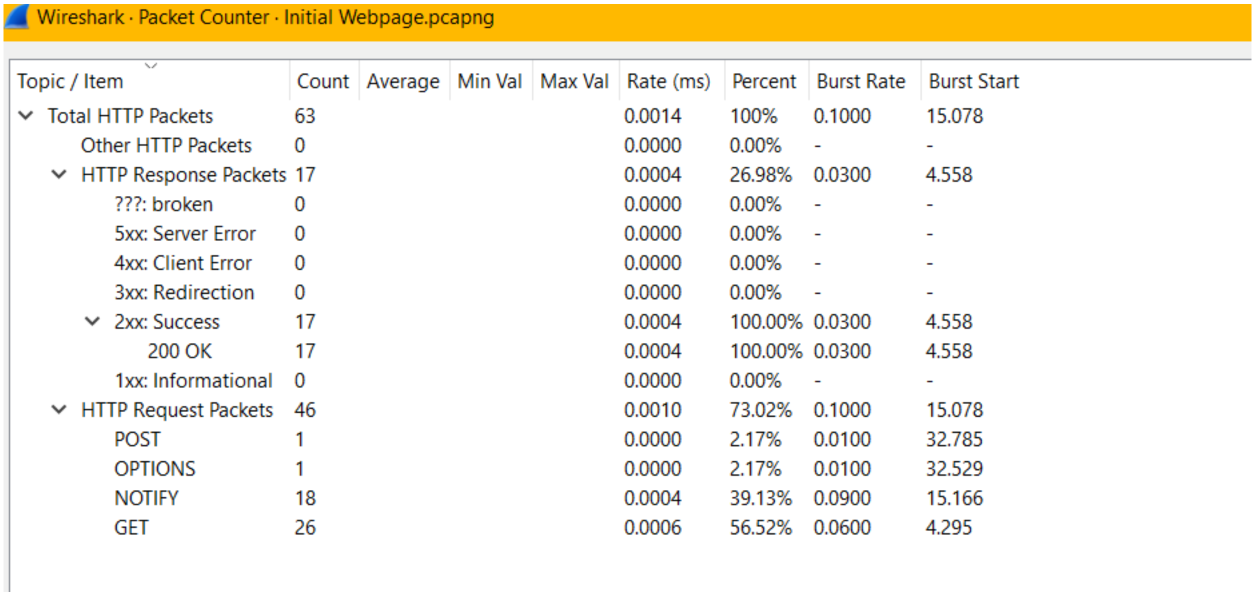
Part 1 or Part A

Question 1

On completion of the packet capture packets by Wireshark, we apply a query to find the number of GET requests.

IP address of IIT Bhilai Web Page is 103.147.138.100

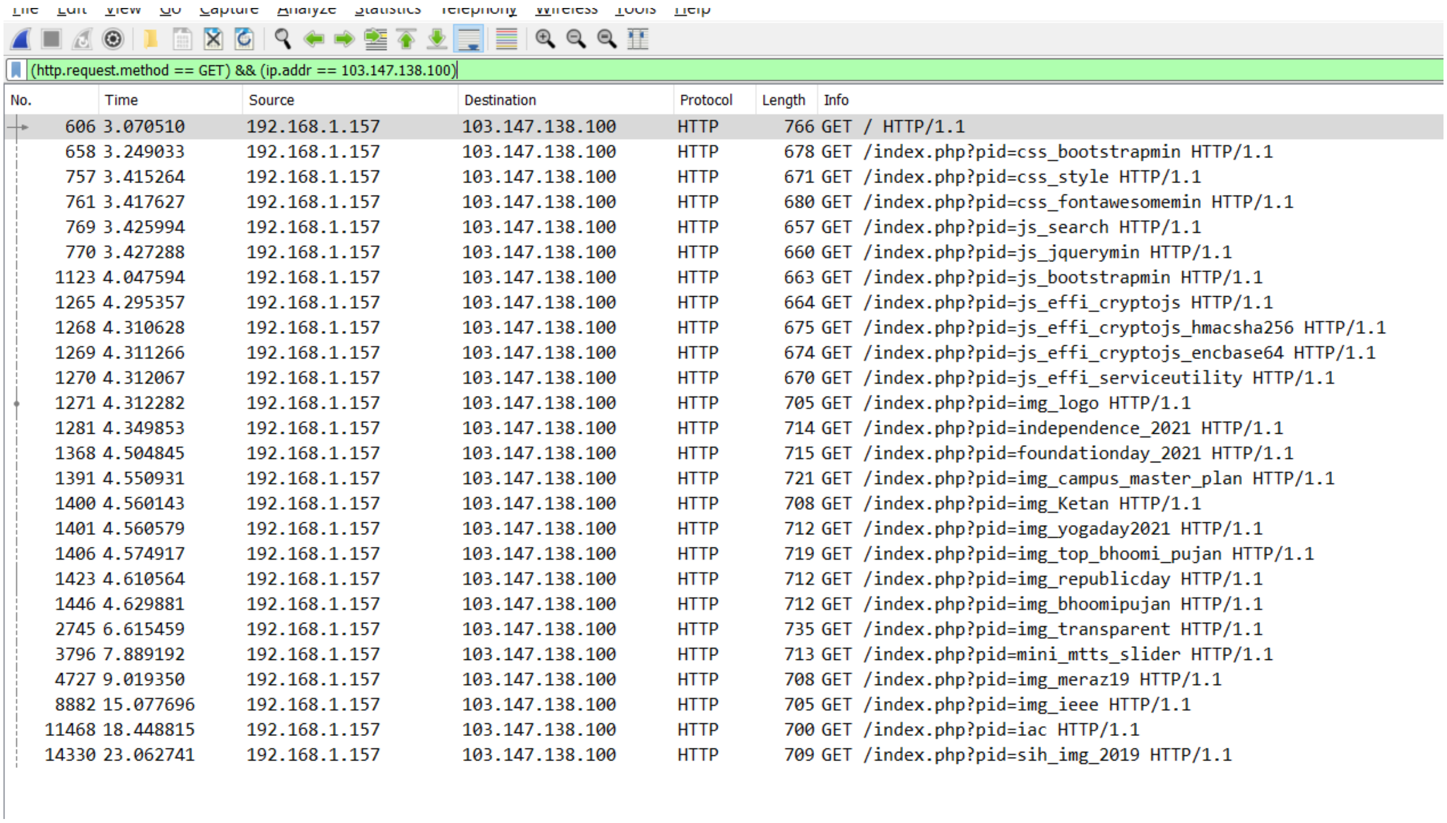
Query applied: (http.request.method == GET) && (ip.addr == 103.147.138.100)



Wireshark · Packet Counter · Initial Webpage.pcapng

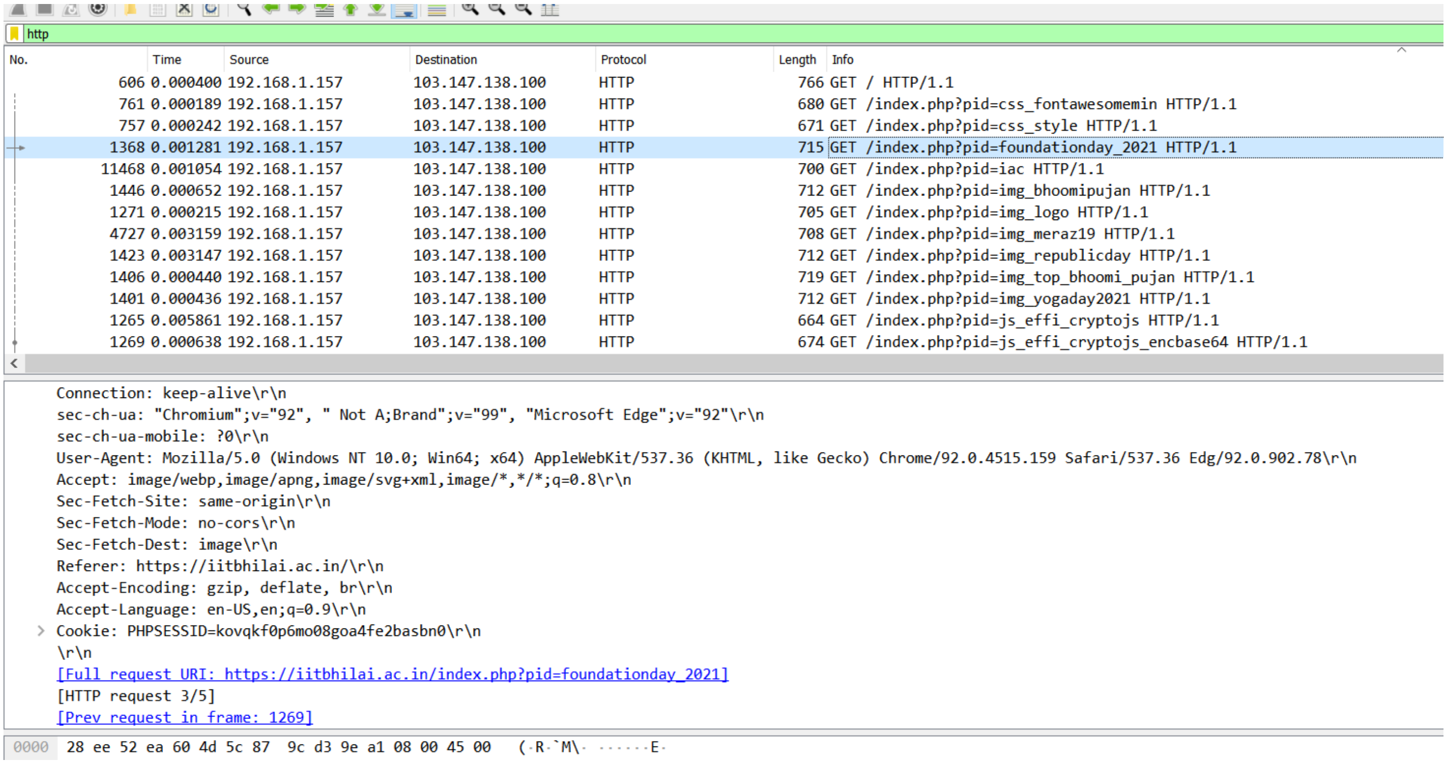
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Total HTTP Packets	63				0.0014	100%	0.1000	15.078
Other HTTP Packets	0				0.0000	0.00%	-	-
HTTP Response Packets	17				0.0004	26.98%	0.0300	4.558
???: broken	0				0.0000	0.00%	-	-
5xx: Server Error	0				0.0000	0.00%	-	-
4xx: Client Error	0				0.0000	0.00%	-	-
3xx: Redirection	0				0.0000	0.00%	-	-
2xx: Success	17				0.0004	100.00%	0.0300	4.558
200 OK	17				0.0004	100.00%	0.0300	4.558
1xx: Informational	0				0.0000	0.00%	-	-
HTTP Request Packets	46				0.0010	73.02%	0.1000	15.078
POST	1				0.0000	2.17%	0.0100	32.785
OPTIONS	1				0.0000	2.17%	0.0100	32.529
NOTIFY	18				0.0004	39.13%	0.0900	15.166
GET	26				0.0006	56.52%	0.0600	4.295

The number of GET requests sent is 26.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(http.request.method == GET) && (ip.addr == 103.147.138.100)

No.	Time	Source	Destination	Protocol	Length	Info
606	3.070510	192.168.1.157	103.147.138.100	HTTP	766	GET / HTTP/1.1
658	3.249033	192.168.1.157	103.147.138.100	HTTP	678	GET /index.php?pid=css_bootstrapmin HTTP/1.1
757	3.415264	192.168.1.157	103.147.138.100	HTTP	671	GET /index.php?pid=css_style HTTP/1.1
761	3.417627	192.168.1.157	103.147.138.100	HTTP	680	GET /index.php?pid=css_fontawesomemin HTTP/1.1
769	3.425994	192.168.1.157	103.147.138.100	HTTP	657	GET /index.php?pid=js_search HTTP/1.1
770	3.427288	192.168.1.157	103.147.138.100	HTTP	660	GET /index.php?pid=js_jquerymin HTTP/1.1
1123	4.047594	192.168.1.157	103.147.138.100	HTTP	663	GET /index.php?pid=js_bootstrapmin HTTP/1.1
1265	4.295357	192.168.1.157	103.147.138.100	HTTP	664	GET /index.php?pid=js_effi_cryptojs HTTP/1.1
1268	4.310628	192.168.1.157	103.147.138.100	HTTP	675	GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1
1269	4.311266	192.168.1.157	103.147.138.100	HTTP	674	GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
1270	4.312067	192.168.1.157	103.147.138.100	HTTP	670	GET /index.php?pid=js_effi_serviceutility HTTP/1.1
1271	4.312282	192.168.1.157	103.147.138.100	HTTP	705	GET /index.php?pid=img_logo HTTP/1.1
1281	4.349853	192.168.1.157	103.147.138.100	HTTP	714	GET /index.php?pid=independence_2021 HTTP/1.1
1368	4.504845	192.168.1.157	103.147.138.100	HTTP	715	GET /index.php?pid=foundationday_2021 HTTP/1.1
1391	4.550931	192.168.1.157	103.147.138.100	HTTP	721	GET /index.php?pid=img_campus_master_plan HTTP/1.1
1400	4.560143	192.168.1.157	103.147.138.100	HTTP	708	GET /index.php?pid=img_Ketan HTTP/1.1
1401	4.560579	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_yogaday2021 HTTP/1.1
1406	4.574917	192.168.1.157	103.147.138.100	HTTP	719	GET /index.php?pid=img_top_bhoomi_pujan HTTP/1.1
1423	4.610564	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_republicday HTTP/1.1
1446	4.629881	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_bhoomipujan HTTP/1.1
2745	6.615459	192.168.1.157	103.147.138.100	HTTP	735	GET /index.php?pid=img_transparent HTTP/1.1
3796	7.889192	192.168.1.157	103.147.138.100	HTTP	713	GET /index.php?pid=mini_mtts_slider HTTP/1.1
4727	9.019350	192.168.1.157	103.147.138.100	HTTP	708	GET /index.php?pid=img_meraz19 HTTP/1.1
8882	15.077696	192.168.1.157	103.147.138.100	HTTP	705	GET /index.php?pid=img_ieee HTTP/1.1
11468	18.448815	192.168.1.157	103.147.138.100	HTTP	700	GET /index.php?pid=iac HTTP/1.1
14330	23.062741	192.168.1.157	103.147.138.100	HTTP	709	GET /index.php?pid=sih_img_2019 HTTP/1.1



```
No.       Time     Source          Destination      Protocol  Length Info
      606 0.000400 192.168.1.157   103.147.138.100  HTTP         766 GET / HTTP/1.1
      761 0.000189 192.168.1.157   103.147.138.100  HTTP         680 GET /index.php?pid=css_fontawesomemin HTTP/1.1
      757 0.000242 192.168.1.157   103.147.138.100  HTTP         671 GET /index.php?pid=css_style HTTP/1.1
     1368 0.001281 192.168.1.157   103.147.138.100  HTTP         715 GET /index.php?pid=foundationday_2021 HTTP/1.1
    11468 0.001054 192.168.1.157   103.147.138.100  HTTP         700 GET /index.php?pid=iac HTTP/1.1
     1446 0.000652 192.168.1.157   103.147.138.100  HTTP         712 GET /index.php?pid=img_bhoomipujan HTTP/1.1
     1271 0.000215 192.168.1.157   103.147.138.100  HTTP         705 GET /index.php?pid=img_logo HTTP/1.1
     4727 0.003159 192.168.1.157   103.147.138.100  HTTP         708 GET /index.php?pid=img_meraz19 HTTP/1.1
     1423 0.003147 192.168.1.157   103.147.138.100  HTTP         712 GET /index.php?pid=img_republicday HTTP/1.1
     1406 0.000440 192.168.1.157   103.147.138.100  HTTP         719 GET /index.php?pid=img_top_bhoomi_pujan HTTP/1.1
     1401 0.000436 192.168.1.157   103.147.138.100  HTTP         712 GET /index.php?pid=img_yogaday2021 HTTP/1.1
     1265 0.005861 192.168.1.157   103.147.138.100  HTTP         664 GET /index.php?pid=js_effi_cryptojs HTTP/1.1
     1269 0.000638 192.168.1.157   103.147.138.100  HTTP         674 GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
```

```
    Connection: keep-alive\r\n
    sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Microsoft Edge";v="92"\r\n
    sec-ch-ua-mobile: ?0\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36 Edg/92.0.902.78\r\n
    Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Sec-Fetch-Site: same-origin\r\n
    Sec-Fetch-Mode: no-cors\r\n
    Sec-Fetch-Dest: image\r\n
    Referer: https://iitbhilai.ac.in/\r\n
    Accept-Encoding: gzip, deflate, br\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: PHPSESSID=kovqkf0p6mo08goa4fe2basbn0\r\n
    \r\n
    [Full request URI: https://iitbhilai.ac.in/index.php?pid=foundationday_2021]
    [HTTP request 3/5]
    [Prev request in frame: 1269]
```

```
0000  28 ee 52 ea 60 4d 5c 87  9c d3 9e a1 08 00 45 00   (·R·`M\· ······E·
```

In this, we can segregate images based on the GET Request that Fetch-Dest is an image and it will accept an image. Similarly, we can check for all the GET Requests to which category they belong.

The total number of GET Requests is split into embedded content and Text. The count is:

Embedded Content GET Requests = 11 (All are images)

Text GET Requests = 15 (HTML, CSS, JS pages).

Note:

In a few cases, we will get a Favicon GET Request for the IIT Bhilai Web Page.

Favicon is an icon associated with a particular website, typically displayed in the address bar of a browser accessing the site or next to the site name in a user's list of bookmarks.

Few browsers support Favicon as a GET Request from the Client, however some of them like Mozilla Firefox, Microsoft Edge, or Google Chrome (older versions do not support this functionality).

Hence in my page rendering, this is not shown as a GET request due to the old version of the browser which my system can support.

So, if Favicon is considered it will become 27 as there are 26 GET Requests as previously mentioned. Favicon is an icon on the address so it is not a part of the Page Rendering and hence it does not come under the category of text or embedded content.

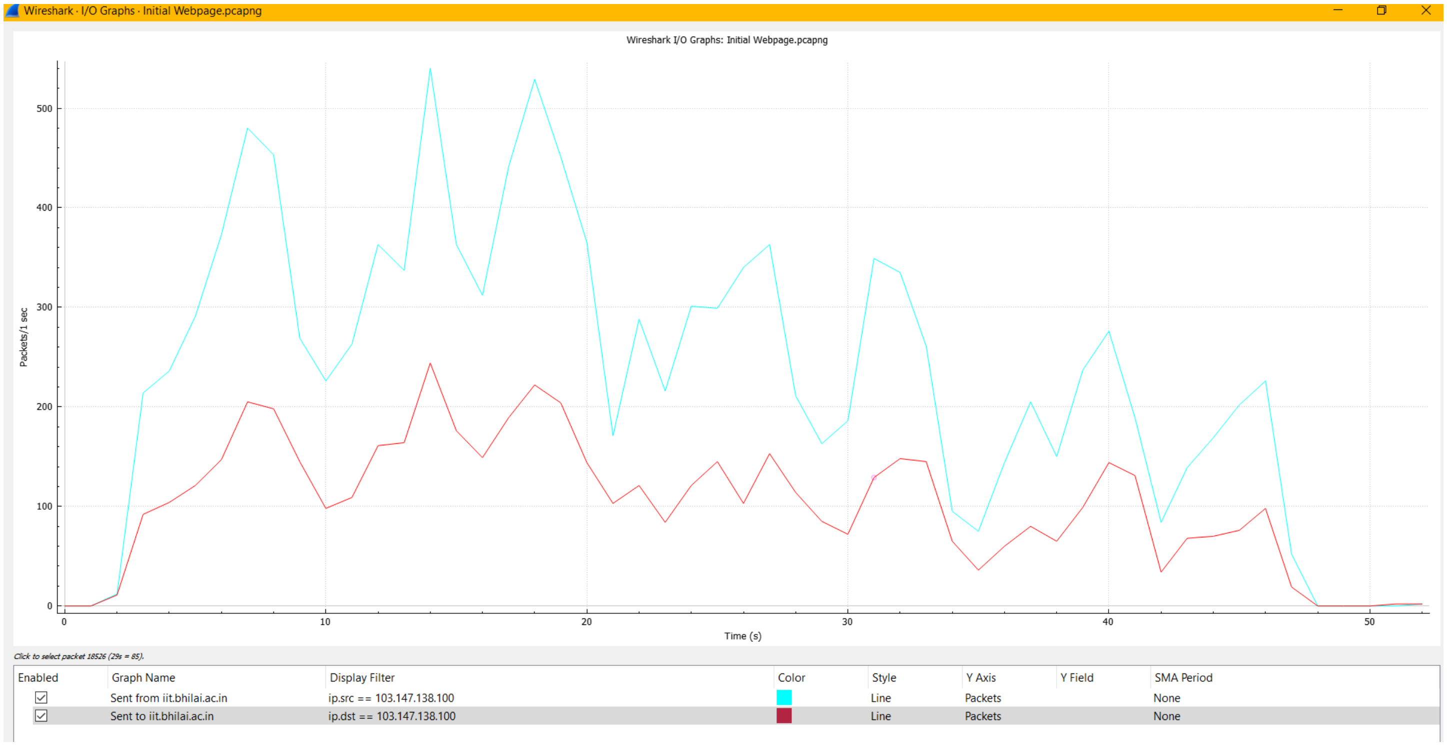
I have submitted the results I have received during the page rendering of my browser and in consensus with the submitted PCAP file.

I/O Graph

Filters Applied:

Packets sent to iitbhilai.ac.in: ip.dst == 103.147.138.100 (Red Lined Graph)

Packets sent from iitbhilai.ac.in: ip.src == 103.147.138.100 (Blue Lined Graph)


Wireshark · I/O Graphs · Initial Webpage.pcapng
Wireshark I/O Graphs: Initial Webpage.pcapng
Packets/1 sec
500
400
300
200
100
0
0
10
20
30
40
50
Time (s)

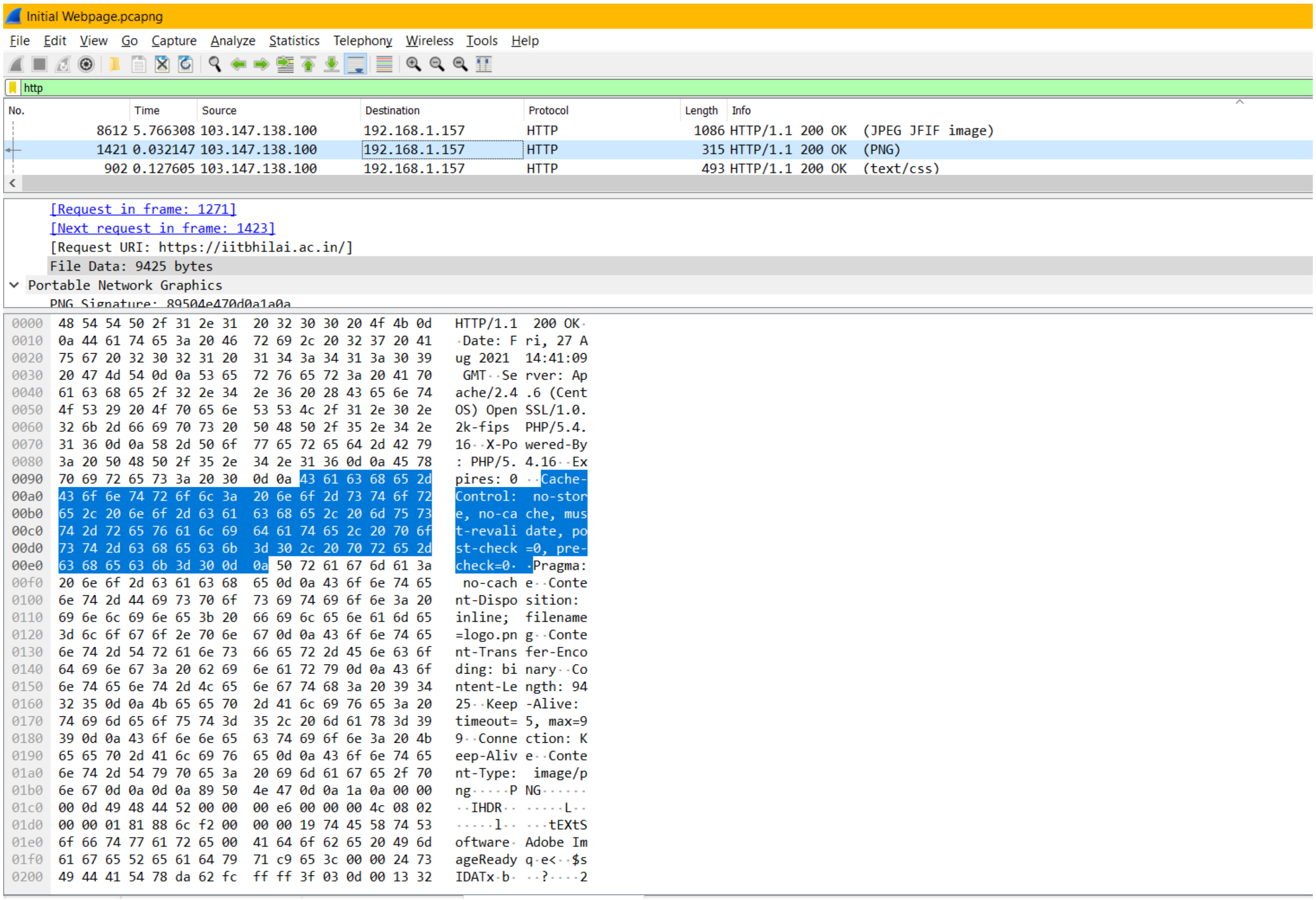
Click to select packet 18526 (29s = 85).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	Sent from iit.bhilai.ac.in	ip.src == 103.147.138.100	🟦	Line	Packets		None
☑	Sent to iit.bhilai.ac.in	ip.dst == 103.147.138.100	🟥	Line	Packets		None

PCAP file: ‘Initial Webpage.pcapng’

Question 2

Image for the Hex Dump


Initial Webpage.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

No.	Time	Source	Destination	Protocol	Length	Info
8612	5.766308	103.147.138.100	192.168.1.157	HTTP	1086	HTTP/1.1 200 OK (JPEG JFIF image)
1421	0.032147	103.147.138.100	192.168.1.157	HTTP	315	HTTP/1.1 200 OK (PNG)
902	0.127605	103.147.138.100	192.168.1.157	HTTP	493	HTTP/1.1 200 OK (text/css)

```
    [Request in frame: 1271]
    [Next request in frame: 1423]
    [Request URI: https://iitbhilai.ac.in/]
    File Data: 9425 bytes
v Portable Network Graphics
    PNG Signature: 89504e470d0a1a0a
```

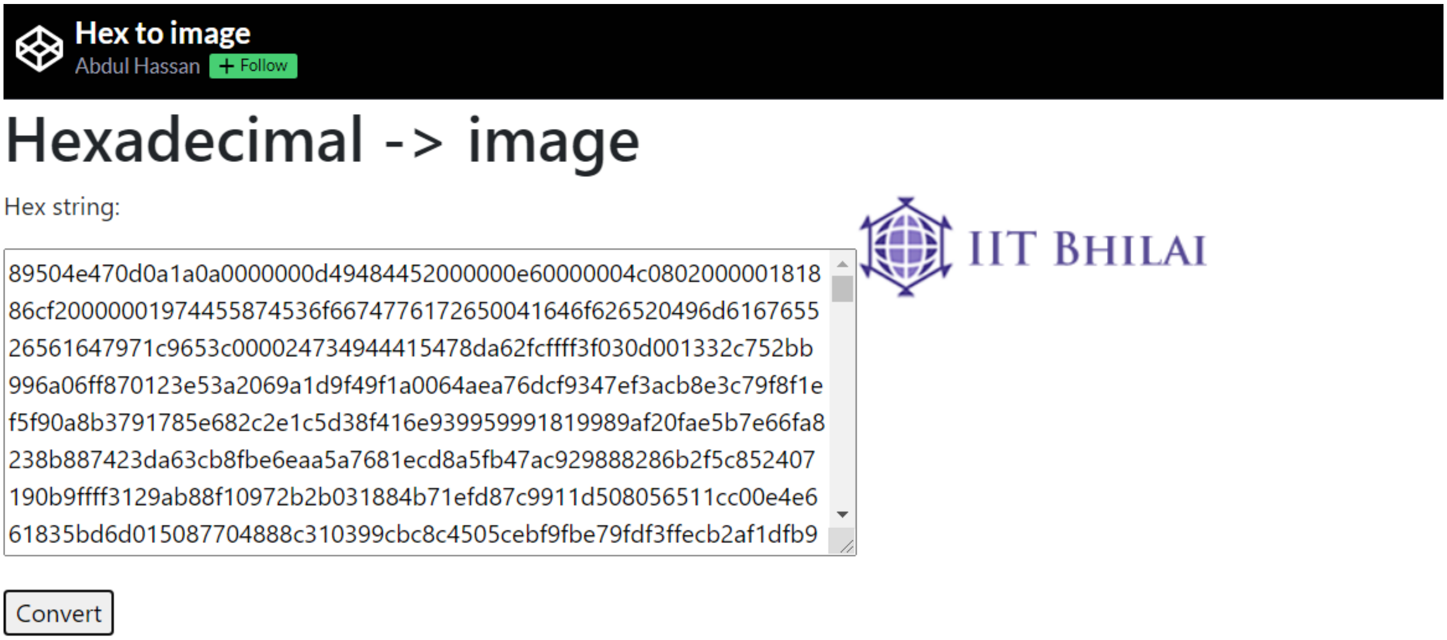
```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 37 20 41   ·Date: F ri, 27 A
0020  75 67 20 32 30 32 31 20  31 34 3a 34 31 3a 30 39   ug 2021  14:41:09
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 0d 0a 58 2d 50 6f  77 65 72 65 64 2d 42 79   16··X-Po wered-By
0080  3a 20 50 48 50 2f 35 2e  34 2e 31 36 0d 0a 45 78   : PHP/5. 4.16··Ex
0090  70 69 72 65 73 3a 20 30  0d 0a 43 61 63 68 65 2d   pires: 0 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6e 6f 2d 73 74 6f 72   Control:  no-stor
00b0  65 2c 20 6e 6f 2d 63 61  63 68 65 2c 20 6d 75 73   e, no-ca che, mus
00c0  74 2d 72 65 76 61 6c 69  64 61 74 65 2c 20 70 6f   t-revali date, po
00d0  73 74 2d 63 68 65 63 6b  3d 30 2c 20 70 72 65 2d   st-check =0, pre-
00e0  63 68 65 63 6b 3d 30 0d  0a 50 72 61 67 6d 61 3a   check=0· ·Pragma:
00f0  20 6e 6f 2d 63 61 63 68  65 0d 0a 43 6f 6e 74 65    no-cach e··Conte
0100  6e 74 2d 44 69 73 70 6f  73 69 74 69 6f 6e 3a 20   nt-Dispo sition: 
0110  69 6e 6c 69 6e 65 3b 20  66 69 6c 65 6e 61 6d 65   inline;  filename
0120  3d 6c 6f 67 6f 2e 70 6e  67 0d 0a 43 6f 6e 74 65   =logo.pn g··Conte
0130  6e 74 2d 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   nt-Trans fer-Enco
0140  64 69 6e 67 3a 20 62 69  6e 61 72 79 0d 0a 43 6f   ding: bi nary··Co
0150  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 39 34   ntent-Le ngth: 94
0160  32 35 0d 0a 4b 65 65 70  2d 41 6c 69 76 65 3a 20   25··Keep -Alive: 
0170  74 69 6d 65 6f 75 74 3d  35 2c 20 6d 61 78 3d 39   timeout= 5, max=9
0180  39 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   9··Conne ction: K
0190  65 65 70 2d 41 6c 69 76  65 0d 0a 43 6f 6e 74 65   eep-Aliv e··Conte
01a0  6e 74 2d 54 79 70 65 3a  20 69 6d 61 67 65 2f 70   nt-Type:  image/p
01b0  6e 67 0d 0a 0d 0a 89 50  4e 47 0d 0a 1a 0a 00 00   ng·····P NG······
01c0  00 0d 49 48 44 52 00 00  00 e6 00 00 00 4c 08 02   ··IHDR·· ·····L··
01d0  00 00 01 81 88 6c f2 00  00 00 19 74 45 58 74 53   ·····l·· ···tEXtS
01e0  6f 66 74 77 61 72 65 00  41 64 6f 62 65 20 49 6d   oftware· Adobe Im
01f0  61 67 65 52 65 61 64 79  71 c9 65 3c 00 00 24 73   ageReady q·e<··$s
0200  49 44 41 54 78 da 62 fc  ff ff 3f 03 0d 00 13 32   IDATx·b· ··?····2
```

The Hex Dump file for the Image is stored in “Hex Dump.txt”

In the file data option, we can copy the hex dump as a hex stream.

The Hex Stream for the Image is stored in Hexstream.txt

Once this is copied, go to the online Hex converter: https://codepen.io/abdhass/full/jdRNdj that converts the hex stream to the necessary image.



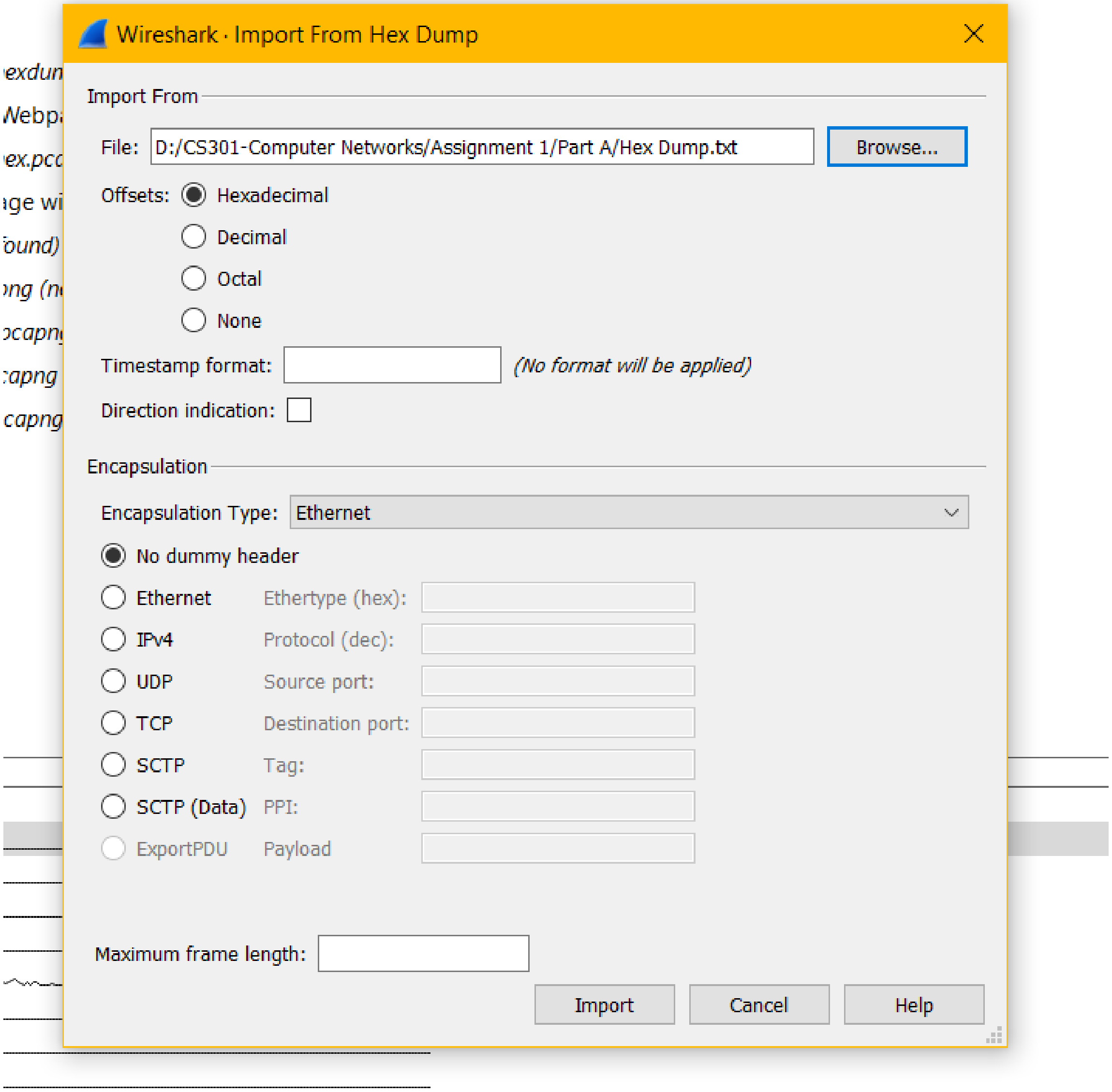
Hexadecimal -> image

Hex string:

```
89504e470d0a1a0a0000000d49484452000000e60000004c0802000001818
86cf20000001974455874536f667477617265004164f626520496d6167655
26561647971c9653c0000247349444415478da62fcffff3f030d001332c752bb
996a06ff870123e53a2069a1d9f49f1a0064aea76dcf9347ef3acb8e3c79f8f1e
f5f90a8b3791785e682c2e1c5d38f416e939959991819989af20fae5b7e66fa8
238b887423da63cb8fbe6eaa5a7681ecd8a5fb47ac929888286b2f5c852407
190b9ffff3129ab88f10972b2b031884b71efd87c9911d508056511cc00e4e6
61835bd6d015087704888c310399cbc8c4505cebf9fbe79fdf3ffecb2af1dfb9
```

This is followed by the Import from Hex Dump process:

Select the hexadecimal option as the input is in that form.



Wireshark · Import From Hex Dump

Import From

File: D:/CS301-Computer Networks/Assignment 1/Part A/Hex Dump.txt [Browse...]

Offsets: ● Hexadecimal
○ Decimal
○ Octal
○ None

Timestamp format: (No format will be applied)

Direction indication: □

Encapsulation

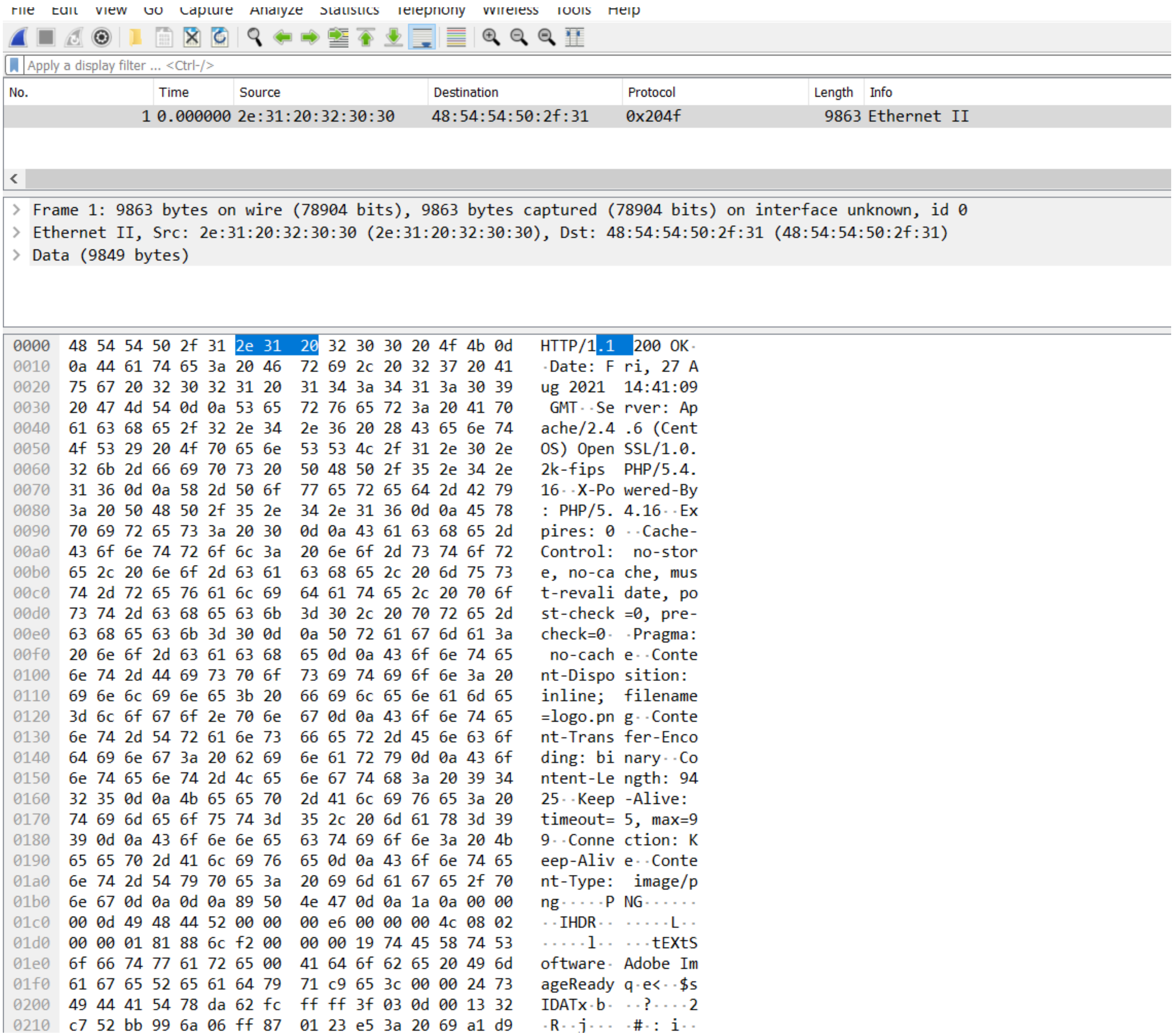
Encapsulation Type: Ethernet

● No dummy header
○ Ethernet Ethertype (hex):
○ IPv4 Protocol (dec):
○ UDP Source port:
○ TCP Destination port:
○ SCTP Tag:
○ SCTP (Data) PPI:
○ ExportPDU Payload

Maximum frame length:

After the import, we get the following file: importhexdump.pcapng (Wireshark File)

The following image is a preview of the capture file.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2e:31:20:32:30:30	48:54:54:50:2f:31	0x204f	9863	Ethernet II

```
> Frame 1: 9863 bytes on wire (78904 bits), 9863 bytes captured (78904 bits) on interface unknown, id 0
> Ethernet II, Src: 2e:31:20:32:30:30 (2e:31:20:32:30:30), Dst: 48:54:54:50:2f:31 (48:54:54:50:2f:31)
> Data (9849 bytes)
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 46  72 69 2c 20 32 37 20 41   ·Date: F ri, 27 A
0020  75 67 20 32 30 32 31 20  31 34 3a 34 31 3a 30 39   ug 2021  14:41:09
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 0d 0a 58 2d 50 6f  77 65 72 65 64 2d 42 79   16··X-Po wered-By
0080  3a 20 50 48 50 2f 35 2e  34 2e 31 36 0d 0a 45 78   : PHP/5. 4.16··Ex
0090  70 69 72 65 73 3a 20 30  0d 0a 43 61 63 68 65 2d   pires: 0 ··Cache-
00a0  43 6f 6e 74 72 6f 6c 3a  20 6e 6f 2d 73 74 6f 72   Control:  no-stor
00b0  65 2c 20 6e 6f 2d 63 61  63 68 65 2c 20 6d 75 73   e, no-ca che, mus
00c0  74 2d 72 65 76 61 6c 69  64 61 74 65 2c 20 70 6f   t-revali date, po
00d0  73 74 2d 63 68 65 63 6b  3d 30 2c 20 70 72 65 2d   st-check =0, pre-
00e0  63 68 65 63 6b 3d 30 0d  0a 50 72 61 67 6d 61 3a   check=0· ·Pragma:
00f0  20 6e 6f 2d 63 61 63 68  65 0d 0a 43 6f 6e 74 65    no-cach e··Conte
0100  6e 74 2d 44 69 73 70 6f  73 69 74 69 6f 6e 3a 20   nt-Dispo sition: 
0110  69 6e 6c 69 6e 65 3b 20  66 69 6c 65 6e 61 6d 65   inline;  filename
0120  3d 6c 6f 67 6f 2e 70 6e  67 0d 0a 43 6f 6e 74 65   =logo.pn g··Conte
0130  6e 74 2d 54 72 61 6e 73  66 65 72 2d 45 6e 63 6f   nt-Trans fer-Enco
0140  64 69 6e 67 3a 20 62 69  6e 61 72 79 0d 0a 43 6f   ding: bi nary··Co
0150  6e 74 65 6e 74 2d 4c 65  6e 67 74 68 3a 20 39 34   ntent-Le ngth: 94
0160  32 35 0d 0a 4b 65 65 70  2d 41 6c 69 76 65 3a 20   25··Keep -Alive: 
0170  74 69 6d 65 6f 75 74 3d  35 2c 20 6d 61 78 3d 39   timeout= 5, max=9
0180  39 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 4b   9··Conne ction: K
0190  65 65 70 2d 41 6c 69 76  65 0d 0a 43 6f 6e 74 65   eep-Aliv e··Conte
01a0  6e 74 2d 54 79 70 65 3a  20 69 6d 61 67 65 2f 70   nt-Type:  image/p
01b0  6e 67 0d 0a 0d 0a 89 50  4e 47 0d 0a 1a 0a 00 00   ng·····P NG······
01c0  00 0d 49 48 44 52 00 00  00 e6 00 00 00 4c 08 02   ··IHDR·· ·····L··
01d0  00 00 01 81 88 6c f2 00  00 00 19 74 45 58 74 53   ·····l·· ···tEXtS
01e0  6f 66 74 77 61 72 65 00  41 64 6f 62 65 20 49 6d   oftware· Adobe Im
01f0  61 67 65 52 65 61 64 79  71 c9 65 3c 00 00 24 73   ageReady q·e<··$s
0200  49 44 41 54 78 da 62 fc  ff ff 3f 03 0d 00 13 32   IDATx·b· ··?····2
0210  c7 52 bb 99 6a 06 ff 87  01 23 e5 3a 20 69 a1 d9   ·R··j··· ·#·: i··
```

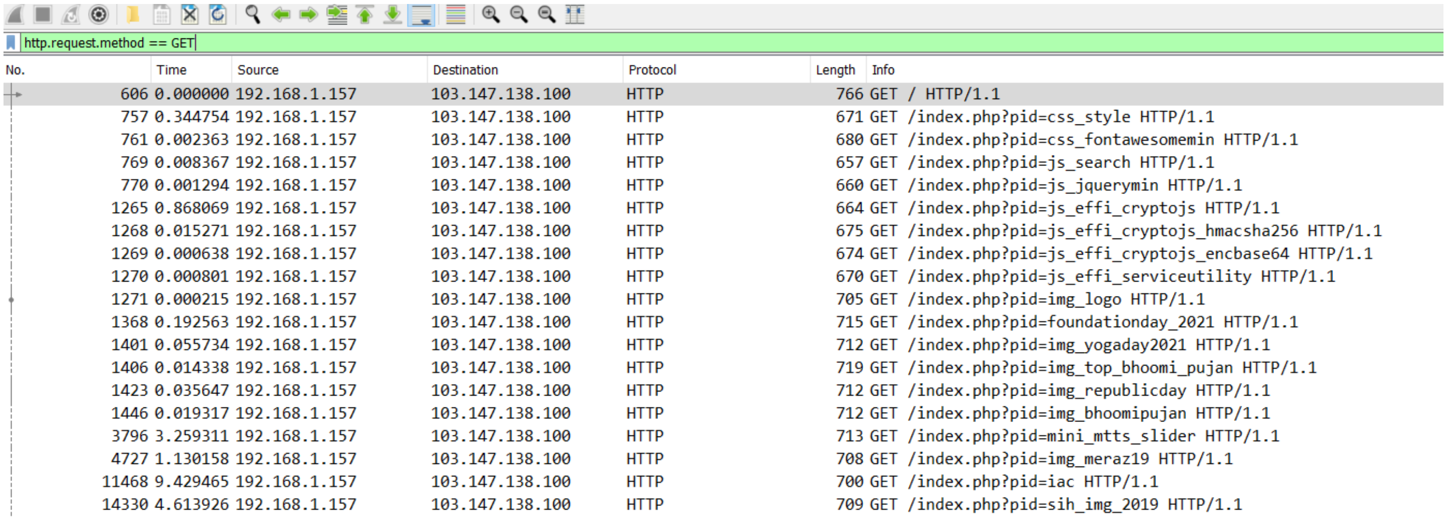
The preview shows that the image has been reconstructed from the hex dump displayed above.

This can be verified by the image that was used for the hex dump.

Also, the hex editor has completed reconstructing the image whose screenshot is attached above.

Question 3

Considering different GET Requests in the following screenshots. There is a mechanism to select the seconds before the display of the previous packet in the format of the Time of the displayed packets.



http.request.method == GET

No.	Time	Source	Destination	Protocol	Length	Info
606	0.000000	192.168.1.157	103.147.138.100	HTTP	766	GET / HTTP/1.1
757	0.344754	192.168.1.157	103.147.138.100	HTTP	671	GET /index.php?pid=css_style HTTP/1.1
761	0.002363	192.168.1.157	103.147.138.100	HTTP	680	GET /index.php?pid=css_fontawesomemin HTTP/1.1
769	0.008367	192.168.1.157	103.147.138.100	HTTP	657	GET /index.php?pid=js_search HTTP/1.1
770	0.001294	192.168.1.157	103.147.138.100	HTTP	660	GET /index.php?pid=js_jquerymin HTTP/1.1
1265	0.868069	192.168.1.157	103.147.138.100	HTTP	664	GET /index.php?pid=js_effi_cryptojs HTTP/1.1
1268	0.015271	192.168.1.157	103.147.138.100	HTTP	675	GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1
1269	0.000638	192.168.1.157	103.147.138.100	HTTP	674	GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
1270	0.000801	192.168.1.157	103.147.138.100	HTTP	670	GET /index.php?pid=js_effi_serviceutility HTTP/1.1
1271	0.000215	192.168.1.157	103.147.138.100	HTTP	705	GET /index.php?pid=img_logo HTTP/1.1
1368	0.192563	192.168.1.157	103.147.138.100	HTTP	715	GET /index.php?pid=foundationday_2021 HTTP/1.1
1401	0.055734	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_yogaday2021 HTTP/1.1
1406	0.014338	192.168.1.157	103.147.138.100	HTTP	719	GET /index.php?pid=img_top_bhoomi_pujan HTTP/1.1
1423	0.035647	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_republicday HTTP/1.1
1446	0.019317	192.168.1.157	103.147.138.100	HTTP	712	GET /index.php?pid=img_bhoomipujan HTTP/1.1
3796	3.259311	192.168.1.157	103.147.138.100	HTTP	713	GET /index.php?pid=mini_mtts_slider HTTP/1.1
4727	1.130158	192.168.1.157	103.147.138.100	HTTP	708	GET /index.php?pid=img_meraz19 HTTP/1.1
11468	9.429465	192.168.1.157	103.147.138.100	HTTP	700	GET /index.php?pid=iac HTTP/1.1
14330	4.613926	192.168.1.157	103.147.138.100	HTTP	709	GET /index.php?pid=sih_img_2019 HTTP/1.1

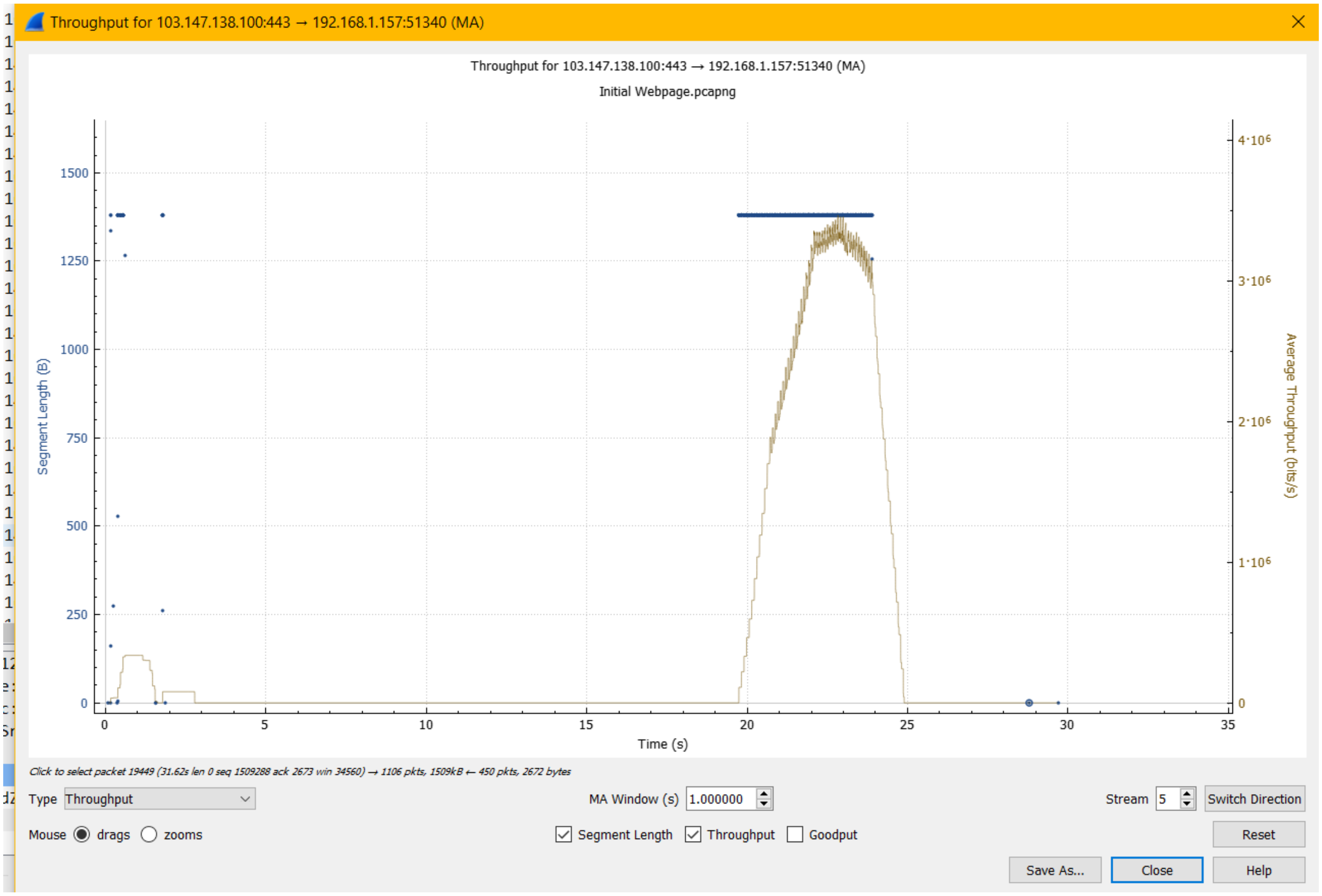
In this image, the Time column is modified to show the Seconds since the previous displayed packet. Since all packets displayed are from GET Request, it will essentially show the interpacket interval from the GET request.

The respective values are in the column.

Question 4

a. No background traffic is present

The throughput graph for a specific packet is: (Variation can be observed)



Throughput for 103.147.138.100:443 → 192.168.1.157:51340 (MA)

Click to select packet 19449 (31.62s len 0 seq 1509288 ack 2673 win 34560) → 1106 pkts, 1509kB ← 450 pkts, 2672 bytes

Type Throughput

MA Window (s) 1.000000

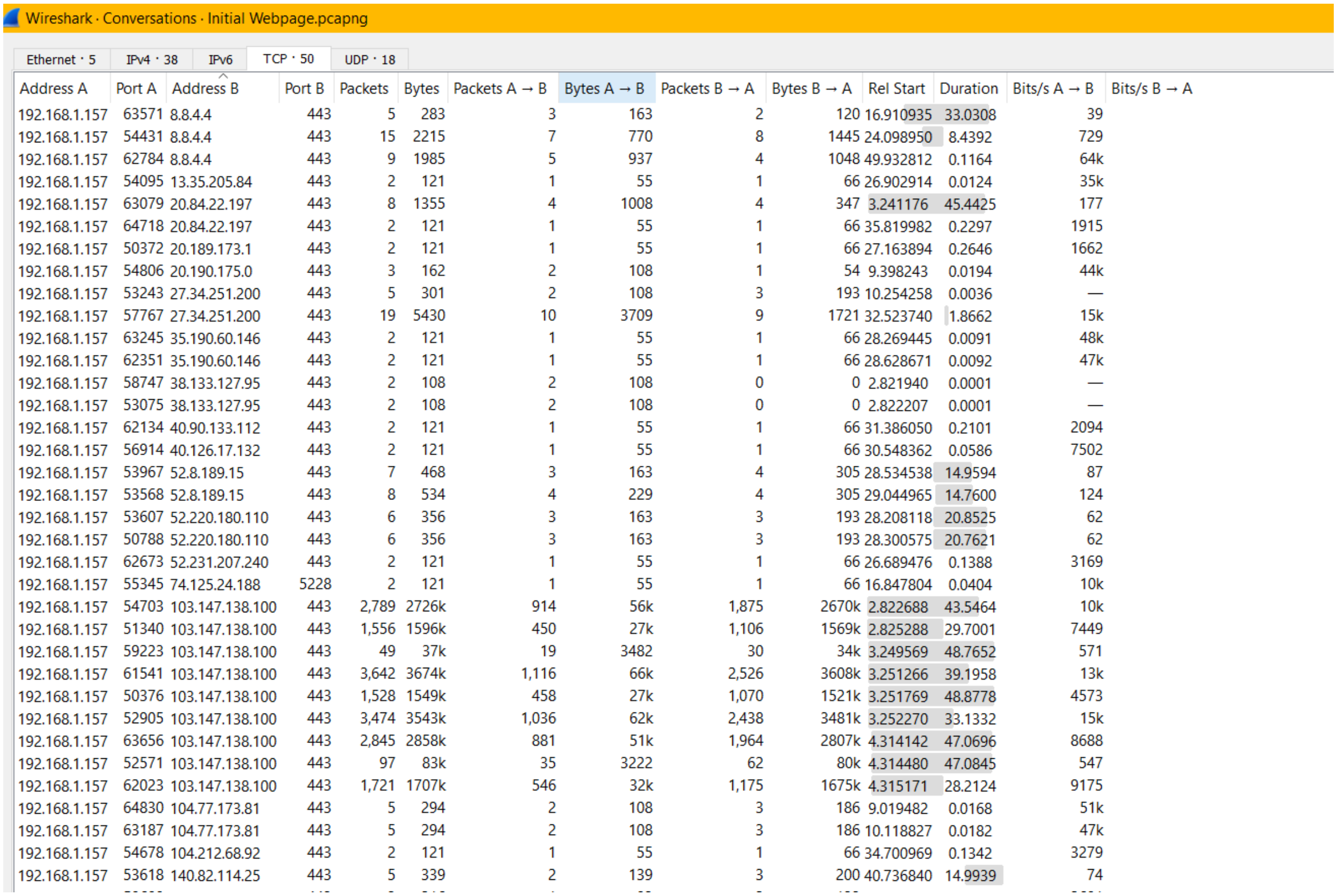
Stream 5

Mouse ● drags ○ zooms

☑ Segment Length ☑ Throughput □ Goodput

Shows the variation in the throughput with time.

The conversation chart:



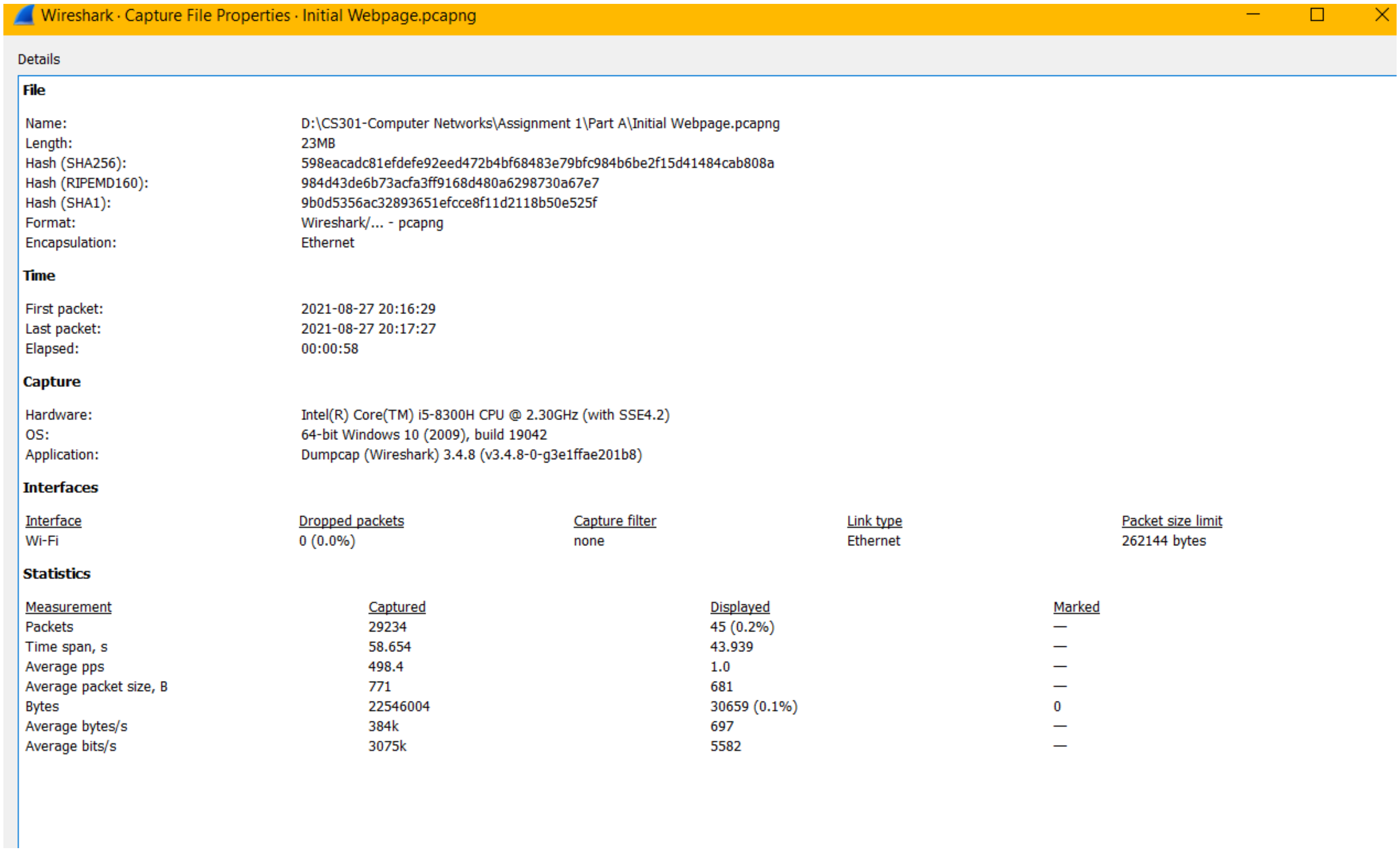
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.157	63571	8.8.4.4	443	5	283	3	163	2	120	16.910935	33.0308	39	
192.168.1.157	54431	8.8.4.4	443	15	2215	7	770	8	1445	24.098950	8.4392	729	
192.168.1.157	62784	8.8.4.4	443	9	1985	5	937	4	1048	49.932812	0.1164	64k	
192.168.1.157	54095	13.35.205.84	443	2	121	1	55	1	66	26.902914	0.0124	35k	
192.168.1.157	63079	20.84.22.197	443	8	1355	4	1008	4	347	3.241176	45.4425	177	
192.168.1.157	64718	20.84.22.197	443	2	121	1	55	1	66	35.819982	0.2297	1915	
192.168.1.157	50372	20.189.173.1	443	2	121	1	55	1	66	27.163894	0.2646	1662	
192.168.1.157	54806	20.190.175.0	443	3	162	2	108	1	54	9.398243	0.0194	44k	
192.168.1.157	53243	27.34.251.200	443	5	301	2	108	3	193	10.254258	0.0036	—	
192.168.1.157	57767	27.34.251.200	443	19	5430	10	3709	9	1721	32.523740	1.8662	15k	
192.168.1.157	63245	35.190.60.146	443	2	121	1	55	1	66	28.269445	0.0091	48k	
192.168.1.157	62351	35.190.60.146	443	2	121	1	55	1	66	28.628671	0.0092	47k	
192.168.1.157	58747	38.133.127.95	443	2	108	2	108	0	0	2.821940	0.0001	—	
192.168.1.157	53075	38.133.127.95	443	2	108	2	108	0	0	2.822207	0.0001	—	
192.168.1.157	62134	40.90.133.112	443	2	121	1	55	1	66	31.386050	0.2101	2094	
192.168.1.157	56914	40.126.17.132	443	2	121	1	55	1	66	30.548362	0.0586	7502	
192.168.1.157	53967	52.8.189.15	443	7	468	3	163	4	305	28.534538	14.9594	87	
192.168.1.157	53568	52.8.189.15	443	8	534	4	229	4	305	29.044965	14.7600	124	
192.168.1.157	53607	52.220.180.110	443	6	356	3	163	3	193	28.208118	20.8525	62	
192.168.1.157	50788	52.220.180.110	443	6	356	3	163	3	193	28.300575	20.7621	62	
192.168.1.157	62673	52.231.207.240	443	2	121	1	55	1	66	26.689476	0.1388	3169	
192.168.1.157	55345	74.125.24.188	5228	2	121	1	55	1	66	16.847804	0.0404	10k	
192.168.1.157	54703	103.147.138.100	443	2,789	2726k	914	56k	1,875	2670k	2.822688	43.5464	10k	
192.168.1.157	51340	103.147.138.100	443	1,556	1596k	450	27k	1,106	1569k	2.825288	29.7001	7449	
192.168.1.157	59223	103.147.138.100	443	49	37k	19	3482	30	34k	3.249569	48.7652	571	
192.168.1.157	61541	103.147.138.100	443	3,642	3674k	1,116	66k	2,526	3608k	3.251266	39.1958	13k	
192.168.1.157	50376	103.147.138.100	443	1,528	1549k	458	27k	1,070	1521k	3.251769	48.8778	4573	
192.168.1.157	52905	103.147.138.100	443	3,474	3543k	1,036	62k	2,438	3481k	3.252270	33.1332	15k	
192.168.1.157	63656	103.147.138.100	443	2,845	2858k	881	51k	1,964	2807k	4.314142	47.0696	8688	
192.168.1.157	52571	103.147.138.100	443	97	83k	35	3222	62	80k	4.314480	47.0845	547	
192.168.1.157	62023	103.147.138.100	443	1,721	1707k	546	32k	1,175	1675k	4.315171	28.2124	9175	
192.168.1.157	64830	104.77.173.81	443	5	294	2	108	3	186	9.019482	0.0168	51k	
192.168.1.157	63187	104.77.173.81	443	5	294	2	108	3	186	10.118827	0.0182	47k	
192.168.1.157	54678	104.212.68.92	443	2	121	1	55	1	66	34.700969	0.1342	3279	
192.168.1.157	53618	140.82.114.25	443	5	339	2	139	3	200	40.736840	14.9939	74	

It shows the total bytes transferred from each connection of 103.147.138.100 (IIT Bhilai Web page) to the local machine.

Throughput is the rate (bits/time unit) at which bits are being sent from sender to receiver.

With the data transferred (in bytes) and the duration of each connection, it is very easy to find the throughput at each connection in detail.

Capture File properties:


Wireshark · Capture File Properties · Initial Webpage.pcapng
Details

File

Name:	D:\CS301-Computer Networks\Assignment 1\Part A\Initial Webpage.pcapng
Length:	23MB
Hash (SHA256):	598eacadc81efdefe92eed472b4bf68483e79bfc984b6be2f15d41484cab808a
Hash (RIPEMD160):	984d43de6b73acfa3ff9168d480a6298730a67e7
Hash (SHA1):	9b0d5356ac32893651efcce8f11d2118b50e525f
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2021-08-27 20:16:29
Last packet:	2021-08-27 20:17:27
Elapsed:	00:00:58

Capture

Hardware:	Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz (with SSE4.2)
OS:	64-bit Windows 10 (2009), build 19042
Application:	Dumpcap (Wireshark) 3.4.8 (v3.4.8-0-g3e1ffae201b8)

Interfaces

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

Statistics

Measurement	Captured	Displayed	Marked
Packets	29234	45 (0.2%)	—
Time span, s	58.654	43.939	—
Average pps	498.4	1.0	—
Average packet size, B	771	681	—
Bytes	22546004	30659 (0.1%)	0
Average bytes/s	384k	697	—
Average bits/s	3075k	5582	—

If you note the displayed packets for the IIT Bhilai Web Page, it will give a total period of 43.939 seconds with the average bytes/s or bits/s, which is the essential throughput for the web page.

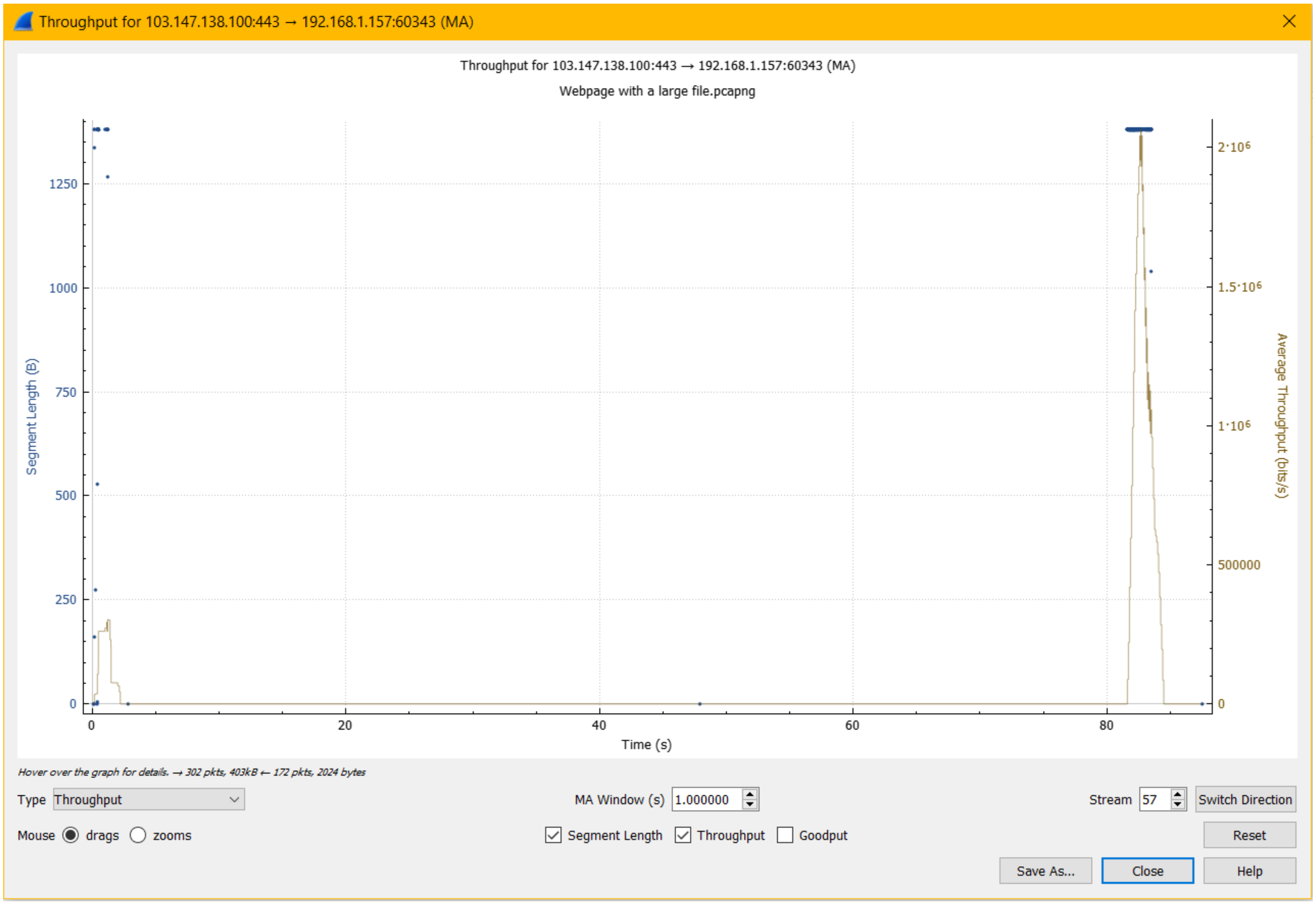
This spans for all the connections and gives an average result i.e., the observed throughput.

It is displayed above as 697 bytes/s or 5582 bits/s.

b. Large file download is going on

PCAP File: Webpage with a large file.pcapng

The throughput graph for a specific packet is: (Variation can be observed)


Throughput for 103.147.138.100:443 → 192.168.1.157:60343 (MA)
Throughput for 103.147.138.100:443 → 192.168.1.157:60343 (MA)
Webpage with a large file.pcapng
Segment Length (B)
1250
1000
750
500
250
0
0
20
40
60
80
Time (s)
2·10⁶
1.5·10⁶
1·10⁶
500000
0
Average Throughput (bits/s)

Hover over the graph for details. → 302 pkts, 403kB ← 172 pkts, 2024 bytes

Type Throughput

MA Window (s) 1.000000

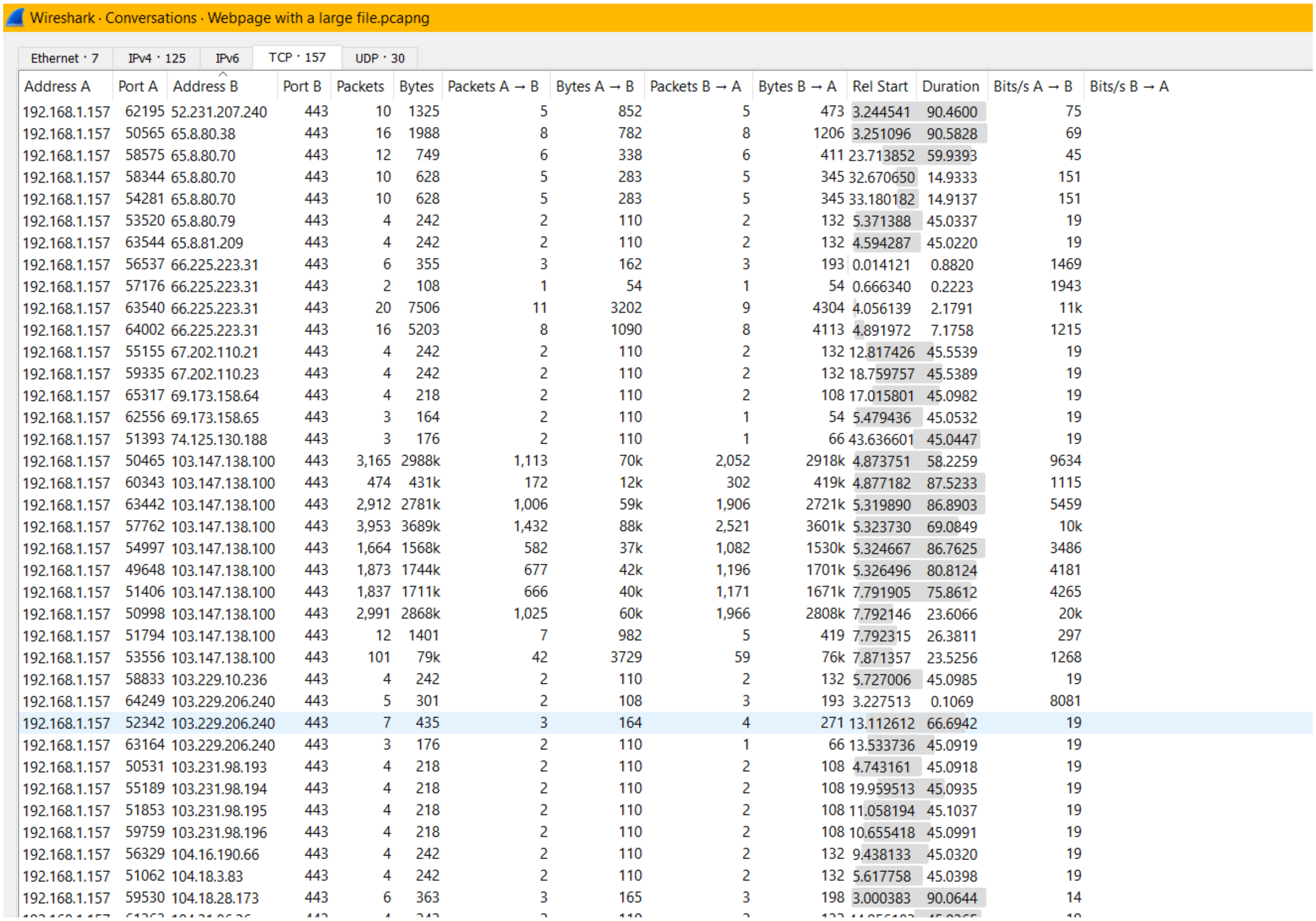
Stream 57

Mouse ● drags ○ zooms

☑ Segment Length ☑ Throughput □ Goodput

Switch Direction
Reset
Save As...
Close
Help

The conversation chart:



Wireshark · Conversations · Webpage with a large file.pcapng

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
192.168.1.157	62195	52.231.207.240	443	10	1325	5	852	5	473	3.244541	90.4600	75	
192.168.1.157	50565	65.8.80.38	443	16	1988	8	782	8	1206	3.251096	90.5828	69	
192.168.1.157	58575	65.8.80.70	443	12	749	6	338	6	411	23.713852	59.9393	45	
192.168.1.157	58344	65.8.80.70	443	10	628	5	283	5	345	32.670650	14.9333	151	
192.168.1.157	54281	65.8.80.70	443	10	628	5	283	5	345	33.180182	14.9137	151	
192.168.1.157	53520	65.8.80.79	443	4	242	2	110	2	132	5.371388	45.0337	19	
192.168.1.157	63544	65.8.81.209	443	4	242	2	110	2	132	4.594287	45.0220	19	
192.168.1.157	56537	66.225.223.31	443	6	355	3	162	3	193	0.014121	0.8820	1469	
192.168.1.157	57176	66.225.223.31	443	2	108	1	54	1	54	0.666340	0.2223	1943	
192.168.1.157	63540	66.225.223.31	443	20	7506	11	3202	9	4304	4.056139	2.1791	11k	
192.168.1.157	64002	66.225.223.31	443	16	5203	8	1090	8	4113	4.891972	7.1758	1215	
192.168.1.157	55155	67.202.110.21	443	4	242	2	110	2	132	12.817426	45.5539	19	
192.168.1.157	59335	67.202.110.23	443	4	242	2	110	2	132	18.759757	45.5389	19	
192.168.1.157	65317	69.173.158.64	443	4	218	2	110	2	108	17.015801	45.0982	19	
192.168.1.157	62556	69.173.158.65	443	3	164	2	110	1	54	5.479436	45.0532	19	
192.168.1.157	51393	74.125.130.188	443	3	176	2	110	1	66	43.636601	45.0447	19	
192.168.1.157	50465	103.147.138.100	443	3,165	2988k	1,113	70k	2,052	2918k	4.873751	58.2259	9634	
192.168.1.157	60343	103.147.138.100	443	474	431k	172	12k	302	419k	4.877182	87.5233	1115	
192.168.1.157	63442	103.147.138.100	443	2,912	2781k	1,006	59k	1,906	2721k	5.319890	86.8903	5459	
192.168.1.157	57762	103.147.138.100	443	3,953	3689k	1,432	88k	2,521	3601k	5.323730	69.0849	10k	
192.168.1.157	54997	103.147.138.100	443	1,664	1568k	582	37k	1,082	1530k	5.324667	86.7625	3486	
192.168.1.157	49648	103.147.138.100	443	1,873	1744k	677	42k	1,196	1701k	5.326496	80.8124	4181	
192.168.1.157	51406	103.147.138.100	443	1,837	1711k	666	40k	1,171	1671k	7.791905	75.8612	4265	
192.168.1.157	50998	103.147.138.100	443	2,991	2868k	1,025	60k	1,966	2808k	7.792146	23.6066	20k	
192.168.1.157	51794	103.147.138.100	443	12	1401	7	982	5	419	7.792315	26.3811	297	
192.168.1.157	53556	103.147.138.100	443	101	79k	42	3729	59	76k	7.871357	23.5256	1268	
192.168.1.157	58833	103.229.10.236	443	4	242	2	110	2	132	5.727006	45.0985	19	
192.168.1.157	64249	103.229.206.240	443	5	301	2	108	3	193	3.227513	0.1069	8081	
192.168.1.157	52342	103.229.206.240	443	7	435	3	164	4	271	13.112612	66.6942	19	
192.168.1.157	63164	103.229.206.240	443	3	176	2	110	1	66	13.533736	45.0919	19	
192.168.1.157	50531	103.231.98.193	443	4	218	2	110	2	108	4.743161	45.0918	19	
192.168.1.157	55189	103.231.98.194	443	4	218	2	110	2	108	19.959513	45.0935	19	
192.168.1.157	51853	103.231.98.195	443	4	218	2	110	2	108	11.058194	45.1037	19	
192.168.1.157	59759	103.231.98.196	443	4	218	2	110	2	108	10.655418	45.0991	19	
192.168.1.157	56329	104.16.190.66	443	4	242	2	110	2	132	9.438133	45.0320	19	
192.168.1.157	51062	104.18.3.83	443	4	242	2	110	2	132	5.617758	45.0398	19	
192.168.1.157	59530	104.18.28.173	443	6	363	3	165	3	198	3.000383	90.0644	14	

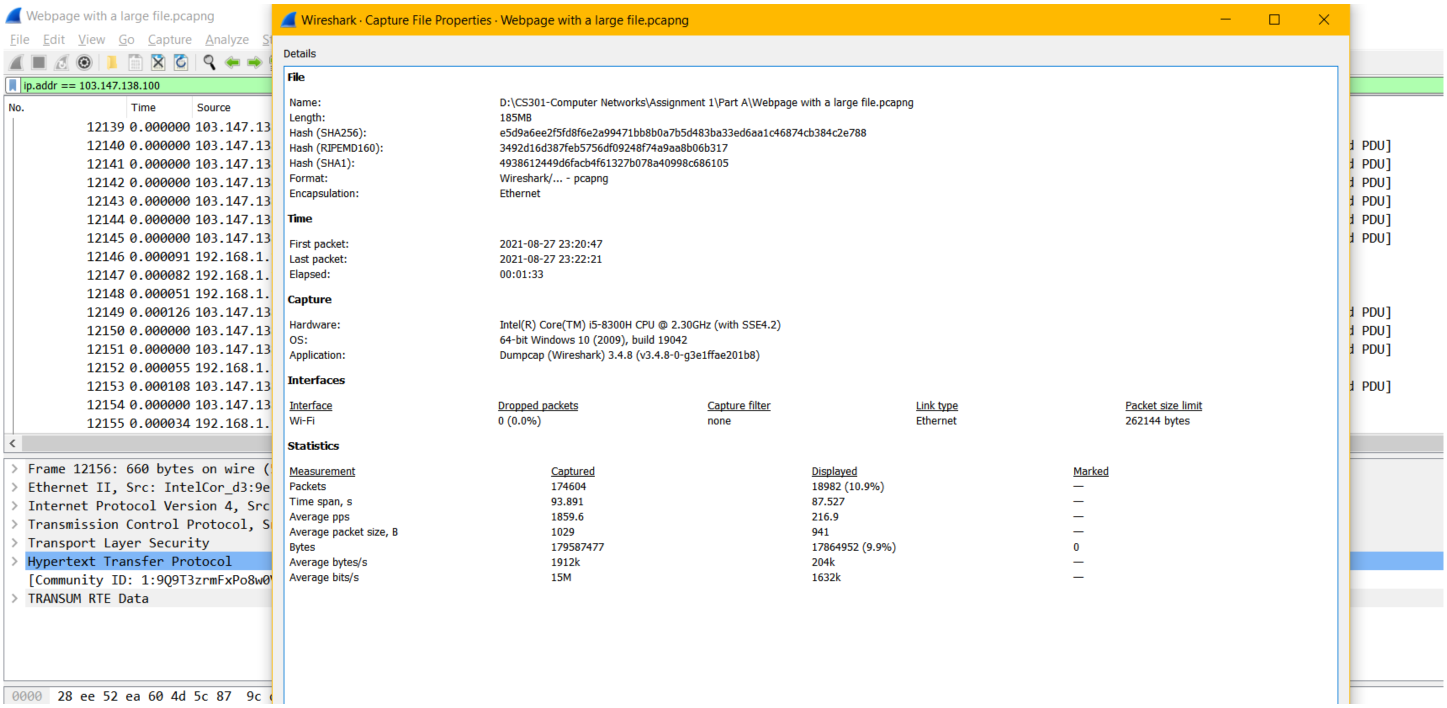
It shows the total bytes transferred from each connection of 103.147.138.100 (IIT Bhilai Web page) to the local machine.

Since the download of a very large file is going on, it is important to focus only on the connections and timely delivery of the web page being rendered. The size will remain the same as (a) part but the loading time will be longer that is the rendering time for the page is more. It can be verified by the longer duration in which the connection is open.

Throughput is the rate (bits/time unit) at which bits are being sent from sender to receiver.

With the data transferred (in bytes) and the duration of each connection, it is very easy to find the throughput at each connection in detail.

Capture File properties:



Webpage with a large file.pcapng
File Edit View Go Capture Analyze St

```
ip.addr == 103.147.138.100

No.     Time     Source
  12139 0.000000 103.147.13
  12140 0.000000 103.147.13
  12141 0.000000 103.147.13
  12142 0.000000 103.147.13
  12143 0.000000 103.147.13
  12144 0.000000 103.147.13
  12145 0.000000 103.147.13
  12146 0.000091 192.168.1.
  12147 0.000082 192.168.1.
  12148 0.000051 192.168.1.
  12149 0.000126 103.147.13
  12150 0.000000 103.147.13
  12151 0.000000 103.147.13
  12152 0.000055 192.168.1.
  12153 0.000108 103.147.13
  12154 0.000000 103.147.13
  12155 0.000034 192.168.1.

> Frame 12156: 660 bytes on wire (
> Ethernet II, Src: IntelCor_d3:9e
> Internet Protocol Version 4, Src
> Transmission Control Protocol, S
> Transport Layer Security
> Hypertext Transfer Protocol
  [Community ID: 1:9Q9T3zrmFxPo8w0
> TRANSUM RTE Data

0000  28 ee 52 ea 60 4d 5c 87  9c
```

Wireshark · Capture File Properties · Webpage with a large file.pcapng

Details

File

Name:	D:\CS301-Computer Networks\Assignment 1\Part A\Webpage with a large file.pcapng
Length:	185MB
Hash (SHA256):	e5d9a6ee2f5fd8f6e2a99471bb8b0a7b5d483ba33ed6aa1c46874cb384c2e788
Hash (RIPEMD160):	3492d16d387feb5756df09248f74a9aa8b06b317
Hash (SHA1):	4938612449d6facb4f61327b078a40998c686105
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2021-08-27 23:20:47
Last packet:	2021-08-27 23:22:21
Elapsed:	00:01:33

Capture

Hardware:	Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz (with SSE4.2)
OS:	64-bit Windows 10 (2009), build 19042
Application:	Dumpcap (Wireshark) 3.4.8 (v3.4.8-0-g3e1ffae201b8)

Interfaces

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

Statistics

Measurement	Captured	Displayed	Marked
Packets	174604	18982 (10.9%)	—
Time span, s	93.891	87.527	—
Average pps	1859.6	216.9	—
Average packet size, B	1029	941	—
Bytes	179587477	17864952 (9.9%)	0
Average bytes/s	1912k	204k	—
Average bits/s	15M	1632k	—

If you note the displayed packets for the IIT Bhilai Web Page, it will give a total period of 87.527 seconds with the average bytes/s or bits/s, which is the essential throughput for the web page.

This spans for all the connections and gives an average result i.e., the observed throughput.

It is displayed above as 204k bytes/s or 1632k bits/s.

Part 2 or Part B

Question 1

PCAP File: stackoverflow.pcapng

Website taken: www.stackoverflow.com (IP Address: 151.101.1.69)

Start capturing packets on Wireshark before loading the website. Enter the URL on the browser and wait for the page to load. Once the page with all its components has loaded then stop the packet capturing.

First, to reach the host in human-readable format, first DNS requests are sent through the TCP mechanism. Once the host is reached, we can open a socket or port on our computer to begin communication.

With the connection established HTTPS (using HTTP1 or HTTP2) packets are used which can be seen by the transmission of packets to and from the localhost. HTTP is not the only protocol in use. The transport is controlled by TCP which does the job of guaranteeing the transmission. HTTP only transfers the packets, data, and headers.

With the transfer of packets, data is transferred in the form of HTML, JSON, CSS files. Other data is also transferred in specific formats which include images, videos, documented files, etc.

HTTP responses are sent from the local machine to acknowledge the packets and requests for the necessary packets or pages or data within the website. The process continues till all the data and information has been acquired by the user.

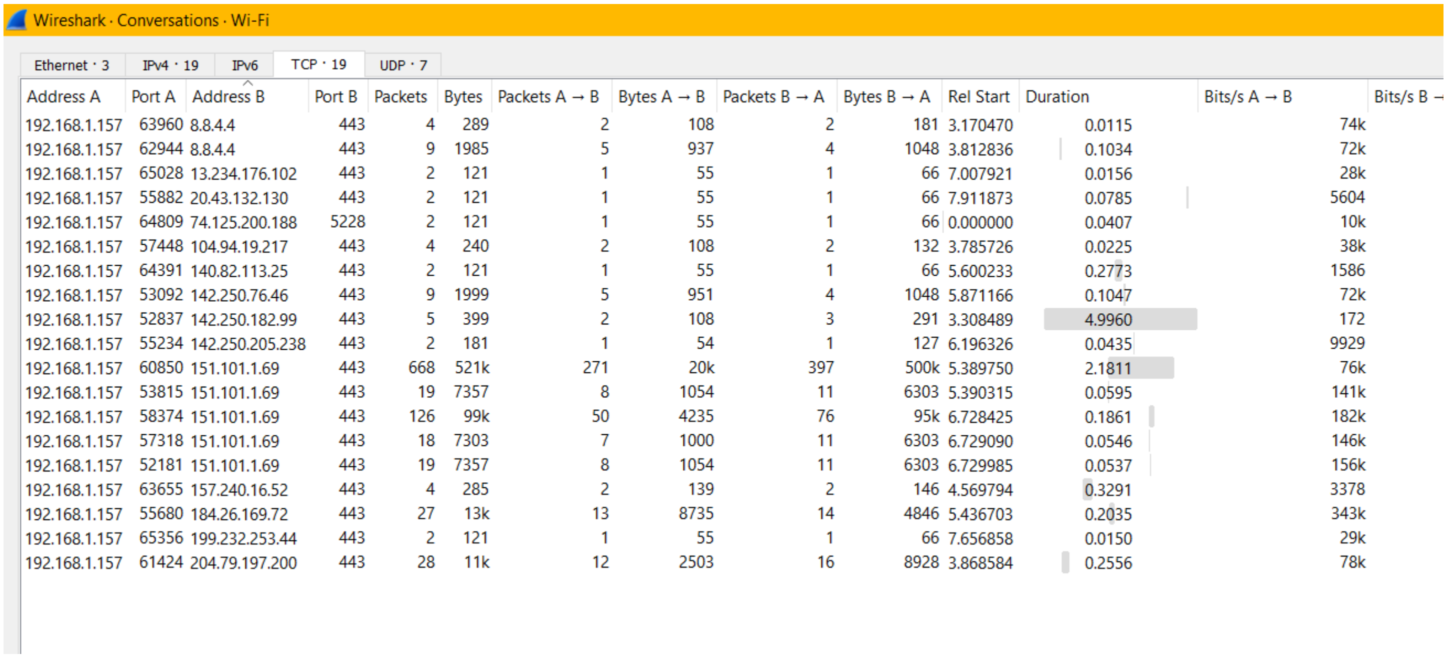
The connections are persistent as multiple objects are transferred back and forth. Multiple connections are also established to transfer more data through more sockets based on the requirements.

Once the rendering and transmission are complete, we can terminate the connection and transfer of files and necessary data. After this the capture can be stopped, data has been received and analysis can be done.

To see the GET Requests in Wireshark, the necessary filter can be applied after all the packets have been loaded.

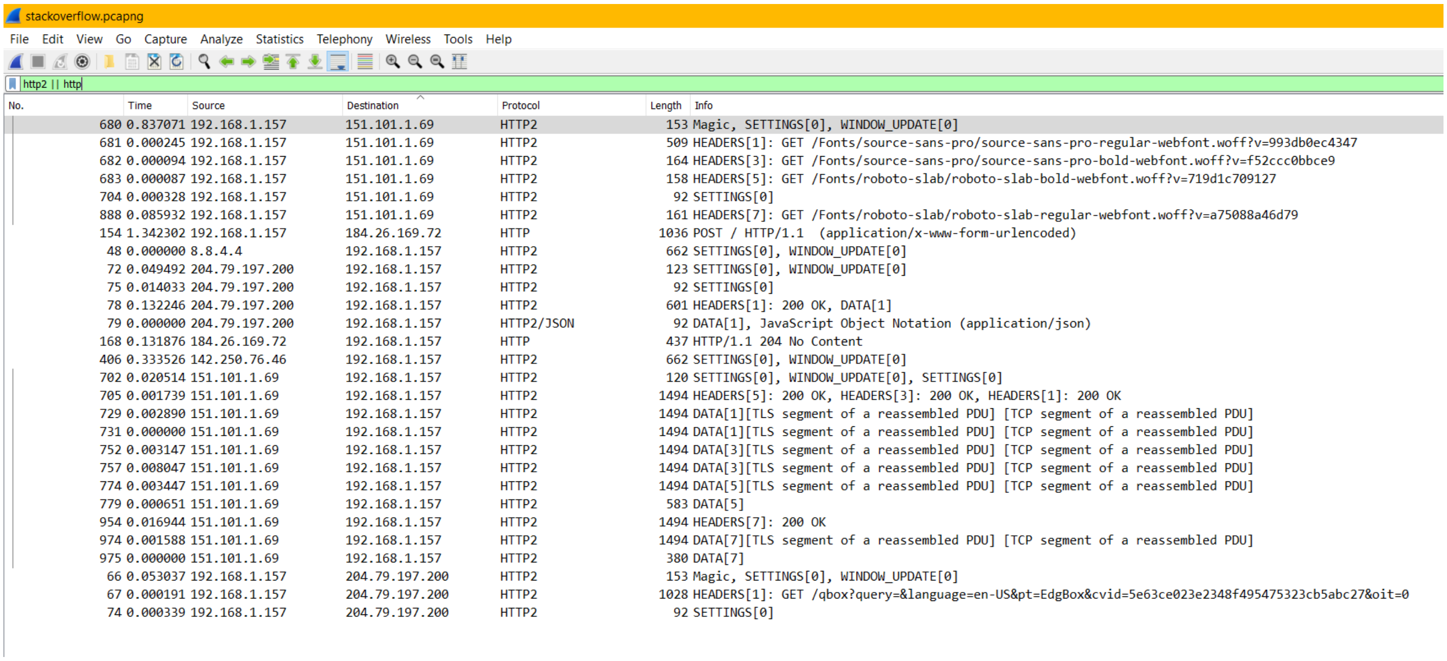
The job of Wireshark is to only capture all the packets that have gone or come from the webpage to the localhost. The computer opens up a port for the transmission of packets and Wireshark uses this to keep a copy of all the packets and associated frames.

Wireshark only helps to analyze the protocols used at each step, the connections to the page, packet transfer, and the end-to-end process. The job of packet assembly and rendering of the page is done by the browser. Wireshark can also be used for troubleshooting during an erroneous load of a page.



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 –
192.168.1.157	63960	8.8.4.4	443	4	289	2	108	2	181	3.170470	0.0115	74k	
192.168.1.157	62944	8.8.4.4	443	9	1985	5	937	4	1048	3.812836	0.1034	72k	
192.168.1.157	65028	13.234.176.102	443	2	121	1	55	1	66	7.007921	0.0156	28k	
192.168.1.157	55882	20.43.132.130	443	2	121	1	55	1	66	7.911873	0.0785	5604	
192.168.1.157	64809	74.125.200.188	5228	2	121	1	55	1	66	0.000000	0.0407	10k	
192.168.1.157	57448	104.94.19.217	443	4	240	2	108	2	132	3.785726	0.0225	38k	
192.168.1.157	64391	140.82.113.25	443	2	121	1	55	1	66	5.600233	0.2773	1586	
192.168.1.157	53092	142.250.76.46	443	9	1999	5	951	4	1048	5.871166	0.1047	72k	
192.168.1.157	52837	142.250.182.99	443	5	399	2	108	3	291	3.308489	4.9960	172	
192.168.1.157	55234	142.250.205.238	443	2	181	1	54	1	127	6.196326	0.0435	9929	
192.168.1.157	60850	151.101.1.69	443	668	521k	271	20k	397	500k	5.389750	2.1811	76k	
192.168.1.157	53815	151.101.1.69	443	19	7357	8	1054	11	6303	5.390315	0.0595	141k	
192.168.1.157	58374	151.101.1.69	443	126	99k	50	4235	76	95k	6.728425	0.1861	182k	
192.168.1.157	57318	151.101.1.69	443	18	7303	7	1000	11	6303	6.729090	0.0546	146k	
192.168.1.157	52181	151.101.1.69	443	19	7357	8	1054	11	6303	6.729985	0.0537	156k	
192.168.1.157	63655	157.240.16.52	443	4	285	2	139	2	146	4.569794	0.3291	3378	
192.168.1.157	55680	184.26.169.72	443	27	13k	13	8735	14	4846	5.436703	0.2035	343k	
192.168.1.157	65356	199.232.253.44	443	2	121	1	55	1	66	7.656858	0.0150	29k	
192.168.1.157	61424	204.79.197.200	443	28	11k	12	2503	16	8928	3.868584	0.2556	78k	

The website uses TCP to transfer the packets. There are 5 TCP connections to transfer the page to the local system (192.168.1.157). Since all the connections run in parallel, the maximum duration will be taken among all 5 connections. So, the maximum value is 2.1811 seconds to load the page.



http2 || http

No.	Time	Source	Destination	Protocol	Length	Info
680	0.837071	192.168.1.157	151.101.1.69	HTTP2	153	Magic, SETTINGS[0], WINDOW_UPDATE[0]
681	0.000245	192.168.1.157	151.101.1.69	HTTP2	509	HEADERS[1]: GET /Fonts/source-sans-pro/source-sans-pro-regular-webfont.woff?v=993db0ec4347
682	0.000094	192.168.1.157	151.101.1.69	HTTP2	164	HEADERS[3]: GET /Fonts/source-sans-pro/source-sans-pro-bold-webfont.woff?v=f52ccc0bbce9
683	0.000087	192.168.1.157	151.101.1.69	HTTP2	158	HEADERS[5]: GET /Fonts/roboto-slab/roboto-slab-bold-webfont.woff?v=719d1c709127
704	0.000328	192.168.1.157	151.101.1.69	HTTP2	92	SETTINGS[0]
888	0.085932	192.168.1.157	151.101.1.69	HTTP2	161	HEADERS[7]: GET /Fonts/roboto-slab/roboto-slab-regular-webfont.woff?v=a75088a46d79
154	1.342302	192.168.1.157	184.26.169.72	HTTP	1036	POST / HTTP/1.1 (application/x-www-form-urlencoded)
48	0.000000	8.8.4.4	192.168.1.157	HTTP2	662	SETTINGS[0], WINDOW_UPDATE[0]
72	0.049492	204.79.197.200	192.168.1.157	HTTP2	123	SETTINGS[0], WINDOW_UPDATE[0]
75	0.014033	204.79.197.200	192.168.1.157	HTTP2	92	SETTINGS[0]
78	0.132246	204.79.197.200	192.168.1.157	HTTP2	601	HEADERS[1]: 200 OK, DATA[1]
79	0.000000	204.79.197.200	192.168.1.157	HTTP2/JSON	92	DATA[1], JavaScript Object Notation (application/json)
168	0.131876	184.26.169.72	192.168.1.157	HTTP	437	HTTP/1.1 204 No Content
406	0.333526	142.250.76.46	192.168.1.157	HTTP2	662	SETTINGS[0], WINDOW_UPDATE[0]
702	0.020514	151.101.1.69	192.168.1.157	HTTP2	120	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
705	0.001739	151.101.1.69	192.168.1.157	HTTP2	1494	HEADERS[5]: 200 OK, HEADERS[3]: 200 OK, HEADERS[1]: 200 OK
729	0.002890	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[1][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
731	0.000000	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[1][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
752	0.003147	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[3][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
757	0.008047	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[3][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
774	0.003447	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[5][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
779	0.000651	151.101.1.69	192.168.1.157	HTTP2	583	DATA[5]
954	0.016944	151.101.1.69	192.168.1.157	HTTP2	1494	HEADERS[7]: 200 OK
974	0.001588	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[7][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
975	0.000000	151.101.1.69	192.168.1.157	HTTP2	380	DATA[7]
66	0.053037	192.168.1.157	204.79.197.200	HTTP2	153	Magic, SETTINGS[0], WINDOW_UPDATE[0]
67	0.000191	192.168.1.157	204.79.197.200	HTTP2	1028	HEADERS[1]: GET /qbox?query=&language=en-US&pt=EdgBox&cvid=5e63ce023e2348f495475323cb5abc27&oit=0
74	0.000339	192.168.1.157	204.79.197.200	HTTP2	92	SETTINGS[0]

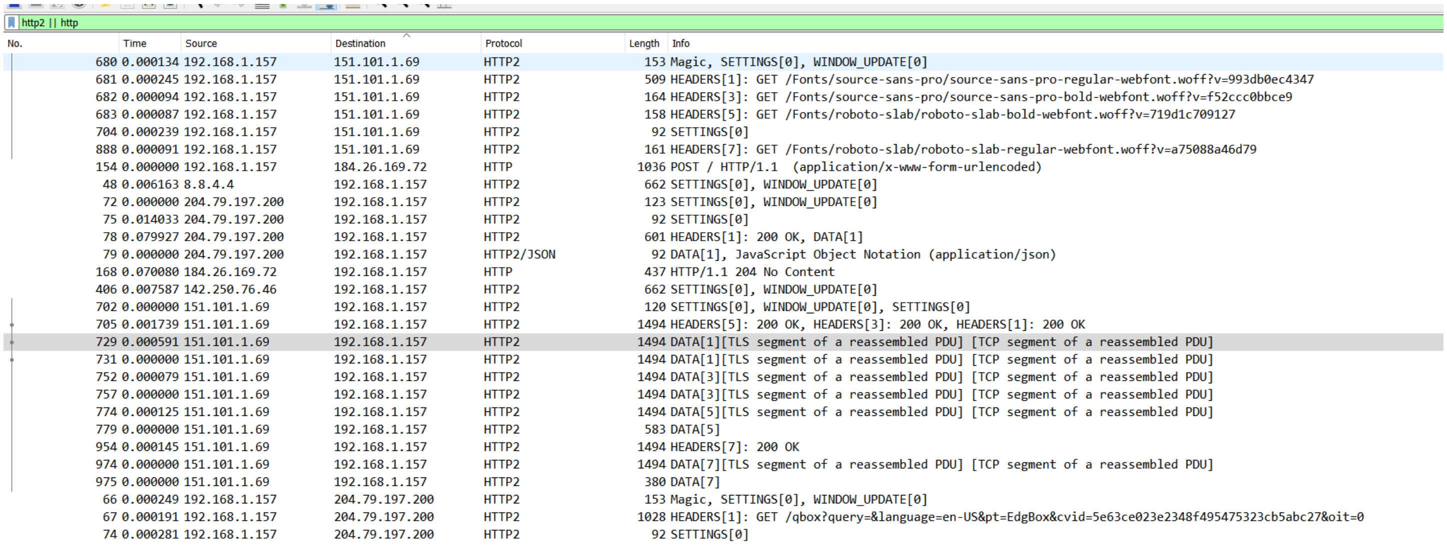
Since all the connections to and from the webpage to my local system use the HTTP2 protocol (verified in the above image), all the connections are persistent. All HTTP2 connections are persistent and only one connection per origin is needed (hence 443 port is used for all 5 connections) by default hence all the 5 connections are persistent.

Among all the packets captured in the HTTP and HTTP2 protocol for the website, objects consist of those packets displayed whose information has some content.

It is important to note that packets for the handshake, checksum, calculation, closure, acknowledgment, etc. cannot be considered. So, if there is some form of content in the packet, file, text, graphics, etc., they are considered as objects.

We need to see those that are transferred across connections 192.168.1.157 and 151.101.1.69 (localhost and webpage). In the image above, not counting the packets that have no content, we have 8 objects that transfer some data. I am not counting packets for headers, settings, and those that belong to a different connection.

To find the object that took the longest to download, we need to consider the connection from the webpage to localhost (we are downloading).



http2 || http

No.	Time	Source	Destination	Protocol	Length	Info
680	0.000134	192.168.1.157	151.101.1.69	HTTP2	153	Magic, SETTINGS[0], WINDOW_UPDATE[0]
681	0.000245	192.168.1.157	151.101.1.69	HTTP2	509	HEADERS[1]: GET /Fonts/source-sans-pro/source-sans-pro-regular-webfont.woff?v=993db0ec4347
682	0.000094	192.168.1.157	151.101.1.69	HTTP2	164	HEADERS[3]: GET /Fonts/source-sans-pro/source-sans-pro-bold-webfont.woff?v=f52ccc0bbce9
683	0.000087	192.168.1.157	151.101.1.69	HTTP2	158	HEADERS[5]: GET /Fonts/roboto-slab/roboto-slab-bold-webfont.woff?v=719d1c709127
704	0.000239	192.168.1.157	151.101.1.69	HTTP2	92	SETTINGS[0]
888	0.000091	192.168.1.157	151.101.1.69	HTTP2	161	HEADERS[7]: GET /Fonts/roboto-slab/roboto-slab-regular-webfont.woff?v=a75088a46d79
154	0.000000	192.168.1.157	184.26.169.72	HTTP	1036	POST / HTTP/1.1 (application/x-www-form-urlencoded)
48	0.006163	8.8.4.4	192.168.1.157	HTTP2	662	SETTINGS[0], WINDOW_UPDATE[0]
72	0.000000	204.79.197.200	192.168.1.157	HTTP2	123	SETTINGS[0], WINDOW_UPDATE[0]
75	0.014033	204.79.197.200	192.168.1.157	HTTP2	92	SETTINGS[0]
78	0.079927	204.79.197.200	192.168.1.157	HTTP2	601	HEADERS[1]: 200 OK, DATA[1]
79	0.000000	204.79.197.200	192.168.1.157	HTTP2/JSON	92	DATA[1], JavaScript Object Notation (application/json)
168	0.070080	184.26.169.72	192.168.1.157	HTTP	437	HTTP/1.1 204 No Content
406	0.007587	142.250.76.46	192.168.1.157	HTTP2	662	SETTINGS[0], WINDOW_UPDATE[0]
702	0.000000	151.101.1.69	192.168.1.157	HTTP2	120	SETTINGS[0], WINDOW_UPDATE[0], SETTINGS[0]
705	0.001739	151.101.1.69	192.168.1.157	HTTP2	1494	HEADERS[5]: 200 OK, HEADERS[3]: 200 OK, HEADERS[1]: 200 OK
729	0.000591	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[1][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
731	0.000000	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[1][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
752	0.000079	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[3][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
757	0.000000	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[3][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
774	0.000125	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[5][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
779	0.000000	151.101.1.69	192.168.1.157	HTTP2	583	DATA[5]
954	0.000145	151.101.1.69	192.168.1.157	HTTP2	1494	HEADERS[7]: 200 OK
974	0.000000	151.101.1.69	192.168.1.157	HTTP2	1494	DATA[7][TLS segment of a reassembled PDU] [TCP segment of a reassembled PDU]
975	0.000000	151.101.1.69	192.168.1.157	HTTP2	380	DATA[7]
66	0.000249	192.168.1.157	204.79.197.200	HTTP2	153	Magic, SETTINGS[0], WINDOW_UPDATE[0]
67	0.000191	192.168.1.157	204.79.197.200	HTTP2	1028	HEADERS[1]: GET /qbox?query=&language=en-US&pt=EdgBox&cvid=5e63ce023e2348f495475323cb5abc27&oit=0
74	0.000281	192.168.1.157	204.79.197.200	HTTP2	92	SETTINGS[0]

Once this is done, we just need to set the time to display the difference between the capture of the previous object.

Check the data transfer from webpage to host and we need the longest download time, so we select the biggest time.

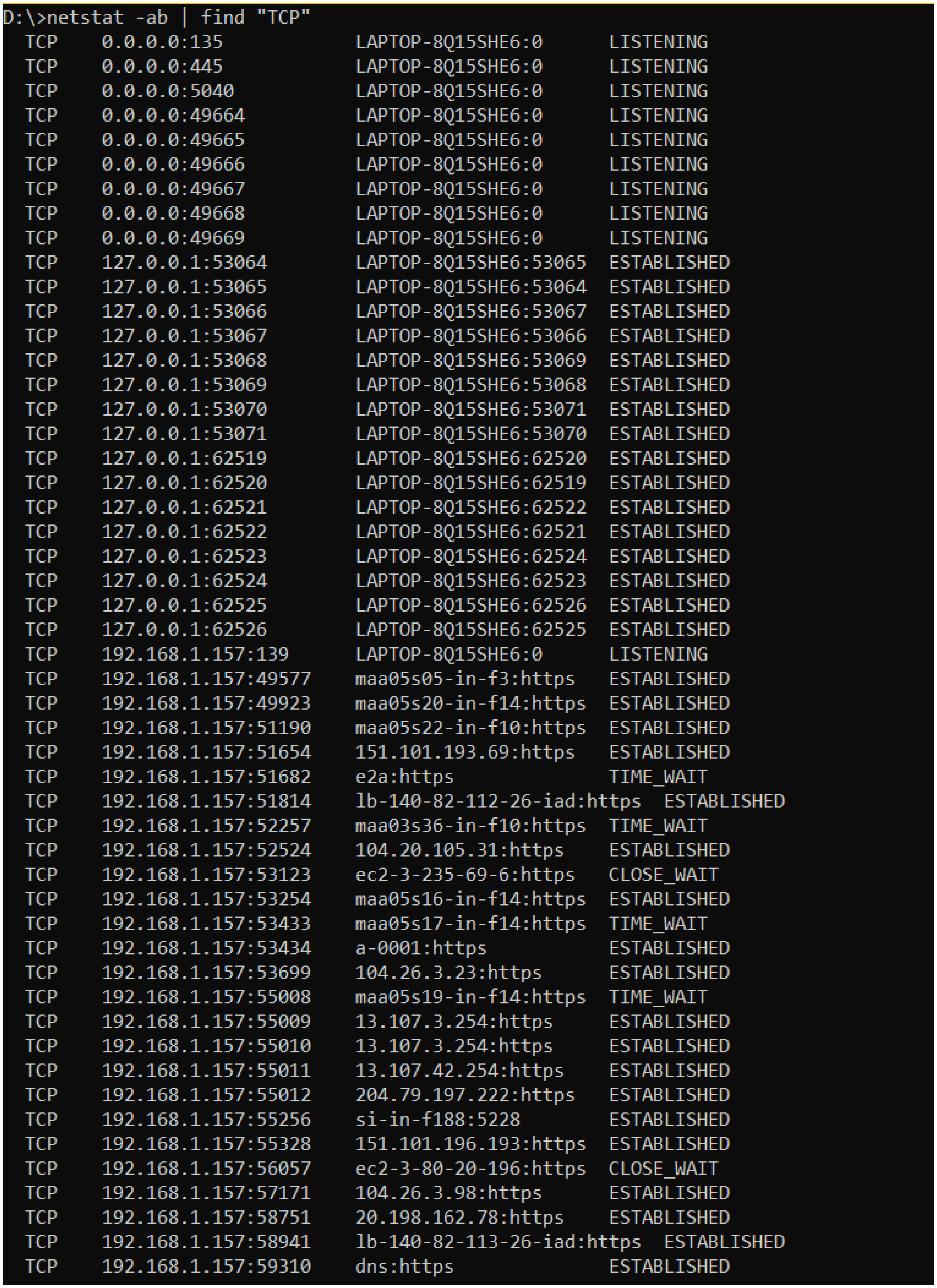
From the above figure, this value is packet/object 729 taking 0.000591 seconds to download.

There is another way to count the objects downloaded by exporting the objects in the File option in Wireshark. However, that is useful for HTTP packets. The website, Stack Overflow uses the HTTP2 protocol for the transfer of data, so this option is of no use. The option to export HTTP2 objects is still under development in the Wireshark GitLab repository (It is written in the documentation of Wireshark).

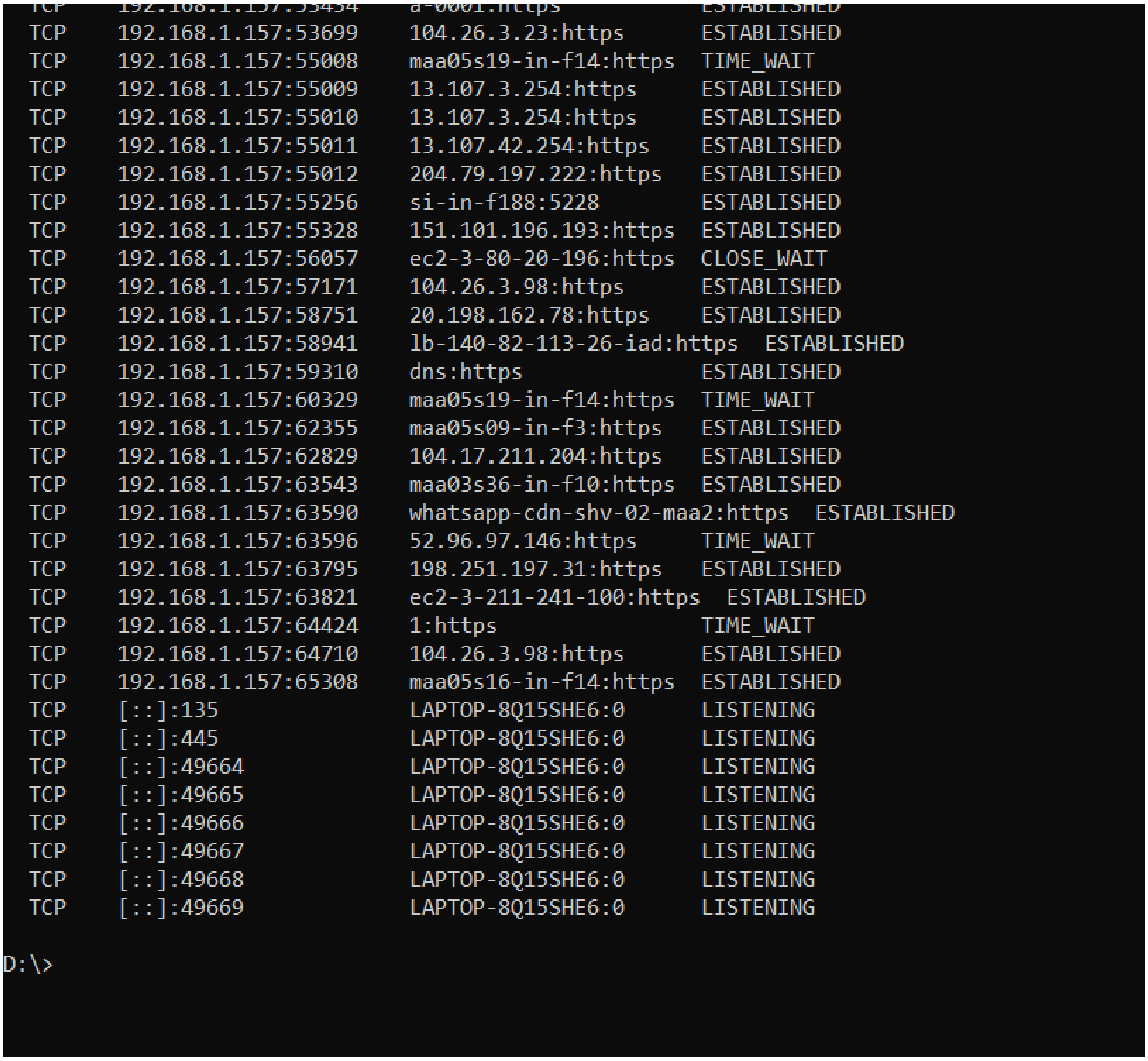
For a website using HTTP only transfer, this method will come in handy otherwise the above method is worthwhile.

Question 2

Active connections that use TCP Ports can be done by using the “netstat -ab” command in the Administrator Command Prompt. This command prints all UDP ports as well, so pipelining “find TCP” will select only the Active TCP Ports.



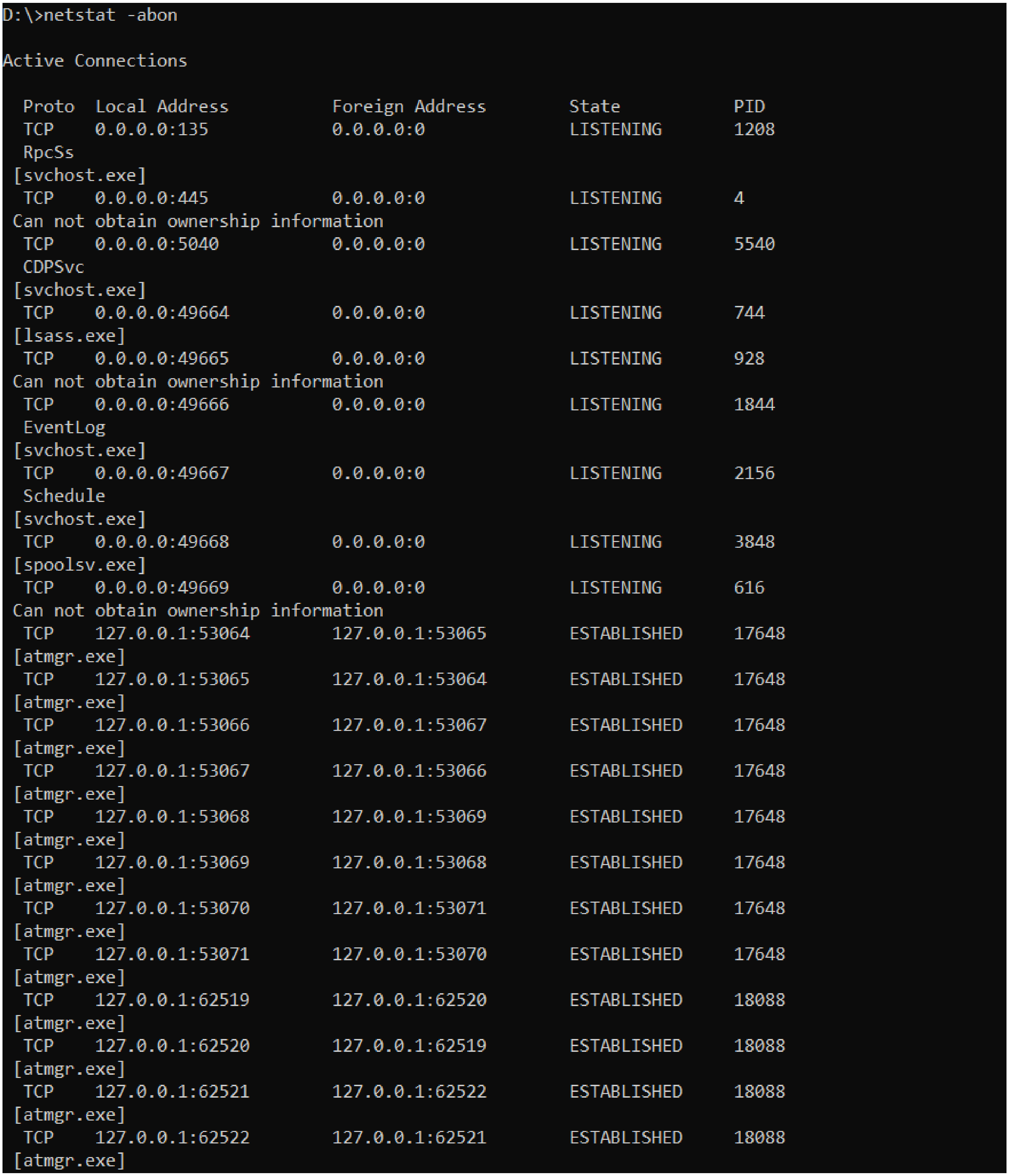
```
D:\>netstat -ab | find "TCP"
  TCP    0.0.0.0:135            LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    0.0.0.0:49669          LAPTOP-8Q15SHE6:0      LISTENING
  TCP    127.0.0.1:53064        LAPTOP-8Q15SHE6:53065  ESTABLISHED
  TCP    127.0.0.1:53065        LAPTOP-8Q15SHE6:53064  ESTABLISHED
  TCP    127.0.0.1:53066        LAPTOP-8Q15SHE6:53067  ESTABLISHED
  TCP    127.0.0.1:53067        LAPTOP-8Q15SHE6:53066  ESTABLISHED
  TCP    127.0.0.1:53068        LAPTOP-8Q15SHE6:53069  ESTABLISHED
  TCP    127.0.0.1:53069        LAPTOP-8Q15SHE6:53068  ESTABLISHED
  TCP    127.0.0.1:53070        LAPTOP-8Q15SHE6:53071  ESTABLISHED
  TCP    127.0.0.1:53071        LAPTOP-8Q15SHE6:53070  ESTABLISHED
  TCP    127.0.0.1:62519        LAPTOP-8Q15SHE6:62520  ESTABLISHED
  TCP    127.0.0.1:62520        LAPTOP-8Q15SHE6:62519  ESTABLISHED
  TCP    127.0.0.1:62521        LAPTOP-8Q15SHE6:62522  ESTABLISHED
  TCP    127.0.0.1:62522        LAPTOP-8Q15SHE6:62521  ESTABLISHED
  TCP    127.0.0.1:62523        LAPTOP-8Q15SHE6:62524  ESTABLISHED
  TCP    127.0.0.1:62524        LAPTOP-8Q15SHE6:62523  ESTABLISHED
  TCP    127.0.0.1:62525        LAPTOP-8Q15SHE6:62526  ESTABLISHED
  TCP    127.0.0.1:62526        LAPTOP-8Q15SHE6:62525  ESTABLISHED
  TCP    192.168.1.157:139      LAPTOP-8Q15SHE6:0      LISTENING
  TCP    192.168.1.157:49577    maa05s05-in-f3:https   ESTABLISHED
  TCP    192.168.1.157:49923    maa05s20-in-f14:https  ESTABLISHED
  TCP    192.168.1.157:51190    maa05s22-in-f10:https  ESTABLISHED
  TCP    192.168.1.157:51654    151.101.193.69:https   ESTABLISHED
  TCP    192.168.1.157:51682    e2a:https              TIME_WAIT
  TCP    192.168.1.157:51814    lb-140-82-112-26-iad:https  ESTABLISHED
  TCP    192.168.1.157:52257    maa03s36-in-f10:https  TIME_WAIT
  TCP    192.168.1.157:52524    104.20.105.31:https    ESTABLISHED
  TCP    192.168.1.157:53123    ec2-3-235-69-6:https   CLOSE_WAIT
  TCP    192.168.1.157:53254    maa05s16-in-f14:https  ESTABLISHED
  TCP    192.168.1.157:53433    maa05s17-in-f14:https  TIME_WAIT
  TCP    192.168.1.157:53434    a-0001:https           ESTABLISHED
  TCP    192.168.1.157:53699    104.26.3.23:https      ESTABLISHED
  TCP    192.168.1.157:55008    maa05s19-in-f14:https  TIME_WAIT
  TCP    192.168.1.157:55009    13.107.3.254:https     ESTABLISHED
  TCP    192.168.1.157:55010    13.107.3.254:https     ESTABLISHED
  TCP    192.168.1.157:55011    13.107.42.254:https    ESTABLISHED
  TCP    192.168.1.157:55012    204.79.197.222:https   ESTABLISHED
  TCP    192.168.1.157:55256    si-in-f188:5228        ESTABLISHED
  TCP    192.168.1.157:55328    151.101.196.193:https  ESTABLISHED
  TCP    192.168.1.157:56057    ec2-3-80-20-196:https  CLOSE_WAIT
  TCP    192.168.1.157:57171    104.26.3.98:https      ESTABLISHED
  TCP    192.168.1.157:58751    20.198.162.78:https    ESTABLISHED
  TCP    192.168.1.157:58941    lb-140-82-113-26-iad:https  ESTABLISHED
  TCP    192.168.1.157:59310    dns:https              ESTABLISHED
```



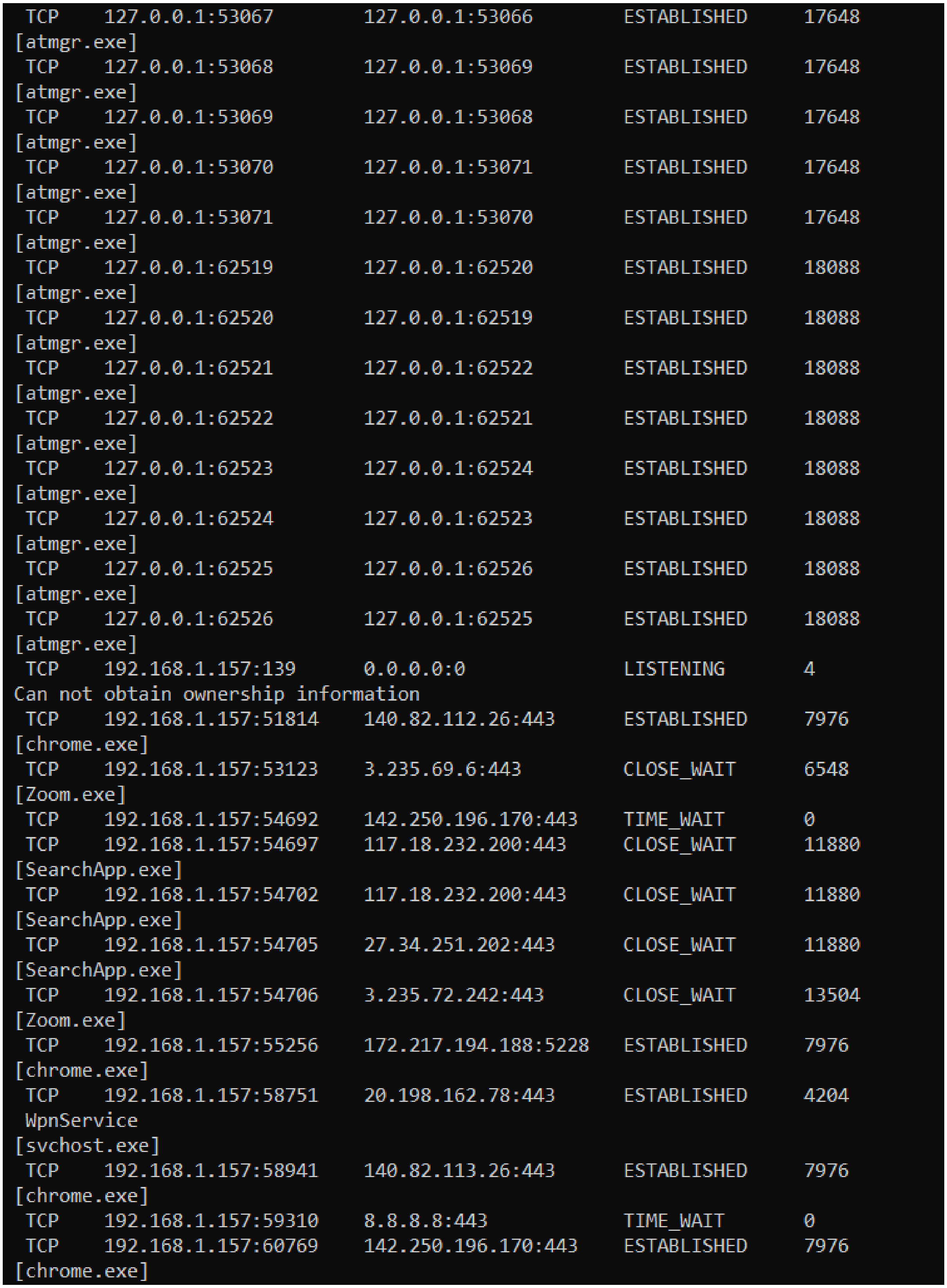
```
  TCP    192.168.1.157:53434    a-0001:https           ESTABLISHED
  TCP    192.168.1.157:53699    104.26.3.23:https      ESTABLISHED
  TCP    192.168.1.157:55008    maa05s19-in-f14:https  TIME_WAIT
  TCP    192.168.1.157:55009    13.107.3.254:https     ESTABLISHED
  TCP    192.168.1.157:55010    13.107.3.254:https     ESTABLISHED
  TCP    192.168.1.157:55011    13.107.42.254:https    ESTABLISHED
  TCP    192.168.1.157:55012    204.79.197.222:https   ESTABLISHED
  TCP    192.168.1.157:55256    si-in-f188:5228        ESTABLISHED
  TCP    192.168.1.157:55328    151.101.196.193:https  ESTABLISHED
  TCP    192.168.1.157:56057    ec2-3-80-20-196:https  CLOSE_WAIT
  TCP    192.168.1.157:57171    104.26.3.98:https      ESTABLISHED
  TCP    192.168.1.157:58751    20.198.162.78:https    ESTABLISHED
  TCP    192.168.1.157:58941    lb-140-82-113-26-iad:https  ESTABLISHED
  TCP    192.168.1.157:59310    dns:https              ESTABLISHED
  TCP    192.168.1.157:60329    maa05s19-in-f14:https  TIME_WAIT
  TCP    192.168.1.157:62355    maa05s09-in-f3:https   ESTABLISHED
  TCP    192.168.1.157:62829    104.17.211.204:https   ESTABLISHED
  TCP    192.168.1.157:63543    maa03s36-in-f10:https  ESTABLISHED
  TCP    192.168.1.157:63590    whatsapp-cdn-shv-02-maa2:https  ESTABLISHED
  TCP    192.168.1.157:63596    52.96.97.146:https     TIME_WAIT
  TCP    192.168.1.157:63795    198.251.197.31:https   ESTABLISHED
  TCP    192.168.1.157:63821    ec2-3-211-241-100:https  ESTABLISHED
  TCP    192.168.1.157:64424    1:https                TIME_WAIT
  TCP    192.168.1.157:64710    104.26.3.98:https      ESTABLISHED
  TCP    192.168.1.157:65308    maa05s16-in-f14:https  ESTABLISHED
  TCP    [::]:135               LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:445               LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49664             LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49665             LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49666             LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49667             LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49668             LAPTOP-8Q15SHE6:0      LISTENING
  TCP    [::]:49669             LAPTOP-8Q15SHE6:0      LISTENING

D:\>
```

We can count the connection directly: 70 are active in the above two images.

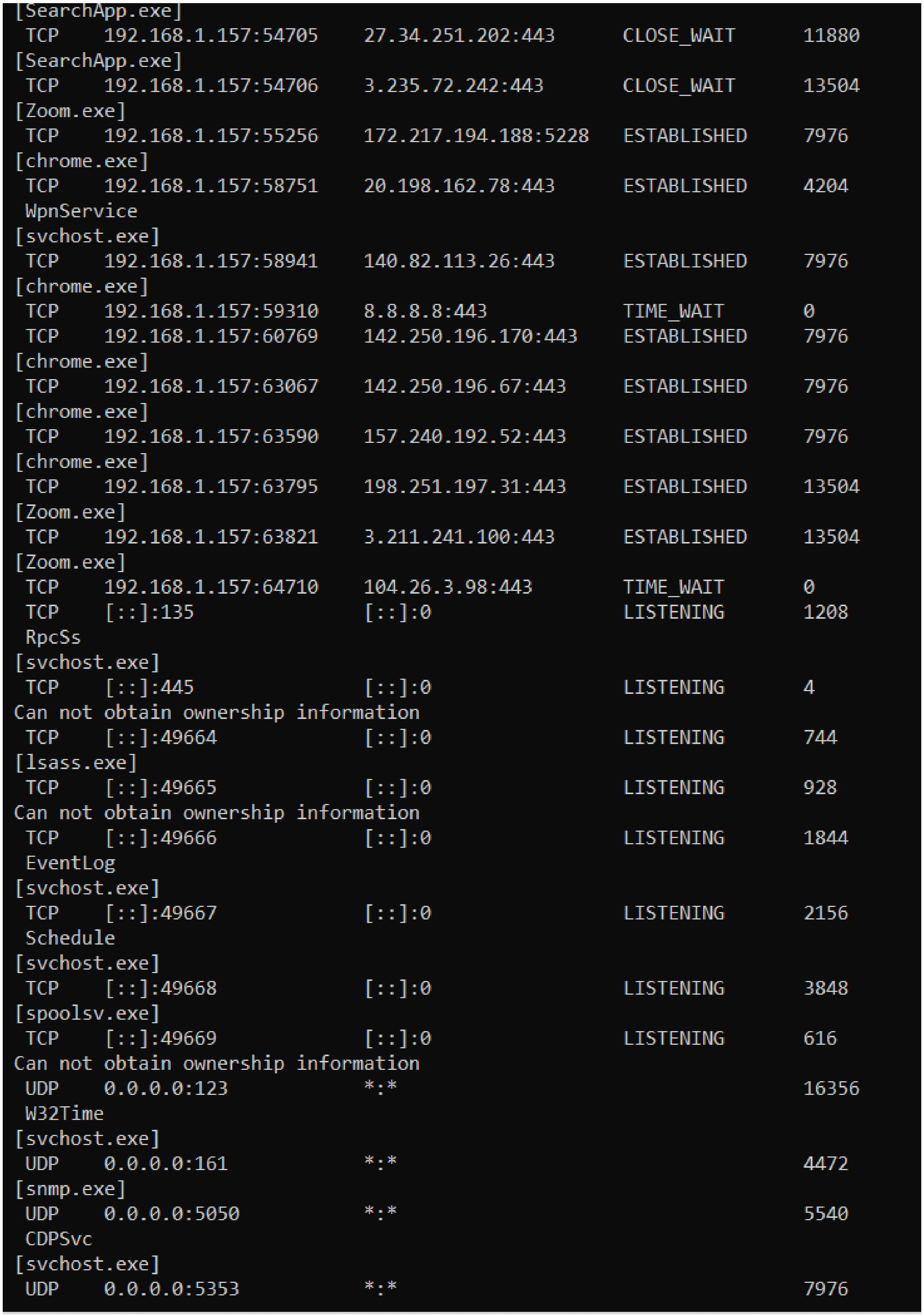
The “netstat -abon” command gives the list of all services that use TCP and UDP ports with the PIDs.



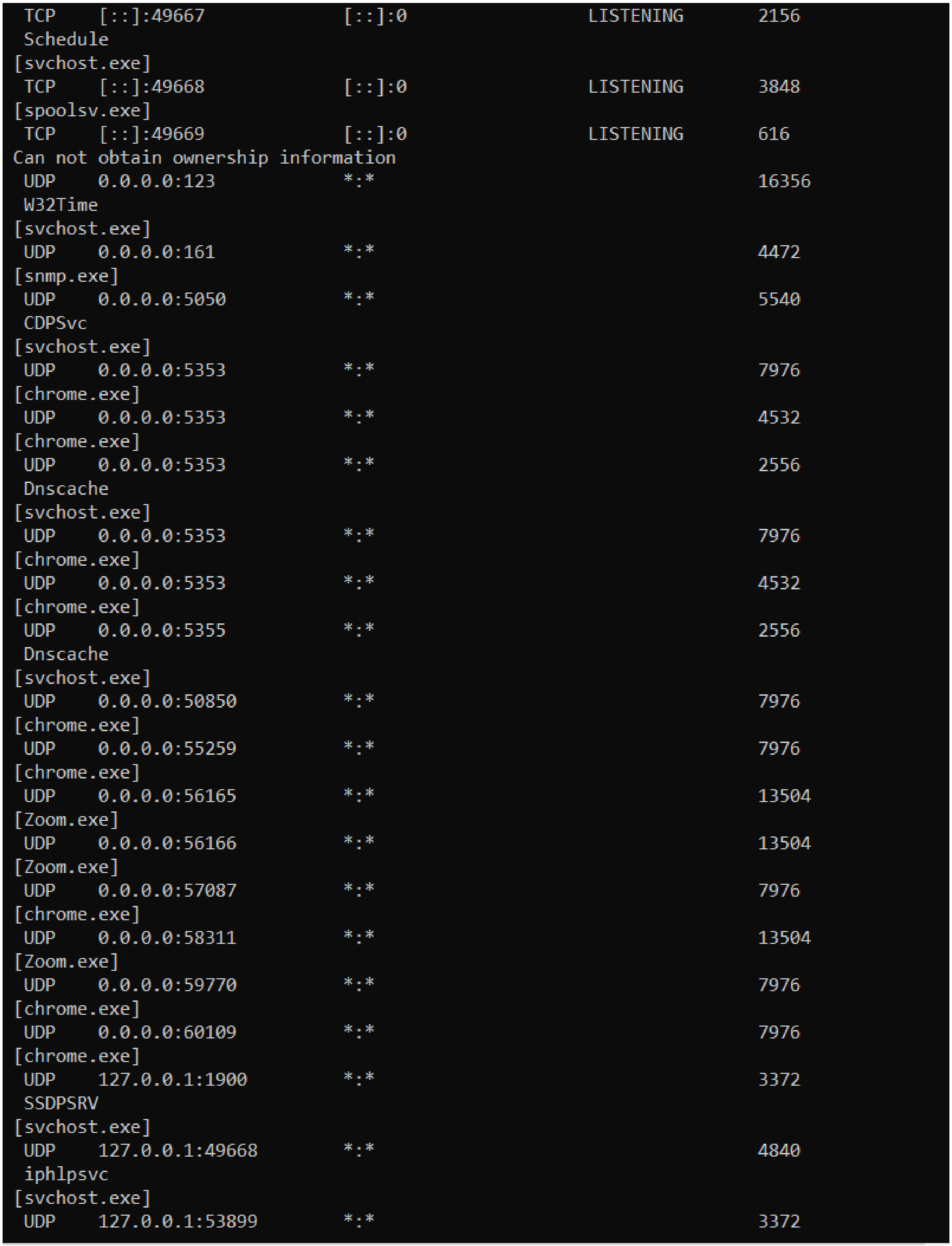
```
D:\>netstat -abon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1208
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5540
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       744
 [lsass.exe]
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       928
 Can not obtain ownership information
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1844
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2156
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       3848
 [spoolsv.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       616
 Can not obtain ownership information
  TCP    127.0.0.1:53064        127.0.0.1:53065        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53065        127.0.0.1:53064        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53066        127.0.0.1:53067        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53067        127.0.0.1:53066        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53068        127.0.0.1:53069        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53069        127.0.0.1:53068        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53070        127.0.0.1:53071        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53071        127.0.0.1:53070        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:62519        127.0.0.1:62520        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62520        127.0.0.1:62519        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62521        127.0.0.1:62522        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62522        127.0.0.1:62521        ESTABLISHED     18088
 [atmgr.exe]
```



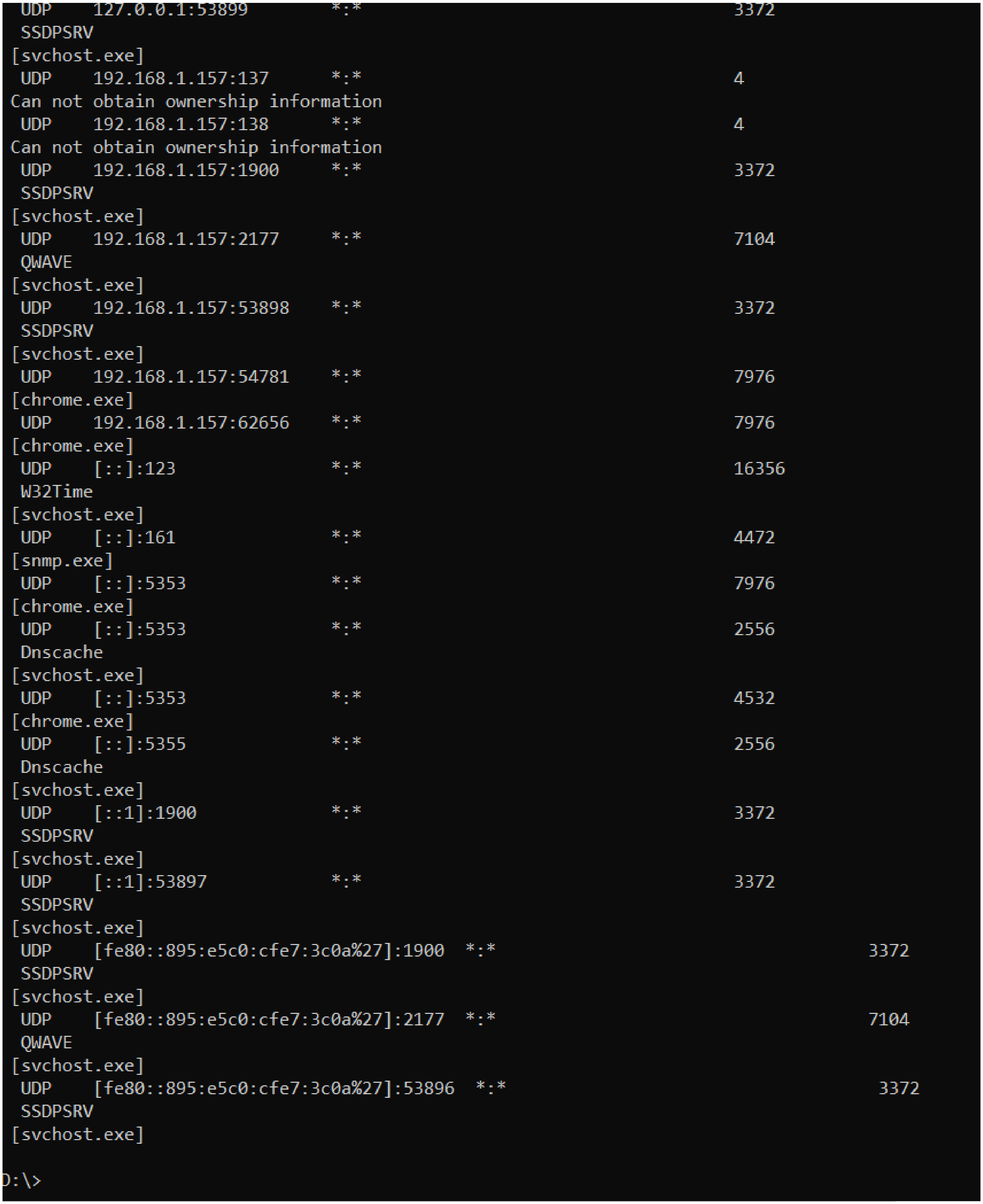
```
  TCP    127.0.0.1:53067        127.0.0.1:53066        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53068        127.0.0.1:53069        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53069        127.0.0.1:53068        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53070        127.0.0.1:53071        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:53071        127.0.0.1:53070        ESTABLISHED     17648
 [atmgr.exe]
  TCP    127.0.0.1:62519        127.0.0.1:62520        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62520        127.0.0.1:62519        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62521        127.0.0.1:62522        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62522        127.0.0.1:62521        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62523        127.0.0.1:62524        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62524        127.0.0.1:62523        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62525        127.0.0.1:62526        ESTABLISHED     18088
 [atmgr.exe]
  TCP    127.0.0.1:62526        127.0.0.1:62525        ESTABLISHED     18088
 [atmgr.exe]
  TCP    192.168.1.157:139      0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    192.168.1.157:51814    140.82.112.26:443      ESTABLISHED     7976
 [chrome.exe]
  TCP    192.168.1.157:53123    3.235.69.6:443         CLOSE_WAIT      6548
 [Zoom.exe]
  TCP    192.168.1.157:54692    142.250.196.170:443    TIME_WAIT       0
  TCP    192.168.1.157:54697    117.18.232.200:443     CLOSE_WAIT      11880
 [SearchApp.exe]
  TCP    192.168.1.157:54702    117.18.232.200:443     CLOSE_WAIT      11880
 [SearchApp.exe]
  TCP    192.168.1.157:54705    27.34.251.202:443      CLOSE_WAIT      11880
 [SearchApp.exe]
  TCP    192.168.1.157:54706    3.235.72.242:443       CLOSE_WAIT      13504
 [Zoom.exe]
  TCP    192.168.1.157:55256    172.217.194.188:5228   ESTABLISHED     7976
 [chrome.exe]
  TCP    192.168.1.157:58751    20.198.162.78:443      ESTABLISHED     4204
  WpnService
 [svchost.exe]
  TCP    192.168.1.157:58941    140.82.113.26:443      ESTABLISHED     7976
 [chrome.exe]
  TCP    192.168.1.157:59310    8.8.8.8:443            TIME_WAIT       0
  TCP    192.168.1.157:60769    142.250.196.170:443    ESTABLISHED     7976
 [chrome.exe]
```



```
[SearchApp.exe]
 TCP    192.168.1.157:54705    27.34.251.202:443      CLOSE_WAIT      11880
[SearchApp.exe]
 TCP    192.168.1.157:54706    3.235.72.242:443       CLOSE_WAIT      13504
[Zoom.exe]
 TCP    192.168.1.157:55256    172.217.194.188:5228   ESTABLISHED     7976
[chrome.exe]
 TCP    192.168.1.157:58751    20.198.162.78:443      ESTABLISHED     4204
 WpnService
[svchost.exe]
 TCP    192.168.1.157:58941    140.82.113.26:443      ESTABLISHED     7976
[chrome.exe]
 TCP    192.168.1.157:59310    8.8.8.8:443            TIME_WAIT       0
 TCP    192.168.1.157:60769    142.250.196.170:443    ESTABLISHED     7976
[chrome.exe]
 TCP    192.168.1.157:63067    142.250.196.67:443     ESTABLISHED     7976
[chrome.exe]
 TCP    192.168.1.157:63590    157.240.192.52:443     ESTABLISHED     7976
[chrome.exe]
 TCP    192.168.1.157:63795    198.251.197.31:443     ESTABLISHED     13504
[Zoom.exe]
 TCP    192.168.1.157:63821    3.211.241.100:443      ESTABLISHED     13504
[Zoom.exe]
 TCP    192.168.1.157:64710    104.26.3.98:443        TIME_WAIT       0
 TCP    [::]:135               [::]:0                 LISTENING       1208
 RpcSs
[svchost.exe]
 TCP    [::]:445               [::]:0                 LISTENING       4
Can not obtain ownership information
 TCP    [::]:49664             [::]:0                 LISTENING       744
[lsass.exe]
 TCP    [::]:49665             [::]:0                 LISTENING       928
Can not obtain ownership information
 TCP    [::]:49666             [::]:0                 LISTENING       1844
 EventLog
[svchost.exe]
 TCP    [::]:49667             [::]:0                 LISTENING       2156
 Schedule
[svchost.exe]
 TCP    [::]:49668             [::]:0                 LISTENING       3848
[spoolsv.exe]
 TCP    [::]:49669             [::]:0                 LISTENING       616
Can not obtain ownership information
 UDP    0.0.0.0:123            *:*                                    16356
 W32Time
[svchost.exe]
 UDP    0.0.0.0:161            *:*                                    4472
[snmp.exe]
 UDP    0.0.0.0:5050           *:*                                    5540
 CDPSvc
[svchost.exe]
 UDP    0.0.0.0:5353           *:*                                    7976
```



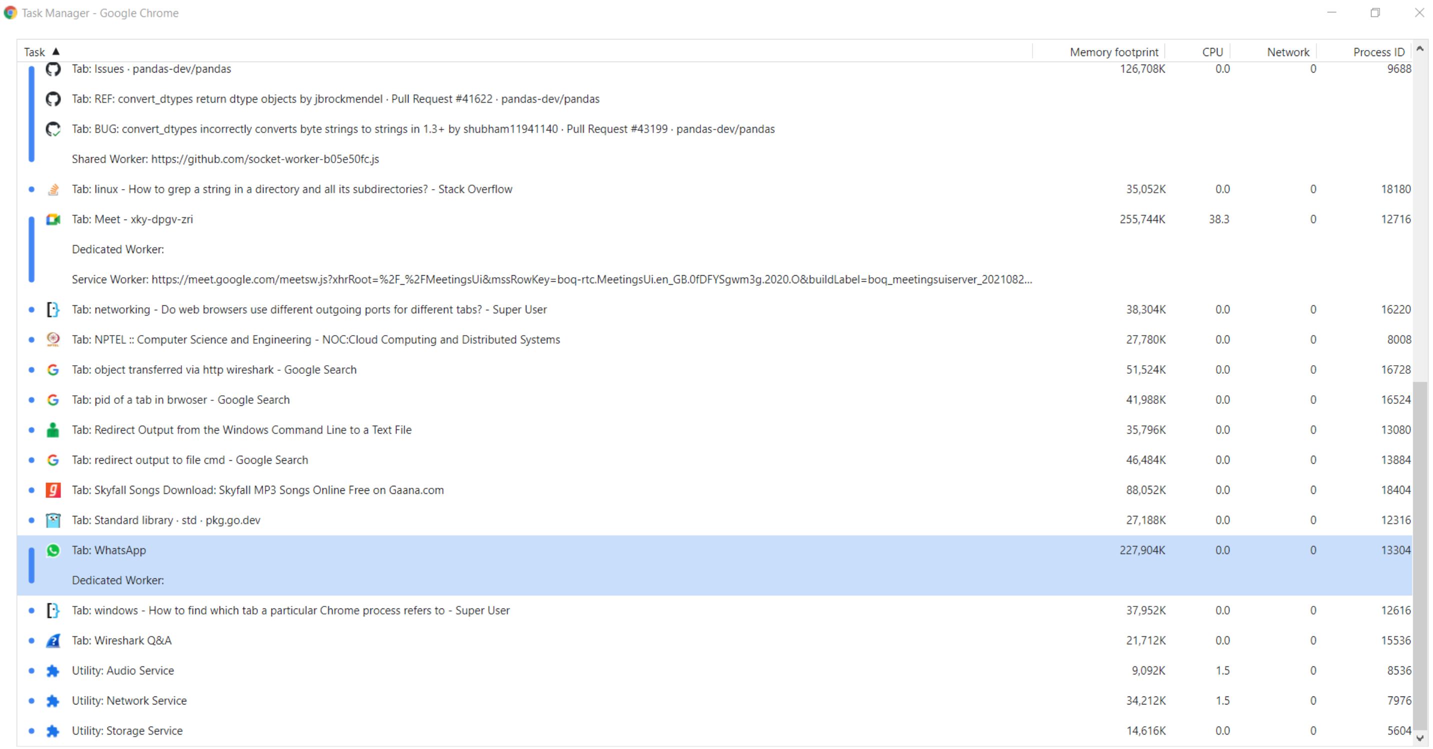
```
 TCP    [::]:49667             [::]:0                 LISTENING       2156
 Schedule
[svchost.exe]
 TCP    [::]:49668             [::]:0                 LISTENING       3848
[spoolsv.exe]
 TCP    [::]:49669             [::]:0                 LISTENING       616
Can not obtain ownership information
 UDP    0.0.0.0:123            *:*                                    16356
 W32Time
[svchost.exe]
 UDP    0.0.0.0:161            *:*                                    4472
[snmp.exe]
 UDP    0.0.0.0:5050           *:*                                    5540
 CDPSvc
[svchost.exe]
 UDP    0.0.0.0:5353           *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:5353           *:*                                    4532
[chrome.exe]
 UDP    0.0.0.0:5353           *:*                                    2556
 Dnscache
[svchost.exe]
 UDP    0.0.0.0:5353           *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:5353           *:*                                    4532
[chrome.exe]
 UDP    0.0.0.0:5355           *:*                                    2556
 Dnscache
[svchost.exe]
 UDP    0.0.0.0:50850          *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:55259          *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:56165          *:*                                    13504
[Zoom.exe]
 UDP    0.0.0.0:56166          *:*                                    13504
[Zoom.exe]
 UDP    0.0.0.0:57087          *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:58311          *:*                                    13504
[Zoom.exe]
 UDP    0.0.0.0:59770          *:*                                    7976
[chrome.exe]
 UDP    0.0.0.0:60109          *:*                                    7976
[chrome.exe]
 UDP    127.0.0.1:1900         *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    127.0.0.1:49668        *:*                                    4840
 iphlpsvc
[svchost.exe]
 UDP    127.0.0.1:53899        *:*                                    3372
```



```
 UDP    127.0.0.1:53899        *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    192.168.1.157:137      *:*                                    4
Can not obtain ownership information
 UDP    192.168.1.157:138      *:*                                    4
Can not obtain ownership information
 UDP    192.168.1.157:1900     *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    192.168.1.157:2177     *:*                                    7104
 QWAVE
[svchost.exe]
 UDP    192.168.1.157:53898    *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    192.168.1.157:54781    *:*                                    7976
[chrome.exe]
 UDP    192.168.1.157:62656    *:*                                    7976
[chrome.exe]
 UDP    [::]:123               *:*                                    16356
 W32Time
[svchost.exe]
 UDP    [::]:161               *:*                                    4472
[snmp.exe]
 UDP    [::]:5353              *:*                                    7976
[chrome.exe]
 UDP    [::]:5353              *:*                                    2556
 Dnscache
[svchost.exe]
 UDP    [::]:5353              *:*                                    4532
[chrome.exe]
 UDP    [::]:5355              *:*                                    2556
 Dnscache
[svchost.exe]
 UDP    [::1]:1900             *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    [::1]:53897            *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    [fe80::895:e5c0:cfe7:3c0a%27]:1900  *:*                                    3372
 SSDPSRV
[svchost.exe]
 UDP    [fe80::895:e5c0:cfe7:3c0a%27]:2177  *:*                                    7104
 QWAVE
[svchost.exe]
 UDP    [fe80::895:e5c0:cfe7:3c0a%27]:53896  *:*                                    3372
 SSDPSRV
[svchost.exe]

D:\>
```

In the above 5 images, we can see that chrome.exe is my web browser. So, all the chrome.exe services can be seen here with the PIDs given. To find the ports, we can see that after a connection TCP/UDP there is a column that gives the IP address of the web page and port like (IP address (spaced by ‘.’): Port). From here, the port number information can be obtained.

On the browser being used (I am using chrome), you can press Shift + Esc, this gives the task manager of the browser.



Task Manager - Google Chrome

Task ▲	Memory footprint	CPU	Network	Process ID
Tab: Issues · pandas-dev/pandas	126,708K	0.0	0	9688
Tab: REF: convert_dtypes return dtype objects by jbrockmendel · Pull Request #41622 · pandas-dev/pandas				
Tab: BUG: convert_dtypes incorrectly converts byte strings to strings in 1.3+ by shubham11941140 · Pull Request #43199 · pandas-dev/pandas				
Shared Worker: https://github.com/socket-worker-b05e50fc.js				
Tab: linux - How to grep a string in a directory and all its subdirectories? - Stack Overflow	35,052K	0.0	0	18180
Tab: Meet - xky-dpgv-zri	255,744K	38.3	0	12716
Dedicated Worker:				
Service Worker: https://meet.google.com/meetsw.js?xhrRoot=%2F_%2FMeetingsUi&mssRowKey=boq-rtc.MeetingsUi.en_GB.0fDFYSgwm3g.2020.O&buildLabel=boq_meetingsuiserver_2021082...				
Tab: networking - Do web browsers use different outgoing ports for different tabs? - Super User	38,304K	0.0	0	16220
Tab: NPTEL :: Computer Science and Engineering - NOC:Cloud Computing and Distributed Systems	27,780K	0.0	0	8008
Tab: object transferred via http wireshark - Google Search	51,524K	0.0	0	16728
Tab: pid of a tab in brwoser - Google Search	41,988K	0.0	0	16524
Tab: Redirect Output from the Windows Command Line to a Text File	35,796K	0.0	0	13080
Tab: redirect output to file cmd - Google Search	46,484K	0.0	0	13884
Tab: Skyfall Songs Download: Skyfall MP3 Songs Online Free on Gaana.com	88,052K	0.0	0	18404
Tab: Standard library · std · pkg.go.dev	27,188K	0.0	0	12316
Tab: WhatsApp	227,904K	0.0	0	13304
Dedicated Worker:				
Tab: windows - How to find which tab a particular Chrome process refers to - Super User	37,952K	0.0	0	12616
Tab: Wireshark Q&A	21,712K	0.0	0	15536
Utility: Audio Service	9,092K	1.5	0	8536
Utility: Network Service	34,212K	1.5	0	7976
Utility: Storage Service	14,616K	0.0	0	5604

In this window, you will get the PID associated with each of the tabs. (See the last column the PID is mentioned)

Once this is obtained, you can manually check with the port associated with a process given the PID. In the above section where 5 images had been posted, with the PID of the service, we can find the port associated.

It is possible that we can use multiple ports for a specific TAB and a single port for multiple TABs. (It depends on the number of processes and PID value).

For a specific TAB, both the above situations can hold. So, sometimes it becomes impossible to distinctly differentiate between port number and PID of a specific TAB but in a few cases, it is possible. (This depends a lot on how the user is using the TABs of their browser and the number of foreground and background running processes).

You can even find the PID string in the list by using other commands like findstr.

Ensure that the connection is active and packet transfer is happening in the specific TAB, then you can obtain all the data easily.

The standard ports for:

1. HTTP – 80.
2. DHCP – 67 or 68.
3. DNS – 53
4. SMTP – 25
5. FTP – 20.

If you observe the images in the ‘netstat -abon’ which are shown above.

We can see that for my local IPv4 Address (192.168.1.157), the port is given next to the value. SMTP, HTTP, FTP all use TCP for their transmission. If you look at the images of all the ports on the browser (chrome.exe), the port numbers are coming as very big numbers (> 50,000). The services being accessed by the browser (any of the above use very large port numbers on the local system).

The port from the browser is using 443 for the transfer of data which is the standard port of HTTPS. This is the place where a standard port is used.

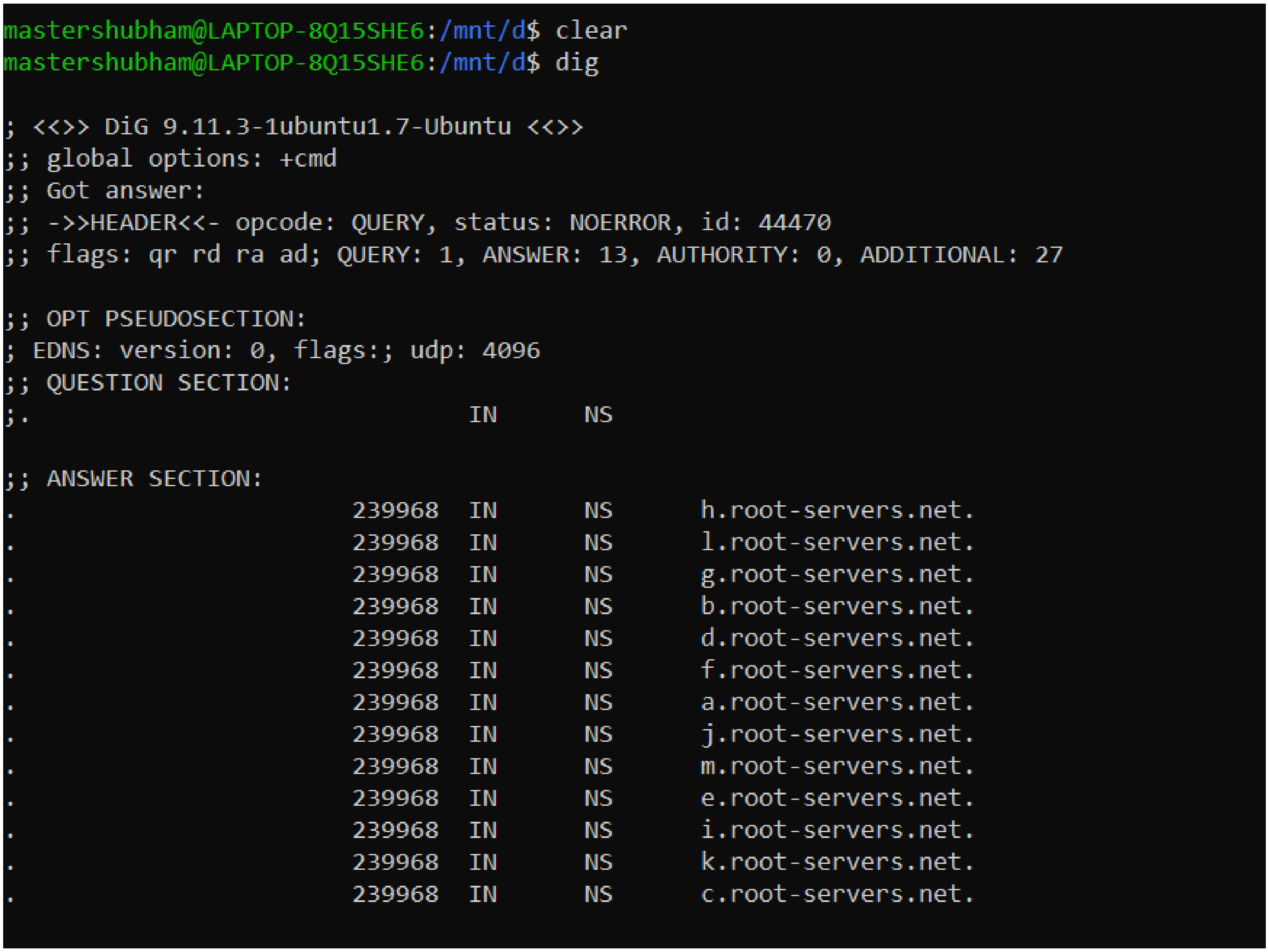
It is important to note that the server for the rendering of pages, setting up of protocols, and transmission of data uses the standard ports (as proved for HTTPS – 443), the client uses very high port numbers for communications (> 50,000) for all its services including HTTP, DHCP, DNS, SMTP, and FTP.

As we need to find its usage in my system, I am using it as a client (192.168.1.157), so the port numbers are not standard for the mentioned protocols.

In my system, none of the services HTTP, DHCP, DNS, SMTP, and FTP use the standard ports for the transmission and retrieval of data.

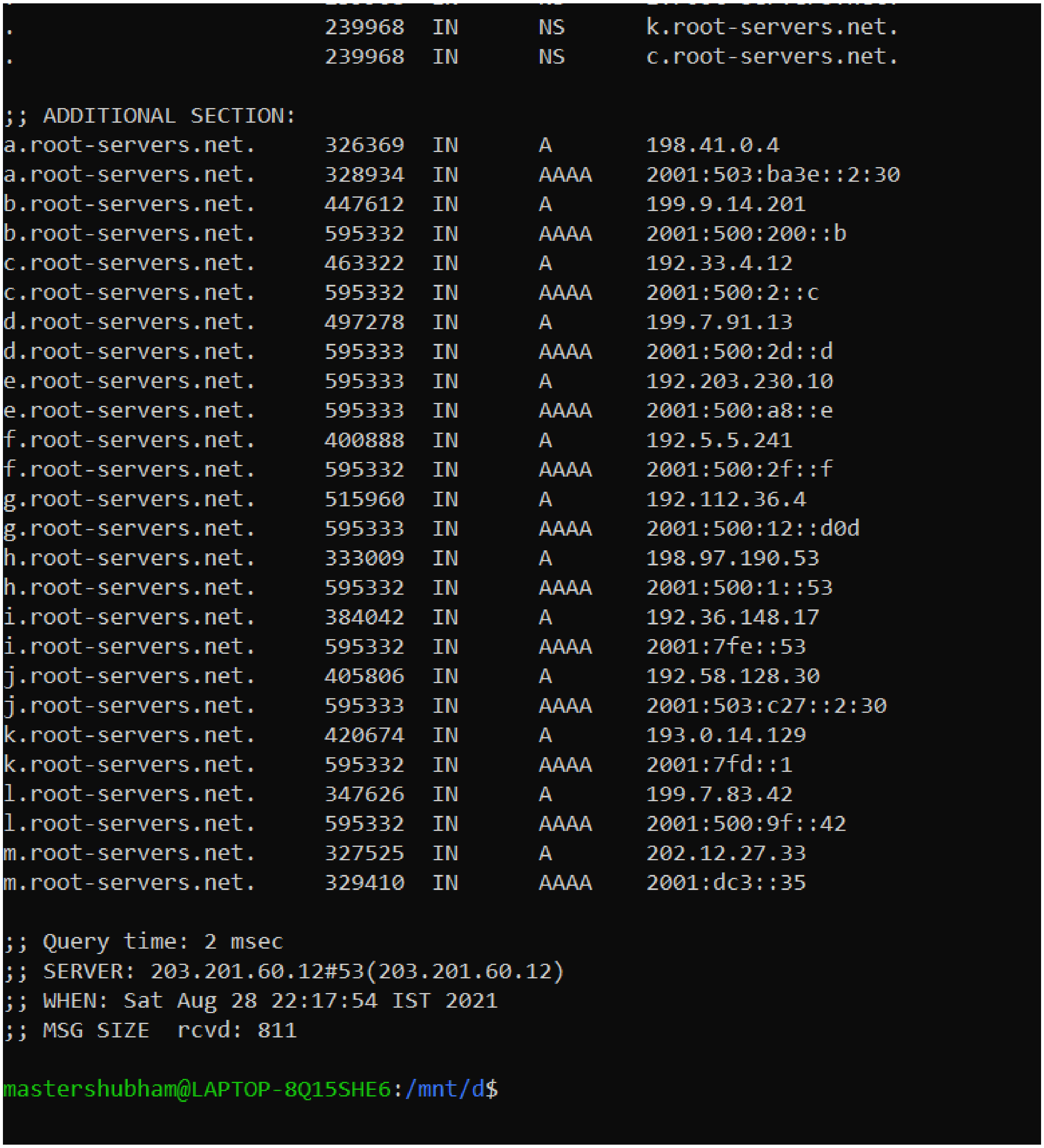
Question 3

Dig command



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ clear
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44470
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       239968  IN      NS      h.root-servers.net.
.                       239968  IN      NS      l.root-servers.net.
.                       239968  IN      NS      g.root-servers.net.
.                       239968  IN      NS      b.root-servers.net.
.                       239968  IN      NS      d.root-servers.net.
.                       239968  IN      NS      f.root-servers.net.
.                       239968  IN      NS      a.root-servers.net.
.                       239968  IN      NS      j.root-servers.net.
.                       239968  IN      NS      m.root-servers.net.
.                       239968  IN      NS      e.root-servers.net.
.                       239968  IN      NS      i.root-servers.net.
.                       239968  IN      NS      k.root-servers.net.
.                       239968  IN      NS      c.root-servers.net.
```

Continued

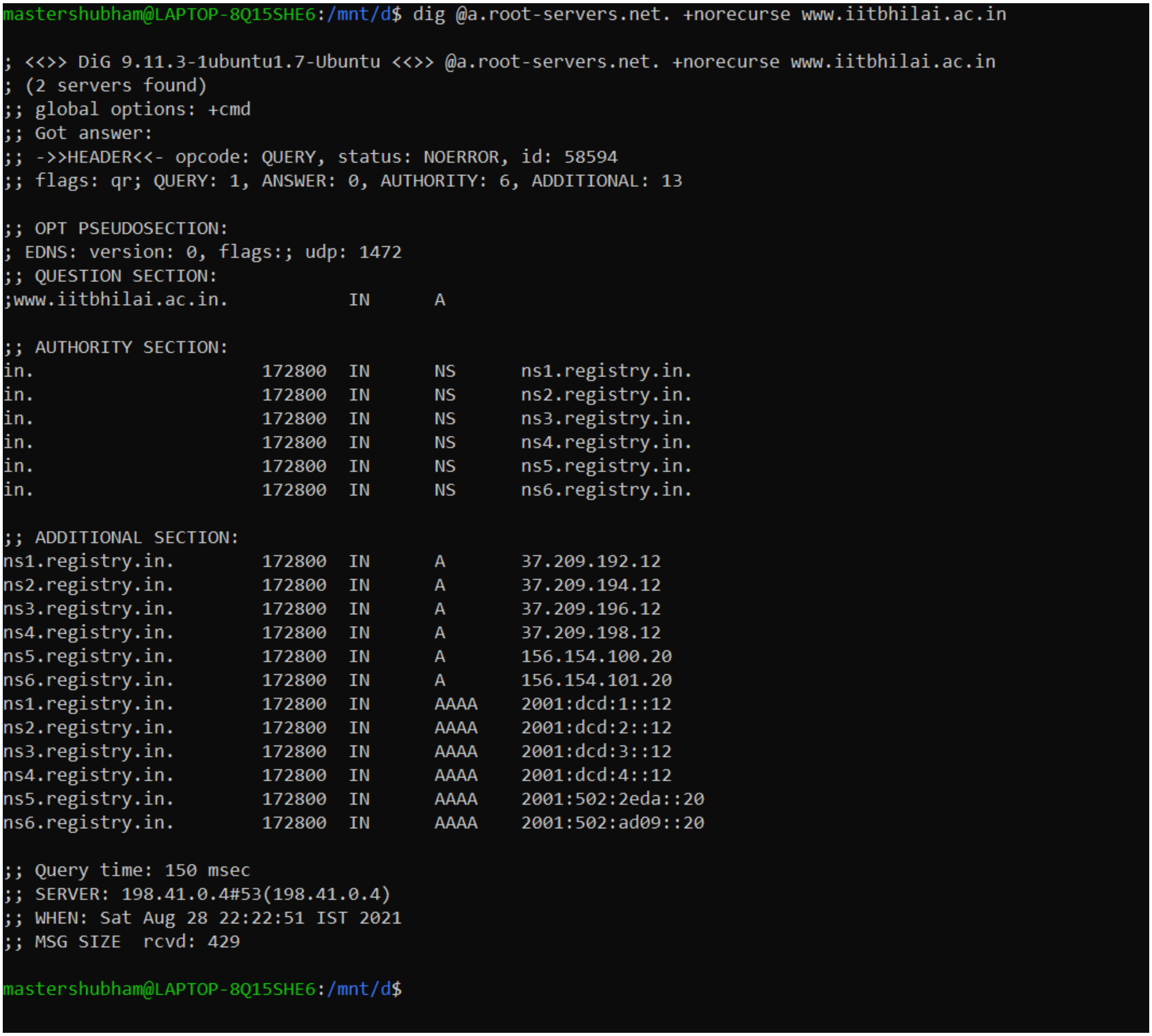


```
.                       239968  IN      NS      k.root-servers.net.
.                       239968  IN      NS      c.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     326369  IN      A       198.41.0.4
a.root-servers.net.     328934  IN      AAAA    2001:503:ba3e::2:30
b.root-servers.net.     447612  IN      A       199.9.14.201
b.root-servers.net.     595332  IN      AAAA    2001:500:200::b
c.root-servers.net.     463322  IN      A       192.33.4.12
c.root-servers.net.     595332  IN      AAAA    2001:500:2::c
d.root-servers.net.     497278  IN      A       199.7.91.13
d.root-servers.net.     595333  IN      AAAA    2001:500:2d::d
e.root-servers.net.     595333  IN      A       192.203.230.10
e.root-servers.net.     595333  IN      AAAA    2001:500:a8::e
f.root-servers.net.     400888  IN      A       192.5.5.241
f.root-servers.net.     595332  IN      AAAA    2001:500:2f::f
g.root-servers.net.     515960  IN      A       192.112.36.4
g.root-servers.net.     595333  IN      AAAA    2001:500:12::d0d
h.root-servers.net.     333009  IN      A       198.97.190.53
h.root-servers.net.     595332  IN      AAAA    2001:500:1::53
i.root-servers.net.     384042  IN      A       192.36.148.17
i.root-servers.net.     595332  IN      AAAA    2001:7fe::53
j.root-servers.net.     405806  IN      A       192.58.128.30
j.root-servers.net.     595333  IN      AAAA    2001:503:c27::2:30
k.root-servers.net.     420674  IN      A       193.0.14.129
k.root-servers.net.     595332  IN      AAAA    2001:7fd::1
l.root-servers.net.     347626  IN      A       199.7.83.42
l.root-servers.net.     595332  IN      AAAA    2001:500:9f::42
m.root-servers.net.     327525  IN      A       202.12.27.33
m.root-servers.net.     329410  IN      AAAA    2001:dc3::35

;; Query time: 2 msec
;; SERVER: 203.201.60.12#53(203.201.60.12)
;; WHEN: Sat Aug 28 22:17:54 IST 2021
;; MSG SIZE  rcvd: 811

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

With this, we get all the 13 root servers across different geographical locations of the world.

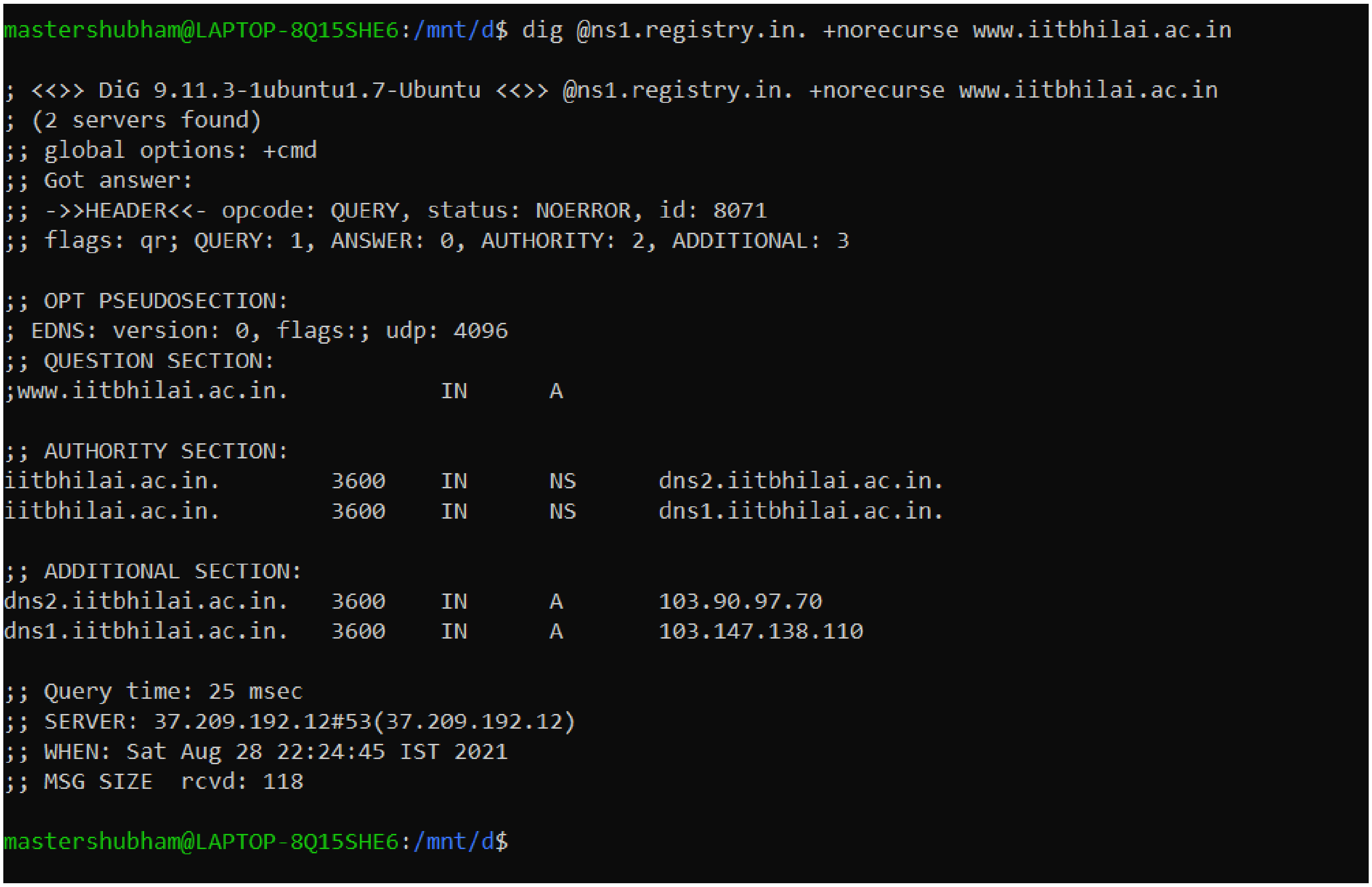
The +norecurse flag is used to ask the server without recursion.

Selecting any root server for www.iitbhilai.ac.in



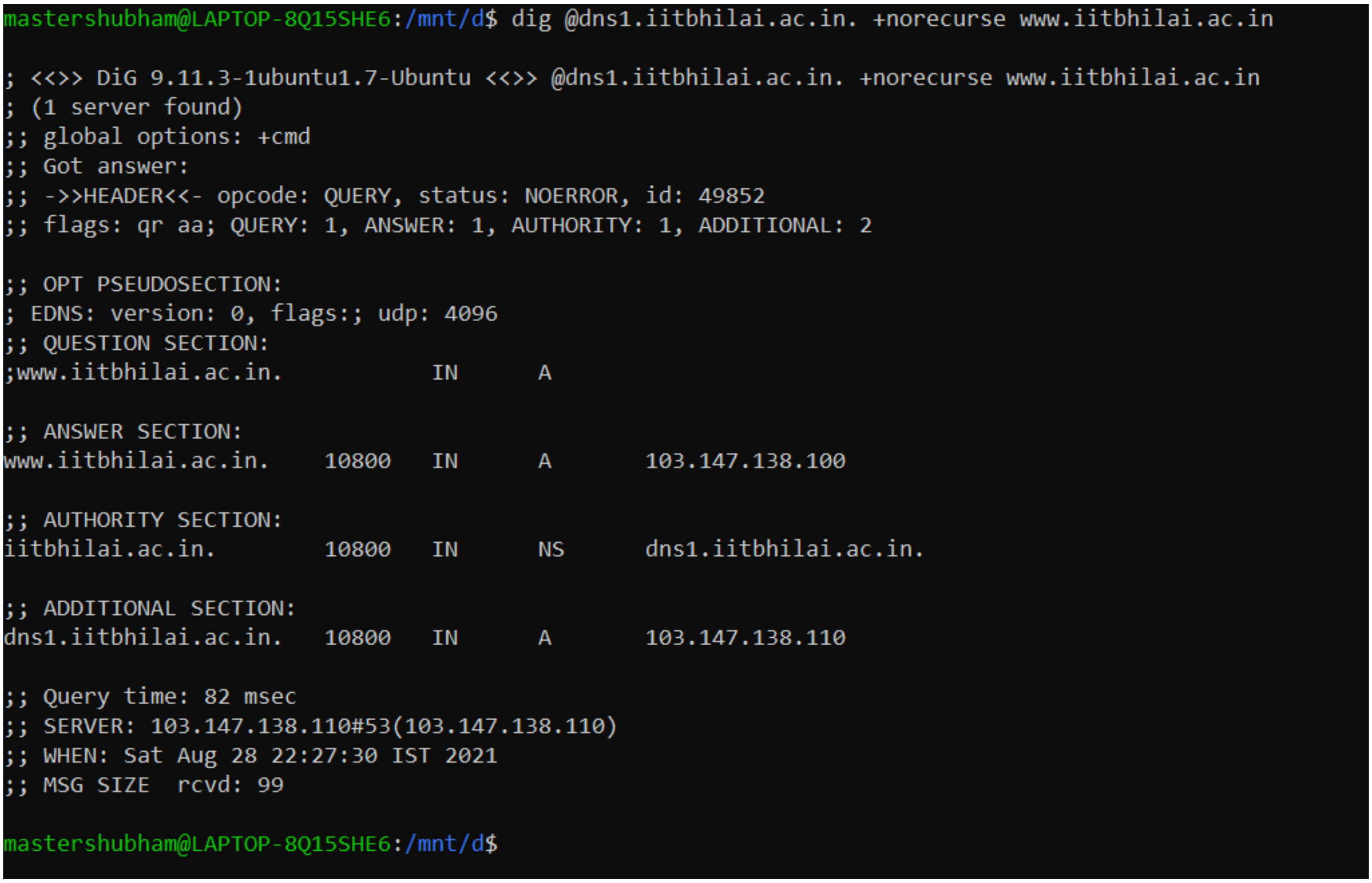
```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @a.root-servers.net. +norecurse www.iitbhilai.ac.in

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @a.root-servers.net. +norecurse www.iitbhilai.ac.in
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58594
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.iitbhilai.ac.in.           IN      A

;; AUTHORITY SECTION:
in.                     172800  IN      NS      ns1.registry.in.
in.                     172800  IN      NS      ns2.registry.in.
in.                     172800  IN      NS      ns3.registry.in.
in.                     172800  IN      NS      ns4.registry.in.
in.                     172800  IN      NS      ns5.registry.in.
in.                     172800  IN      NS      ns6.registry.in.

;; ADDITIONAL SECTION:
ns1.registry.in.        172800  IN      A       37.209.192.12
ns2.registry.in.        172800  IN      A       37.209.194.12
ns3.registry.in.        172800  IN      A       37.209.196.12
ns4.registry.in.        172800  IN      A       37.209.198.12
ns5.registry.in.        172800  IN      A       156.154.100.20
ns6.registry.in.        172800  IN      A       156.154.101.20
ns1.registry.in.        172800  IN      AAAA    2001:dcd:1::12
ns2.registry.in.        172800  IN      AAAA    2001:dcd:2::12
ns3.registry.in.        172800  IN      AAAA    2001:dcd:3::12
ns4.registry.in.        172800  IN      AAAA    2001:dcd:4::12
ns5.registry.in.        172800  IN      AAAA    2001:502:2eda::20
ns6.registry.in.        172800  IN      AAAA    2001:502:ad09::20

;; Query time: 150 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sat Aug 28 22:22:51 IST 2021
;; MSG SIZE  rcvd: 429

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Top Level Domain Server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @ns1.registry.in. +norecurse www.iitbhilai.ac.in

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @ns1.registry.in. +norecurse www.iitbhilai.ac.in
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8071
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; 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: 25 msec
;; SERVER: 37.209.192.12#53(37.209.192.12)
;; WHEN: Sat Aug 28 22:24:45 IST 2021
;; MSG SIZE  rcvd: 118

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Authoritative Name server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @dns1.iitbhilai.ac.in. +norecurse www.iitbhilai.ac.in

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @dns1.iitbhilai.ac.in. +norecurse www.iitbhilai.ac.in
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49852
;; flags: qr aa; 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.    10800   IN      A       103.147.138.100

;; AUTHORITY SECTION:
iitbhilai.ac.in.        10800   IN      NS      dns1.iitbhilai.ac.in.

;; ADDITIONAL SECTION:
dns1.iitbhilai.ac.in.   10800   IN      A       103.147.138.110

;; Query time: 82 msec
;; SERVER: 103.147.138.110#53(103.147.138.110)
;; WHEN: Sat Aug 28 22:27:30 IST 2021
;; MSG SIZE  rcvd: 99

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

The name servers used in this process are:

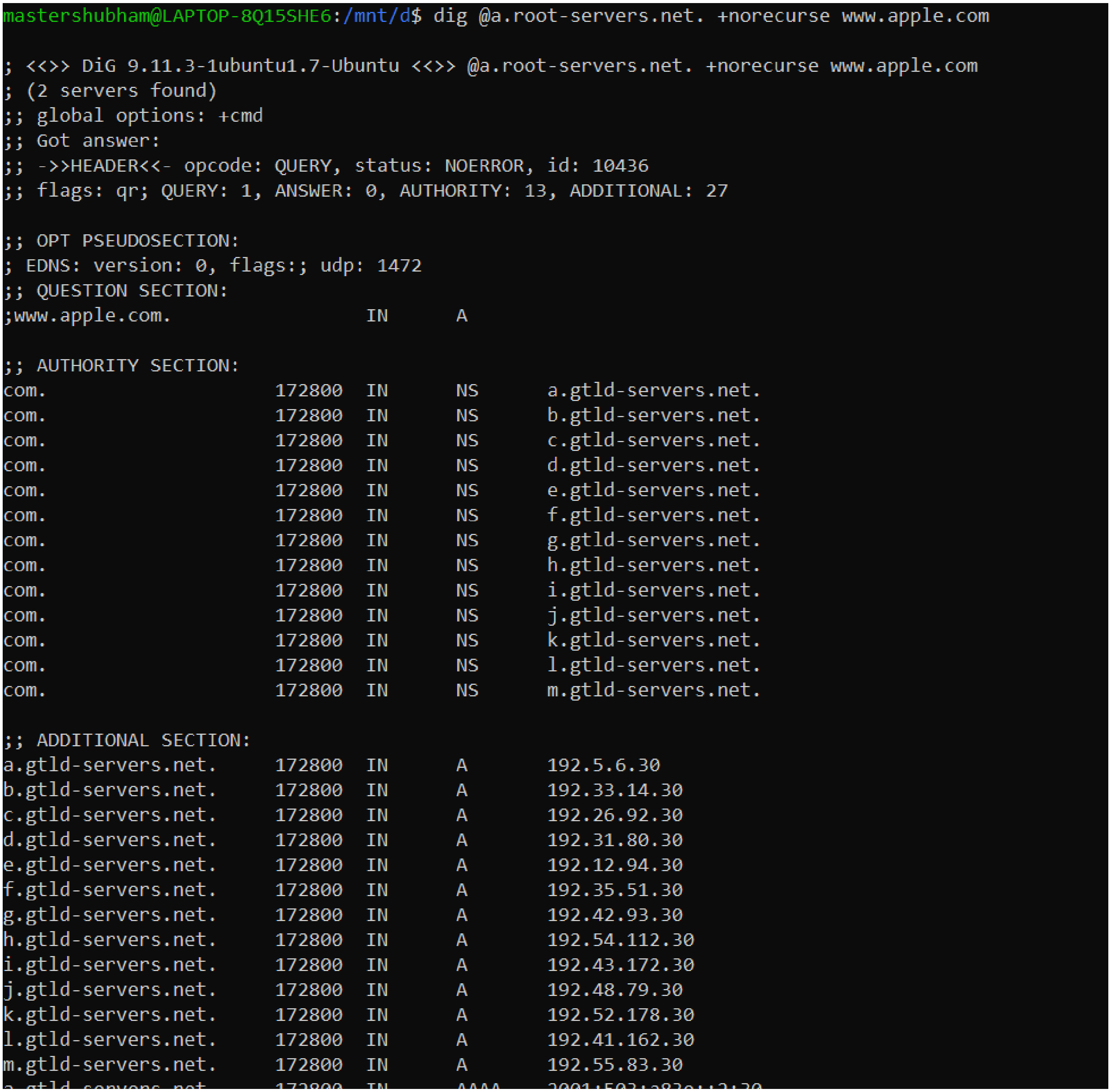
Root Server – a.root-server.net (198.41.0.4)

Top Level Domain Server – ns1.registry.in (37.209.192.12)

Authoritative Name Server – dns1.iitbhilai.ac.in (103.147.138.110)

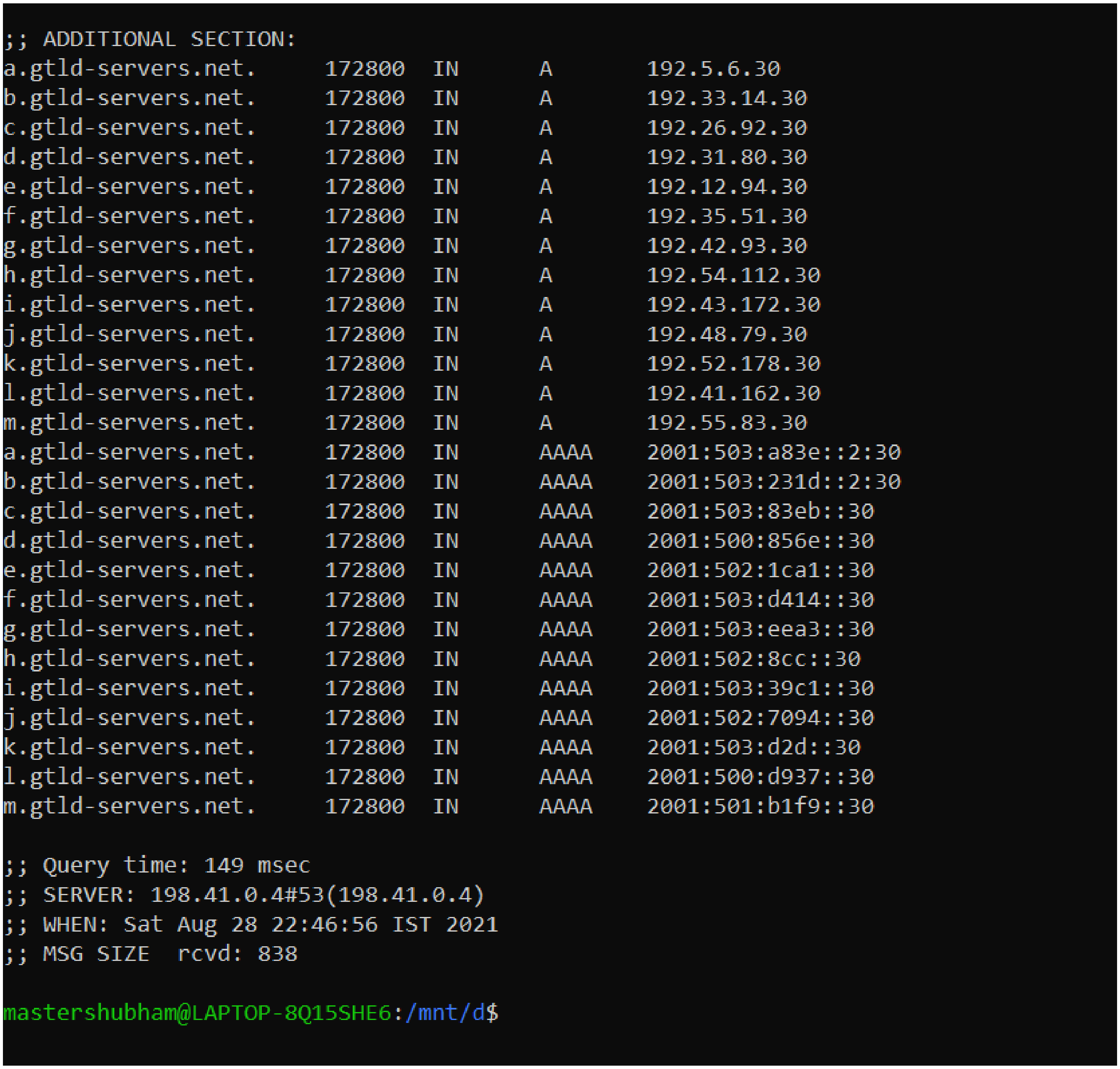
Website – www.iitbhilai.ac.in (103.147.138.100)

Selecting any root server for www.apple.com



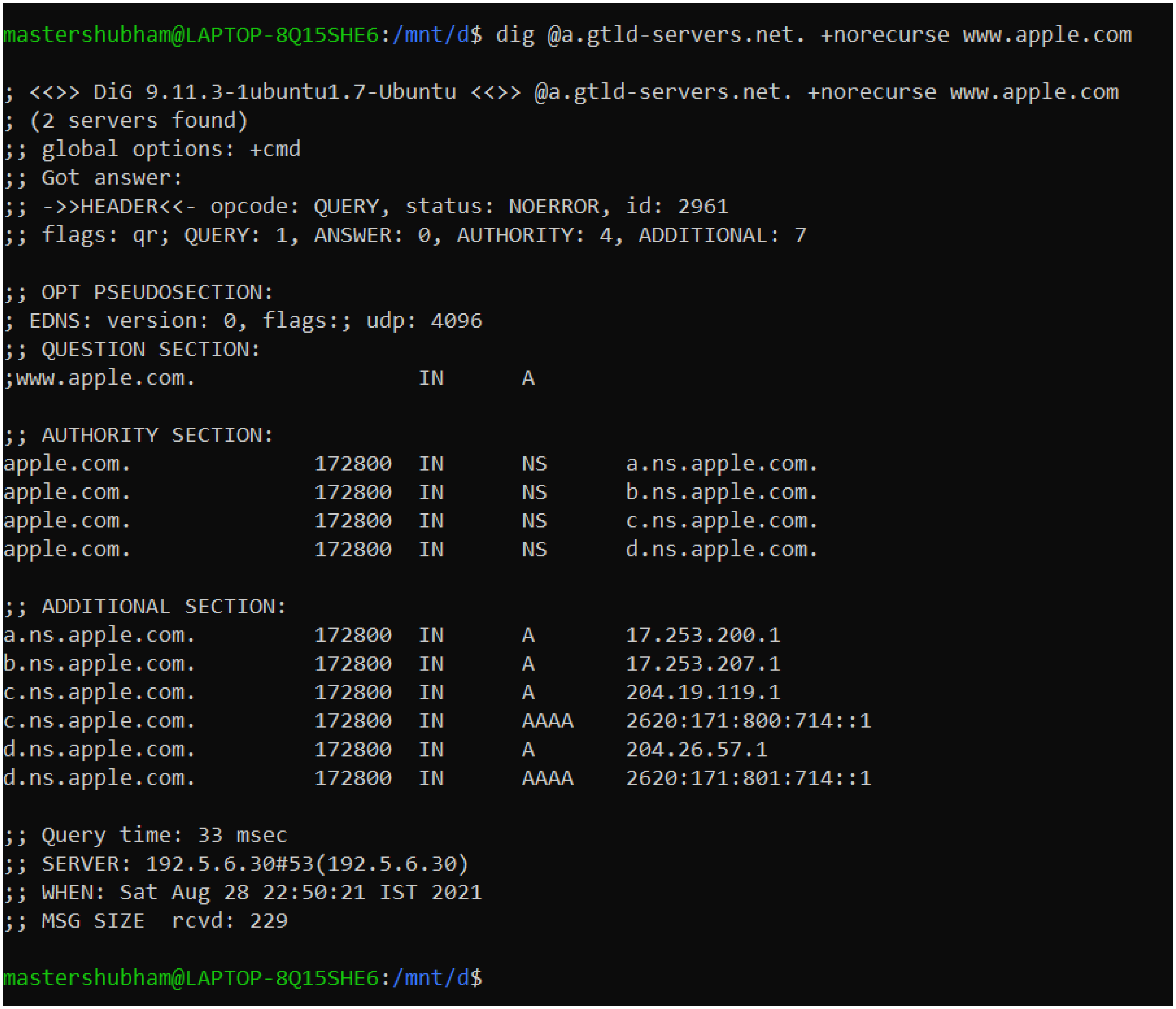
```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @a.root-servers.net. +norecurse www.apple.com

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @a.root-servers.net. +norecurse www.apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10436
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;www.apple.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
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
```

Continued



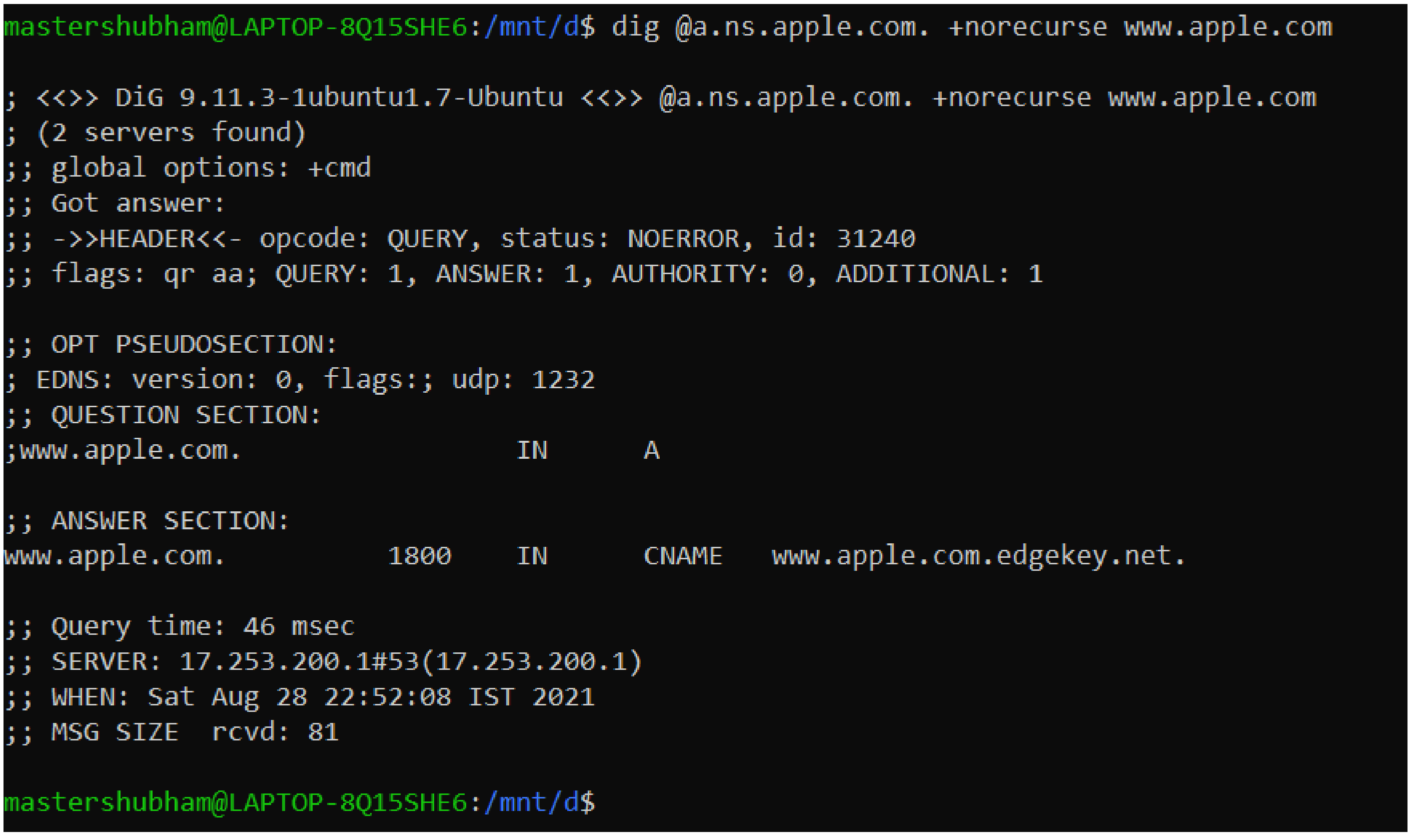
```
;; ADDITIONAL SECTION:
a.gtld-servers.net.     172800  IN      A       192.5.6.30
b.gtld-servers.net.     172800  IN      A       192.33.14.30
c.gtld-servers.net.     172800  IN      A       192.26.92.30
d.gtld-servers.net.     172800  IN      A       192.31.80.30
e.gtld-servers.net.     172800  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: 149 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sat Aug 28 22:46:56 IST 2021
;; MSG SIZE  rcvd: 838

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Top Level Domain Server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @a.gtld-servers.net. +norecurse www.apple.com

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @a.gtld-servers.net. +norecurse www.apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2961
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7

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

;; AUTHORITY SECTION:
apple.com.              172800  IN      NS      a.ns.apple.com.
apple.com.              172800  IN      NS      b.ns.apple.com.
apple.com.              172800  IN      NS      c.ns.apple.com.
apple.com.              172800  IN      NS      d.ns.apple.com.

;; ADDITIONAL SECTION:
a.ns.apple.com.         172800  IN      A       17.253.200.1
b.ns.apple.com.         172800  IN      A       17.253.207.1
c.ns.apple.com.         172800  IN      A       204.19.119.1
c.ns.apple.com.         172800  IN      AAAA    2620:171:800:714::1
d.ns.apple.com.         172800  IN      A       204.26.57.1
d.ns.apple.com.         172800  IN      AAAA    2620:171:801:714::1

;; Query time: 33 msec
;; SERVER: 192.5.6.30#53(192.5.6.30)
;; WHEN: Sat Aug 28 22:50:21 IST 2021
;; MSG SIZE  rcvd: 229

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Authoritative Name server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @a.ns.apple.com. +norecurse www.apple.com

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @a.ns.apple.com. +norecurse www.apple.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31240
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.apple.com.          1800    IN      CNAME   www.apple.com.edgekey.net.

;; Query time: 46 msec
;; SERVER: 17.253.200.1#53(17.253.200.1)
;; WHEN: Sat Aug 28 22:52:08 IST 2021
;; MSG SIZE  rcvd: 81

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

The name servers used in this process are:

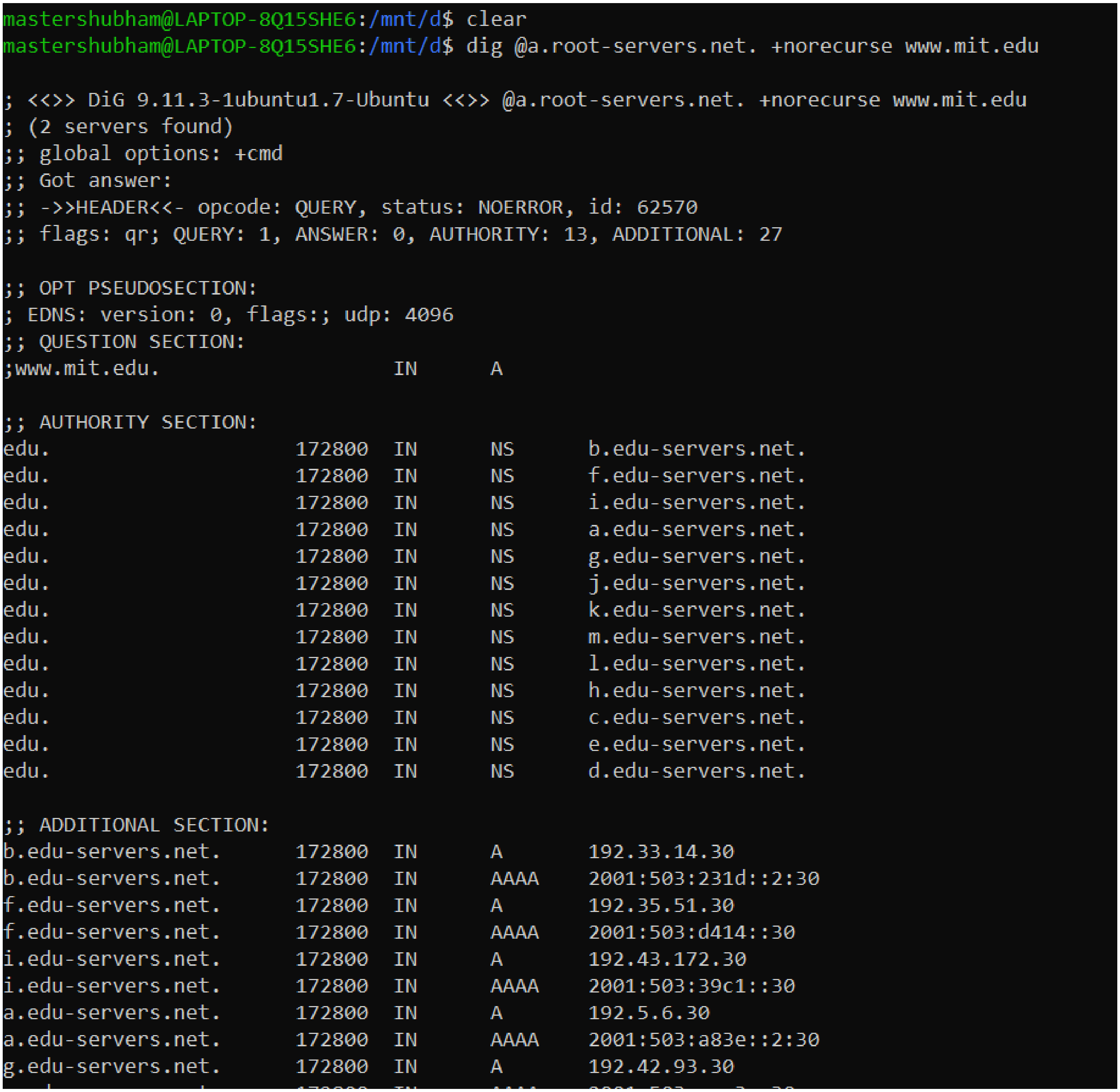
Root Server – a.root-server.net (198.41.0.4)

Top-Level Domain Server – a.gtld-server.net (192.5.6.30)

Authoritative Name Server – a.ns.apple.com (17.253.200.1)

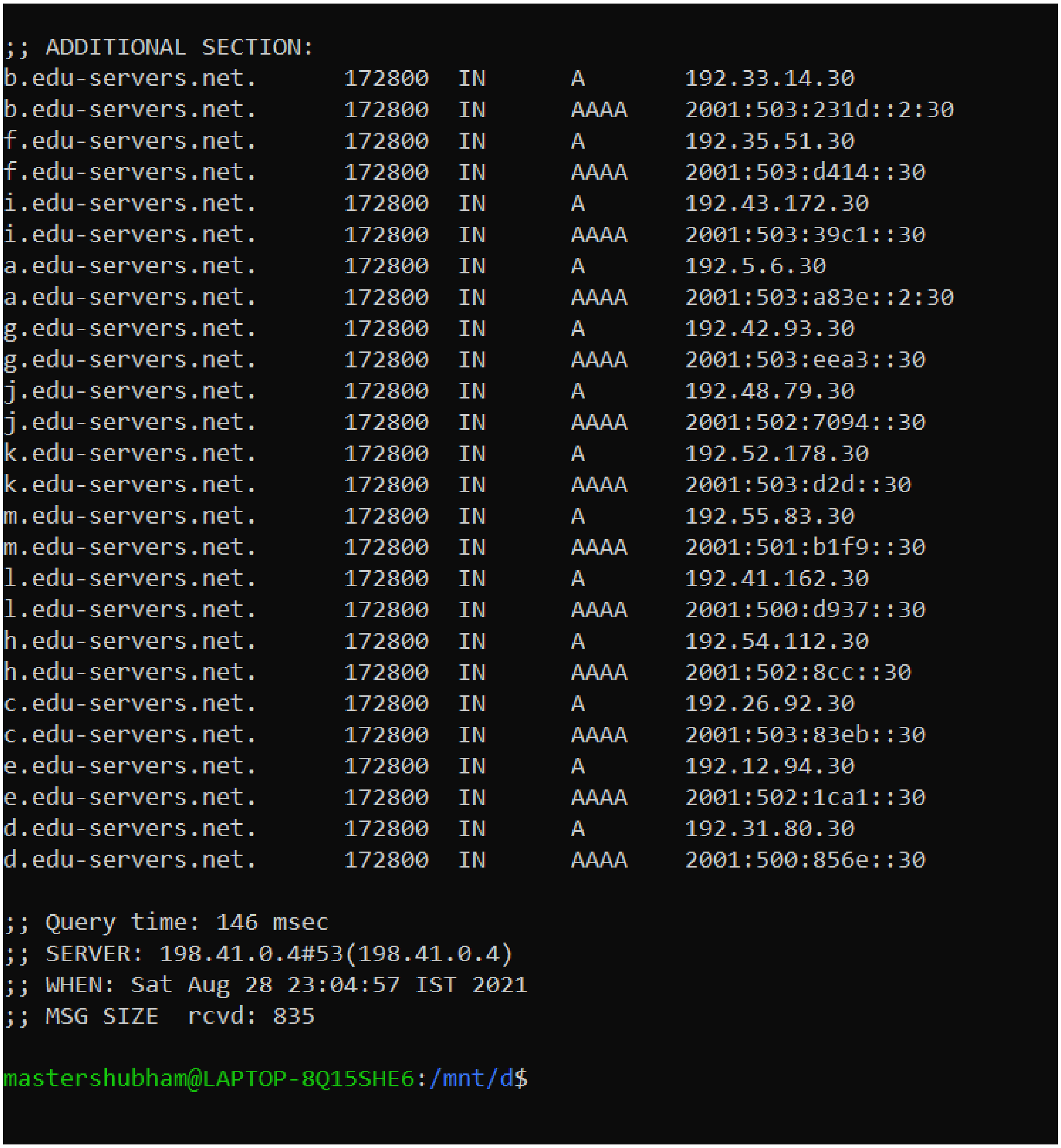
Website – www.apple.com

Selecting any root server for www.mit.edu



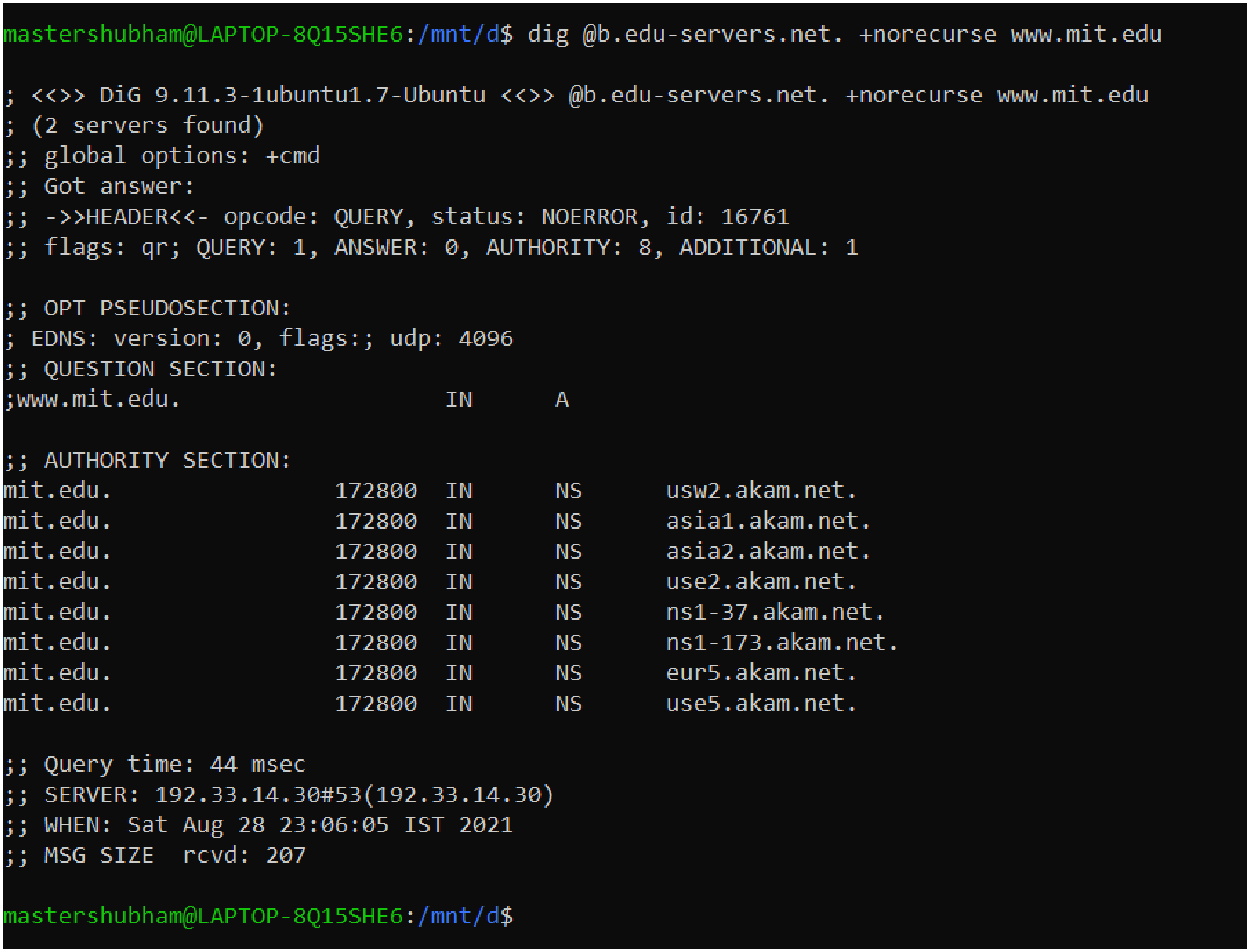
```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ clear
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @a.root-servers.net. +norecurse www.mit.edu

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @a.root-servers.net. +norecurse www.mit.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62570
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

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

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

;; ADDITIONAL SECTION:
b.edu-servers.net.      172800  IN      A       192.33.14.30
b.edu-servers.net.      172800  IN      AAAA    2001:503:231d::2:30
f.edu-servers.net.      172800  IN      A       192.35.51.30
f.edu-servers.net.      172800  IN      AAAA    2001:503:d414::30
i.edu-servers.net.      172800  IN      A       192.43.172.30
i.edu-servers.net.      172800  IN      AAAA    2001:503:39c1::30
a.edu-servers.net.      172800  IN      A       192.5.6.30
a.edu-servers.net.      172800  IN      AAAA    2001:503:a83e::2:30
g.edu-servers.net.      172800  IN      A       192.42.93.30
```

Continued



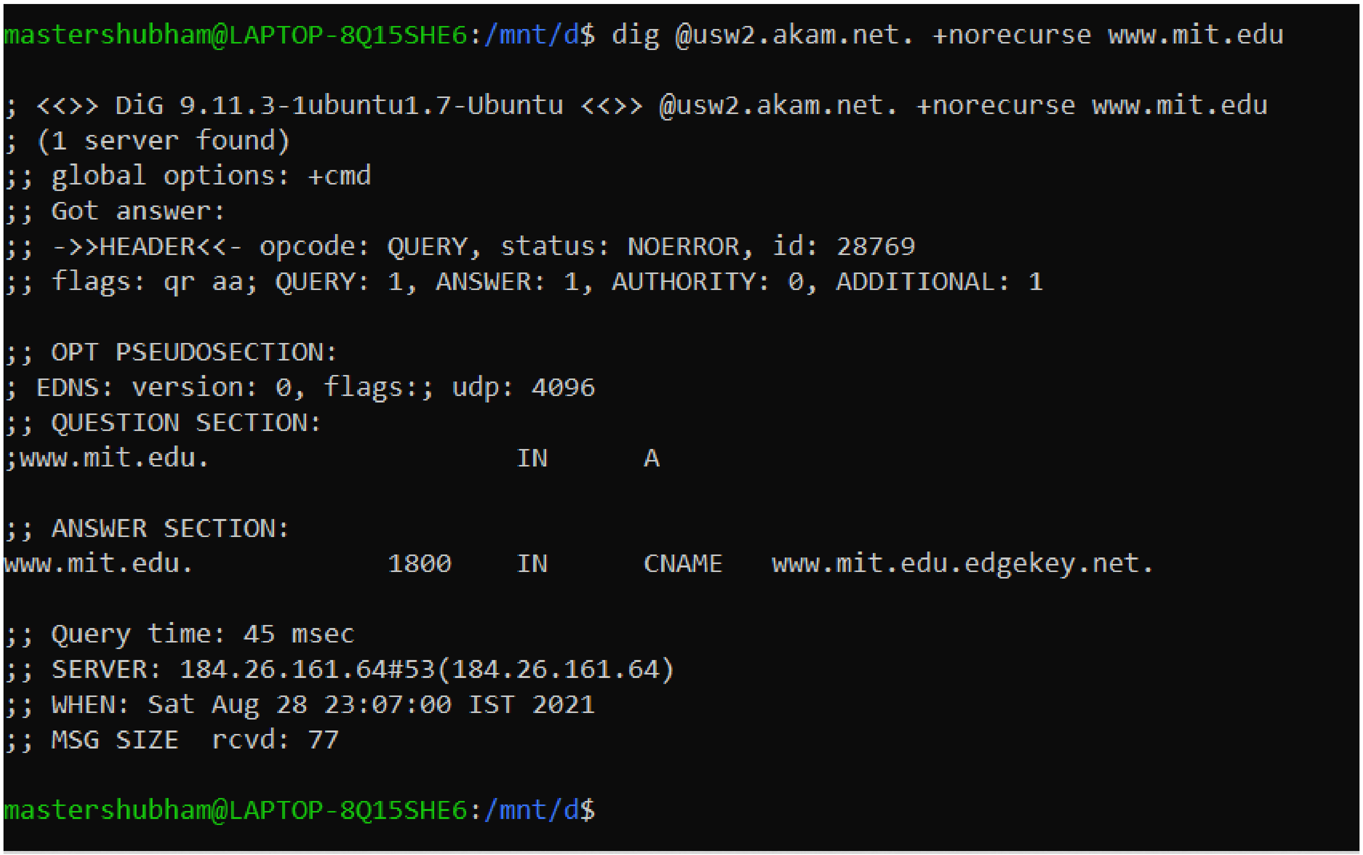
```
;; ADDITIONAL SECTION:
b.edu-servers.net.      172800  IN      A       192.33.14.30
b.edu-servers.net.      172800  IN      AAAA    2001:503:231d::2:30
f.edu-servers.net.      172800  IN      A       192.35.51.30
f.edu-servers.net.      172800  IN      AAAA    2001:503:d414::30
i.edu-servers.net.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

;; Query time: 146 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Sat Aug 28 23:04:57 IST 2021
;; MSG SIZE  rcvd: 835

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Top Level Domain Server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @b.edu-servers.net. +norecurse www.mit.edu

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @b.edu-servers.net. +norecurse www.mit.edu
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16761
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 1

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

;; AUTHORITY SECTION:
mit.edu.                172800  IN      NS      usw2.akam.net.
mit.edu.                172800  IN      NS      asia1.akam.net.
mit.edu.                172800  IN      NS      asia2.akam.net.
mit.edu.                172800  IN      NS      use2.akam.net.
mit.edu.                172800  IN      NS      ns1-37.akam.net.
mit.edu.                172800  IN      NS      ns1-173.akam.net.
mit.edu.                172800  IN      NS      eur5.akam.net.
mit.edu.                172800  IN      NS      use5.akam.net.

;; Query time: 44 msec
;; SERVER: 192.33.14.30#53(192.33.14.30)
;; WHEN: Sat Aug 28 23:06:05 IST 2021
;; MSG SIZE  rcvd: 207

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

Selecting Authoritative Name server



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d$ dig @usw2.akam.net. +norecurse www.mit.edu

; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> @usw2.akam.net. +norecurse www.mit.edu
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28769
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.mit.edu.            1800    IN      CNAME   www.mit.edu.edgekey.net.

;; Query time: 45 msec
;; SERVER: 184.26.161.64#53(184.26.161.64)
;; WHEN: Sat Aug 28 23:07:00 IST 2021
;; MSG SIZE  rcvd: 77

mastershubham@LAPTOP-8Q15SHE6:/mnt/d$
```

The name servers used in this process are:

Root Server – a.root-server.net (198.41.0.4)

Top-Level Domain Server – b.edu-server.net (192.33.14.30)

Authoritative Name Server – usw2.akam.net (184.26.161.64)

Website – www.mit.edu

Part 3 or Part C

Question 1

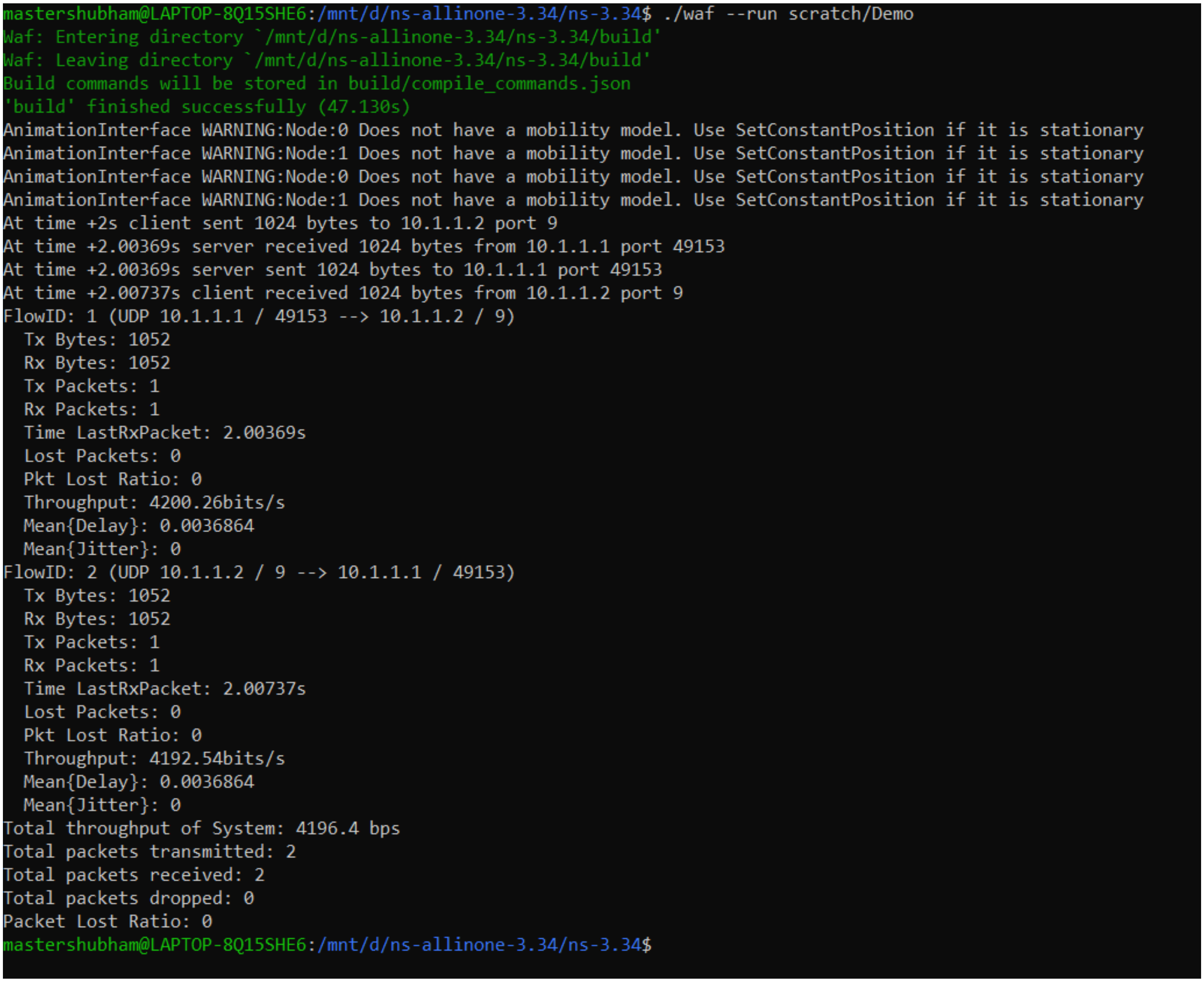
Name: Shubham Gupta

X = Number of letters in my last name = number of letters in “Gupta” = len(“Gupta”) = 5

So, X = 5.

The initial file is submitted at Demo.cc. The NetAnim file is submitted as Initial.xml

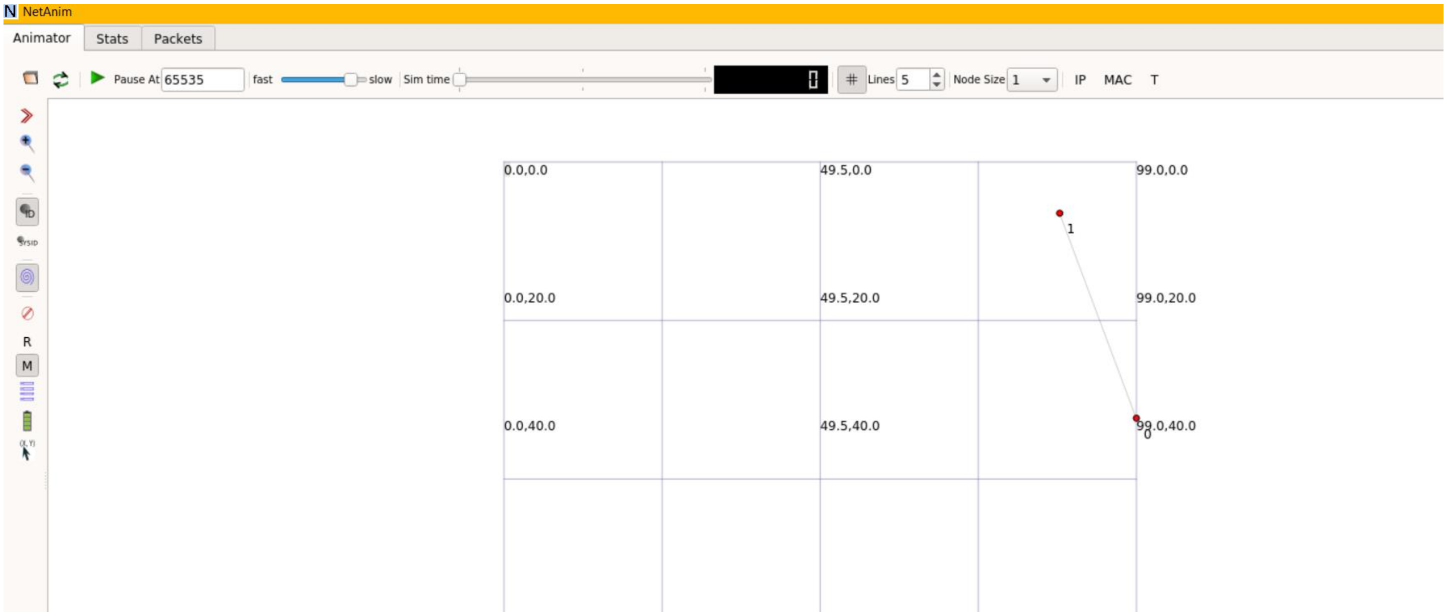
The output of the build of the file



```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d/ns-allinone-3.34/ns-3.34$ ./waf --run scratch/Demo
Waf: Entering directory `/mnt/d/ns-allinone-3.34/ns-3.34/build'
Waf: Leaving directory `/mnt/d/ns-allinone-3.34/ns-3.34/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (47.130s)
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
At time +2s client sent 1024 bytes to 10.1.1.2 port 9
At time +2.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +2.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +2.00737s client received 1024 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1 / 49153 --> 10.1.1.2 / 9)
  Tx Bytes: 1052
  Rx Bytes: 1052
  Tx Packets: 1
  Rx Packets: 1
  Time LastRxPacket: 2.00369s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 4200.26bits/s
  Mean{Delay}: 0.0036864
  Mean{Jitter}: 0
FlowID: 2 (UDP 10.1.1.2 / 9 --> 10.1.1.1 / 49153)
  Tx Bytes: 1052
  Rx Bytes: 1052
  Tx Packets: 1
  Rx Packets: 1
  Time LastRxPacket: 2.00737s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 4192.54bits/s
  Mean{Delay}: 0.0036864
  Mean{Jitter}: 0
Total throughput of System: 4196.4 bps
Total packets transmitted: 2
Total packets received: 2
Total packets dropped: 0
Packet Lost Ratio: 0
mastershubham@LAPTOP-8Q15SHE6:/mnt/d/ns-allinone-3.34/ns-3.34$
```

This gives an overall of 4196.4 bps after the transmission of the packets.

The initial Demo.cc file gives an XML file whose image in NetAnim is as follows

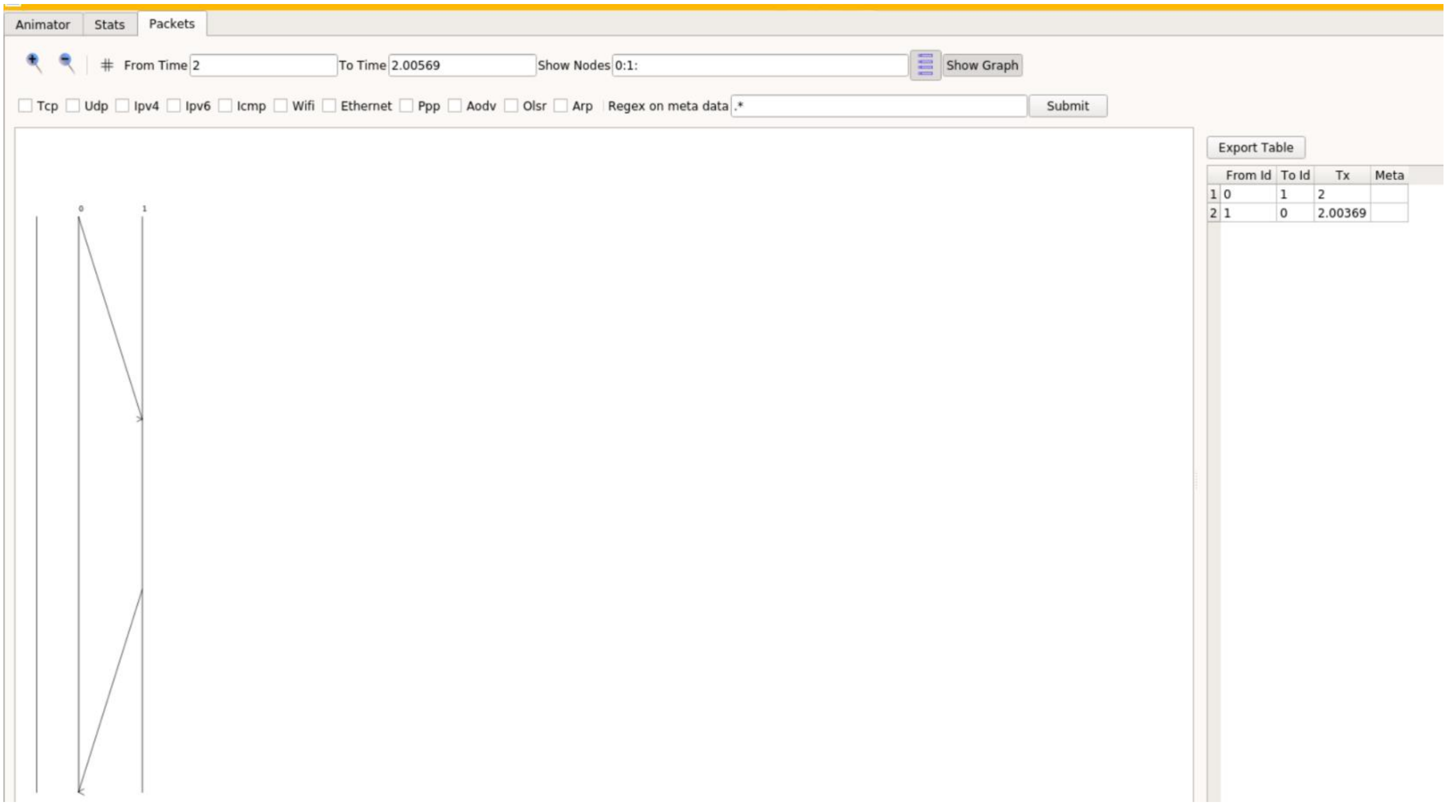


Pause At 65535

Lines 5

Node Size 1

The packet transfer graph:


Animator
Stats
Packets
Show Graph
□ Tcp □ Udp □ Ipv4 □ Ipv6 □ Icmp □ Wifi □ Ethernet □ Ppp □ Aodv □ Olsr □ Arp
Submit
Export Table
0
1

From Time 2

To Time 2.00569

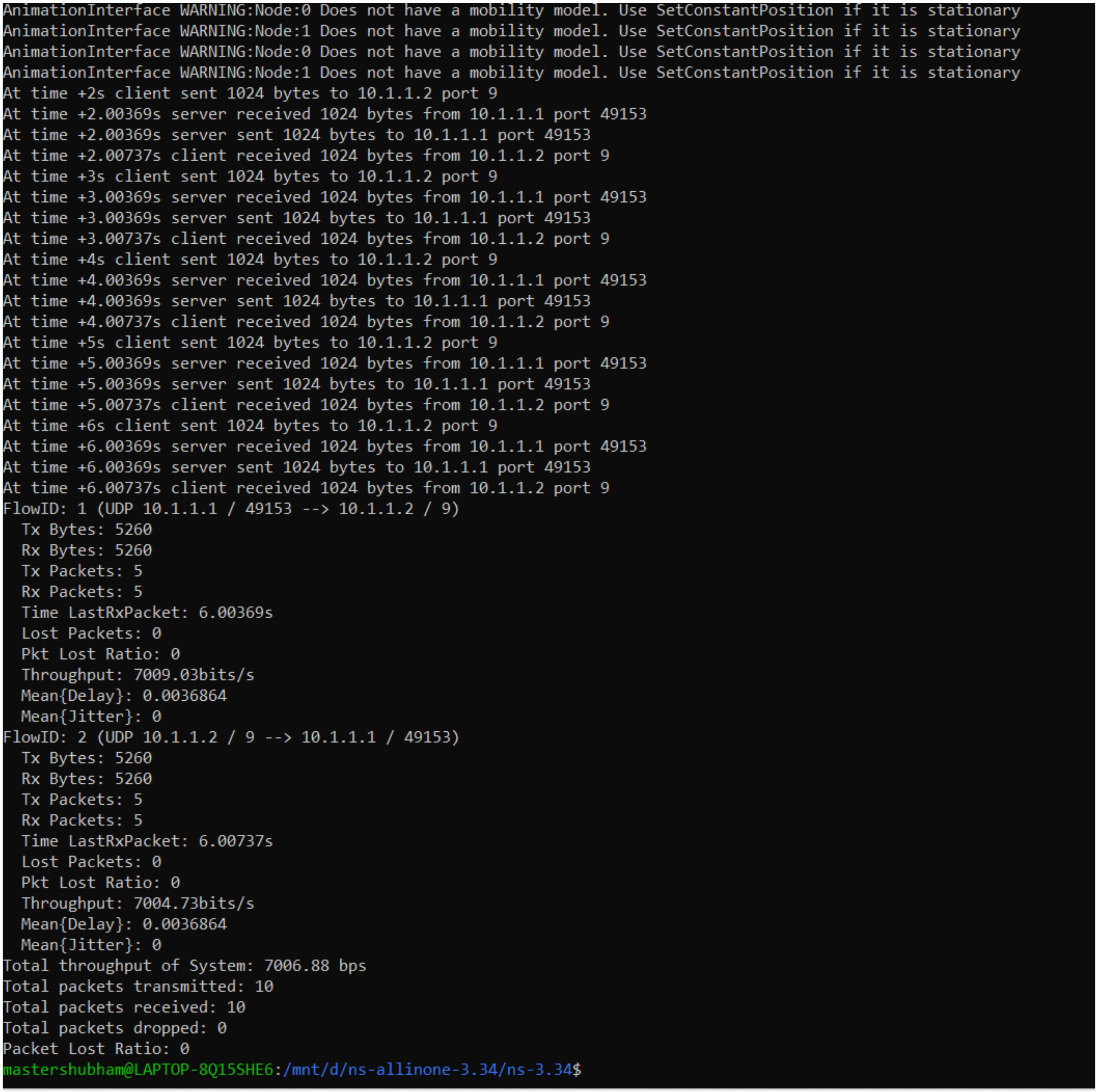
Show Nodes 0:1:

Regex on meta data .*

	From Id	To Id	Tx	Meta
1	0	1	2	
2	1	0	2.00369	

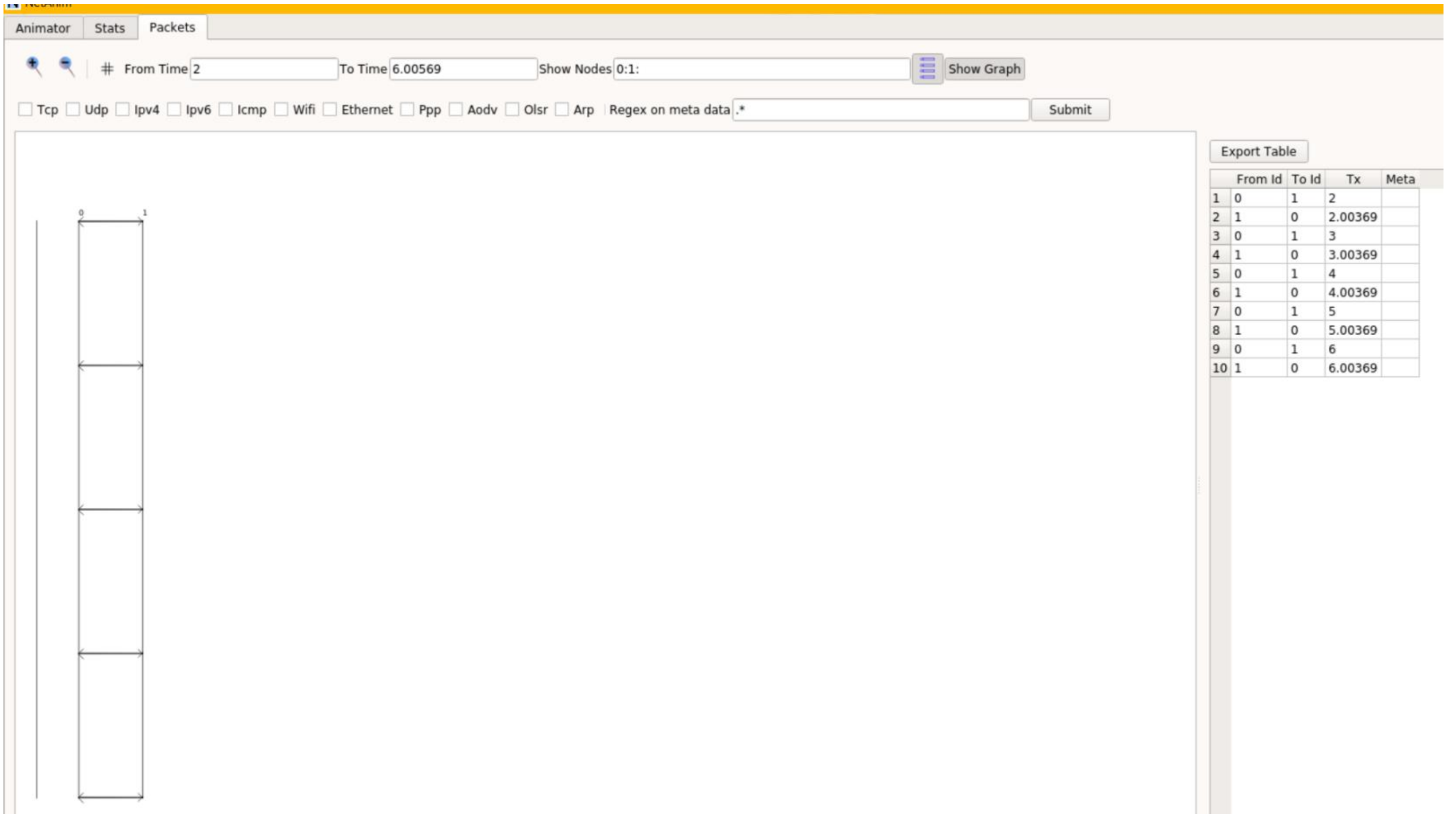
It is very important to note that the above figure that an entire connection is made, acknowledged after which the packet transmission is completed.

The modification in the Demo.cc file is on Line 134 where the parameter of the UintegerValue is changed from 1 to 5 as (X = 5). This modified file is saved as Demo1.cc. The NetAnim file is submitted as ‘X Messages.xml’



```
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
At time +2s client sent 1024 bytes to 10.1.1.2 port 9
At time +2.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +2.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +2.00737s client received 1024 bytes from 10.1.1.2 port 9
At time +3s client sent 1024 bytes to 10.1.1.2 port 9
At time +3.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +3.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +3.00737s client received 1024 bytes from 10.1.1.2 port 9
At time +4s client sent 1024 bytes to 10.1.1.2 port 9
At time +4.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +4.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +4.00737s client received 1024 bytes from 10.1.1.2 port 9
At time +5s client sent 1024 bytes to 10.1.1.2 port 9
At time +5.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +5.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +5.00737s client received 1024 bytes from 10.1.1.2 port 9
At time +6s client sent 1024 bytes to 10.1.1.2 port 9
At time +6.00369s server received 1024 bytes from 10.1.1.1 port 49153
At time +6.00369s server sent 1024 bytes to 10.1.1.1 port 49153
At time +6.00737s client received 1024 bytes from 10.1.1.2 port 9
FlowID: 1 (UDP 10.1.1.1 / 49153 --> 10.1.1.2 / 9)
  Tx Bytes: 5260
  Rx Bytes: 5260
  Tx Packets: 5
  Rx Packets: 5
  Time LastRxPacket: 6.00369s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 7009.03bits/s
  Mean{Delay}: 0.0036864
  Mean{Jitter}: 0
FlowID: 2 (UDP 10.1.1.2 / 9 --> 10.1.1.1 / 49153)
  Tx Bytes: 5260
  Rx Bytes: 5260
  Tx Packets: 5
  Rx Packets: 5
  Time LastRxPacket: 6.00737s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 7004.73bits/s
  Mean{Delay}: 0.0036864
  Mean{Jitter}: 0
Total throughput of System: 7006.88 bps
Total packets transmitted: 10
Total packets received: 10
Total packets dropped: 0
Packet Lost Ratio: 0
mastershubham@LAPTOP-8Q15SHE6:/mnt/d/ns-allinone-3.34/ns-3.34$
```

The packet transfer graph



From Time 2 To Time 6.00569 Show Nodes 0:1:

□ Tcp □ Udp □ Ipv4 □ Ipv6 □ Icmp □ Wifi □ Ethernet □ Ppp □ Aodv □ Olsr □ Arp Regex on meta data .*

	From Id	To Id	Tx	Meta
1	0	1	2	
2	1	0	2.00369	
3	0	1	3	
4	1	0	3.00369	
5	0	1	4	
6	1	0	4.00369	
7	0	1	5	
8	1	0	5.00369	
9	0	1	6	
10	1	0	6.00369	

If you closely observe, the client knows that he will be transferring multiple packets, hence he completes building the connection, communication, and acknowledgment beforehand.

As multiple packets are transferred, the client sends the packets one after another every second immediately.

The main reason for the difference in throughput is that for one packet the entire pre-processing needs to be completed followed by the transfer. This comes with a significant overhead of time as no data is transferred. As no data is transferred but the time keeps ticking, so the overall data with the time comes down.

In the case of transferring X = 5 packets in both directions, the data transferred is more which takes very little time to transfer. More data being transferred in lesser time increases throughput. The initial pre-processing is performed but the time becomes very less compared to overall time as the data transfer time dominates increasing the throughput.

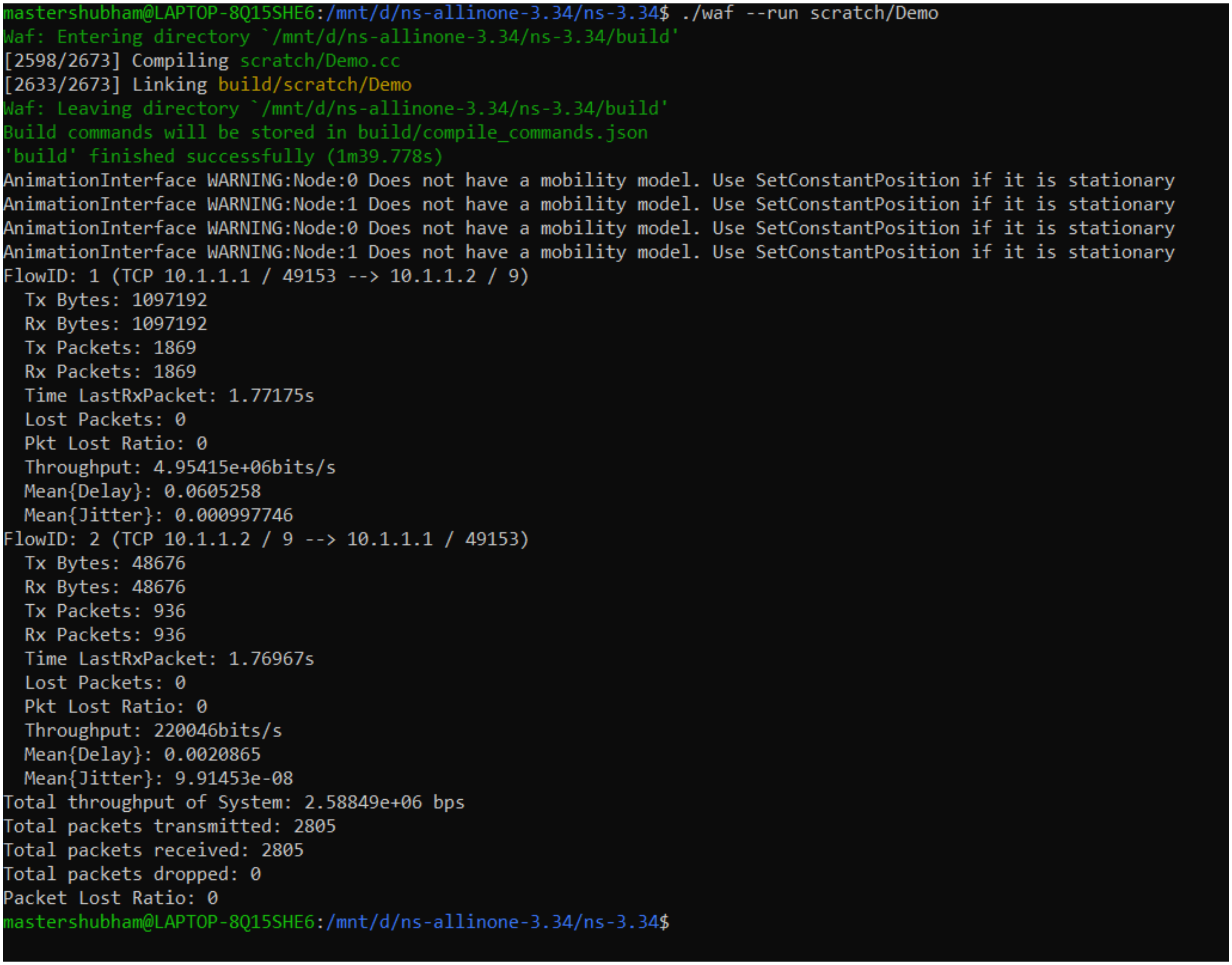
In the 1st case, the pre-processing time dominates causing lower throughput whereas in the 2nd case, the data transfer time dominates causing higher throughput.

The graphs and Linux command line output show the same. The NetAnim Animator output remains the same for both files.

Question 2

The modified CC file Demo2.cc file is attached in the Part C folder of the submission. The NetAnim file is submitted as ‘1 MB Transfer.xml’.

The output is shown below.



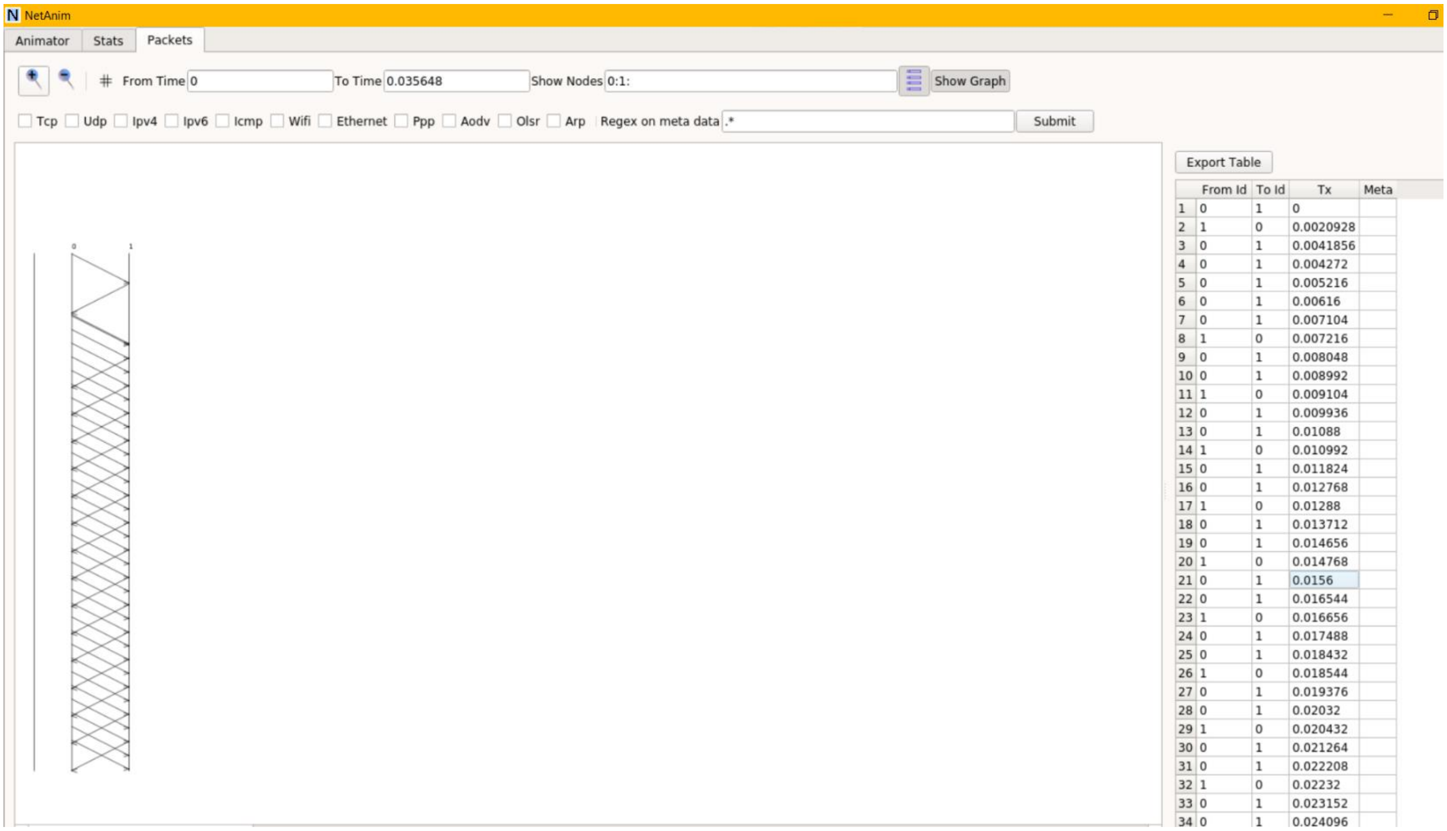
```
mastershubham@LAPTOP-8Q15SHE6:/mnt/d/ns-allinone-3.34/ns-3.34$ ./waf --run scratch/Demo
Waf: Entering directory `/mnt/d/ns-allinone-3.34/ns-3.34/build'
[2598/2673] Compiling scratch/Demo.cc
[2633/2673] Linking build/scratch/Demo
Waf: Leaving directory `/mnt/d/ns-allinone-3.34/ns-3.34/build'
Build commands will be stored in build/compile_commands.json
'build' finished successfully (1m39.778s)
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:0 Does not have a mobility model. Use SetConstantPosition if it is stationary
AnimationInterface WARNING:Node:1 Does not have a mobility model. Use SetConstantPosition if it is stationary
FlowID: 1 (TCP 10.1.1.1 / 49153 --> 10.1.1.2 / 9)
  Tx Bytes: 1097192
  Rx Bytes: 1097192
  Tx Packets: 1869
  Rx Packets: 1869
  Time LastRxPacket: 1.77175s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 4.95415e+06bits/s
  Mean{Delay}: 0.0605258
  Mean{Jitter}: 0.000997746
FlowID: 2 (TCP 10.1.1.2 / 9 --> 10.1.1.1 / 49153)
  Tx Bytes: 48676
  Rx Bytes: 48676
  Tx Packets: 936
  Rx Packets: 936
  Time LastRxPacket: 1.76967s
  Lost Packets: 0
  Pkt Lost Ratio: 0
  Throughput: 220046bits/s
  Mean{Delay}: 0.0020865
  Mean{Jitter}: 9.91453e-08
Total throughput of System: 2.58849e+06 bps
Total packets transmitted: 2805
Total packets received: 2805
Total packets dropped: 0
Packet Lost Ratio: 0
mastershubham@LAPTOP-8Q15SHE6:/mnt/d/ns-allinone-3.34/ns-3.34$
```

The throughput observed in the 1 MB file transmission is 2588490. If you look at the order of the transmission it is 10^6 which shows that very large data is transferred in a very short time.

In the echo-client (Question 1) vs 1 MB file transfer, lesser throughput is observed in the echo-client which gives a few thousand bps throughput.

The reason for the high very throughput is the creation of a bulk transfer point-to-point link. The initialization in point 0 is with a Bulk Sender and point 1 is a Bulk Sink. It is designed to transmit a very large amount of continued data in a short time giving an enormous throughput.

The initial echo-client server had a fixed bandwidth that could send a maximum of 5Mbps comprising of one packet at a time. This also causes a reduced throughput.



From Time 0 To Time 0.035648 Show Nodes 0:1:

□ Tcp □ Udp □ Ipv4 □ Ipv6 □ Icmp □ Wifi □ Ethernet □ Ppp □ Aodv □ Olsr □ Arp Regex on meta data .*

	From Id	To Id	Tx	Meta
1	0	1	0	
2	1	0	0.0020928	
3	0	1	0.0041856	
4	0	1	0.004272	
5	0	1	0.005216	
6	0	1	0.00616	
7	0	1	0.007104	
8	1	0	0.007216	
9	0	1	0.008048	
10	0	1	0.008992	
11	1	0	0.009104	
12	0	1	0.009936	
13	0	1	0.01088	
14	1	0	0.010992	
15	0	1	0.011824	
16	0	1	0.012768	
17	1	0	0.01288	
18	0	1	0.013712	
19	0	1	0.014656	
20	1	0	0.014768	
21	0	1	0.0156	
22	0	1	0.016544	
23	1	0	0.016656	
24	0	1	0.017488	
25	0	1	0.018432	
26	1	0	0.018544	
27	0	1	0.019376	
28	0	1	0.02032	
29	1	0	0.020432	
30	0	1	0.021264	
31	0	1	0.022208	
32	1	0	0.02232	
33	0	1	0.023152	
34	0	1	0.024096	

If you look at the graph above, the pre-processing takes very minimal time after which 1000+ packets are transferred. The packet transfer completely dominates the setup time. In echo-client, we are transferring 4-8 packets where the pre-processing will have a significant impact (this is greatly reduced in front of 2800). On top of this, the connection is designed for a bulk transfer from sender to the receiver which gives that throughput (see the first one -> $5*10^6$).

These 2 factors cause it to have a very large throughput during the large file transfer.

The export table can be accessed in the XML file submitted that shows the history of the packet transfer.

Throughput can be improved by using links that have lower congestion. Prioritizing the packets which are needed over the packets that can be delayed. Using the bulk transfer to transfer large data instead of a normal echo server reduces the latency and optimizes the throughput.

Building a dedicated link using exclusive ports is the best bet to maximize throughput as a private channel is provided for the necessary data transfer.

A point-to-point (P2P) link opens a socket for the bulk transfer of data from the source to the destination. It creates a dedicated link only for the intended data transfer. Since there are no interruptions and pipelines used for the transfer, the data is bound to get the entire bandwidth for faster transmission.

Giving a dedicated channel with explicit ports will allow singular transmission of the file only giving a much better throughput. Providing a private line following a direct path will provide an unparalleled Quality of Service (QoS). The absence of other traffic, high reliability, zero disruptions, low latency combined with no need for encryption, and other features present in a non-dedicated channel gives an enormous throughput -> $5*10^6$.

The echo client does not form extensive ports nor a dedicated private channel for the packet transmission. It uses the regular channel for transmission that might be providing bandwidth to other services in the system that gives a low throughput. The echo client also does not use bulk transfer for the packets which is optimized for transmission of large packets and uses the normal echo server for the transfer resulting in low throughput.

Hence, the throughput for the 1 MB file transfer matches with the Data Rate of the P2P link.