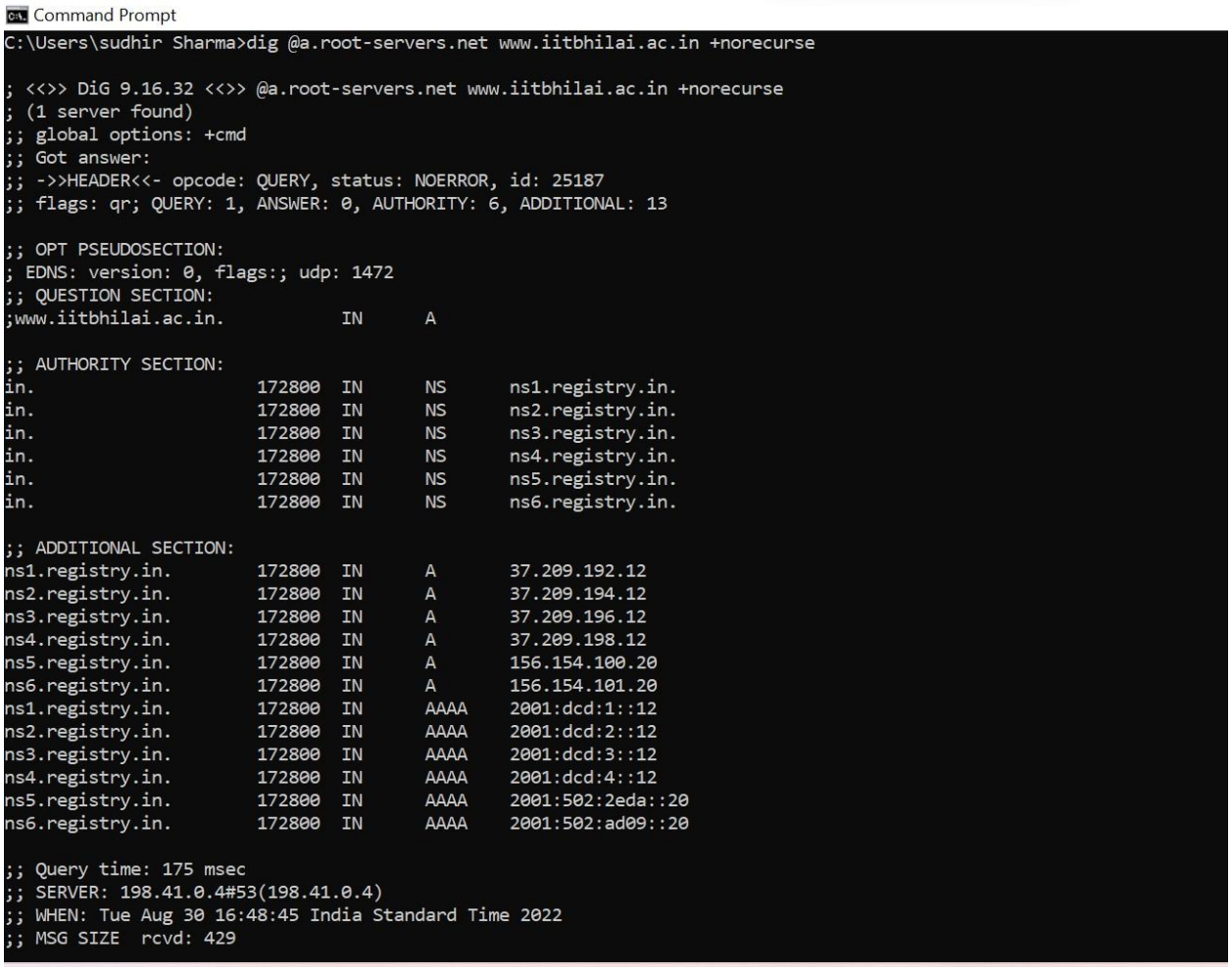


Figure 1.20: dig @a.root-servers.net www.iitbhilai.ac.in +norecurse

dig @ns1.registry.in www.iitbhilai.ac.in +norecurse

```
C:\Users\sudhir Sharma>dig @ns1.registry.in www.iitbhilai.ac.in +norecurse

; <<>> DiG 9.16.32 <<>> @ns1.registry.in www.iitbhilai.ac.in +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34294
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.iitbhilai.ac.in.           IN      A

;; AUTHORITY SECTION:
iitbhilai.ac.in.        3600    IN      NS      dns2.iitbhilai.ac.in.
iitbhilai.ac.in.        3600    IN      NS      dns1.iitbhilai.ac.in.

;; ADDITIONAL SECTION:
dns2.iitbhilai.ac.in.   3600    IN      A       103.90.97.70
dns1.iitbhilai.ac.in.   3600    IN      A       103.147.138.110

;; Query time: 38 msec
;; SERVER: 37.209.192.12#53(37.209.192.12)
;; WHEN: Tue Aug 30 16:50:01 India Standard Time 2022
;; MSG SIZE  rcvd: 118


C:\Users\sudhir Sharma>
```

Figure 1.21: dig @ns1.registry.in www.iitbhilai.ac.in +norecurse

dig @dns1.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse

```
C:\Users\sudhir Sharma>dig @dns1.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse

; <<>> DiG 9.16.32 <<>> @dns1.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29639
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.iitbhilai.ac.in.           IN      A

;; ANSWER SECTION:
www.iitbhilai.ac.in.    8641    IN      A       192.168.10.115

;; AUTHORITY SECTION:
iitbhilai.ac.in.        8641    IN      NS      dns2.iitbhilai.ac.in.

;; ADDITIONAL SECTION:
dns2.iitbhilai.ac.in.   8641    IN      A       192.168.10.72

;; Query time: 4 msec
;; SERVER: 192.168.10.87#53(192.168.10.87)
;; WHEN: Tue Aug 30 16:51:59 India Standard Time 2022
;; MSG SIZE  rcvd: 99


C:\Users\sudhir Sharma>
```

Figure 1.22: dig @dns1.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse

ANSWER SECTION:

www.iitbhilai.ac.in. 8641 IN A 192.168.10.115

Website: www.webex.com Command: **dig @a.root-servers.net www.webex.com +norecurse**

Select Command Prompt

```
C:\Users\sudhir Sharma>dig @a.root-servers.net www.webex.com +norecurse

; <<>> DiG 9.16.32 <<>> @a.root-servers.net www.webex.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38228
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.webex.com.                 IN      A

;; AUTHORITY SECTION:
com.                    172800  IN      NS      a.gtld-servers.net.
com.                    172800  IN      NS      b.gtld-servers.net.
com.                    172800  IN      NS      c.gtld-servers.net.
com.                    172800  IN      NS      d.gtld-servers.net.
com.                    172800  IN      NS      e.gtld-servers.net.
com.                    172800  IN      NS      f.gtld-servers.net.
com.                    172800  IN      NS      g.gtld-servers.net.
com.                    172800  IN      NS      h.gtld-servers.net.
com.                    172800  IN      NS      i.gtld-servers.net.
com.                    172800  IN      NS      j.gtld-servers.net.
com.                    172800  IN      NS      k.gtld-servers.net.
com.                    172800  IN      NS      l.gtld-servers.net.
com.                    172800  IN      NS      m.gtld-servers.net.

;; ADDITIONAL SECTION:
a.gtld-servers.net.     172800  IN      A       192.5.6.30
b.gtld-servers.net.     172800  IN      A       192.33.14.30
c.gtld-servers.net.     172800  IN      A       192.26.92.30
d.gtld-servers.net.     172800  IN      A       192.31.80.30
e.gtld-servers.net.     172800  IN      A       192.12.94.30
f.gtld-servers.net.     172800  IN      A       192.35.51.30
g.gtld-servers.net.     172800  IN      A       192.42.93.30
h.gtld-servers.net.     172800  IN      A       192.54.112.30
i.gtld-servers.net.     172800  IN      A       192.43.172.30
```

```
;; ADDITIONAL SECTION:
a.gtld-servers.net.     172800  IN      A       192.5.6.30
b.gtld-servers.net.     172800  IN      A       192.33.14.30
c.gtld-servers.net.     172800  IN      A       192.26.92.30
d.gtld-servers.net.     172800  IN      A       192.31.80.30
e.gtld-servers.net.     172800  IN      A       192.12.94.30
f.gtld-servers.net.     172800  IN      A       192.35.51.30
g.gtld-servers.net.     172800  IN      A       192.42.93.30
h.gtld-servers.net.     172800  IN      A       192.54.112.30
i.gtld-servers.net.     172800  IN      A       192.43.172.30
j.gtld-servers.net.     172800  IN      A       192.48.79.30
k.gtld-servers.net.     172800  IN      A       192.52.178.30
l.gtld-servers.net.     172800  IN      A       192.41.162.30
m.gtld-servers.net.     172800  IN      A       192.55.83.30
a.gtld-servers.net.     172800  IN      AAAA    2001:503:a83e::2:30
b.gtld-servers.net.     172800  IN      AAAA    2001:503:231d::2:30
c.gtld-servers.net.     172800  IN      AAAA    2001:503:83eb::30
d.gtld-servers.net.     172800  IN      AAAA    2001:500:856e::30
e.gtld-servers.net.     172800  IN      AAAA    2001:502:1ca1::30
f.gtld-servers.net.     172800  IN      AAAA    2001:503:d414::30
g.gtld-servers.net.     172800  IN      AAAA    2001:503:eea3::30
h.gtld-servers.net.     172800  IN      AAAA    2001:502:8cc::30
i.gtld-servers.net.     172800  IN      AAAA    2001:503:39c1::30
j.gtld-servers.net.     172800  IN      AAAA    2001:502:7094::30
k.gtld-servers.net.     172800  IN      AAAA    2001:503:d2d::30
l.gtld-servers.net.     172800  IN      AAAA    2001:500:d937::30
m.gtld-servers.net.     172800  IN      AAAA    2001:501:b1f9::30

;; Query time: 132 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Aug 30 16:56:27 India Standard Time 2022
;; MSG SIZE  rcvd: 838


C:\Users\sudhir Sharma>
```

Figure 1.23: dig @a.root-servers.net www.webex.com +norecurse

dig @e.gtld-servers.net www.webex.com +norecurse

```
C:\Users\sudhir Sharma>dig @e.gtld-servers.net www.webex.com +norecurse

; <<>> DiG 9.16.32 <<>> @e.gtld-servers.net www.webex.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35209
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.webex.com.                 IN      A

;; AUTHORITY SECTION:
webex.com.              172800  IN      NS      ns1.as13445.net.
webex.com.              172800  IN      NS      ns2.as13445.net.

;; Query time: 230 msec
;; SERVER: 192.12.94.30#53(192.12.94.30)
;; WHEN: Tue Aug 30 16:59:18 India Standard Time 2022
;; MSG SIZE  rcvd: 89


C:\Users\sudhir Sharma>
```

Figure 1.24: dig @e.gtld-servers.net www.webex.com +norecurse

dig @ns1.as13445.net www.webex.com +norecurse

```
C:\Users\sudhir Sharma>dig @ns1.as13445.net www.webex.com +norecurse

; <<>> DiG 9.16.32 <<>> @ns1.as13445.net www.webex.com +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54922
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 80e5f63bb228b5148bd86fc3630df4abf33cf4cd8276e851 (good)
;; QUESTION SECTION:
;www.webex.com.                 IN      A

;; ANSWER SECTION:
www.webex.com.          60      IN      CNAME   all-www.webex.com.edgekey.net.

;; Query time: 40 msec
;; SERVER: 66.163.52.1#53(66.163.52.1)
;; WHEN: Tue Aug 30 16:59:47 India Standard Time 2022
;; MSG SIZE  rcvd: 113


C:\Users\sudhir Sharma>
```

Figure 1.25: dig @ns1.as13445.net www.webex.com +norecurse

Answer Section: www.webex.com CNAME all-www.webex.com.edgekey.net

Website: www.videolan.org Command**: dig @a.root-servers.net www.videolan.org +norecurse**

Command Prompt

```
C:\Users\sudhir Sharma>dig @a.root-servers.net www.videolan.org +norecurse

; <<>> DiG 9.16.32 <<>> @a.root-servers.net www.videolan.org +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14870
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.videolan.org.              IN      A

;; AUTHORITY SECTION:
org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      a2.org.afilias-nst.info.
org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      b2.org.afilias-nst.org.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    172800  IN      NS      d0.org.afilias-nst.org.

;; ADDITIONAL SECTION:
a0.org.afilias-nst.info. 172800 IN      A       199.19.56.1
a2.org.afilias-nst.info. 172800 IN      A       199.249.112.1
b0.org.afilias-nst.org. 172800  IN      A       199.19.54.1
b2.org.afilias-nst.org. 172800  IN      A       199.249.120.1
c0.org.afilias-nst.info. 172800 IN      A       199.19.53.1
d0.org.afilias-nst.org. 172800  IN      A       199.19.57.1
a0.org.afilias-nst.info. 172800 IN      AAAA    2001:500:e::1
a2.org.afilias-nst.info. 172800 IN      AAAA    2001:500:40::1
b0.org.afilias-nst.org. 172800  IN      AAAA    2001:500:c::1
b2.org.afilias-nst.org. 172800  IN      AAAA    2001:500:48::1
c0.org.afilias-nst.info. 172800 IN      AAAA    2001:500:b::1
d0.org.afilias-nst.org. 172800  IN      AAAA    2001:500:f::1

;; Query time: 135 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Aug 30 17:03:42 India Standard Time 2022
```

Figure 1.26: dig @a.root-servers.net www.videolan.org +norecurse

dig @d0.org.afilias-nst.org www.videolan.org +norecurse

```
C:\Users\sudhir Sharma>dig @d0.org.afilias-nst.org www.videolan.org +norecurse

; <<>> DiG 9.16.32 <<>> @d0.org.afilias-nst.org www.videolan.org +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54075
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.videolan.org.              IN      A

;; AUTHORITY SECTION:
videolan.org.           3600    IN      NS      ns2.videolan.org.
videolan.org.           3600    IN      NS      ns1.videolan.org.

;; ADDITIONAL SECTION:
ns1.videolan.org.       3600    IN      A       213.36.253.2
ns2.videolan.org.       3600    IN      A       163.172.105.155

;; Query time: 67 msec
;; SERVER: 199.19.57.1#53(199.19.57.1)
;; WHEN: Tue Aug 30 17:04:26 India Standard Time 2022
;; MSG SIZE  rcvd: 113


C:\Users\sudhir Sharma>
```

Figure 1.27: dig @d0.org.afilias-nst.org www.videolan.org +norecurse

dig @ns2.videolan.org www.videolan.org +norecurse

```
C:\Users\sudhir Sharma>dig @ns2.videolan.org www.videolan.org +norecurse

; <<>> DiG 9.16.32 <<>> @ns2.videolan.org www.videolan.org +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33349
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0802ac9b2725cc5e01000000630df5db03e4b804351dfbc9 (good)
;; QUESTION SECTION:
;www.videolan.org.              IN      A

;; ANSWER SECTION:
www.videolan.org.       300     IN      A       213.36.253.2

;; AUTHORITY SECTION:
videolan.org.           300     IN      NS      ns2.videolan.org.
videolan.org.           300     IN      NS      ns1.videolan.org.

;; ADDITIONAL SECTION:
ns1.videolan.org.       300     IN      A       213.36.253.2
ns2.videolan.org.       300     IN      A       163.172.105.155
ns1.videolan.org.       300     IN      AAAA    2a01:e0d:1:3:58bf:fa02:c0de:60

;; Query time: 141 msec
;; SERVER: 163.172.105.155#53(163.172.105.155)
;; WHEN: Tue Aug 30 17:04:51 India Standard Time 2022
;; MSG SIZE  rcvd: 185


C:\Users\sudhir Sharma>
```

Figure 1.28: dig @ns2.videolan.org www.videolan.org +norecurse

SOLUTION OF PROBLEM 3

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4556
 [httpd.exe]
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1344
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4556
 [httpd.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       5016
 [mysqld.exe]
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9780
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       576
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       956
 Can not obtain ownership information
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       2012
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       4000
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       4396
 [spoolsv.exe]
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       336
 Can not obtain ownership information
  TCP    10.2.73.187:139        0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    10.2.73.187:49409      20.198.119.84:443      ESTABLISHED     5468
  WpnService
 [svchost.exe]
  TCP    10.2.73.187:50156      52.2.219.0:443         ESTABLISHED     7852
  WpnService
 [svchost.exe]
  TCP    10.2.73.187:50156      52.2.219.0:443         ESTABLISHED     7852
 [CoreSync.exe]
  TCP    10.2.73.187:50341      142.250.192.69:443     TIME_WAIT       0
  TCP    10.2.73.187:50342      142.250.192.69:443     TIME_WAIT       0
  TCP    10.2.73.187:50346      20.50.80.210:443       TIME_WAIT       0
  TCP    10.2.73.187:50347      51.104.15.252:443      ESTABLISHED     14760
 [msedgewebview2.exe]
  TCP    10.2.73.187:50348      51.104.15.252:443      ESTABLISHED     14760
 [msedgewebview2.exe]
  TCP    10.2.73.187:50351      142.250.76.69:443      ESTABLISHED     14964
 [EasyMail.UwpApp.exe]
  TCP    10.2.73.187:50352      142.250.76.69:443      ESTABLISHED     14964
 [EasyMail.UwpApp.exe]
  TCP    10.2.73.187:50353      142.250.196.35:443     ESTABLISHED     15804
 [msedge.exe]
  TCP    10.2.73.187:50354      52.182.141.63:443      ESTABLISHED     14132
 [chrome.exe]
  TCP    10.2.73.187:50355      52.182.141.63:443      ESTABLISHED     14132
 [chrome.exe]
  TCP    10.2.73.187:50356      52.182.141.63:443      ESTABLISHED     14132
 [chrome.exe]
  TCP    10.2.73.187:50357      13.107.21.200:443      ESTABLISHED     10524
 [SearchHost.exe]
  TCP    10.2.73.187:50358      52.98.57.114:443       ESTABLISHED     10524
 [SearchHost.exe]
  TCP    10.2.73.187:50359      13.107.6.158:443       ESTABLISHED     10524
 [SearchHost.exe]
  TCP    10.2.73.187:59502      52.194.176.114:443     ESTABLISHED     7852
 [CoreSync.exe]
  TCP    10.2.73.187:59545      40.70.161.7:443        CLOSE_WAIT      7048
 [mcafee-security.exe]
  TCP    10.2.73.187:59549      142.251.10.188:5228    ESTABLISHED     14132
 [chrome.exe]
  TCP    127.0.0.1:15292        0.0.0.0:0              LISTENING       18088
 [Adobe Desktop Service.exe]
  TCP    127.0.0.1:15393        0.0.0.0:0              LISTENING       18088
 [Adobe Desktop Service.exe]
  TCP    127.0.0.1:16494        0.0.0.0:0              LISTENING       18088
```

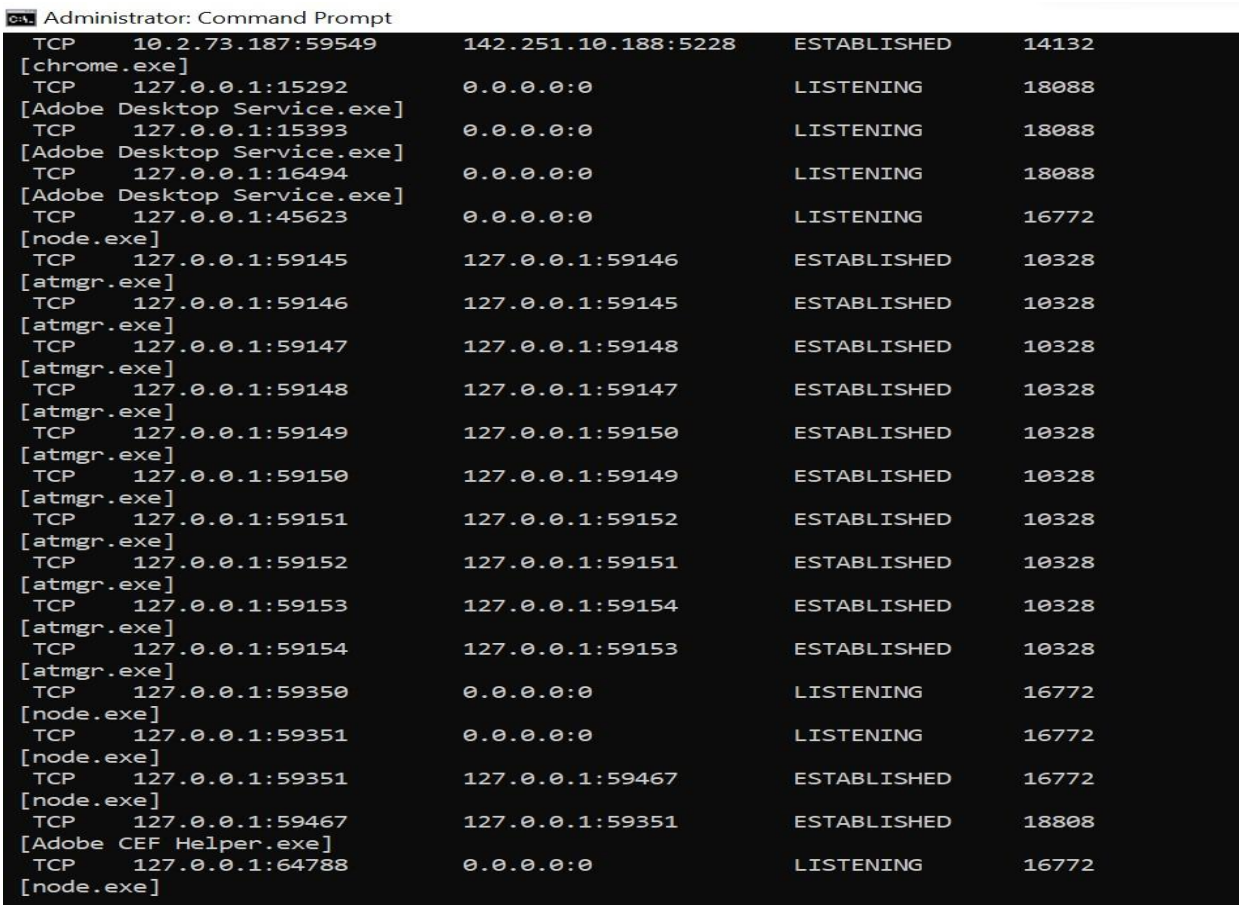


FIGURE 1.18: ACTIVE TCP PORTS

-b Displays the executable involved in creating each connection or listening port. -o Displays the owning process ID associated with each connection.
-a Displays all connections and listening ports.
-p Shows connections for the protocol specified by proto e.g.
TCP. -n Displays addresses and port numbers in numerical form.

The ports and PIDs of the web browser is in the last column. The browser name is chrome and the PID is 14132. The ports of browser are 53833, 53834, 53835, 53836, 53837, 53838, 53839, 53840, 53841.These are present in the local address column.

One of the tabs has www.iitbhilai.ac.in opened. The ip address of this website is 92.168.10.115. All the rows in figure 1.18 with this ip address in foreign address column corresponds to iitbhilai website. To see all of them together we can use the FINDSTR command (figure 1.19)

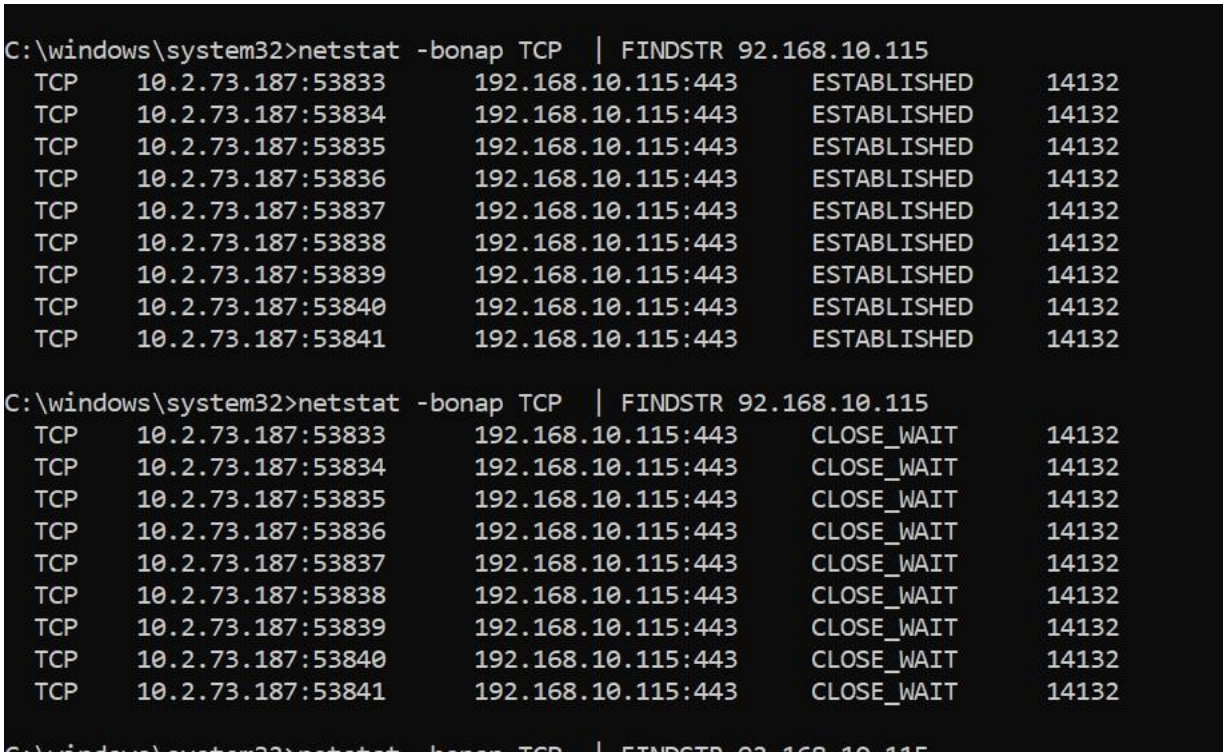


Figure 1.19: Active TCP ports of IIT Bhilai website

There can be many TCP connections from a single tab and therefore can have multiple different ports.

Initially port 80 (standard port for HTTP) is used for listening. The program svchost.exe used port 135 (DCE), 445
(Microsoft-DS (Directory Services)), 5040 (Windows Deployment Services server (which is TCP 5040 by default)) etc.