CS301 Computer Networks Assignment 2

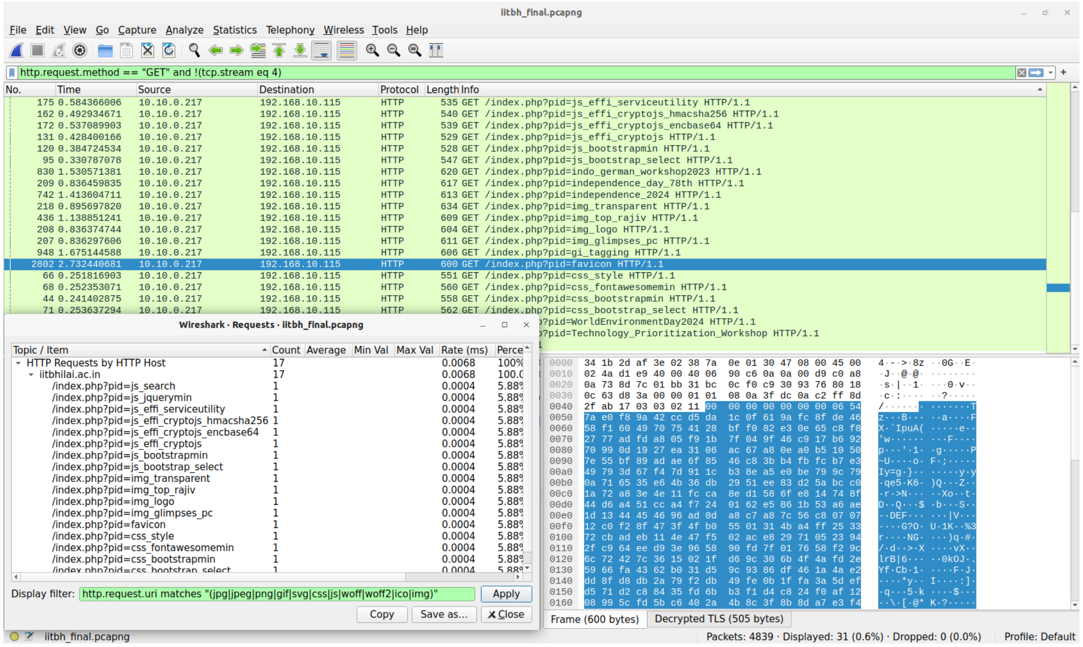
Ojus Goel

August 31, 2024

PART 1: HTTP

1. 31 get requests are sent when we browse IIT Bhilai main page (iitbhilai.ac.in).
   (a) 14 of these requests are for text content
   (b) 17 requests are for the embedded content.

   To check for embedded content, we followed: Statistic - HTTP - Request - Display filter. and applied the filter for embedded content as show in the screenshot below. We got 17 requests for embedded content.



iitbh_final.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "GET" and !(tcp.stream eq 4)
```

```
No.    Time         Source       Destination     Protocol Length Info
  175 0.584366006  10.10.0.217  192.168.10.115  HTTP     535 GET /index.php?pid=js_effi_serviceutility HTTP/1.1
  162 0.492934671  10.10.0.217  192.168.10.115  HTTP     540 GET /index.php?pid=js_effi_cryptojs_hmacsha256 HTTP/1.1
  172 0.537089903  10.10.0.217  192.168.10.115  HTTP     539 GET /index.php?pid=js_effi_cryptojs_encbase64 HTTP/1.1
  131 0.428400166  10.10.0.217  192.168.10.115  HTTP     529 GET /index.php?pid=js_effi_cryptojs HTTP/1.1
  120 0.384724534  10.10.0.217  192.168.10.115  HTTP     528 GET /index.php?pid=js_bootstrapmin HTTP/1.1
   95 0.330787078  10.10.0.217  192.168.10.115  HTTP     547 GET /index.php?pid=js_bootstrap_select HTTP/1.1
  830 1.530571381  10.10.0.217  192.168.10.115  HTTP     620 GET /index.php?pid=indo_german_workshop2023 HTTP/1.1
  209 0.836459835  10.10.0.217  192.168.10.115  HTTP     617 GET /index.php?pid=independence_day_78th HTTP/1.1
  742 1.413604711  10.10.0.217  192.168.10.115  HTTP     613 GET /index.php?pid=independence_2024 HTTP/1.1
  218 0.895697820  10.10.0.217  192.168.10.115  HTTP     634 GET /index.php?pid=img_transparent HTTP/1.1
  436 1.138851241  10.10.0.217  192.168.10.115  HTTP     609 GET /index.php?pid=img_top_rajiv HTTP/1.1
  208 0.836374744  10.10.0.217  192.168.10.115  HTTP     604 GET /index.php?pid=img_logo HTTP/1.1
  207 0.836297606  10.10.0.217  192.168.10.115  HTTP     611 GET /index.php?pid=img_glimpses_pc HTTP/1.1
  948 1.675144588  10.10.0.217  192.168.10.115  HTTP     606 GET /index.php?pid=gi_tagging HTTP/1.1
 2802 2.732440681  10.10.0.217  192.168.10.115  HTTP     600 GET /index.php?pid=favicon HTTP/1.1
   66 0.251816903  10.10.0.217  192.168.10.115  HTTP     551 GET /index.php?pid=css_style HTTP/1.1
   68 0.252353071  10.10.0.217  192.168.10.115  HTTP     560 GET /index.php?pid=css_fontawesomemin HTTP/1.1
   44 0.241402875  10.10.0.217  192.168.10.115  HTTP     558 GET /index.php?pid=css_bootstrapmin HTTP/1.1
   71 0.253637294  10.10.0.217  192.168.10.115  HTTP     562 GET /index.php?pid=css_bootstrap_select HTTP/1.1
                                                             ?pid=WorldEnvironmentDay2024 HTTP/1.1
                                                             ?pid=Technology_Prioritization_Workshop HTTP/1.1
```

```
Topic / Item                                  Count Average Min Val Max Val Rate (ms) Perce
HTTP Requests by HTTP Host                    17                            0.0068    100%
  iitbhilai.ac.in                             17                            0.0068    100.(
    /index.php?pid=js_search                  1                             0.0004    5.88%
    /index.php?pid=js_jquerymin               1                             0.0004    5.88%
    /index.php?pid=js_effi_serviceutility     1                             0.0004    5.88%
    /index.php?pid=js_effi_cryptojs_hmacsha256 1                            0.0004    5.88%
    /index.php?pid=js_effi_cryptojs_encbase64 1                             0.0004    5.88%
    /index.php?pid=js_effi_cryptojs           1                             0.0004    5.88%
    /index.php?pid=js_bootstrapmin            1                             0.0004    5.88%
    /index.php?pid=js_bootstrap_select        1                             0.0004    5.88%
    /index.php?pid=img_transparent            1                             0.0004    5.88%
    /index.php?pid=img_top_rajiv              1                             0.0004    5.88%
    /index.php?pid=img_logo                   1                             0.0004    5.88%
    /index.php?pid=img_glimpses_pc            1                             0.0004    5.88%
    /index.php?pid=favicon                    1                             0.0004    5.88%
    /index.php?pid=css_style                  1                             0.0004    5.88%
    /index.php?pid=css_fontawesomemin         1                             0.0004    5.88%
    /index.php?pid=css_bootstrapmin           1                             0.0004    5.88%
    /index.php?pid=css_bootstrap_select       1                             0.0004    5.88%
```

Display filter: `http.request.uri matches "(jpg|jpeg|png|gif|svg|css|js|woff|woff2|ico|img)"`

```
0000  34 1b 2d af 3e 02 38 7a  0e 01 30 47 08 00 45 00   4·-·>·8z ··0G··E·
0010  02 4a d1 e9 40 00 40 06  90 c6 0a 0a 00 d9 c0 a8   ·J··@·@· ········
0020  0a 73 8d 7c 01 bb 31 bc  0c f0 c9 30 93 76 80 18   ·s·|··1· ···0·v··
0030  0c 63 d8 3a 00 00 01 01  08 0a 3f dc 0a c2 ff 8d   ·c·:···· ··?·····
0040  2f ab 17 03 03 02 11 00  00 00 00 00 00 00 06 54   /······· ·······T
0050  7a e0 f8 9a 42 cc d5 da  1c 0f 61 9a fc 8f de 46   z···B··· ··a····F
0060  58 f1 60 49 70 75 41 28  bf f0 82 e3 0e 65 c8 f8   X·`IpuA( ·····e··
0070  27 77 ad fd a8 05 f9 1b  7f 04 9f 46 c9 17 b6 92   'w······ ···F····
0080  70 99 0d 19 27 ea 31 06  ac 67 a8 0e a0 b5 10 50   p···'·1· ·g·····P
0090  7e 55 bf 89 ad ae 6f 85  46 c8 3b b4 fb fc b7 e3   ~U····o· F·;·····
00a0  49 79 3d 67 f4 7d 91 1c  b3 8e a5 e0 be 79 9c 79   Iy=g·}·· ·····y·y
00b0  0a 71 65 35 e6 4b 36 db  29 51 ee 83 d2 5a bc c0   ·qe5·K6· )Q···Z··
00c0  1a 72 a8 3e 4e 11 fc ca  8e d1 58 6f e8 14 74 8f   ·r·>N··· ··Xo··t·
00d0  44 d6 a4 51 cc a4 f7 24  01 62 e5 86 1b 53 a6 ae   D··Q···$ ·b···S··
00e0  1d 13 44 45 46 96 ad 0d  a8 c7 a8 7c 56 c8 07 07   ··DEF··· ···|V···
00f0  12 c0 f2 8f 47 3f 4f b0  55 01 31 4b a4 ff 25 33   ····G?O· U·1K··%3
0100  72 cb ad eb 11 4e 47 f5  02 ac e8 29 71 05 23 94   r····NG· ···)q·#·
0110  2f c9 64 ee d9 3e 96 58  90 fd 7f 01 76 58 f2 9c   /·d··>·X ····vX··
0120  6c 72 42 7c 36 15 02 1f  d6 9c 30 6b 4f 4a fd 2e   lrB|6··· ··0kOJ·.
0130  59 66 fa 43 62 b0 31 d5  9c 93 86 df 46 1a 4a e2   Yf·Cb·1· ····F·J·
0140  dd 8f d8 db 2a 79 f2 db  49 fe 0b 1f fa 3a 5d ef   ····*y·· I····:]·
0150  d5 71 d2 c8 84 35 fd 6b  b3 f1 d4 c8 24 f0 af 12   ·q···5·k ····$···
0160  08 99 5c fd 5b c6 40 2a  4b 8c 3f 8b 8d a7 e3 f4   ··\·[·@* K·?·····
```

Packets: 4839 · Displayed: 31 (0.6%) · Dropped: 0 (0.0%)   Profile: Default

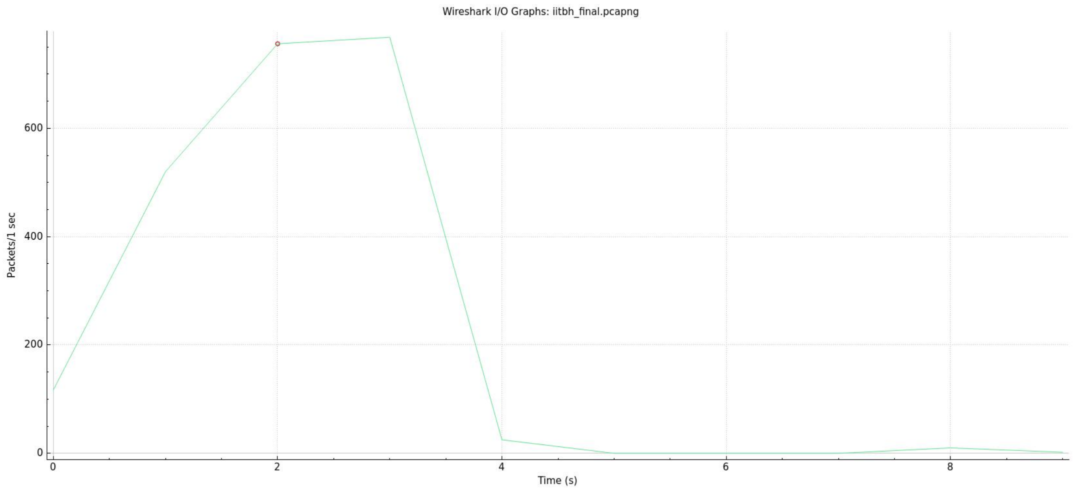


Figure : IO graph for packets sent to iitbhilai.ac.in.

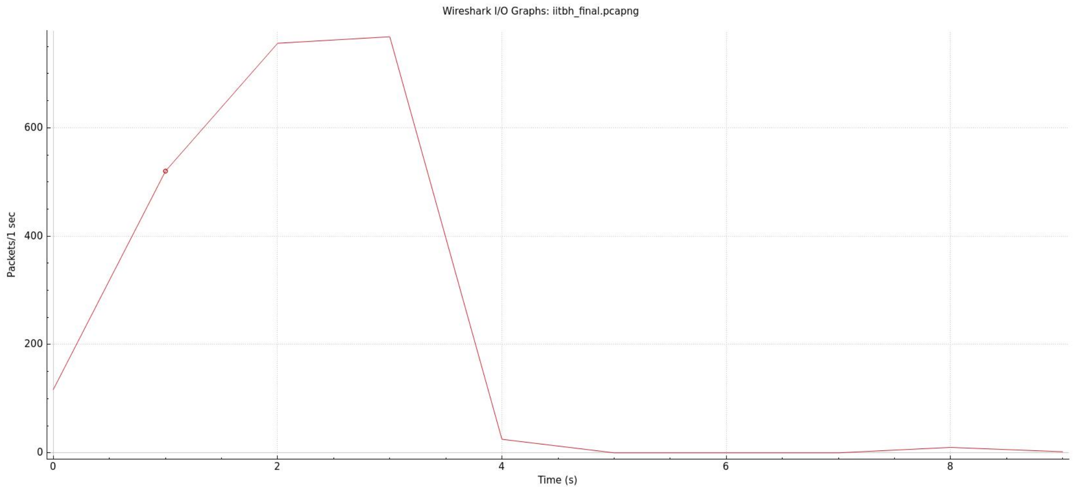


Figure : IO graph for packets received from iitbhilai.ac.in.

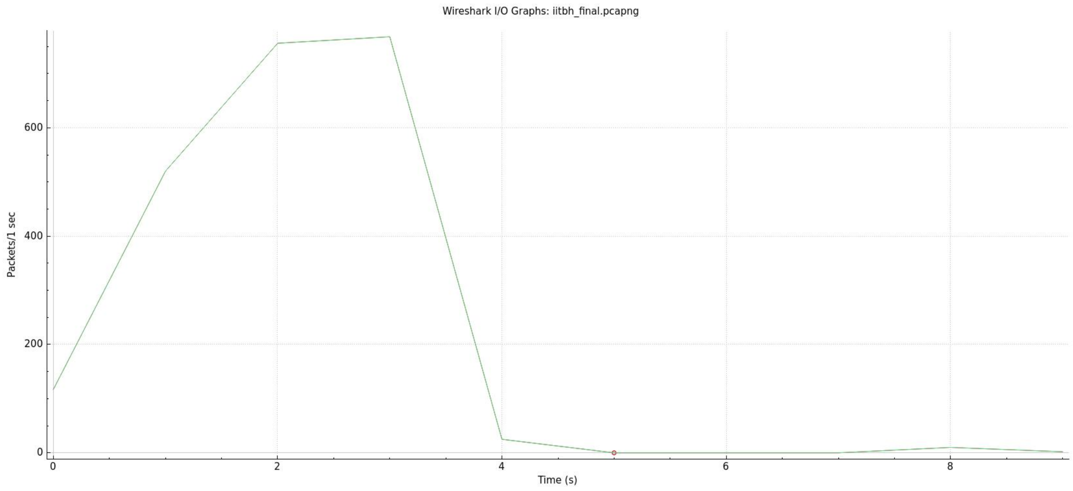
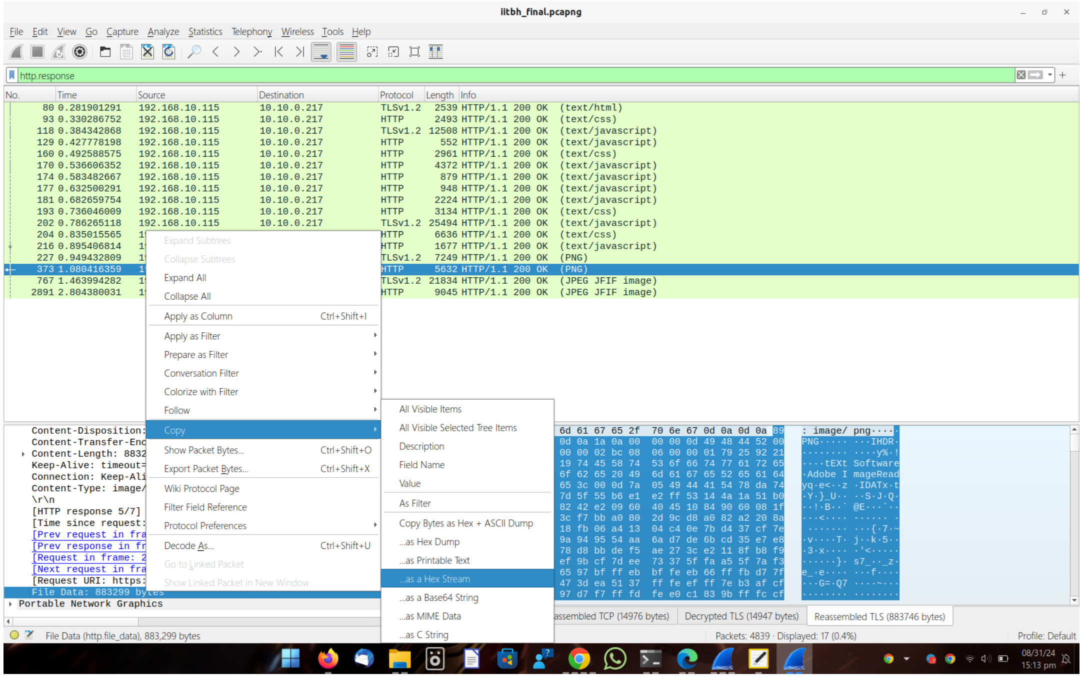


Figure : Combined IO graph for packets sent and received from iitbhilai.ac.in.

2. The total amount of data being received in the corresponding HTTP response message for each HTTP get request.

Get request frame number	**Response frame number**	**Amount of Data**
172	216	1100
131	202	47944
175	181	5361
72	177	379
162	174	302
120	170	37045
95	129	31697
82	118	116840
11	80	36976
71	204	6065
68	193	31004
44	160	121033
66	93	19232
218	373	883299
208	227	36312
769	2891	555508
206	767	154263
	Total	**2,112,360**

3. To reconstruct the image, we first need the hex stream. The hex was obtained as shown by the steps in screenshot below:



http.response

```
No.  Time        Source          Destination  Protocol Length Info
  80 0.281901291 192.168.10.115  10.10.0.217  TLSv1.2   2539 HTTP/1.1 200 OK  (text/html)
  93 0.330286752 192.168.10.115  10.10.0.217  HTTP      2493 HTTP/1.1 200 OK  (text/css)
 118 0.384342868 192.168.10.115  10.10.0.217  TLSv1.2  12508 HTTP/1.1 200 OK  (text/javascript)
 129 0.427778198 192.168.10.115  10.10.0.217  HTTP       552 HTTP/1.1 200 OK  (text/javascript)
 160 0.492588575 192.168.10.115  10.10.0.217  HTTP      2961 HTTP/1.1 200 OK  (text/css)
 170 0.536606352 192.168.10.115  10.10.0.217  HTTP      4372 HTTP/1.1 200 OK  (text/javascript)
 174 0.583482667 192.168.10.115  10.10.0.217  HTTP       879 HTTP/1.1 200 OK  (text/javascript)
 177 0.632500291 192.168.10.115  10.10.0.217  HTTP       948 HTTP/1.1 200 OK  (text/javascript)
 181 0.682659754 192.168.10.115  10.10.0.217  HTTP      2224 HTTP/1.1 200 OK  (text/javascript)
 193 0.736046009 192.168.10.115  10.10.0.217  HTTP      3134 HTTP/1.1 200 OK  (text/css)
 202 0.786265118 192.168.10.115  10.10.0.217  TLSv1.2  25494 HTTP/1.1 200 OK  (text/javascript)
 204 0.835015565 1                            HTTP      6636 HTTP/1.1 200 OK  (text/css)
 216 0.895406814 1                            HTTP      1677 HTTP/1.1 200 OK  (text/javascript)
 227 0.949432809 1                            TLSv1.2   7249 HTTP/1.1 200 OK  (PNG)
 373 1.080416359 1                            HTTP      5632 HTTP/1.1 200 OK  (PNG)
 767 1.463994282 1                            TLSv1.2  21834 HTTP/1.1 200 OK  (JPEG JFIF image)
2891 2.804380031 1                            HTTP      9045 HTTP/1.1 200 OK  (JPEG JFIF image)
```

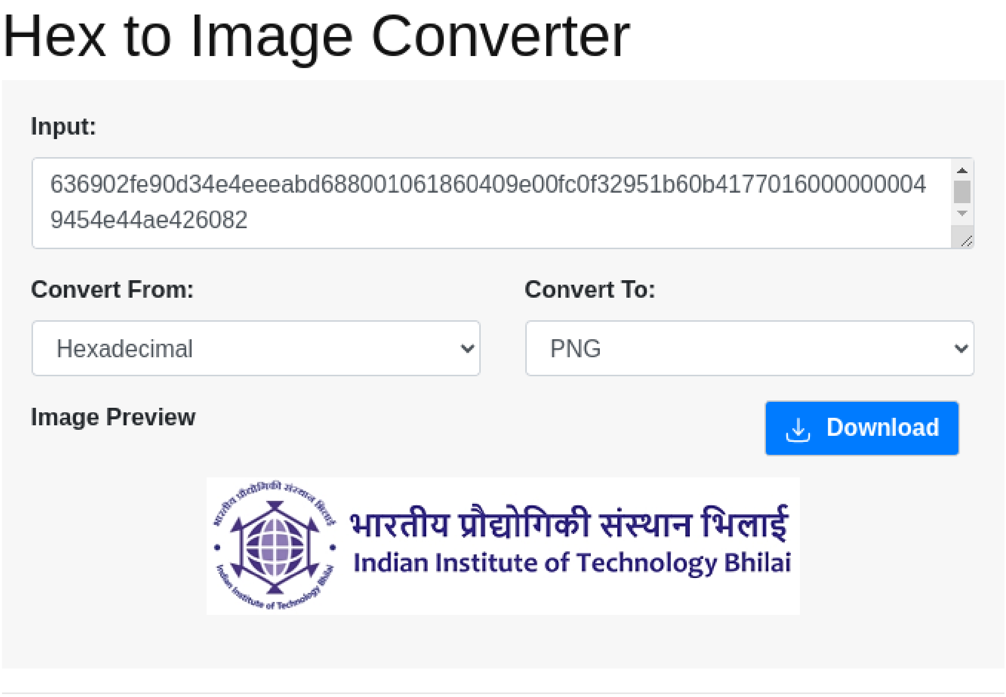
```
  Content-Disposition:
  Content-Transfer-Enc
▸ Content-Length: 8832
  Keep-Alive: timeout=
  Connection: Keep-Ali
  Content-Type: image/
  \r\n
  [HTTP response 5/7]
  [Time since request:
  [Prev request in fra
  [Prev response in fr
  [Request in frame: 2
  [Next request in fra
  [Request URI: https:
  File Data: 883299 bytes
▸ Portable Network Graphics
```

```
6d 61 67 65 2f  70 6e 67 0d 0a 0d 0a 89   : image/ png····
0d 0a 1a 0a 00  00 00 0d 49 48 44 52 00   PNG·····  ···IHDR·
00 00 02 bc 08  06 00 00 01 79 25 92 21   ········  ····y%·!
19 74 45 58 74  53 6f 66 74 77 61 72 65   ····tEXt Software
6f 62 65 20 49  6d 61 67 65 52 65 61 64   ·Adobe I mageRead
65 3c 00 0d 7a  05 49 44 41 54 78 da 74   yq·e<··z ·IDATx·t
7d 5f 55 b6 e1  e2 ff 53 14 4a 1a 51 b0   ·Y·}_U·· ··S·J·Q·
82 42 e2 09 60  40 45 10 84 90 60 08 1f   ··!·B··` @E···`··
3c f7 bb a0 80  2d 9c d8 a0 82 a2 20 8a   ···<···· ·······
18 fb 06 a4 13  04 c4 0e 7b d4 37 cf 7e   ········ ···{·7·~
9a 94 95 54 aa  6a d7 de 6b cd 35 e7 e8   ·v····T· j··k·5··
78 d8 bb de f5  ae 27 3c e2 11 8f b8 f9   ·3·x···· ·'<·····
ef 9b cf 7d ee  73 37 5f fa a5 5f 7a f3   ······}· s7_···_z·
65 97 bf ff eb  bf fe eb 66 ff fb d7 7f   e_·e···· ···f····
47 3d ea 51 37  ff fe ef ff 7e b3 af cf   ···G=·Q7 ····~···
97 d7 f7 ff fd  fe e0 c1 83 9b ff fc cf   ········ ········
```

File Data (http.file_data), 883,299 bytes

Packets: 4839 · Displayed: 17 (0.4%)

Figure : Steps to get the Hex stream



Hex to Image Converter

Input:

```
636902fe90d34e4eeeabd688001061860409e00fc0f32951b60b4177016000000004
9454e44ae426082
```

Convert From: Hexadecimal

Convert To: PNG

Image Preview

Download
भारतीय प्रौद्योगिकी संस्थान भिलाई
Indian Institute of Technology Bhilai

Figure : Hex to Image converter

भारतीय प्रौद्योगिकी संस्थान भिलाई
Indian Institute of Technology Bhilai

Figure : Final Converted Image

4. (a) No

   (b) Yes, the server returned the content of the file explicitly. We can tell this by checking the response status code. The server returned a status code “200 OK” which indicates that the server has returned the requested content. Also we didn’t get “304 Not modified”, this means that the content wasn’t returned by cache, but explicitly returned by the server.

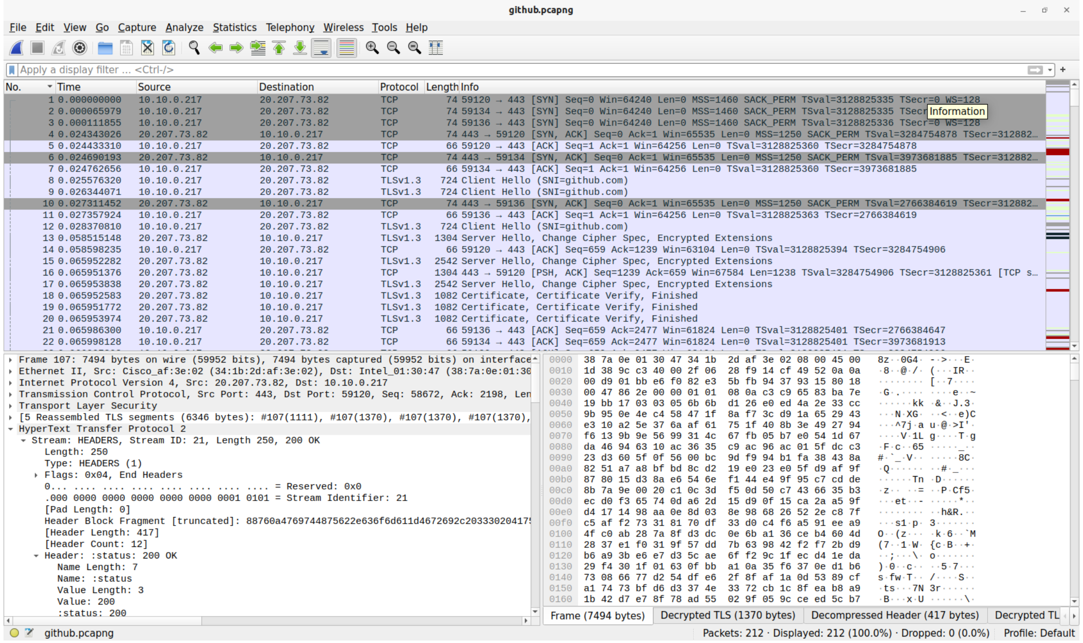
   (c) No

   (d) i. HTTP Status Code - 200

   ii. Response Phrase - OK

   The server explicitly returns the content of the file. The reason is same as explained in part b.

5. **The end-to-end process of web page loading:** Establishing TCP Connection: To establish TCP connection, three-way handshake is required. The client 10.10.0.217 initiates a TCP connection using 3 different ports as seen in first 3 frames (frame 1 - frame 3). The SYN flag indicated that the client is requesting a connection.discuss the end-to-end process of web page loading using Wireshark. The server responds to this with SYN, ACK flags. This acknowledges the request and indicates that server is ready to establish connection. The client sends back ACK packets which completes the three way handshake, and secure connection is established. The client also sends ”Client Hello” messages. And the server responds with ”Server Hello” messages.


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

```
No.     Time          Source          Destination     Protocol  Length Info
      1 0.000000000   10.10.0.217     20.207.73.82    TCP         74 59120 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3128825335 TSecr=0 WS=128
      2 0.000065979   10.10.0.217     20.207.73.82    TCP         74 59134 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3128825335 TSecr
      3 0.000111855   10.10.0.217     20.207.73.82    TCP         74 59136 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3128825336 TSecr=0 WS=128
      4 0.024343026   20.207.73.82    10.10.0.217     TCP         74 443 → 59120 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=3284754878 TSecr=312882…
      5 0.024433310   10.10.0.217     20.207.73.82    TCP         66 59120 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3128825360 TSecr=3284754878
      6 0.024690193   20.207.73.82    10.10.0.217     TCP         74 443 → 59134 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=3973681885 TSecr=312882…
      7 0.024762656   10.10.0.217     20.207.73.82    TCP         66 59134 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3128825360 TSecr=3973681885
      8 0.025576320   10.10.0.217     20.207.73.82    TLSv1.3    724 Client Hello (SNI=github.com)
      9 0.026344071   10.10.0.217     20.207.73.82    TLSv1.3    724 Client Hello (SNI=github.com)
     10 0.027311452   20.207.73.82    10.10.0.217     TCP         74 443 → 59136 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1250 SACK_PERM TSval=2766384619 TSecr=312882…
     11 0.027357924   10.10.0.217     20.207.73.82    TCP         66 59136 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3128825363 TSecr=2766384619
     12 0.028370810   10.10.0.217     20.207.73.82    TLSv1.3    724 Client Hello (SNI=github.com)
     13 0.058515148   20.207.73.82    10.10.0.217     TLSv1.3   1304 Server Hello, Change Cipher Spec, Encrypted Extensions
     14 0.058598235   10.10.0.217     20.207.73.82    TCP         66 59120 → 443 [ACK] Seq=659 Ack=1239 Win=63104 Len=0 TSval=3128825394 TSecr=3284754906
     15 0.065952282   20.207.73.82    10.10.0.217     TLSv1.3   2542 Server Hello, Change Cipher Spec, Encrypted Extensions
     16 0.065951376   20.207.73.82    10.10.0.217     TCP       1304 443 → 59120 [PSH, ACK] Seq=1239 Ack=659 Win=67584 Len=1238 TSval=3284754906 TSecr=3128825361 [TCP s…
     17 0.065953838   20.207.73.82    10.10.0.217     TLSv1.3   2542 Server Hello, Change Cipher Spec, Encrypted Extensions
     18 0.065952583   20.207.73.82    10.10.0.217     TLSv1.3   1082 Certificate, Certificate Verify, Finished
     19 0.065951772   20.207.73.82    10.10.0.217     TLSv1.3   1082 Certificate, Certificate Verify, Finished
     20 0.065953974   20.207.73.82    10.10.0.217     TLSv1.3   1082 Certificate, Certificate Verify, Finished
     21 0.065986300   10.10.0.217     20.207.73.82    TCP         66 59136 → 443 [ACK] Seq=659 Ack=2477 Win=61824 Len=0 TSval=3128825401 TSecr=2766384647
     22 0.065998128   10.10.0.217     20.207.73.82    TCP         66 59134 → 443 [ACK] Seq=659 Ack=2477 Win=61824 Len=0 TSval=3128825401 TSecr=3973681913
```

```
▸ Frame 107: 7494 bytes on wire (59952 bits), 7494 bytes captured (59952 bits) on interface
▸ Ethernet II, Src: Cisco_af:3e:02 (34:1b:2d:af:3e:02), Dst: Intel_01:30:47 (38:7a:0e:01:30
▸ Internet Protocol Version 4, Src: 20.207.73.82, Dst: 10.10.0.217
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 59120, Seq: 58672, Ack: 2198, Len
▸ Transport Layer Security
▸ [5 Reassembled TLS segments (6346 bytes): #107(1111), #107(1370), #107(1370), #107(1370),
▾ HyperText Transfer Protocol 2
  ▾ Stream: HEADERS, Stream ID: 21, Length 250, 200 OK
      Length: 250
      Type: HEADERS (1)
    ▸ Flags: 0x04, End Headers
      0... .... .... .... .... .... .... .... = Reserved: 0x0
      .000 0000 0000 0000 0000 0000 0001 0101 = Stream Identifier: 21
      [Pad Length: 0]
      Header Block Fragment [truncated]: 88760a4769744875622e636f6d611d4672692c20333020417
      [Header Length: 417]
      [Header Count: 12]
    ▾ Header: :status: 200 OK
        Name Length: 7
        Name: :status
        Value Length: 3
        Value: 200
        :status: 200
```

```
0000  38 7a 0e 01 30 47 34 1b  2d af 3e 02 08 00 45 00   8z··0G4· -·>···E·
0010  1d 38 9c c3 40 00 2f 06  28 f9 14 cf 49 52 0a 0a   ·8··@·/· (···IR··
0020  00 d9 01 bb e6 f0 82 e3  5b fb 94 37 93 15 80 18   ········ [··7····
0030  00 47 86 2e 00 00 01 01  08 0a c3 c9 65 83 ba 7e   ·G.····· ····e··~
0040  19 bb 17 03 03 05 6b 6b  d1 26 e0 ed 4a 2e 33 cc   ······kk ·&··J.3·
0050  9b 95 0e 4e c4 58 47 1f  8a f7 3c d9 1a 65 29 43   ···N·XG· ··<··e)C
0060  e3 10 a2 5e 37 6a af 61  75 1f 40 8b 3e 49 27 94   ···^7j·a u·@·>I'·
0070  f6 13 9b 9e 56 99 31 4c  67 fb 05 b7 e0 54 1d 67   ····V·1L g····T·g
0080  da 46 94 63 10 ac 36 35  c9 ac 96 ac 01 5f dc c3   ·F·c··65 ·····_··
0090  23 d3 60 5f 0f 56 00 bc  9d f9 94 b1 fa 38 43 8a   #·`_·V·· ·····8C·
00a0  82 51 a7 a8 bf bd 8c d2  19 e0 23 e0 5f d9 af 9f   ·Q······ ··#·_···
00b0  87 80 15 d3 8a e6 54 6e  f1 44 e4 9f 95 c7 cd de   ······Tn ·D······
00c0  8b 7a 9e 00 20 c1 0c 3d  f5 0d 50 c7 43 66 35 b3   ·z·· ··= ··P·Cf5·
00d0  ec d0 f3 65 74 0d a6 2d  15 d9 0f 15 ca 2a a5 9f   ···et··- ·····*··
00e0  d4 17 14 98 aa 0e 8d 03  8e 98 68 26 52 2e c8 7f   ········ ··h&R.··
00f0  c5 af f2 73 31 81 70 df  33 d0 c4 f6 a5 91 ee a9   ···s1·p· 3·······
0100  4f c0 ab 28 7a 8f d3 dc  0e 6b a1 36 ce b4 60 4d   O··(z··· ·k·6··`M
0110  28 37 e1 f0 31 9f 57 dd  7b 63 98 42 f2 f7 2b d9   (7··1·W· {c·B··+·
0120  b6 a9 3b e6 e7 d3 5c ae  6f f2 9c 1f ec d4 1e da   ··;···\· o·······
0130  29 f4 30 1f 01 63 0f bb  a1 0a 35 f6 37 0e d1 b6   )·0··c·· ··5·7···
0140  73 08 66 77 d2 54 df e6  2f 8f af 1a 0d 53 89 cf   s·fw·T·· /····S··
0150  a1 74 73 bf d6 d3 37 4e  33 72 cb 1c 8f ea b8 a9   ·ts···7N 3r······
0160  1b 42 d7 e7 8f 78 ad 55  02 9f 05 9c ce ed 5c b7   ·B···x·U ······\·
```

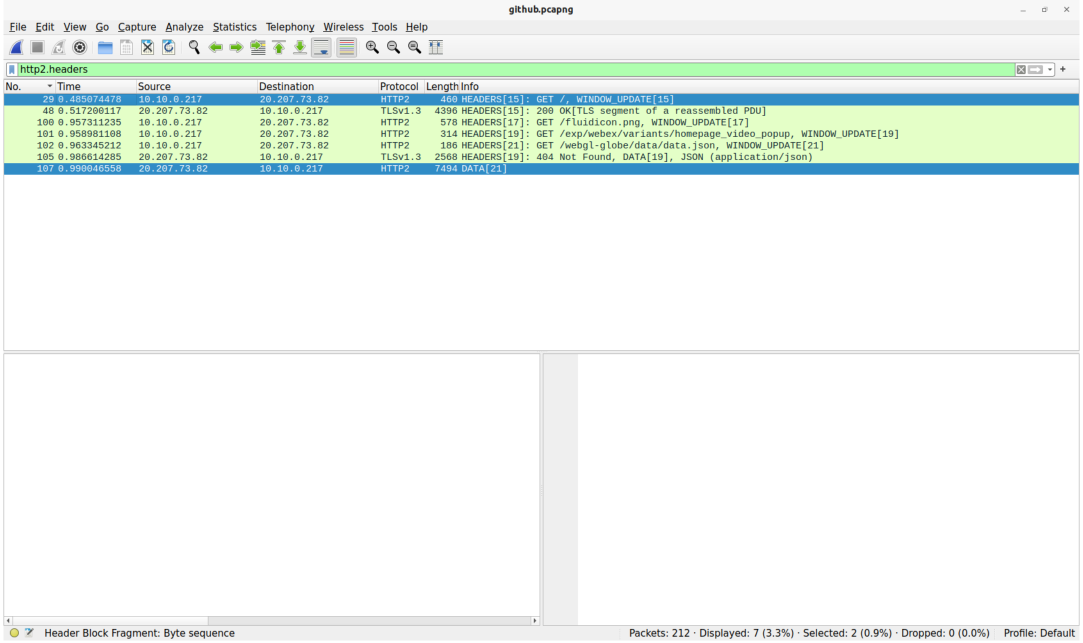
github.pcapng   Packets: 212 · Displayed: 212 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

Time to Load the page = Timestamp of first GET request - Timestamp of last response message.

Timestamp of first GET Command = 0.485074478

Timestamp of last "HTTP 200 OK" (response message) = 0.990046558

Time to load the page = 0.990046558 - 0.485074478 = **0.50497208 seconds**

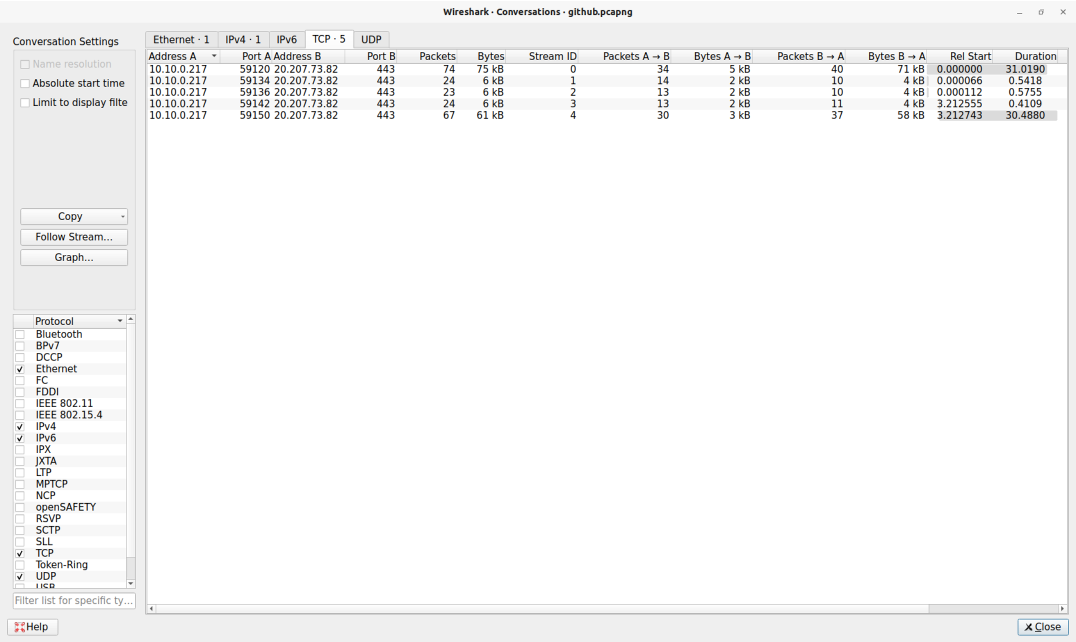

github.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http2.headers

```
No.     Time          Source          Destination     Protocol  Length Info
     29 0.485074478   10.10.0.217     20.207.73.82    HTTP2      460 HEADERS[15]: GET /, WINDOW_UPDATE[15]
     48 0.517200117   20.207.73.82    10.10.0.217     TLSv1.3   4396 HEADERS[15]: 200 OK[TLS segment of a reassembled PDU]
    100 0.957311235   10.10.0.217     20.207.73.82    HTTP2      578 HEADERS[17]: GET /fluidicon.png, WINDOW_UPDATE[17]
    101 0.958981108   10.10.0.217     20.207.73.82    HTTP2      314 HEADERS[19]: GET /exp/webex/variants/homepage_video_popup, WINDOW_UPDATE[19]
    102 0.963345212   10.10.0.217     20.207.73.82    HTTP2      186 HEADERS[21]: GET /webgl-globe/data/data.json, WINDOW_UPDATE[21]
    105 0.986614285   20.207.73.82    10.10.0.217     TLSv1.3   2568 HEADERS[19]: 404 Not Found, DATA[19], JSON (application/json)
    107 0.990046558   20.207.73.82    10.10.0.217     HTTP2     7494 DATA[21]
```

Header Block Fragment: Byte sequence   Packets: 212 · Displayed: 7 (3.3%) · Selected: 2 (0.9%) · Dropped: 0 (0.0%)   Profile: Default

We have used **5 TCP connections** to download this page.



Wireshark · Conversations · github.pcapng

Conversation Settings

☐ Name resolution
☐ Absolute start time
☐ Limit to display filte

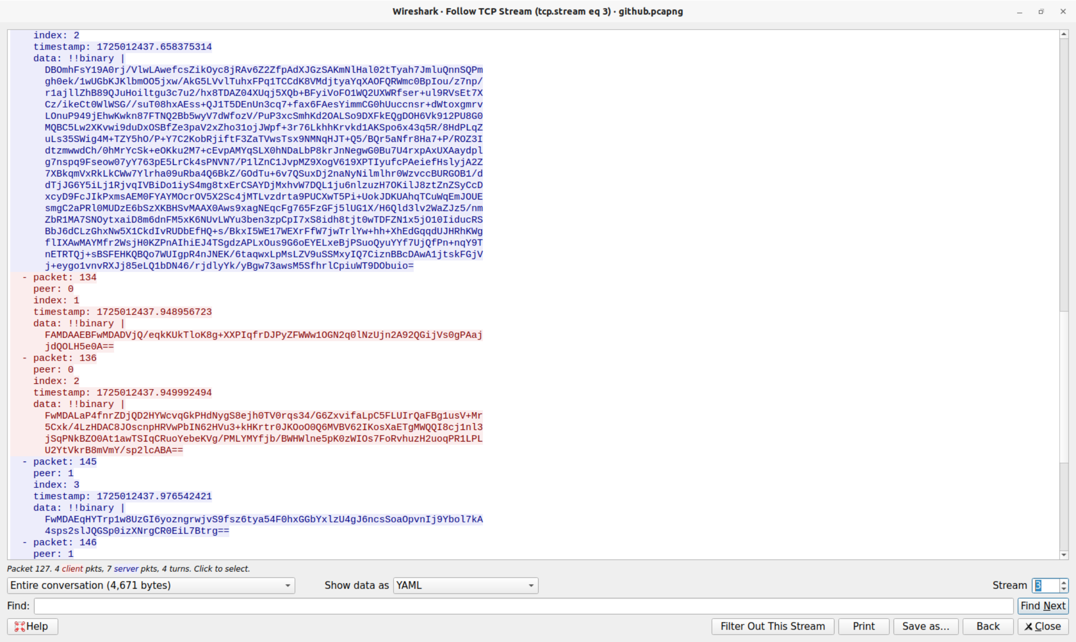
Ethernet · 1 | IPv4 · 1 | IPv6 | TCP · 5 | UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.10.0.217	59120	20.207.73.82	443	74	75 kB	0	34	5 kB	40	71 kB	0.000000	31.0190
10.10.0.217	59134	20.207.73.82	443	24	6 kB	1	14	2 kB	10	4 kB	0.000066	0.5418
10.10.0.217	59136	20.207.73.82	443	23	6 kB	2	13	2 kB	10	4 kB	0.000112	0.5755
10.10.0.217	59142	20.207.73.82	443	24	6 kB	3	13	2 kB	11	4 kB	3.212555	0.4109
10.10.0.217	59150	20.207.73.82	443	67	61 kB	4	30	3 kB	37	58 kB	3.212743	30.4880

Protocol

☐ Bluetooth
☐ BPv7
☐ DCCP
☑ Ethernet
☐ FC
☐ FDDI
☐ IEEE 802.11
☐ IEEE 802.15.4
☑ IPv4
☑ IPv6
☐ IPX
☐ JXTA
☐ LTP
☐ MPTCP
☐ NCP
☐ openSAFETY
☐ RSVP
☐ SCTP
☐ SLL
☑ TCP
☐ Token-Ring
☑ UDP

Since multiple packets are shared over a single connection, therefore these **connections are persistent**. Also, HTTP2 uses persistent connections generally.



Wireshark · Follow TCP Stream (tcp.stream eq 3) · github.pcapng

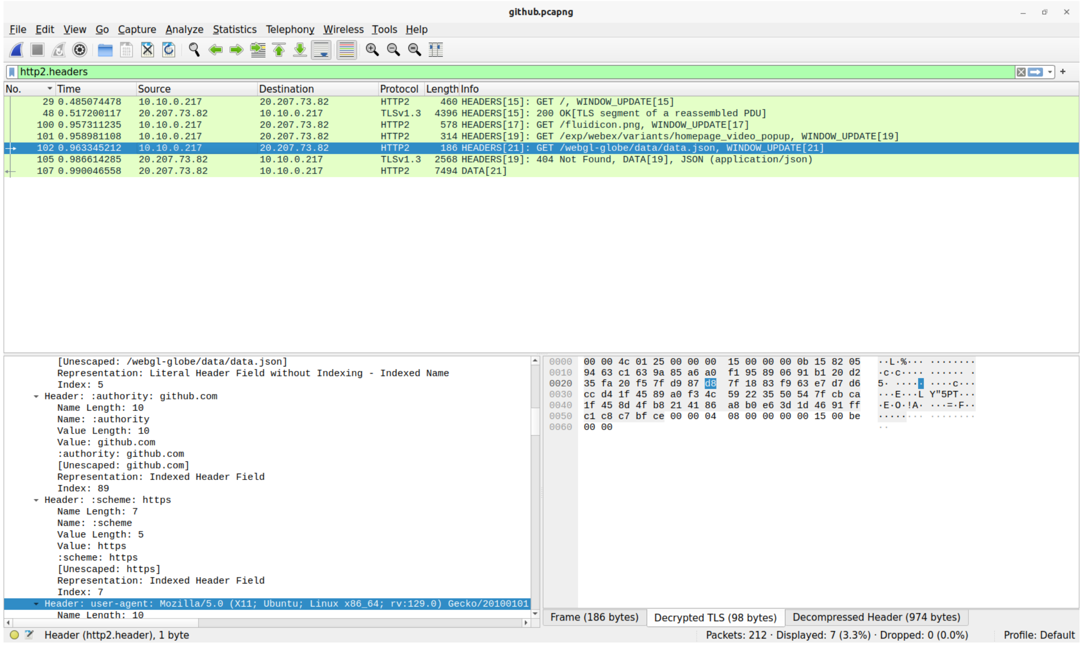
```
    index: 2
    timestamp: 1725012437.658375314
    data: !!binary |
      DBOmhFsY19A0rj/VlwLAwefcsZikOyc8jRAv6Z2ZfpAdXJGzSAKmNlHal02tTyah7JmluQnnSQPm
      gh0ek/1wUGbKJKlbmOO5jxw/AkG5LVvlTuhxFPq1TCCdK8VMdjtyaYqXAOFQRWmc0BpIou/z7np/
      r1ajllZhB89QJuHoiltgu3c7u2/hx8TDAZ04XUqj5XQb+BFyiVoFO1WQ2UXWRfser+ul9RVsEt7X
      Cz/ikeCt0WlWSG//suT08hxAEss+QJ1T5DEnUn3cq7+fax6FAesYimmCG0hUuccnsr+dWtoxgmrv
      LOnuP949jEhwKwkn87FTNQ2Bb5wyV7dWfozV/PuP3xcSmhKd2OALSo9DXFkEQgDOH6Vk912PU8G0
      MQBC5Lw2XKvwi9duDxOSBfZe3paV2xZho31ojJWpf+3r76LkhhKrvkd1AKSpo6x43q5R/8HdPLqZ
      uLs35SWig4M+TZY5hO/P+Y7C2KobRjiftF3ZaTVwsTsx9NMNqHJT+Q5/BQr5aNfr8Ha7+P/ROZ3I
      dtzmwwdCh/0hMrYcSk+eOKku2M7+cEvpAMYqSLX0hNDaLbP8krJnNegwG0Bu7U4rxpAxUXAaydpl
      g7nspq9Fseow07yY763pE5LrCk4sPNVN7/P1lZnC1JvpMZ9XogV619XPTIyufcPAeiefHslyjA2Z
      7XBkqmVxRkLkCWw7Ylrha09uRba4Q6BkZ/GOdTu+6v7QSuxDj2naNyNilmlhr0WzvccBURGOB1/d
      dTjJG6Y5iLj1RjvqIVBiDo1iyS4mg8txErCSAYDjMxhvW7DQL1ju6nlzuzH7OKilJ8ztZnZSyCcD
      xcyD9FcJIkPxmsAEM0FYAYMOcrOV5X2Sc4jMTLvzdrta9PUCXwT5Pi+UokJDKUAhqTCuWqEmJOUE
      smgC2aPRl0MUDzE6bSzXKBHSvMAAX0Aws9xagNEqcFg765FzGFj5lUG1X/H6Qld3lv2WaZJz5/nm
      ZbR1MA7SNOytxaiD8m6dnFM5xK6NUvLWYu3ben3zpCpI7xS8idh8tjt0wTDFZN1x5jO10IiducRS
      BbJ6dCLzGhxNw5X1CkdIvRUDbEfHQ+s/BkxI5WE17WEXrFfW7jwTrlYw+hh+XhEdGqqdUJHRhKWg
      flIXAwMAYMfr2WsjH0KZPnAIhiEJ4TSgdzAPLxOus9G6oEYELxeBjPSuoQyuYYf7UjQfPn+nqY9T
      nETRTQj+sBSFEHKQBQo7WUIgpR4nJNEK/6taqwxLpMsLZV9uSSMxyIQ7CiznBBcDAwA1jtskFGjV
      j+eygo1vnvRXJj85eLQ1bDN46/rjdlyYk/yBgw73awsM5SfhrlCpiuWT9DObuio=
  - packet: 134
    peer: 0
    index: 1
    timestamp: 1725012437.948956723
    data: !!binary |
      FAMDAAEBFwMDADVjQ/eqkKUkTloK8g+XXPIqfrDJPyZFWWw1OGN2q0lNzUjn2A92QGijVs0gPAaj
      jdQOLH5e0A==
  - packet: 136
    peer: 0
    index: 2
    timestamp: 1725012437.949992494
    data: !!binary |
      FwMDALaP4fnrZDjQD2HYWcvqGkPHdNygS8ejh0TV0rqs34/G6ZxvifaLpC5FLUIrQaFBg1usV+Mr
      5Cxk/4LzHDAC8JOscnpHRVwPbIN62HVu3+kHKrtr0JKOoO0Q6MVBV62IKosXaETgMWQQI8cj1nl3
      jSqPNkBZO0At1awTSIqCRuoYebeKVg/PMLYMYfjb/BWHWlne5pK0zWIOs7FoRvhuzH2uoqPR1LPL
      U2YtVkrB8mVmY/sp2lcABA==
  - packet: 145
    peer: 1
    index: 3
    timestamp: 1725012437.976542421
    data: !!binary |
      FwMDAEqHYTrp1w8UzGI6yozngrwjvS9fsz6tya54F0hxGGbYxlzU4gJ6ncsSoaOpvnIj9Ybol7kA
      4sps2slJQGSp0izXNrgCR0EiL7Btrg==
  - packet: 146
    peer: 1
```

Packet 127. 4 client pkts, 7 server pkts, 4 turns. Click to select.

Entire conversation (4,671 bytes) | Show data as YAML | Stream 3

Find:

Number of objects transferred = Number of GET requests. Since we have 4 GET Requests, 4 objects should be transferred. GET request in frame 29 is returned by response in frame 48. We do not have any response to GET request in frame 100. For GET request in frame 101, we have response in frame 105, but the response is 404 Not found, so no object is transferred. The GET request in frame 102 is answered in frame 107. So total 2 objects have been actually transferred over the connection.


github.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http2.headers
```

```
No.   Time        Source         Destination    Protocol  Length Info
   29 0.485074478 10.10.0.217    20.207.73.82   HTTP2      460 HEADERS[15]: GET /, WINDOW_UPDATE[15]
   48 0.517200117 20.207.73.82   10.10.0.217    TLSv1.3   4396 HEADERS[15]: 200 OK[TLS segment of a reassembled PDU]
  100 0.957311235 10.10.0.217    20.207.73.82   HTTP2      578 HEADERS[17]: GET /fluidicon.png, WINDOW_UPDATE[17]
  101 0.958981108 10.10.0.217    20.207.73.82   HTTP2      314 HEADERS[19]: GET /exp/webex/variants/homepage_video_popup, WINDOW_UPDATE[19]
  102 0.963345212 10.10.0.217    20.207.73.82   HTTP2      186 HEADERS[21]: GET /webgl-globe/data/data.json, WINDOW_UPDATE[21]
  105 0.986614285 20.207.73.82   10.10.0.217    TLSv1.3   2568 HEADERS[19]: 404 Not Found, DATA[19], JSON (application/json)
  107 0.990046558 20.207.73.82   10.10.0.217    HTTP2     7494 DATA[21]
```

```
        [Unescaped: /webgl-globe/data/data.json]
        Representation: Literal Header Field without Indexing - Indexed Name
        Index: 5
    Header: :authority: github.com
        Name Length: 10
        Name: :authority
        Value Length: 10
        Value: github.com
        :authority: github.com
        [Unescaped: github.com]
        Representation: Indexed Header Field
        Index: 89
    Header: :scheme: https
        Name Length: 7
        Name: :scheme
        Value Length: 5
        Value: https
        :scheme: https
        [Unescaped: https]
        Representation: Indexed Header Field
        Index: 7
    Header: user-agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:129.0) Gecko/20100101
        Name Length: 10
```

```
0000  00 00 4c 01 25 00 00 00  15 00 00 00 0b 15 82 05   ··L·%···  ········
0010  94 63 c1 63 9a 85 a6 a0  f1 95 89 06 91 b1 20 d2   ·c·c····  ······ ·
0020  35 fa 20 f5 7f d9 87 d8  7f 18 83 f9 63 e7 d7 d6   5· ·····  ····c···
0030  cc d4 1f 45 89 a0 f3 4c  59 22 35 50 54 7f cb ca   ···E···L  Y"5PT···
0040  1f 45 8d 4f b8 21 41 86  a8 b0 e6 3d 1d 46 91 ff   ·E·O·!A·  ···=·F··
0050  c1 c8 c7 bf ce 00 00 04  08 00 00 00 00 15 00 be   ········  ········
0060  00 00                                              ··
```

Frame (186 bytes) | Decrypted TLS (98 bytes) | Decompressed Header (974 bytes)

Header (http2.header), 1 byte   Packets: 212 · Displayed: 7 (3.3%) · Dropped: 0 (0.0%)   Profile: Default

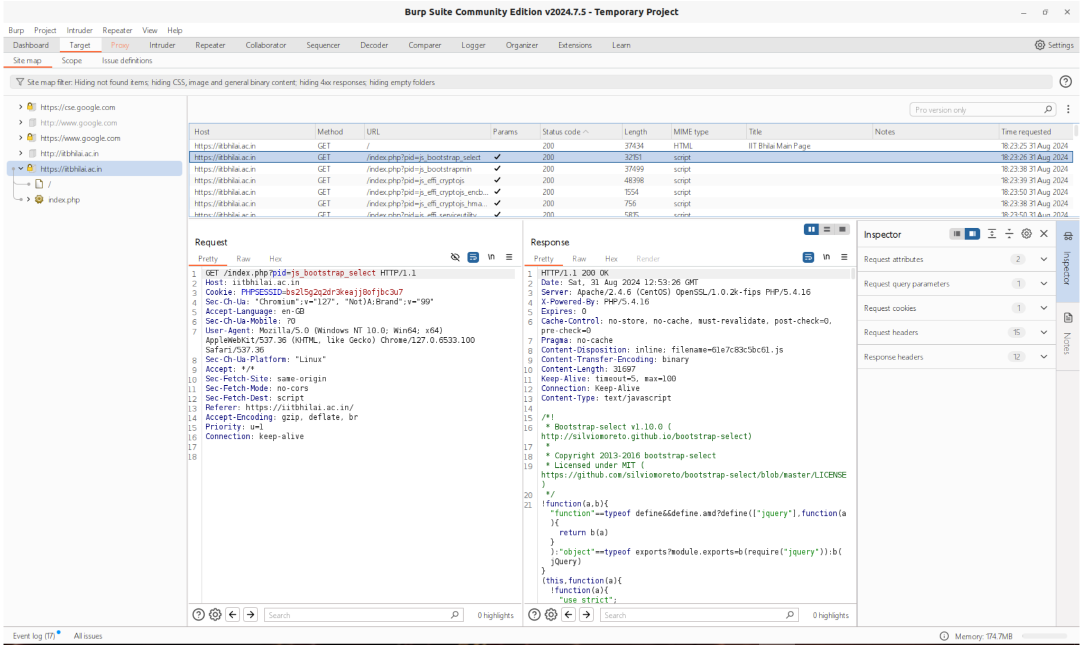
Time for get request in frame 29 = 0.032125639 s

Time for get request in frame 101 = 0.027633177 s

Time for get request in frame 102 = 0.026701346 s

Accept-Encoding: **So the object requested in frame 29 took longest to download.**

6. **iitbhilai.ac.in**


Burp Suite Community Edition v2024.7.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Site map Scope Issue definitions
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
https://cse.google.com
http://www.google.com
https://www.google.com
http://iitbhilai.ac.in
https://iitbhilai.ac.in
/
index.php
Pro version only
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request cookies 1
Request headers 15
Response headers 12
Inspector
Notes
Search
0 highlights
Event log (17)
All issues
Memory: 174.7MB

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://iitbhilai.ac.in	GET	/		200	37434	HTML	IIT Bhilai Main Page		18:23:25 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_bootstrap_select	✓	200	32151	script			18:23:26 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_bootstrapmin	✓	200	37499	script			18:23:38 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_effi_cryptojs	✓	200	48398	script			18:23:39 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_effi_cryptojs_encb...	✓	200	1554	script			18:23:50 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_effi_cryptojs_hma...	✓	200	756	script			18:23:38 31 Aug 2024
https://iitbhilai.ac.in	GET	/index.php?pid=js_effi_serviceutility	✓	200	5815	script			18:23:50 31 Aug 2024

```
GET /index.php?pid=js_bootstrap_select HTTP/1.1
Host: iitbhilai.ac.in
Cookie: PHPSESSID=bs2l5g2q2dr3keajj8ofjbc3u7
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Accept-Language: en-GB
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://iitbhilai.ac.in/
Accept-Encoding: gzip, deflate, br
Priority: u=1
Connection: keep-alive


```

```
HTTP/1.1 200 OK
Date: Sat, 31 Aug 2024 12:53:26 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Expires: 0
Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
pre-check=0
Pragma: no-cache
Content-Disposition: inline; filename=61e7c83c5bc61.js
Content-Transfer-Encoding: binary
Content-Length: 31697
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/javascript

/*!
 * Bootstrap-select v1.10.0 (
http://silviomoreto.github.io/bootstrap-select)
 *
 * Copyright 2013-2016 bootstrap-select
 * Licensed under MIT (
https://github.com/silviomoreto/bootstrap-select/blob/master/LICENSE
)
 */
!function(a,b){
  "function"==typeof define&&define.amd?define(["jquery"],function(a
  ){
    return b(a)
  }
  ):"object"==typeof exports?module.exports=b(require("jquery")):b(
  jQuery)
}
(this,function(a){
  !function(a){
    "use strict";
```

HTTP Request Headers:

(a) GET /index.php?pid=js_bootstrap_select HTTP/1.1: Specifies HTTP method being used

(b) Host: Specifies domain name of requested server.

(c) Cookie: This sends cookie from client to server.

(d) Sec-Ch-Ua: It provides info about browser and version

(e) Accept-Language: Specifies preferred language for response.

(f) User-Agent: Specifies info about browser, OS, etc of client.

(g) Sec-Ch-Ua-Platform: This specifies the platform / Operating System of client.

(h) Accept: This tells the type of info which can be processed by the client.

(i) Sec-Fetch-Site: Provides info about context of fetch. It tells about relation between request's initiator origin and requested resource's origin.

(j) Sec-Fetch-Mode: It provides info about mode of fetch.

(k) Sec-Fetch-Dest: It tells the destination of request.

(l) Referer:It specifies URL of webpage which initiated the request.

(m) Accept-Encoding: It tells about the type of encoding accepted by the client.

(n) Priority: It specifies the priority of the request.

(o) Connection: This indicates that the client wants to keep the connection open for more request (Persistent connection) .

HTTP Response Headers:

(a) HTTP/1.1 200 OK: Status code indicating that the request was succesful.

(b) Date: This provides date and time at which the response was generated by the server.

(c) Server: It provides info about server which is handling the request.

(d) X-Powered-By: It indicates the scripting language used on server

(e) Expires: It is used to control caching and specifies that the response should be considered expired immediately.

(f) Cache-Control: It tells about what to do with the cache like should be store the cache or not, etc.

(g) Pragma: It is also used to control caching.

(h) Content-Disposition: It tells how the content should be displayed.

(i) Content-Transfer-Encoding: It tells the encoding of the content being transferred.

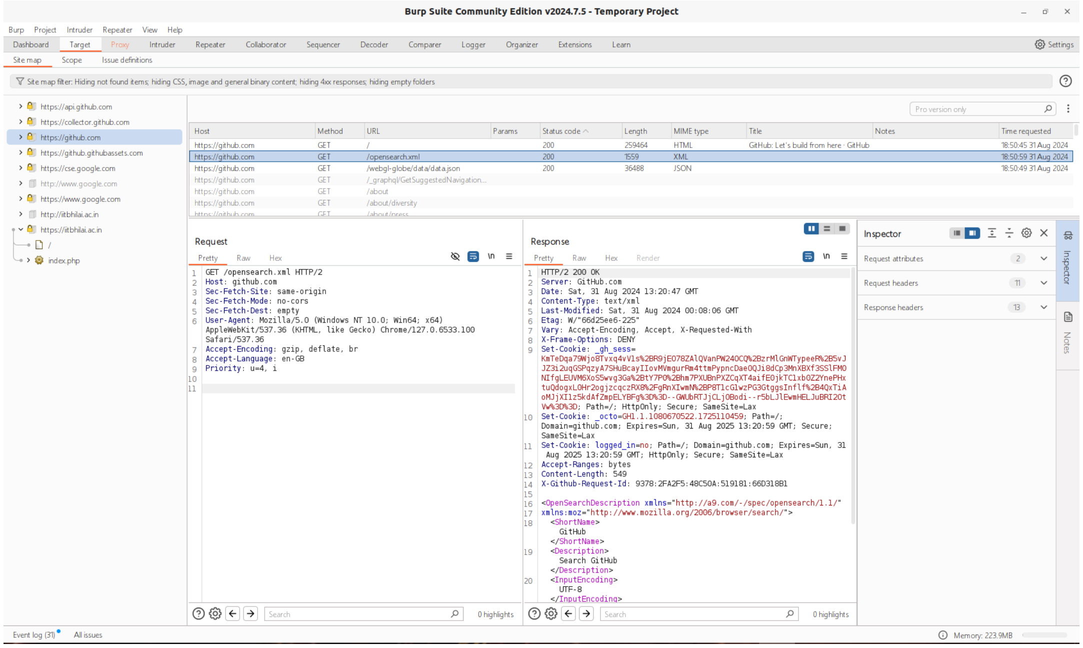
(j) Content-Length: It tells about length of content i.e. size of response body.

(k) Keep-Alive: It is used to control persistent collection.

(l) Connection: This specifies whether the connection should remain open or not after current request/response.

(m) Content-Type: This indicated MIME type of content.

github.com



Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://github.com	GET	/		200	259464	HTML	GitHub: Let's build from here · GitHub		18:50:45 31 Aug 2024
https://github.com	GET	/opensearch.xml		200	1559	XML			18:50:59 31 Aug 2024
https://github.com	GET	/webgl-globe/data/data.json		200	36488	JSON			18:50:49 31 Aug 2024
https://github.com	GET	/_graphql/GetSuggestedNavigation...							
https://github.com	GET	/about							
https://github.com	GET	/about/diversity							
https://github.com	GET	/about/press							

```
GET /opensearch.xml HTTP/2
Host: github.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB
Priority: u=4, i

```

```
HTTP/2 200 OK
Server: GitHub.com
Date: Sat, 31 Aug 2024 13:20:47 GMT
Content-Type: text/xml
Last-Modified: Sat, 31 Aug 2024 00:08:06 GMT
Etag: W/"66d25ee6-225"
Vary: Accept-Encoding, Accept, X-Requested-With
X-Frame-Options: DENY
Set-Cookie: _gh_sess=
KmTeDqa79Wjo8Tvxq4vVls%2BR9jEO78ZAlQVanPW24OCQ%2BzrMlGnWTypeeR%2B5vJ
JZ3i2uqGSPqzyA7SHuBcayIIovMVmgurRm4ttmPypncDae0QJi8dCp3MnXBXf3SSlFM0
NIfgLEUVM6XoS5wvg3Ga%2BtY7P0%2Bhm7PXUBnPXZCqXT4aifE0jkTClxb0Z2YnePHx
tuQdogxL0Hr2ogjzcqczRX8%2FgRnXIwmN%2BP8TlcGlwzPG3GtggsInflf%2B4QxTiA
oMJjXIlz5kdAfZmpELYBFg%3D%3D--GWUbRTJjCLj0Bodi--r5bLJlEwmHELJuBRI2Ot
Vw%3D%3D; Path=/; HttpOnly; Secure; SameSite=Lax
Set-Cookie: _octo=GH1.1.1080670522.1725110459; Path=/;
Domain=github.com; Expires=Sun, 31 Aug 2025 13:20:59 GMT; Secure;
SameSite=Lax
Set-Cookie: logged_in=no; Path=/; Domain=github.com; Expires=Sun, 31
 Aug 2025 13:20:59 GMT; HttpOnly; Secure; SameSite=Lax
Accept-Ranges: bytes
Content-Length: 549
X-Github-Request-Id: 9378:2FA2F5:48C50A:519181:66D318B1

<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/"
xmlns:moz="http://www.mozilla.org/2006/browser/search/">
  <ShortName>
    GitHub
  </ShortName>
  <Description>
    Search GitHub
  </Description>
  <InputEncoding>
    UTF-8
  </InputEncoding>
```

Some of the headers are same as above. To avoid redundancy, explaining only different headers.

HTTP Request Headers:

All the request headers are already covered above.

HTTP Response Headers:

(a) Last-Modified: It tells last date and time when the requested object was modified.

(b) Etag: It is a unique identifier for specific version of resource.

(c) Vary: This indicated that the response may vary depending on value of certain request headers.

(d) X-Frame-Options: This prevents page from being displayed in a frame. It is a security feature.

(e) Set-Cookie: It is used to set cookies on client side.

(f) Accept-Ranges: It specifies whether server allows user to access specific range of resource.

(g) X-Github-Request-Id: Github uses this to trace requests through their infrastructure and identify specific requests in log.

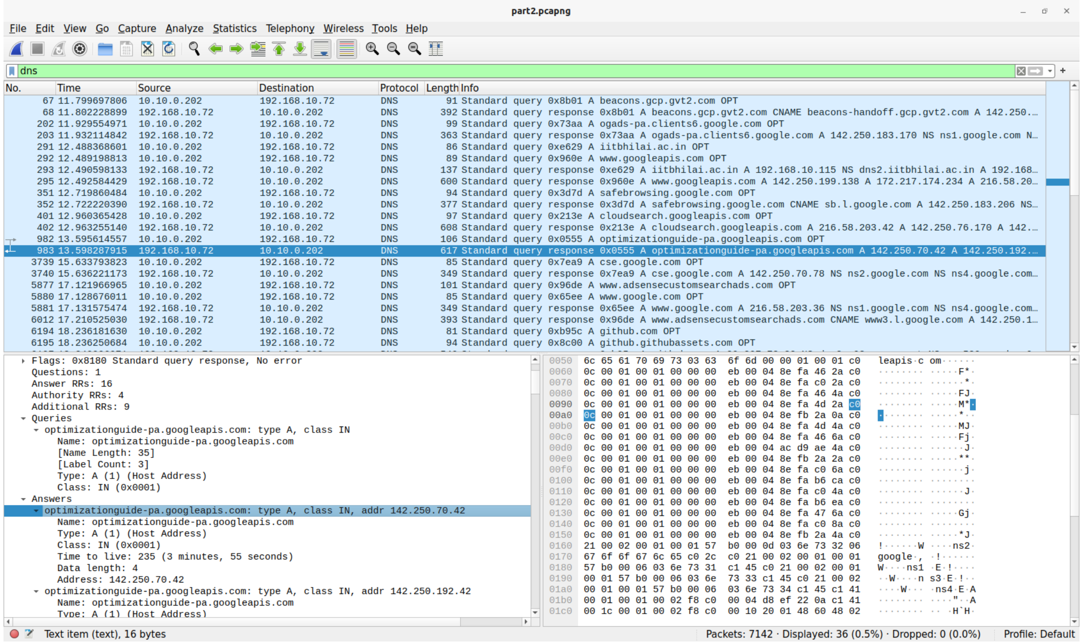
PART 2: DNS

1. I accessed iitbhilai.ac.in and github.com. I observed 36 DNS packets in total.

   (a) Domain Name and corresponding returned IP.

Domain Name	IP
iitbhilai.ac.in	192.168.10.115
user-images.githubusercontent.com	185.199.109.133
github.com	20.207.73.82
github-cloud.s3.amazonaws.com	16.15.176.198
api.github.com	20.207.73.85
optimizationguide-pa.googleapis.com	142.250.70.42
avatars.githubusercontent.com	185.199.110.133

   (b) Yes, for example: The IP of DNS server for optimizationguide-pa.googleapis.com is 142.250.70.42


part2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.  Time         Source         Destination    Protocol Length Info
  67 11.799697806 10.10.0.202    192.168.10.72  DNS       91 Standard query 0x8b01 A beacons.gcp.gvt2.com OPT
  68 11.802228899 192.168.10.72  10.10.0.202    DNS      392 Standard query response 0x8b01 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.250.…
 202 11.929554971 10.10.0.202    192.168.10.72  DNS       99 Standard query 0x73aa A ogads-pa.clients6.google.com OPT
 203 11.932114842 192.168.10.72  10.10.0.202    DNS      363 Standard query response 0x73aa A ogads-pa.clients6.google.com A 142.250.183.170 NS ns1.google.com N…
 291 12.488368601 10.10.0.202    192.168.10.72  DNS       86 Standard query 0xe629 A iitbhilai.ac.in OPT
 292 12.489198813 10.10.0.202    192.168.10.72  DNS       89 Standard query 0x960e A www.googleapis.com OPT
 293 12.490598133 192.168.10.72  10.10.0.202    DNS      137 Standard query response 0xe629 A iitbhilai.ac.in A 192.168.10.115 NS dns2.iitbhilai.ac.in A 192.168…
 295 12.492584429 192.168.10.72  10.10.0.202    DNS      600 Standard query response 0x960e A www.googleapis.com A 142.250.199.138 A 172.217.174.234 A 216.58.20…
 351 12.719860484 10.10.0.202    192.168.10.72  DNS       94 Standard query 0x3d7d A safebrowsing.google.com OPT
 352 12.722220390 192.168.10.72  10.10.0.202    DNS      377 Standard query response 0x3d7d A safebrowsing.google.com CNAME sb.l.google.com A 142.250.183.206 NS…
 401 12.960365428 10.10.0.202    192.168.10.72  DNS       97 Standard query 0x213e A cloudsearch.googleapis.com OPT
 402 12.963255140 192.168.10.72  10.10.0.202    DNS      608 Standard query response 0x213e A cloudsearch.googleapis.com A 216.58.203.42 A 142.250.76.170 A 142.…
 982 13.595614557 10.10.0.202    192.168.10.72  DNS      106 Standard query 0x0555 A optimizationguide-pa.googleapis.com OPT
 983 13.598287915 192.168.10.72  10.10.0.202    DNS      617 Standard query response 0x0555 A optimizationguide-pa.googleapis.com A 142.250.70.42 A 142.250.192.…
3739 15.633793823 10.10.0.202    192.168.10.72  DNS       85 Standard query 0x7ea9 A cse.google.com OPT
3740 15.636221173 192.168.10.72  10.10.0.202    DNS      349 Standard query response 0x7ea9 A cse.google.com A 142.250.70.78 NS ns2.google.com NS ns4.google.com…
5877 17.121966965 10.10.0.202    192.168.10.72  DNS      101 Standard query 0x96de A www.adsensecustomsearchads.com OPT
5880 17.128676011 10.10.0.202    192.168.10.72  DNS       85 Standard query 0x65ee A www.google.com OPT
5881 17.131575474 192.168.10.72  10.10.0.202    DNS      349 Standard query response 0x65ee A www.google.com A 216.58.203.36 NS ns1.google.com NS ns4.google.com…
6012 17.210525030 192.168.10.72  10.10.0.202    DNS      393 Standard query response 0x96de A www.adsensecustomsearchads.com CNAME www3.l.google.com A 142.250.1…
6194 18.236181630 10.10.0.202    192.168.10.72  DNS       81 Standard query 0xb95c A github.com OPT
6195 18.236250684 10.10.0.202    192.168.10.72  DNS       94 Standard query 0x8c00 A github.githubassets.com OPT
```

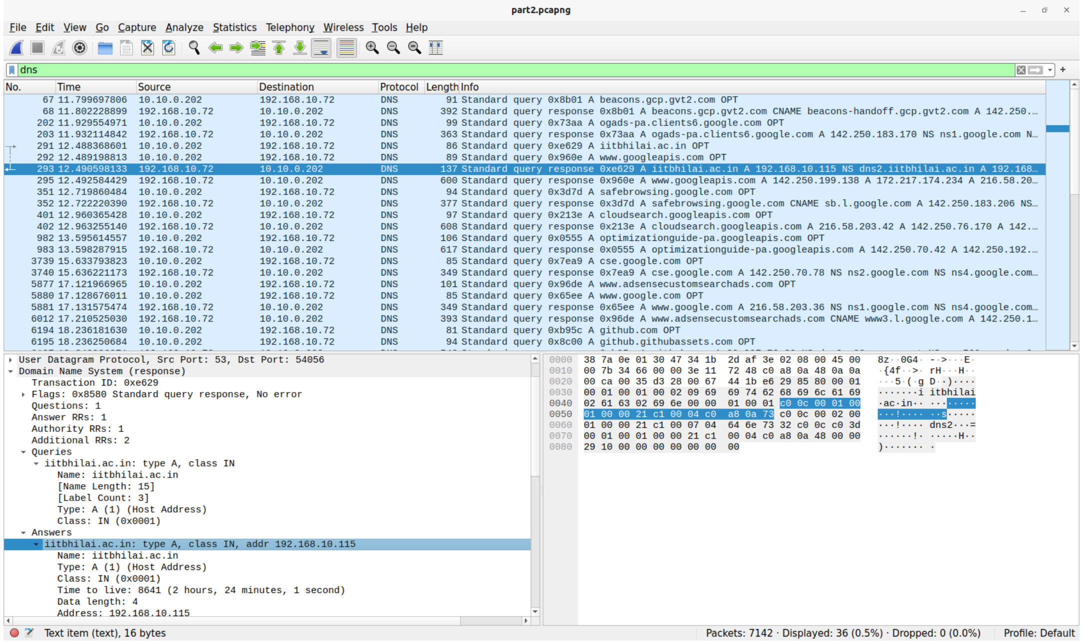
```
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 16
  Authority RRs: 4
  Additional RRs: 9
  Queries
    optimizationguide-pa.googleapis.com: type A, class IN
      Name: optimizationguide-pa.googleapis.com
      [Name Length: 35]
      [Label Count: 3]
      Type: A (1) (Host Address)
      Class: IN (0x0001)
  Answers
    optimizationguide-pa.googleapis.com: type A, class IN, addr 142.250.70.42
      Name: optimizationguide-pa.googleapis.com
      Type: A (1) (Host Address)
      Class: IN (0x0001)
      Time to live: 235 (3 minutes, 55 seconds)
      Data length: 4
      Address: 142.250.70.42
    optimizationguide-pa.googleapis.com: type A, class IN, addr 142.250.192.42
      Name: optimizationguide-pa.googleapis.com
      Type: A (1) (Host Address)
```

```
0050  6c 65 61 70 69 73 03 63  6f 6d 00 00 01 00 01 c0   leapis·c om······
0060  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 46 2a c0   ········ ·····F*·
0070  0c 00 01 00 01 00 00 00  eb 00 04 8e fa c0 2a c0   ········ ······*·
0080  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 46 4a c0   ········ ·····FJ·
0090  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 4d 2a c0   ········ ·····M*·
00a0  0c 00 01 00 01 00 00 00  eb 00 04 8e fb 2a 0a c0   ········ ·····*··
00b0  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 4d 4a c0   ········ ·····MJ·
00c0  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 46 6a c0   ········ ·····Fj·
00d0  0c 00 01 00 01 00 00 00  eb 00 04 ac d9 ae 4a c0   ········ ······J·
00e0  0c 00 01 00 01 00 00 00  eb 00 04 8e fb 2a 2a c0   ········ ·····**·
00f0  0c 00 01 00 01 00 00 00  eb 00 04 8e fa c0 6a c0   ········ ······j·
0100  0c 00 01 00 01 00 00 00  eb 00 04 8e fa b6 ca c0   ········ ········
0110  0c 00 01 00 01 00 00 00  eb 00 04 8e fa c0 4a c0   ········ ······J·
0120  0c 00 01 00 01 00 00 00  eb 00 04 8e fa b6 ea c0   ········ ········
0130  0c 00 01 00 01 00 00 00  eb 00 04 8e fa 47 6a c0   ········ ·····Gj·
0140  0c 00 01 00 01 00 00 00  eb 00 04 8e fa c0 8a c0   ········ ········
0150  0c 00 01 00 01 00 00 00  eb 00 04 8e fb 2a 4a c0   ········ ·····*J·
0160  21 00 02 00 01 00 01 57  b0 00 0d 03 6e 73 32 06   !······W ····ns2·
0170  67 6f 6f 67 6c 65 c0 2c  c0 21 00 02 00 01 00 01   google·, ·!······
0180  57 b0 00 06 03 6e 73 31  c1 45 c0 21 00 02 00 01   W····ns1 ·E·!····
0190  00 01 57 b0 00 06 03 6e  73 33 c1 45 c0 21 00 02   ··W····n s3·E·!··
01a0  00 01 00 01 57 b0 00 06  03 6e 73 34 c1 45 c1 41   ····W··· ·ns4·E·A
01b0  00 01 00 01 00 02 f8 c0  00 04 d8 ef 22 0a c1 41   ········ ····"··A
01c0  00 1c 00 01 00 02 f8 c0  00 10 20 01 48 60 48 02   ········ ·· ·H`H·
```

Text item (text), 16 bytes

Packets: 7142 · Displayed: 36 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

The IP of DNS server for iitbhilai.ac.in is 192.168.10.115


part2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns

```
No.   Time         Source          Destination     Protocol Length Info
   67 11.799697806 10.10.0.202     192.168.10.72   DNS        91 Standard query 0x8b01 A beacons.gcp.gvt2.com OPT
   68 11.802228899 192.168.10.72   10.10.0.202     DNS       392 Standard query response 0x8b01 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.250.…
  202 11.929554971 10.10.0.202     192.168.10.72   DNS        99 Standard query 0x73aa A ogads-pa.clients6.google.com OPT
  203 11.932114842 192.168.10.72   10.10.0.202     DNS       363 Standard query response 0x73aa A ogads-pa.clients6.google.com A 142.250.183.170 NS ns1.google.com N…
  291 12.488368601 10.10.0.202     192.168.10.72   DNS        86 Standard query 0xe629 A iitbhilai.ac.in OPT
  292 12.489198813 10.10.0.202     192.168.10.72   DNS        89 Standard query 0x960e A www.googleapis.com OPT
  293 12.490598133 192.168.10.72   10.10.0.202     DNS       137 Standard query response 0xe629 A iitbhilai.ac.in A 192.168.10.115 NS dns2.iitbhilai.ac.in A 192.168…
  295 12.492584429 192.168.10.72   10.10.0.202     DNS       600 Standard query response 0x960e A www.googleapis.com A 142.250.199.138 A 172.217.174.234 A 216.58.20…
  351 12.719860484 10.10.0.202     192.168.10.72   DNS        94 Standard query 0x3d7d A safebrowsing.google.com OPT
  352 12.722220390 192.168.10.72   10.10.0.202     DNS       377 Standard query response 0x3d7d A safebrowsing.google.com CNAME sb.l.google.com A 142.250.183.206 NS…
  401 12.960365428 10.10.0.202     192.168.10.72   DNS        97 Standard query 0x213e A cloudsearch.googleapis.com OPT
  402 12.963255140 192.168.10.72   10.10.0.202     DNS       608 Standard query response 0x213e A cloudsearch.googleapis.com A 216.58.203.42 A 142.250.76.170 A 142.…
  982 13.595614557 10.10.0.202     192.168.10.72   DNS       106 Standard query 0x0555 A optimizationguide-pa.googleapis.com OPT
  983 13.598287915 192.168.10.72   10.10.0.202     DNS       617 Standard query response 0x0555 A optimizationguide-pa.googleapis.com A 142.250.70.42 A 142.250.192.…
 3739 15.633793823 10.10.0.202     192.168.10.72   DNS        85 Standard query 0x7ea9 A cse.google.com OPT
 3740 15.636221173 192.168.10.72   10.10.0.202     DNS       349 Standard query response 0x7ea9 A cse.google.com A 142.250.70.78 NS ns2.google.com NS ns4.google.com…
 5877 17.121966965 10.10.0.202     192.168.10.72   DNS       101 Standard query 0x96de A www.adsensecustomsearchads.com OPT
 5880 17.128676011 10.10.0.202     192.168.10.72   DNS        85 Standard query 0x65ee A www.google.com OPT
 5881 17.131575474 192.168.10.72   10.10.0.202     DNS       349 Standard query response 0x65ee A www.google.com A 216.58.203.36 NS ns1.google.com NS ns4.google.com…
 6012 17.210525030 192.168.10.72   10.10.0.202     DNS       393 Standard query response 0x96de A www.adsensecustomsearchads.com CNAME www3.l.google.com A 142.250.1…
 6194 18.236181630 10.10.0.202     192.168.10.72   DNS        81 Standard query 0xb95c A github.com OPT
 6195 18.236250684 10.10.0.202     192.168.10.72   DNS        94 Standard query 0x8c00 A github.githubassets.com OPT
```

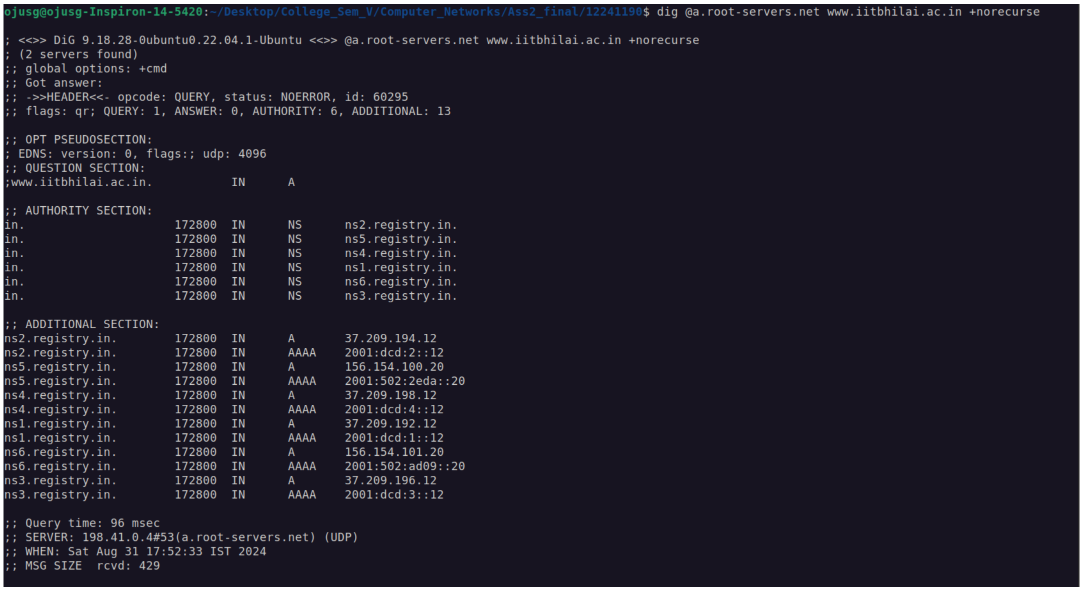
```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 54056
▾ Domain Name System (response)
    Transaction ID: 0xe629
  ▸ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 1
    Additional RRs: 2
  ▾ Queries
    ▾ iitbhilai.ac.in: type A, class IN
        Name: iitbhilai.ac.in
        [Name Length: 15]
        [Label Count: 3]
        Type: A (1) (Host Address)
        Class: IN (0x0001)
  ▾ Answers
    ▾ iitbhilai.ac.in: type A, class IN, addr 192.168.10.115
        Name: iitbhilai.ac.in
        Type: A (1) (Host Address)
        Class: IN (0x0001)
        Time to live: 8641 (2 hours, 24 minutes, 1 second)
        Data length: 4
        Address: 192.168.10.115
```

```
0000  38 7a 0e 01 30 47 34 1b  2d af 3e 02 08 00 45 00   8z··0G4· -·>···E·
0010  00 7b 34 66 00 00 3e 11  72 48 c0 a8 0a 48 0a 0a   ·{4f··>· rH···H··
0020  00 ca 00 35 d3 28 00 67  44 1b e6 29 85 80 00 01   ···5·(·g D··)····
0030  00 01 00 01 00 02 09 69  69 74 62 68 69 6c 61 69   ·······i itbhilai
0040  02 61 63 02 69 6e 00 00  01 00 01 c0 0c 00 01 00   ·ac·in·· ········
0050  01 00 00 21 c1 00 04 c0  a8 0a 73 c0 0c 00 02 00   ···!···· ··s·····
0060  01 00 00 21 c1 00 07 04  64 6e 73 32 c0 0c c0 3d   ···!···· dns2···=
0070  00 01 00 01 00 00 21 c1  00 04 c0 a8 0a 48 00 00   ······!· ·····H··
0080  29 10 00 00 00 00 00 00  00                        )······· ·
```

Text item (text), 16 bytes   Packets: 7142 · Displayed: 36 (0.5%) · Dropped: 0 (0.0%)   Profile: Default

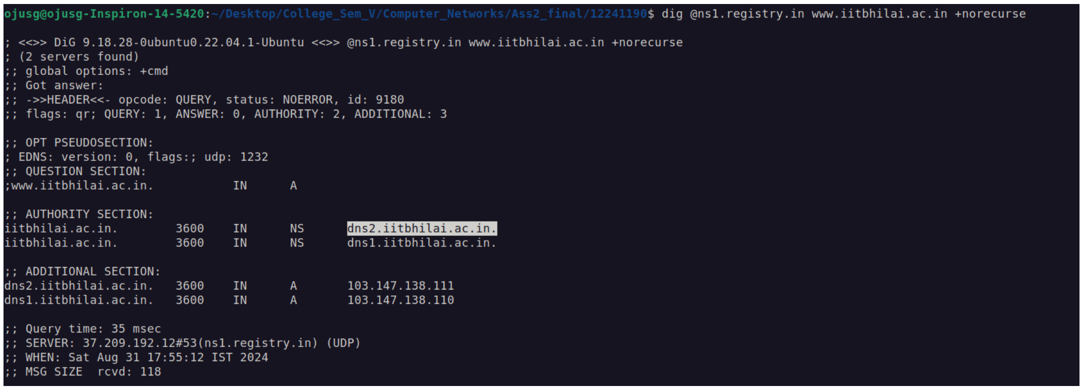
2. **dig @a.root-servers.net www.iitbhilai.ac.in +norecurse**

   This command returns name server for .in domain.

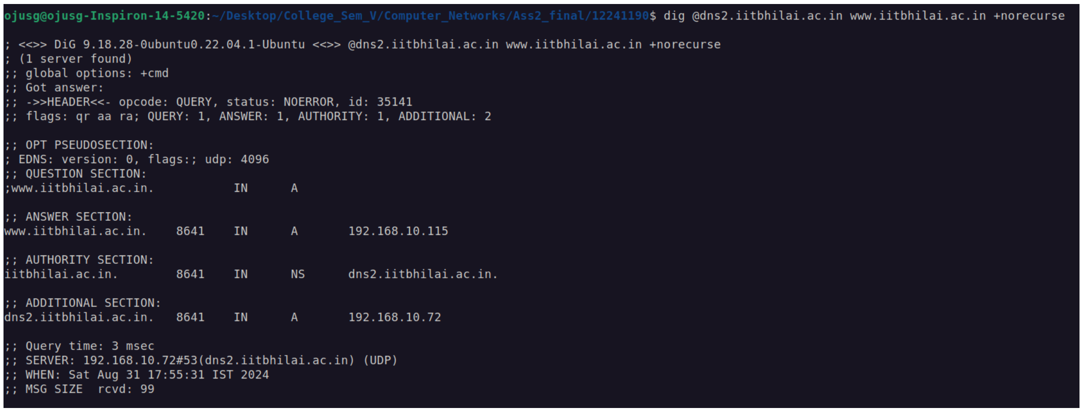


```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @a.root-servers.net www.iitbhilai.ac.in +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @a.root-servers.net www.iitbhilai.ac.in +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60295
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

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

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

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

;; Query time: 96 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Sat Aug 31 17:52:33 IST 2024
;; MSG SIZE  rcvd: 429
```

Now run the above command again but replace @a.root-servers.net with any of the names in authority section. Repeat this step until we get an answer.



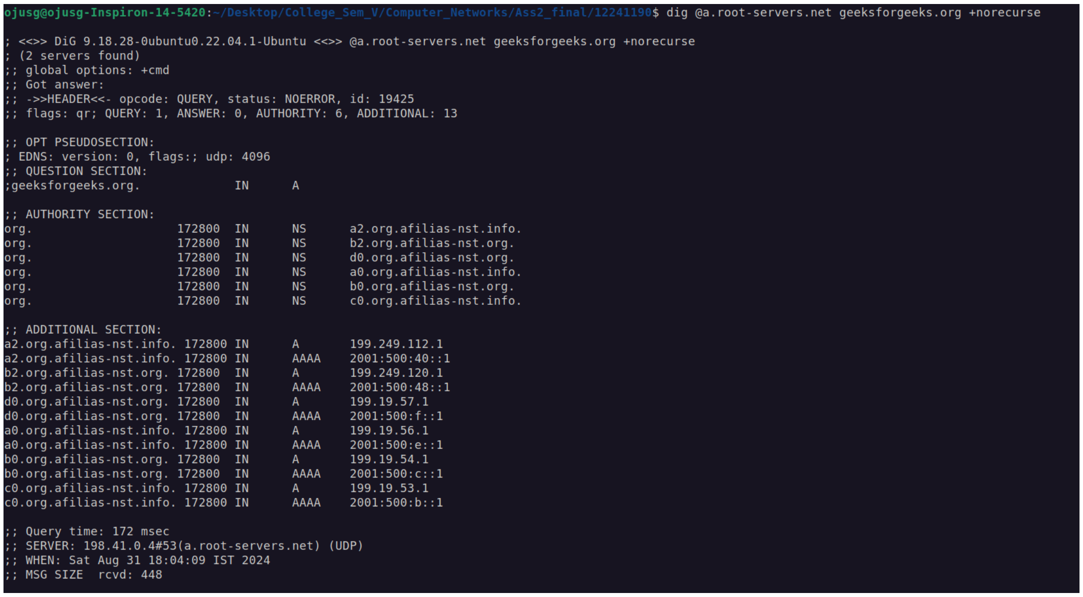
```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @ns1.registry.in www.iitbhilai.ac.in +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @ns1.registry.in www.iitbhilai.ac.in +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9180
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 3

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

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

;; ADDITIONAL SECTION:
dns2.iitbhilai.ac.in.   3600    IN      A       103.147.138.111
dns1.iitbhilai.ac.in.   3600    IN      A       103.147.138.110

;; Query time: 35 msec
;; SERVER: 37.209.192.12#53(ns1.registry.in) (UDP)
;; WHEN: Sat Aug 31 17:55:12 IST 2024
;; MSG SIZE  rcvd: 118
```



```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @dns2.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @dns2.iitbhilai.ac.in www.iitbhilai.ac.in +norecurse
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35141
;; flags: qr aa ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

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

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

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

;; Query time: 3 msec
;; SERVER: 192.168.10.72#53(dns2.iitbhilai.ac.in) (UDP)
;; WHEN: Sat Aug 31 17:55:31 IST 2024
;; MSG SIZE  rcvd: 99
```

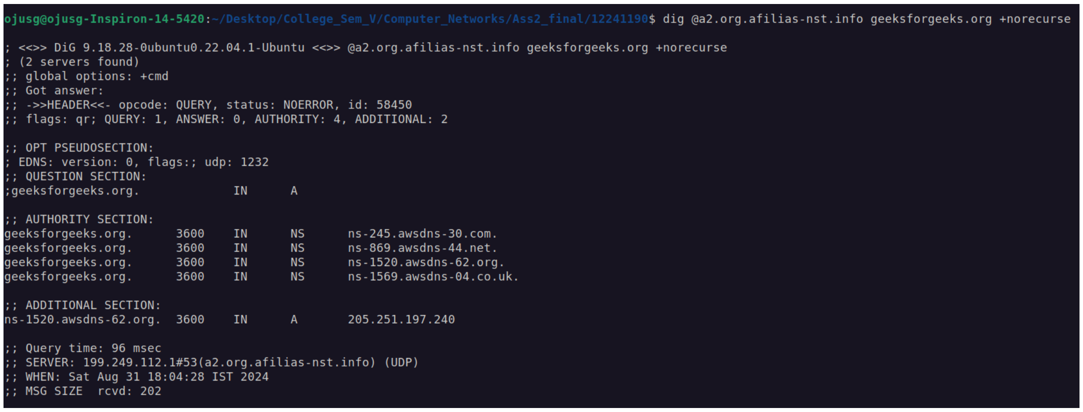
We got the answer **192.168.10.115**
In this way we went through the hierarchy from the root without recursion.

Repeating all the above steps for geeksforgeeks.org

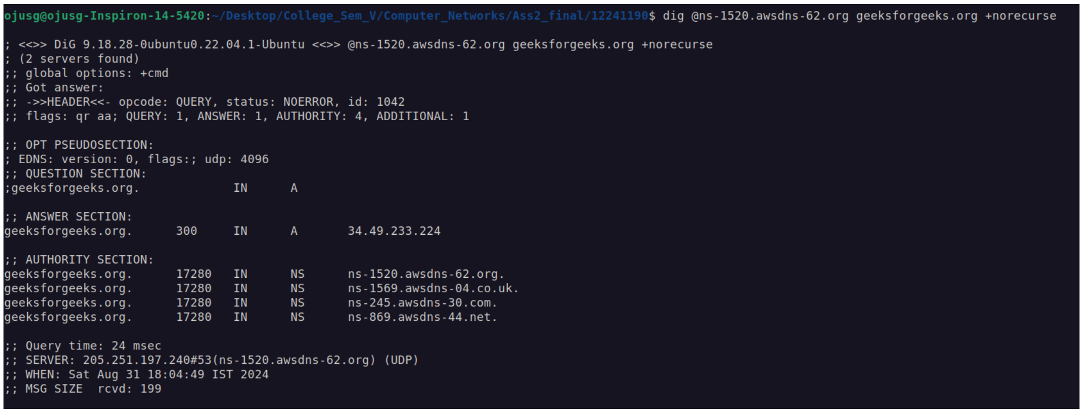


```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @a.root-servers.net geeksforgeeks.org +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @a.root-servers.net geeksforgeeks.org +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19425
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 6, ADDITIONAL: 13

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

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

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

;; Query time: 172 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Sat Aug 31 18:04:09 IST 2024
;; MSG SIZE  rcvd: 448
```

Now run the above command again but replace @a.root-servers.net with any of the names in authority section. Repeat this step until we get an answer.



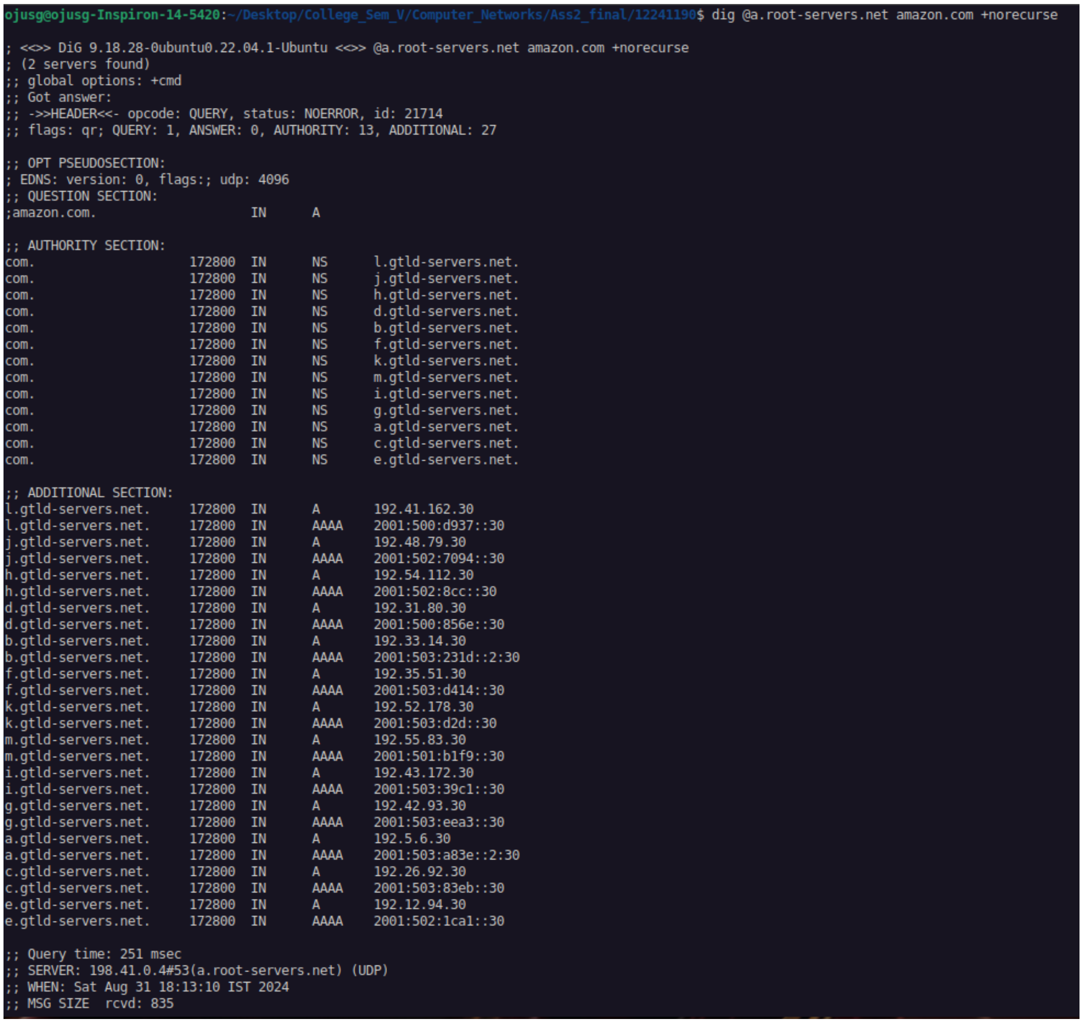
```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @a2.org.afilias-nst.info geeksforgeeks.org +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @a2.org.afilias-nst.info geeksforgeeks.org +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58450
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 2

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

;; AUTHORITY SECTION:
geeksforgeeks.org.      3600    IN      NS      ns-245.awsdns-30.com.
geeksforgeeks.org.      3600    IN      NS      ns-869.awsdns-44.net.
geeksforgeeks.org.      3600    IN      NS      ns-1520.awsdns-62.org.
geeksforgeeks.org.      3600    IN      NS      ns-1569.awsdns-04.co.uk.

;; ADDITIONAL SECTION:
ns-1520.awsdns-62.org.  3600    IN      A       205.251.197.240

;; Query time: 96 msec
;; SERVER: 199.249.112.1#53(a2.org.afilias-nst.info) (UDP)
;; WHEN: Sat Aug 31 18:04:28 IST 2024
;; MSG SIZE  rcvd: 202
```



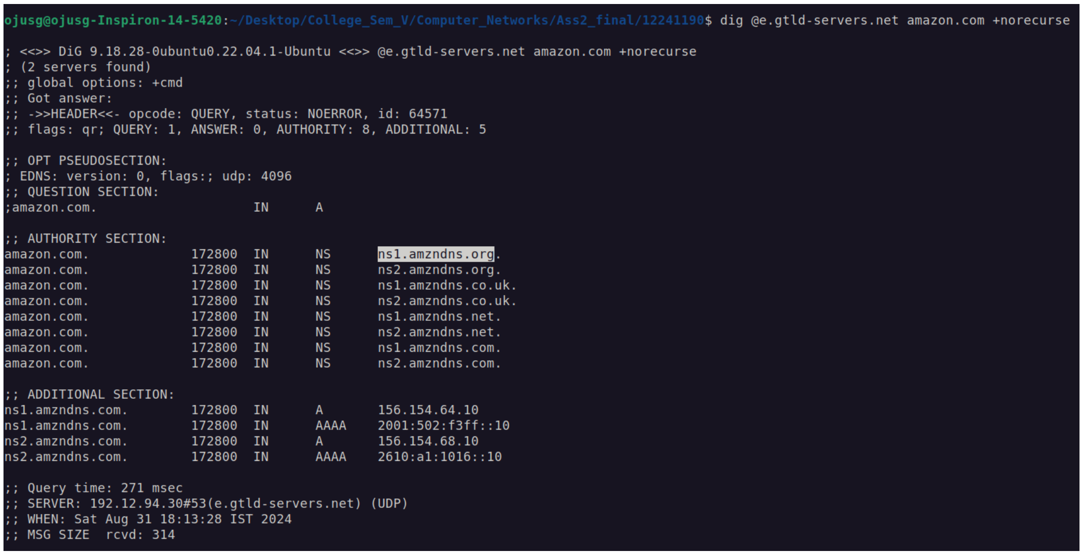
```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @ns-1520.awsdns-62.org geeksforgeeks.org +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @ns-1520.awsdns-62.org geeksforgeeks.org +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1042
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;geeksforgeeks.org.             IN      A

;; ANSWER SECTION:
geeksforgeeks.org.      300     IN      A       34.49.233.224

;; AUTHORITY SECTION:
geeksforgeeks.org.      17280   IN      NS      ns-1520.awsdns-62.org.
geeksforgeeks.org.      17280   IN      NS      ns-1569.awsdns-04.co.uk.
geeksforgeeks.org.      17280   IN      NS      ns-245.awsdns-30.com.
geeksforgeeks.org.      17280   IN      NS      ns-869.awsdns-44.net.

;; Query time: 24 msec
;; SERVER: 205.251.197.240#53(ns-1520.awsdns-62.org) (UDP)
;; WHEN: Sat Aug 31 18:04:49 IST 2024
;; MSG SIZE  rcvd: 199
```

We got the answer **34.49.233.224**

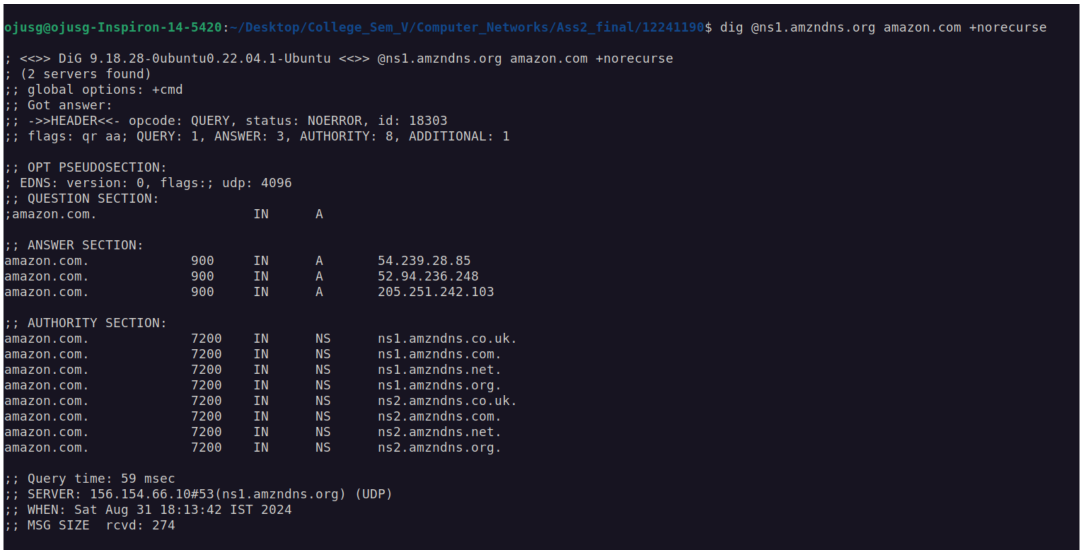
Repeating all the above steps for amazon.com



```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @a.root-servers.net amazon.com +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @a.root-servers.net amazon.com +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21714
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 27

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

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

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

;; Query time: 251 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Sat Aug 31 18:13:10 IST 2024
;; MSG SIZE  rcvd: 835
```



```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @e.gtld-servers.net amazon.com +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @e.gtld-servers.net amazon.com +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64571
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 8, ADDITIONAL: 5

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

;; AUTHORITY SECTION:
amazon.com.             172800  IN      NS      ns1.amzndns.org.
amazon.com.             172800  IN      NS      ns2.amzndns.org.
amazon.com.             172800  IN      NS      ns1.amzndns.co.uk.
amazon.com.             172800  IN      NS      ns2.amzndns.co.uk.
amazon.com.             172800  IN      NS      ns1.amzndns.net.
amazon.com.             172800  IN      NS      ns2.amzndns.net.
amazon.com.             172800  IN      NS      ns1.amzndns.com.
amazon.com.             172800  IN      NS      ns2.amzndns.com.

;; ADDITIONAL SECTION:
ns1.amzndns.com.        172800  IN      A       156.154.64.10
ns1.amzndns.com.        172800  IN      AAAA    2001:502:f3ff::10
ns2.amzndns.com.        172800  IN      A       156.154.68.10
ns2.amzndns.com.        172800  IN      AAAA    2610:a1:1016::10

;; Query time: 271 msec
;; SERVER: 192.12.94.30#53(e.gtld-servers.net) (UDP)
;; WHEN: Sat Aug 31 18:13:28 IST 2024
;; MSG SIZE  rcvd: 314
```



```
ojusg@ojusg-Inspiron-14-5420:~/Desktop/College_Sem_V/Computer_Networks/Ass2_final/12241190$ dig @ns1.amzndns.org amazon.com +norecurse

; <<>> DiG 9.18.28-0ubuntu0.22.04.1-Ubuntu <<>> @ns1.amzndns.org amazon.com +norecurse
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18303
;; flags: qr aa; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 1

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

;; ANSWER SECTION:
amazon.com.             900     IN      A       54.239.28.85
amazon.com.             900     IN      A       52.94.236.248
amazon.com.             900     IN      A       205.251.242.103

;; AUTHORITY SECTION:
amazon.com.             7200    IN      NS      ns1.amzndns.co.uk.
amazon.com.             7200    IN      NS      ns1.amzndns.com.
amazon.com.             7200    IN      NS      ns1.amzndns.net.
amazon.com.             7200    IN      NS      ns1.amzndns.org.
amazon.com.             7200    IN      NS      ns2.amzndns.co.uk.
amazon.com.             7200    IN      NS      ns2.amzndns.com.
amazon.com.             7200    IN      NS      ns2.amzndns.net.
amazon.com.             7200    IN      NS      ns2.amzndns.org.

;; Query time: 59 msec
;; SERVER: 156.154.66.10#53(ns1.amzndns.org) (UDP)
;; WHEN: Sat Aug 31 18:13:42 IST 2024
;; MSG SIZE  rcvd: 274
```

We got the answer **54.239.28.85, 52.94.236.248, 205.251.242.103**