# Computer Networks II

## Lab Assignments for Jan 8th

Sai Harsha Kottapalli - CS17BTECH11036
Sagar Jain - CS17BTECH11034

# Question I - HTTP

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Jan 2020 11:51:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 08 Jan 2020 06:59:01 GMT\r\n
    ETag: "80-59b9b6d6f7996"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.274531268 seconds]
    [Request in frame: 111]
    [Next request in frame: 119]
    [Next response in frame: 120]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
```

The above figure is for server response.

```
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 117]
    [Next request in frame: 119]
```

The above figure is for browser request.

1. Browser is running HTTP 1.1
   Server is running HTTP 1.1

2. Browser can languages: en-US,en
3. IP address of my computer - 172.16.2.167

gaia.cs.umass.edu server IP address - 128.119.245.12

4. status code returned - 200
5. Last-Modified: Wed, 08 Jan 2020 06:59:01 GMT\r\n
6. Content-Length: 128\r\n
7. No the raw data and packet listing window has same data.

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Jan 2020 11:51:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 08 Jan 2020 06:59:01 GMT\r\n
    ETag: "80-59b9b6d6f7996"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.274531268 seconds]
    [Request in frame: 111]
    [Next request in frame: 119]
    [Next response in frame: 120]

00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3··Last- Modified
00e0  3a 20 57 65 64 2c 20 30  38 20 4a 61 6e 20 32 30   : Wed, 0 8 Jan 20
00f0  32 30 20 30 36 3a 35 39  3a 30 31 20 47 4d 54 0d   20 06:59 :01 GMT·
0100  0a 45 54 61 67 3a 20 22  38 30 2d 35 39 62 39 62   ·ETag: " 80-59b9b
0110  36 64 36 66 37 39 39 36  22 0d 0a 41 63 63 65 70   6d6f7996 "··Accep
0120  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
0130  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
0140  20 31 32 38 0d 0a 4b 65  65 70 2d 41 6c 69 76 65    128··Ke ep-Alive
0150  3a 20 74 69 6d 65 6f 75  74 3d 35 2c 20 6d 61 78   : timeou t=5, max
0160  3d 31 30 30 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   =100··Co nnection
0170  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 43 6f   : Keep-A live··Co
0180  6e 74 65 6e 74 2d 54 79  70 65 3a 20 74 65 78 74   ntent-Ty pe: text
0190  2f 68 74 6d 6c 3b 20 63  68 61 72 73 65 74 3d 55   /html; c harset=U
01a0  54 46 2d 38 0d 0a 0d 0a  3c 68 74 6d 6c 3e 0a 43   TF-8···· <html>·C
01b0  6f 6e 67 72 61 74 75 6c  61 74 69 6f 6e 73 2e 20   ongratul ations.
01c0  20 59 6f 75 27 76 65 20  64 6f 77 6e 6c 6f 61 64    You've  download
01d0  65 64 20 74 68 65 20 66  69 6c 65 20 0a 68 74 74   ed the f ile ·htt
01e0  70 3a 2f 2f 67 61 69 61  2e 63 73 2e 75 6d 61 73   p://gaia .cs.umas
01f0  73 2e 65 64 75 2f 77 69  72 65 73 68 61 72 6b 2d   s.edu/wi reshark-
0200  6c 61 62 73 2f 48 54 54  50 2d 77 69 72 65 73 68   labs/HTT P-wiresh
0210  61 72 6b 2d 66 69 6c 65  31 2e 68 74 6d 6c 21 0a   ark-file 1.html!·
```

figure for 7th question.

8. No

```
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 21]
    [Next request in frame: 32]
```

figure for 8th question

9. Yes. From below figure we can see the response text.

```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Jan 2020 12:19:09 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 08 Jan 2020 06:59:01 GMT\r\n
    ETag: "173-59b9b6d6f5286"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.278481909 seconds]
    [Request in frame: 15]
    [Next request in frame: 32]
    [Next response in frame: 57]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
▸ Line-based text data: text/html (10 lines)

0160  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100··C onnectio
0170  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
0180  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0190  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
01a0  55 54 46 2d 38 0d 0a 0d  0a 0a 3c 68 74 6d 6c 3e   UTF-8··· ·<html>
01b0  0a 0a 43 6f 6e 67 72 61  74 75 6c 61 74 69 6f 6e   ··Congra tulation
01c0  73 20 61 67 61 69 6e 21  20 20 4e 6f 77 20 79 6f   s again!   Now yo
01d0  75 27 76 65 20 64 6f 77  6e 6c 6f 61 64 65 64 20   u've dow nloaded
01e0  74 68 65 20 66 69 6c 65  20 6c 61 62 32 2d 32 2e   the file  lab2-2.
01f0  68 74 6d 6c 2e 20 3c 62  72 3e 0a 54 68 69 73 20   html. <b r>·This
0200  66 69 6c 65 27 73 20 6c  61 73 74 20 6d 6f 64 69   file's l ast modi
0210  66 69 63 61 74 69 6f 6e  20 64 61 74 65 20 77 69   fication  date wi
0220  6c 6c 20 6e 6f 74 20 63  68 61 6e 67 65 2e 20 20   ll not c hange.
0230  3c 70 3e 0a 54 68 75 73  20 20 69 66 20 79 6f 75   <p>·Thus   if you
0240  20 64 6f 77 6e 6c 6f 61  64 20 74 68 69 73 20 6d    downloa d this m
0250  75 6c 74 69 70 6c 65 20  74 69 6d 65 73 20 6f 6e   ultiple  times on
0260  20 79 6f 75 72 20 62 72  6f 77 73 65 72 2c 20 61    your br owser, a
0270  20 63 6f 6d 70 6c 65 74  65 20 63 6f 70 79 20 3c    complet e copy <
0280  62 72 3e 0a 77 69 6c 6c  20 6f 6e 6c 79 20 62 65   br>·will  only be
0290  20 73 65 6e 74 20 6f 6e  63 65 20 62 79 20 74 68    sent on ce by th
02a0  65 20 73 65 72 76 65 72  20 64 75 65 20 74 6f 20   e server  due to
02b0  74 68 65 20 69 6e 63 6c  75 73 69 6f 6e 20 6f 66   the incl usion of
02c0  20 74 68 65 20 49 4e 2d  4d 4f 44 49 46 49 45 44    the IN- MODIFIED
02d0  2d 53 49 4e 43 45 3c 62  72 3e 0a 66 69 65 6c 64   -SINCE<b r>·field
02e0  20 69 6e 20 79 6f 75 72  20 62 72 6f 77 73 65 72    in your  browser
02f0  27 73 20 48 54 54 50 20  47 45 54 20 72 65 71 75   's HTTP  GET requ
0300  65 73 74 20 74 6f 20 74  68 65 20 73 65 72 76 65   est to t he serve
0310  72 2e 0a 0a 3c 2f 68 74  6d 6c 3e 0a               r.··</ht ml>·
```

10. Yes. The header is -

If-Modified-Since: Wed, 08 Jan 2020 06:59:01 GMT\r\n

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  If-None-Match: "173-59b9b6d6f5286"\r\n
  If-Modified-Since: Wed, 08 Jan 2020 06:59:01 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 2/2]
  [Prev request in frame: 15]
  [Response in frame: 57]
```

11. No server did not explicitly return the contents of the file this time. In the figure, we can status code 304 and length is also ver less.

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Wed, 08 Jan 2020 12:19:11 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=99\r\n
  ETag: "173-59b9b6d6f5286"\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.293156174 seconds]
  [Prev request in frame: 15]
  [Prev response in frame: 21]
  [Request in frame: 32]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

12. one .

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 72 | 3.502202680 | 192.168.110.24 | 128.119.245.12 | HTTP | 532 | GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 |
| 83 | 3.781396540 | 128.119.245.12 | 192.168.110.24 | HTTP | 583 | HTTP/1.1 200 OK (text/html) |

13. three.

```
[3 Reassembled TCP Segments (4861 bytes): #79(1448), #81(2896), #83(517)]
  [Frame: 79, payload: 0-1447 (1448 bytes)]
  [Frame: 81, payload: 1448-4343 (2896 bytes)]
  [Frame: 83, payload: 4344-4860 (517 bytes)]
  [Segment count: 3]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057…]
```

14. below figure, HTTP/1.1 200 OK
15. No.

```
▾ [3 Reassembled TCP Segments (4861 bytes): #79(1448), #81(2896), #83(517)]
    [Frame: 79, payload: 0-1447 (1448 bytes)]
    [Frame: 81, payload: 1448-4343 (2896 bytes)]
    [Frame: 83, payload: 4344-4860 (517 bytes)]
    [Segment count: 3]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057…]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Jan 2020 14:00:57 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 08 Jan 2020 06:59:01 GMT\r\n
    ETag: "1194-59b9b6d6dd3b3"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.279193860 seconds]
    [Request in frame: 72]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
▾ Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
```

16. Three.

They were all sent to 128.119.245.12

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 491 | 7.327363934 | 192.168.110.24 | 128.119.245.12 | HTTP | 532 | GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 |
| 507 | 7.594658165 | 128.119.245.12 | 192.168.110.24 | HTTP | 1139 | HTTP/1.1 200 OK (text/html) |
| 509 | 7.634705712 | 192.168.110.24 | 128.119.245.12 | HTTP | 464 | GET /pearson.png HTTP/1.1 |
| 527 | 7.895433611 | 128.119.245.12 | 192.168.110.24 | HTTP | 781 | HTTP/1.1 200 OK (PNG) |
| 531 | 7.901287730 | 192.168.110.24 | 128.119.245.12 | HTTP | 478 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1 |
| 693 | 8.718447975 | 128.119.245.12 | 192.168.110.24 | HTTP | 1472 | HTTP/1.1 200 OK (JPEG JFIF image) |

17. Based on timestamps.

First image request was sent at 7.63sec and response received at 7.89sec.

Then second image request was sent at 7.90sec and response received at 8.71sec.

Source port for first is 38866 and second is 38872.

So images were retrieved serially from different tcp ports.

Refer example figure for port number location.

```
▾ Transmission Control Protocol, Src Port: 38866, Dst Port: 80, Seq: 467, Ack: 1074, Len: 398
    Source Port: 38866
    Destination Port: 80
    [Stream index: 16]
    [TCP Segment Len: 398]
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 421 | 4.462015382 | 192.168.110.24 | 128.119.245.12 | HTTP | 548 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 444 | 4.725857725 | 128.119.245.12 | 192.168.110.24 | HTTP | 783 | HTTP/1.1 401 Unauthorized (text/html) |
| 1069 | 19.626154765 | 192.168.110.24 | 128.119.245.12 | HTTP | 633 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 |
| 1085 | 19.883965697 | 128.119.245.12 | 192.168.110.24 | HTTP | 556 | HTTP/1.1 200 OK (text/html) |

18. HTTP/1.1 401 Unauthorized

19. Authorization field.

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.79 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame: 1085]
```

# Question II - TCP

| No. | Time | Source | Destination | Protocol | Lengtl | Info |
|---|---|---|---|---|---|---|
| 7 | 4.675312 | 192.168.1.102 | 128.119.245.12 | TCP | 62 | 4127 → 80 [SYN |
| 8 | 4.694429 | 128.119.245.12 | 192.168.1.102 | TCP | 62 | 80 → 4127 [SYN |
| 9 | 4.694458 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 4127 → 80 [ACK |
| 10 | 4.694850 | 192.168.1.102 | 128.119.245.12 | HTTP | 555 | GET /ethereal- |
| 11 | 4.717289 | 128.119.245.12 | 192.168.1.102 | TCP | 60 | 80 → 4127 [ACK |
| 12 | 4.718993 | 128.119.245.12 | 192.168.1.102 | HTTP | 439 | HTTP/1.1 200 O |
| 13 | 4.724332 | 192.168.1.102 | 128.119.245.12 | HTTP | 541 | GET /favicon.i |
| 14 | 4.750366 | 128.119.245.12 | 192.168.1.102 | HTTP | 1395 | HTTP/1.1 404 N |
| 15 | 4.859777 | 192.168.1.102 | 128.119.245.12 | TCP | 54 | 4127 → 80 [ACK |

```
▸ Frame 7: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:a
▾ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x01cb (459)
  ▸ Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.102
    Destination: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 4127
    Destination Port: 80
    [Stream index: 0]
```

**<u>Answer 1</u>**:

From the above figure, it is clear that the **source IP address is 192.168.1.102** and the **source port number is 4127**.

**<u>Answer 2</u>**:

Similarly, the **IP address of gaia.cs.umass.edu is 128.119.245.12** and the **port number it is receiving and sending TCP segments from is 80**.

| | | | | |
|---|---|---|---|---|
| 51 | 13.827199463 | 172.16.2.238 | 172.217.160.142 | TCP |
| 52 | 13.846981032 | 172.217.160.142 | 172.16.2.238 | TCP |
| 53 | 14.449166616 | 172.16.2.238 | 128.119.245.12 | TCP |
| 54 | 14.449246580 | 172.16.2.238 | 128.119.245.12 | TCP |
| 55 | 14.700371686 | 172.16.2.238 | 128.119.245.12 | TCP |
| 56 | 14.744774662 | 128.119.245.12 | 172.16.2.238 | TCP |
| 57 | 14.744916036 | 172.16.2.238 | 128.119.245.12 | TCP |
| 58 | 14.745025825 | 128.119.245.12 | 172.16.2.238 | TCP |
| 59 | 14.745104141 | 172.16.2.238 | 128.119.245.12 | TCP |
| 60 | 14.746289039 | 172.16.2.238 | 128.119.245.12 | TCP |
| 61 | 14.746677481 | 172.16.2.238 | 128.119.245.12 | TCP |

```
▶ Frame 55: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: IntelCor_f1:43:89 (2c:6e:85:f1:43:89), Dst: Hewlet
▼ Internet Protocol Version 4, Src: 172.16.2.238, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x41fa (16890)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd43f [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.2.238
    Destination: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 47838, Dst Port: 80, Seq: 0,
    Source Port: 47838
    Destination Port: 80
    [Stream index: 10]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
```

**Answer 3**:

From the above, the **source (mine)  IP address is 172.16.2.238** and **the source port is 47838**.

| | | | | | | |
|---|---|---|---|---|---|---|
| 53 | 14.449166616 | 172.16.2.238 | 128.119.245.12 | TCP | 74 | 47834 → 80 [SYN] |
| 54 | 14.449246580 | 172.16.2.238 | 128.119.245.12 | TCP | 74 | 47836 → 80 [SYN] |
| 55 | 14.700371686 | 172.16.2.238 | 128.119.245.12 | TCP | 74 | 47838 → 80 [SYN] |
| 56 | 14.744774662 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47834 [SYN, |
| 57 | 14.744916036 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47834 → 80 [ACK] |
| 58 | 14.745025825 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47836 [SYN, |
| 59 | 14.745104141 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47836 → 80 [ACK] |
| 60 | 14.746289039 | 172.16.2.238 | 128.119.245.12 | TCP | 758 | 47834 → 80 [PSH, |
| 61 | 14.746677481 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] |
| 62 | 14.746705238 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] |
| 63 | 14.746744525 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] |
| 64 | 14.746752862 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] |
| 65 | 15.080001048 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47838 [SYN, |
| 66 | 15.080123911 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47838 → 80 [ACK] |
| 67 | 15.192219778 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] |

```
    Header checksum: 0x2d3f [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.2.238
    Destination: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 47834, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 47834
    Destination Port: 80
    [Stream index: 8]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x002 (SYN)
    Window size value: 29200
    [Calculated window size: 29200]
    Checksum: 0x7a68 [unverified]
```

**<u>Answer 4</u>**:

The **sequence number is 0**. The flag present in the segment i.e. 0x002 identifies the segment as an SYN segment.

| | | | | | | |
|---|---|---|---|---|---|---|
| 55 | 14.700371686 | 172.16.2.238 | 128.119.245.12 | TCP | 74 | 47838 → 80 [SYN] Seq=0 Win=29200 L |
| 56 | 14.744774662 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47834 [SYN, ACK] Seq=0 Ack=1 |
| 57 | 14.744916036 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47834 → 80 [ACK] Seq=1 Ack=1 Win=2 |
| 58 | 14.745025825 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47836 [SYN, ACK] Seq=0 Ack=1 |
| 59 | 14.745104141 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47836 → 80 [ACK] Seq=1 Ack=1 Win=2 |
| 60 | 14.746289039 | 172.16.2.238 | 128.119.245.12 | TCP | 758 | 47834 → 80 [PSH, ACK] Seq=1 Ack=1 |
| 61 | 14.746677481 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] Seq=693 Ack=1 Win |
| 62 | 14.746705238 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] Seq=2141 Ack=1 Wi |
| 63 | 14.746744525 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] Seq=3589 Ack=1 Wi |
| 64 | 14.746752862 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] Seq=5037 Ack=1 Wi |
| 65 | 15.080001048 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | 80 → 47838 [SYN, ACK] Seq=0 Ack=1 |
| 66 | 15.080123911 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | 47838 → 80 [ACK] Seq=1 Ack=1 Win=2 |
| 67 | 15.192219778 | 172.16.2.238 | 128.119.245.12 | TCP | 1514 | 47834 → 80 [ACK] Seq=6485 Ack=1 Wi |

```
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 172.16.2.238
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 47834, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 47834
    [Stream index: 8]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    1010 .... = Header Length: 40 bytes (10)
  ▶ Flags: 0x012 (SYN, ACK)
    Window size value: 28960
    [Calculated window size: 28960]
    Checksum: 0x82e8 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
```

**<u>Answer 5</u>**:

a) The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is **0**.
b) the value of the ACKnowledgement field in the SYNACK segment is **1**.
c) The flag value in the segment i.e. **0x012** identifies the segment as an SYNACK segment.

```
58 14.745025825  128.119.245.12   172.16.2.238     TCP   74 80 → 47836 [SYN, ACK] Seq=0 Ack=1 Wi
59 14.745104141  172.16.2.238     128.119.245.12   TCP   66 47836 → 80 [ACK] Seq=1 Ack=1 Win=293
60 14.746289039  172.16.2.238     128.119.245.12   TCP  758 47834 → 80 [PSH, ACK] Seq=1 Ack=1 Wi
61 14.746677481  172.16.2.238     128.119.245.12   TCP 1514 47834 → 80 [ACK] Seq=693 Ack=1 Win=2
62 14.746705238  172.16.2.238     128.119.245.12   TCP 1514 47834 → 80 [ACK] Seq=2141 Ack=1 Win=
63 14.746744525  172.16.2.238     128.119.245.12   TCP 1514 47834 → 80 [ACK] Seq=3589 Ack=1 Win=
64 14.746752862  172.16.2.238     128.119.245.12   TCP 1514 47834 → 80 [ACK] Seq=5037 Ack=1 Win=
65 15.080001048  128.119.245.12   172.16.2.238     TCP   74 80 → 47838 [SYN, ACK] Seq=0 Ack=1 Wi
66 15.080123911  172.16.2.238     128.119.245.12   TCP   66 47838 → 80 [ACK] Seq=1 Ack=1 Win=293
```

```
▶ Frame 60: 758 bytes on wire (6064 bits), 758 bytes captured (6064 bits) on interface 0
▶ Ethernet II, Src: IntelCor_f1:43:89 (2c:6e:85:f1:43:89), Dst: HewlettP_50:48:e7 (78:48:59:50:48:e7)
▼ Internet Protocol Version 4, Src: 172.16.2.238, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 744
    Identification: 0xe8fc (59644)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0x2a91 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.2.238
    Destination: 128.119.245.12
▼ Transmission Control Protocol, Src Port: 47834, Dst Port: 80, Seq: 1, Ack: 1, Len: 692
    Source Port: 47834
    Destination Port: 80
    [Stream index: 8]
    [TCP Segment Len: 692]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 693    (relative sequence number)]
```

```
0030  00 e5 76 05 00 00 01 01  08 0a 70 97 88 4c ab 02   ··v····· ··p··L··
0040  1d 0f 50 4f 53 54 20 2f  77 69 72 65 73 68 61 72   ··POST / wireshar
0050  6b 2d 6c 61 62 73 2f 6c  61 62 33 2d 31 2d 72 65   k-labs/l ab3-1-re
0060  70 6c 79 2e 68 74 6d 20  48 54 54 50 2f 31 2e 31   ply.htm  HTTP/1.1
0070  0d 0a 48 6f 73 74 3a 20  67 61 69 61 2e 63 73 2e   ··Host:  gaia.cs.
0080  75 6d 61 73 73 2e 65 64  75 0d 0a 43 6f 6e 6e 65   umass.ed u··Conne
0090  63 74 69 6f 6e 3a 20 6b  65 65 70 2d 61 6c 69 76   ction: k eep-aliv
00a0  65 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74   e··Conte nt-Lengt
```

**Answer 6**:

the sequence number of the TCP segment containing the HTTP POST Command is **1**.

```
80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
80 [PSH, ACK] Seq=1 Ack=1 Win=29312 L
80 [ACK] Seq=693 Ack=1 Win=29312 Len=
80 [ACK] Seq=2141 Ack=1 Win=29312 Len
80 [ACK] Seq=3589 Ack=1 Win=29312 Len
80 [ACK] Seq=5037 Ack=1 Win=29312 Len
38 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
80 [ACK] Seq=1 Ack=1 Win=29312 Len=0
80 [ACK] Seq=6485 Ack=1 Win=29312 Len
80 [ACK] Seq=7933 Ack=1 Win=29312 Len
```

**<u>Answer 7</u>**:

The first six sequence numbers are:

**1, 693, 2141, 3589, 5037, 6485**

The following table shows the first six segments sent and their respective acknowledgements.

| Sno. | Sent Time | Ack Receive Time |
|---|---|---|
| 1 | 14.746289039 | 15.498213918 |
| 2 | 14.746677481 | 15.499693863 |
| 3 | 14.746705238 | TCP delayed acknowledgement |
| 4 | 14.746744525 | TCP delayed acknowledgement |
| 5 | 14.746752862 | 15.499809970 |
| 6 | 15.192219778 | 15.499905148 |

The definition used to estimate the Round trip time (RTT) is as follows:

**EstimatedRTT = (1 – α) * EstimatedRTT + α * SampleRTT**
**α=0.125**

**Solution:**
ertt = 15.498213918 - 14.746289039
ertt = (1-0.125)*ertt + 0.125*(15.499693863-14.746677481)
ertt = (1-0.125)*ertt + 0.125*(15.499809970-14.746752862)
ertt = (1-0.125)*ertt + 0.125*(15.499905148-15.192219778)

**Therefore, EstimatedRTT = 0.697s**

For the segments whose acknowledgements have been skipped due to TCP delayed acknowledgements, the calculations have been omitted and only the last segment is considered.

## Answer 8:

The length of each of the segments is 758, 1514, 1514, 1514, 1514, 1514.

## Answer 9:

```
Acknowledgment number: 1    (relative ack
1010 .... = Header Length: 40 bytes (10)
▸ Flags: 0x012 (SYN, ACK)
Window size value: 28960
[Calculated window size: 28960]
Checksum: 0x82e8 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
```

The minimum amount of available buffer space is advertised is same as Calculated window size = **28960 bytes**

## Answer 10:

Yes, there is one re-transmitted segment in the trace file, to find this segment I went through the segment trace and looked for an entry which was highlighted. An alternate way to do this would be to sort the segments by sequence number and check if any two consecutive segments in this list are identical.

| | | | | | | |
|---|---|---|---|---|---|---|
| 103 | 15.812253302 | 128.119.245.12 | 172.16.2.238 | TCP | 66 | 80 → 47834 [ACK] Seq=1 |
| 104 | 15.812270937 | 128.119.245.12 | 172.16.2.238 | TCP | 66 | 80 → 47834 [ACK] Seq=1 |
| 105 | 15.812287288 | 128.119.245.12 | 172.16.2.238 | TCP | 66 | 80 → 47834 [ACK] Seq=1 |
| 106 | 15.812304362 | 128.119.245.12 | 172.16.2.238 | TCP | 66 | 80 → 47834 [ACK] Seq=1 |
| 107 | 15.812324914 | 128.119.245.12 | 172.16.2.238 | TCP | 74 | [TCP Retransmission] 80 |
| 108 | 15.812349197 | 172.16.2.238 | 128.119.245.12 | TCP | 66 | [TCP Dup ACK 59#1] 4783 |

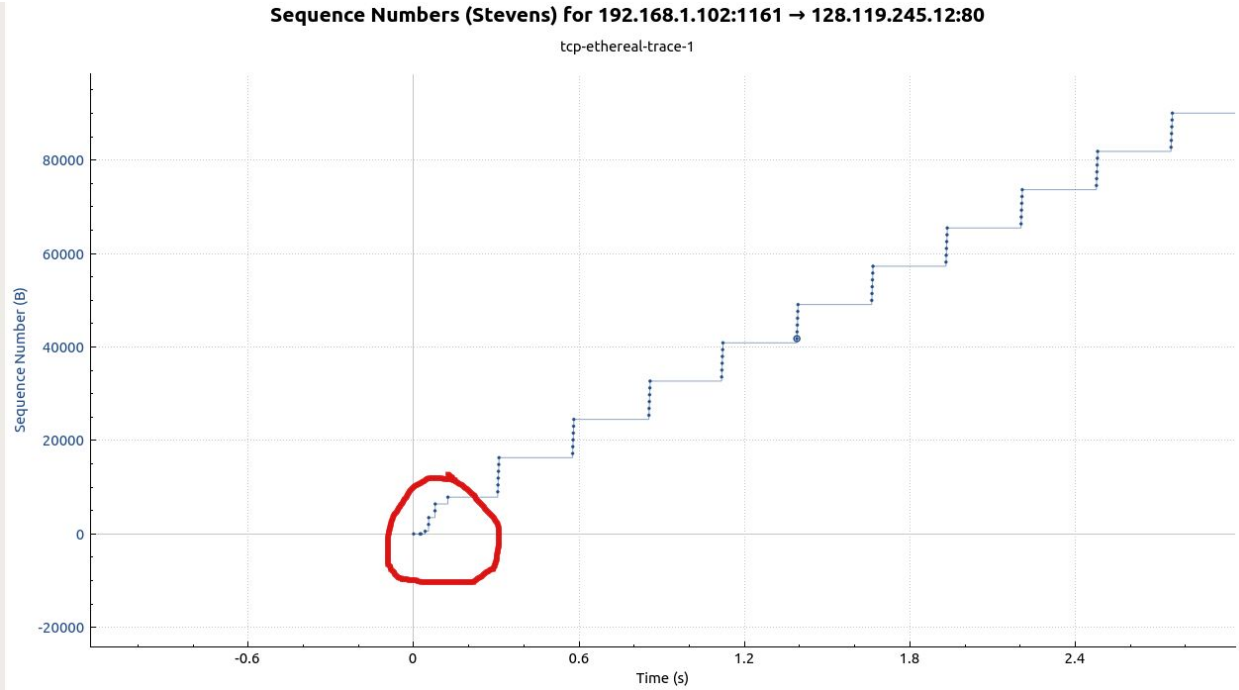
## Answer 11:

The receiver typically acknowledges **1514 bytes** in an ack. In case of delayed acknowledgement, this number can be larger i.e. a multiple of **1514 bytes**.

## Answer 12:

The transmission of the file begins at 14.746289039 and goes on till 19.729136628, the size of the file is 152138 bytes. So the throughput is 152138/(19.729136628-14.746289039) = 30532.34 bytes/sec i.e. 30.5 KB/s

## Answer 13:

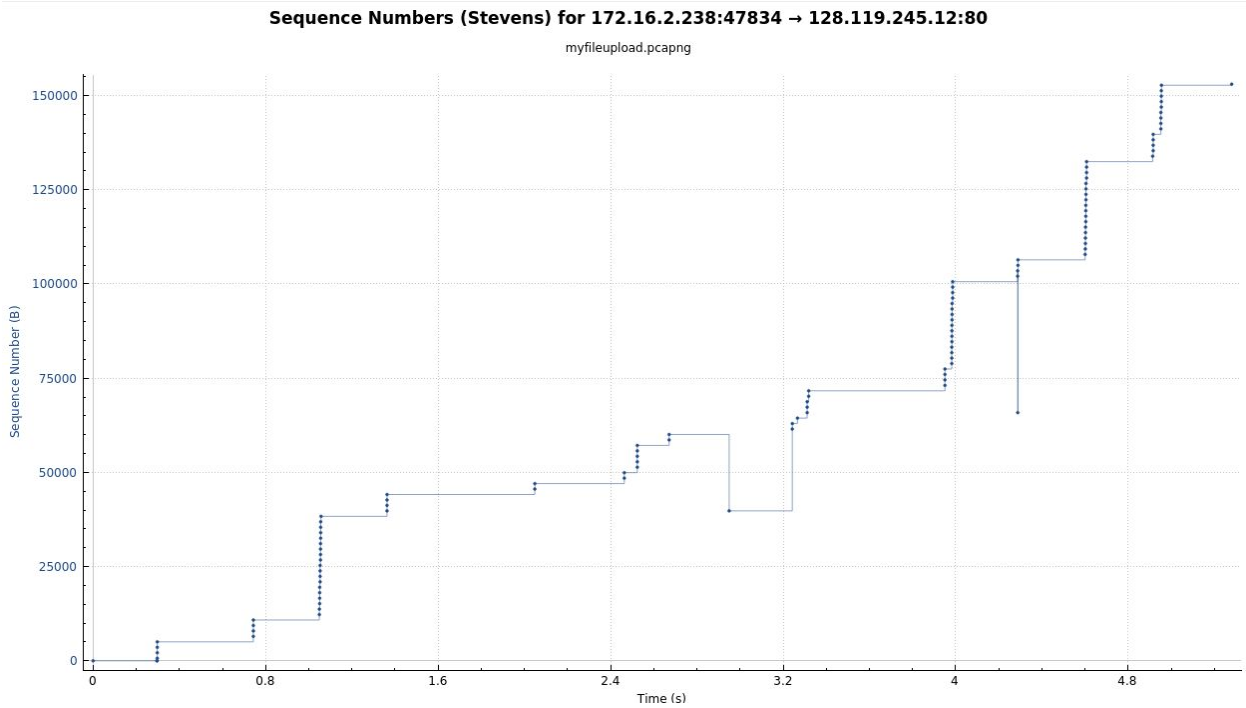



For the given trace the slow start begins at around 0.03s. Slow start is marked above. The congestion avoidance begins just after this exponential increase after the slow start.

The measured data differs from idealistic expectation in the following ways:

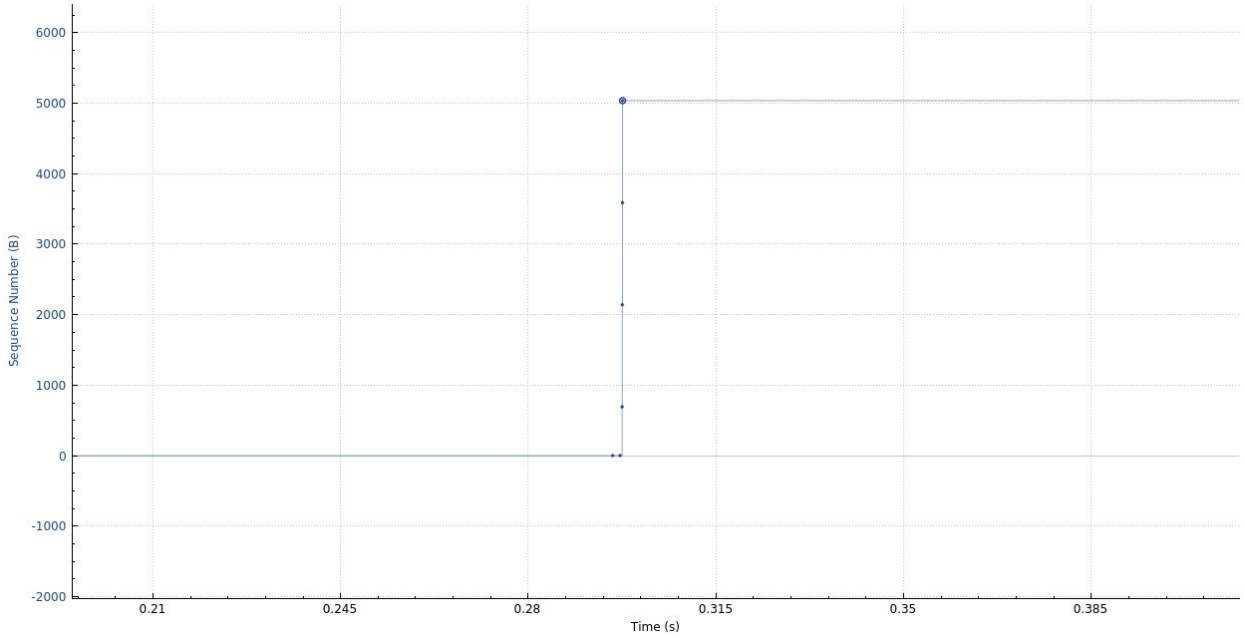
1) No smooth curves at the slow start and congestion avoidance.
2) Not full utilisation of window size.

**<u>Answer 14</u>**:




The above is the Time-Sequence-Graph(Stevens) for upload from my computer.

If we have a closer look as in below:




We can see that the slow start period begins at about **0.296s**.

The congestion avoidance stage is not very clearly visible in the obtained graph but it roughly begins at 1.35s.

The measured data differs from idealistic expectation in the following ways:

1) No smooth curves at the slow start and congestion avoidance.
2) Not full utilisation of window size.
3) Transmission delay acknowledgement causes discrepancies.

# DNS

1.

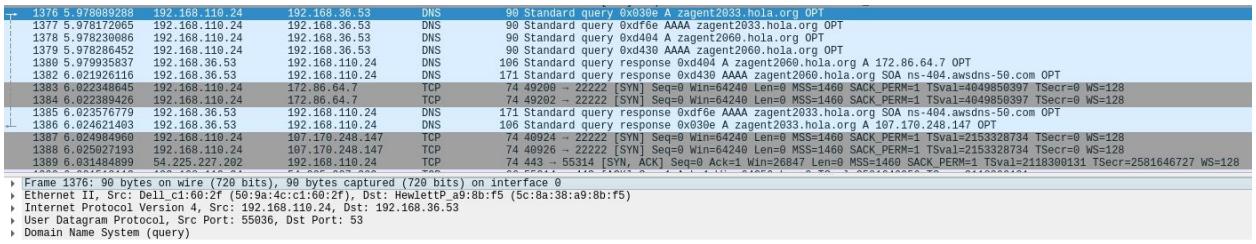
```
archelaus@archelaus  ~  nslookup www.iith.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.iith.ac.in
Address: 192.168.36.56
```

2.

```
archelaus@archelaus  ~  nslookup -type=NS ox.ac.uk
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
ox.ac.uk        nameserver = dns0.ox.ac.uk.
ox.ac.uk        nameserver = ns2.ja.net.
ox.ac.uk        nameserver = auth5.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth6.dns.ox.ac.uk.
ox.ac.uk        nameserver = auth4.dns.ox.ac.uk.
ox.ac.uk        nameserver = dns2.ox.ac.uk.
ox.ac.uk        nameserver = dns1.ox.ac.uk.

Authoritative answers can be found from:
```

3. Since using dns from a europe institute response was refused. i used iith dns server instead.

```
archelaus@archelaus  ~  nslookup mail.yahoo.com dns1.iith.ac.in
Server:         dns1.iith.ac.in
Address:        192.168.35.52#53

Non-authoritative answer:
mail.yahoo.com  canonical name = edge.gycpi.b.yahoodns.net.
Name:   edge.gycpi.b.yahoodns.net
Address: 106.10.236.37
Name:   edge.gycpi.b.yahoodns.net
Address: 106.10.236.40
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.10.11
Name:   edge.gycpi.b.yahoodns.net
Address: 119.161.10.12
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:98:800::e5
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:98:800::e6
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:e4:1604::1001
Name:   edge.gycpi.b.yahoodns.net
Address: 2406:2000:e4:1604::1000
```

4. 

| | | | | | | |
|---|---|---|---|---|---|---|
| 1376 | 5.978089288 | 192.168.110.24 | 192.168.36.53 | DNS | 90 | Standard query 0x030e A zagent2033.hola.org OPT |
| 1377 | 5.978172065 | 192.168.110.24 | 192.168.36.53 | DNS | 90 | Standard query 0xdf6e AAAA zagent2033.hola.org OPT |
| 1378 | 5.978230086 | 192.168.110.24 | 192.168.36.53 | DNS | 90 | Standard query 0xd404 A zagent2060.hola.org OPT |
| 1379 | 5.978286452 | 192.168.110.24 | 192.168.36.53 | DNS | 90 | Standard query 0xd430 AAAA zagent2060.hola.org OPT |
| 1380 | 5.979935837 | 192.168.36.53 | 192.168.110.24 | DNS | 106 | Standard query response 0xd404 A zagent2060.hola.org A 172.86.64.7 OPT |
| 1382 | 6.021926116 | 192.168.36.53 | 192.168.110.24 | DNS | 171 | Standard query response 0xd430 AAAA zagent2060.hola.org SOA ns-404.awsdns-50.com OPT |
| 1383 | 6.022348645 | 192.168.110.24 | 172.86.64.7 | TCP | 74 | 49200 → 22222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4049850397 TSecr=0 WS=128 |
| 1384 | 6.022389426 | 192.168.110.24 | 172.86.64.7 | TCP | 74 | 49202 → 22222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4049850397 TSecr=0 WS=128 |
| 1385 | 6.023576779 | 192.168.36.53 | 192.168.110.24 | DNS | 171 | Standard query response 0xdf6e AAAA zagent2033.hola.org SOA ns-404.awsdns-50.com OPT |
| 1386 | 6.024621403 | 192.168.36.53 | 192.168.110.24 | DNS | 106 | Standard query response 0x030e A zagent2033.hola.org A 107.170.248.147 OPT |
| 1387 | 6.024984960 | 192.168.110.24 | 107.170.248.147 | TCP | 74 | 40924 → 22222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2153328734 TSecr=0 WS=128 |
| 1388 | 6.025027193 | 192.168.110.24 | 107.170.248.147 | TCP | 74 | 40926 → 22222 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2153328734 TSecr=0 WS=128 |
| 1389 | 6.031484899 | 54.225.227.202 | 192.168.110.24 | TCP | 74 | 443 → 55314 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=2118300131 TSecr=2581646727 WS=128 |

```
Frame 1376: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
Ethernet II, Src: Dell_c1:60:2f (50:9a:4c:c1:60:2f), Dst: HewlettP_a9:8b:f5 (5c:8a:38:a9:8b:f5)
Internet Protocol Version 4, Src: 192.168.110.24, Dst: 192.168.36.53
User Datagram Protocol, Src Port: 55036, Dst Port: 53
Domain Name System (query)
```

Here, in packet details we can see “User Datagram Protocol” indicating it is sent over UDP.

5. destination port for the DNS query message is 53.
   source port of DNS response message is port 53.

```
▸ Frame 1380: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
▸ Ethernet II, Src: HewlettP_a9:8b:f5 (5c:8a:38:a9:8b:f5), Dst: Dell_c1:60:2f (50:9a:4c:c1:60:2f)
▸ Internet Protocol Version 4, Src: 192.168.36.53, Dst: 192.168.110.24
▸ User Datagram Protocol, Src Port: 53, Dst Port: 52557
▾ Domain Name System (response)
    Transaction ID: 0xd404
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Answers
  ▸ Additional records
```

```
▸ Frame 1376: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
▸ Ethernet II, Src: Dell_c1:60:2f (50:9a:4c:c1:60:2f), Dst: HewlettP_a9:8b:f5 (5c:8a:38:a9:8b:f5)
▸ Internet Protocol Version 4, Src: 192.168.110.24, Dst: 192.168.36.53
▸ User Datagram Protocol, Src Port: 55036, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x030e
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▸ Queries
  ▸ Additional records
    [Response In: 1386]
```

*From here on Lan was down so i had to change locations hence, different network.*

6. The IP address to which DNS query message is sent 192.168.36.53

| No. | Time | Source | Destination | Protoc | Length | Info |
|---|---|---|---|---|---|---|
| 233 | 3.096823… | 192.168.103.1… | 192.168.36.53 | DNS | 102 | Standard query 0xd6f8 A www.ietf.org.cdn.cloudflare.net OPT |
| 245 | 3.145950… | 192.168.36.53 | 192.168.103.165 | DNS | 134 | Standard query response 0xd6f8 A www.ietf.org.cdn.cloudflare.net A 104.20.0.85 A 104.20.1.85 OPT |
| 543 | 4.627460… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0xe0bd A zagent886.hola.org OPT |
| 544 | 4.627587… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0x6933 AAAA zagent886.hola.org OPT |
| 545 | 4.627697… | 192.168.103.1… | 192.168.36.53 | DNS | 90 | Standard query 0x3187 A zagent2063.hola.org OPT |
| 546 | 4.627807… | 192.168.103.1… | 192.168.36.53 | DNS | 90 | Standard query 0x6b97 AAAA zagent2063.hola.org OPT |
| 547 | 4.628993… | 192.168.36.53 | 192.168.103.165 | DNS | 105 | Standard query response 0xe0bd A zagent886.hola.org A 184.164.147.6 OPT |
| 548 | 4.629137… | 192.168.36.53 | 192.168.103.165 | DNS | 171 | Standard query response 0x6b97 AAAA zagent2063.hola.org SOA ns-404.awsdns-50.com OPT |
| 549 | 4.629147… | 192.168.36.53 | 192.168.103.165 | DNS | 106 | Standard query response 0x3187 A zagent2063.hola.org A 144.172.64.12 OPT |
| 560 | 4.670972… | 192.168.36.53 | 192.168.103.165 | DNS | 170 | Standard query response 0x6933 AAAA zagent886.hola.org SOA ns-404.awsdns-50.com OPT |

As we can see from figure ifconfig cannot show the gateway nor dns server.

```
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.103.165  netmask 255.255.254.0  broadcast 192.168.103.
255
        inet6 fe80::5035:7eb1:afc8:3c04  prefixlen 64  scopeid 0x20<link>
        ether 50:9a:4c:c1:60:2f  txqueuelen 1000  (Ethernet)
        RX packets 630340  bytes 82940414 (82.9 MB)
        RX errors 0  dropped 8776  overruns 0  frame 0
        TX packets 202030  bytes 45439656 (45.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 92359  bytes 7311026 (7.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 92359  bytes 7311026 (7.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether cc:2f:71:13:06:87  txqueuelen 1000  (Ethernet)
        RX packets 97271  bytes 63276552 (63.2 MB)
        RX errors 0  dropped 15  overruns 0  frame 0
        TX packets 120435  bytes 25486250 (25.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Hence i use this command - $ nmcli dev show | grep 'DNS'
to check dns ip address which matches with query destination.

```
archelaus@archelaus  ~  nmcli dev show | grep 'DNS'
IP4.DNS[1]:                                192.168.36.53
IP4.DNS[2]:                                192.168.35.52
```

7. The DNS record is of Type A with no answers in it.

```
▾ Domain Name System (query)
    Transaction ID: 0xd6f8
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN
```

8. 2 answers are present. It has host, type, class, ip address.
   On elongating it, we also find TTL and data length.

```
▾ Domain Name System (response)
    Transaction ID: 0xd6f8
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN
  ▾ Answers
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
    ▸ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.1.85
```

```
▾ Answers
  ▾ www.ietf.org.cdn.cloudflare.net: type A, class IN, addr 104.20.0.85
      Name: www.ietf.org.cdn.cloudflare.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 300
      Data length: 4
      Address: 104.20.0.85
```

9.

```
255 3.190301… 192.168.103.1… 104.20.0.85      TLSv…  571 Client Hello
256 3.190949… 192.168.103.1… 104.20.0.85      TLSv…  571 Client Hello
259 3.232818… 104.20.0.85    192.168.103.165  TCP     60 443 → 54656 [ACK] Seq=1 Ack=518 Win=30720 Len=0

▸ Frame 255: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0
▸ Ethernet II, Src: Dell_c1:60:2f (50:9a:4c:c1:60:2f), Dst: HewlettP_a9:8b:f1 (5c:8a:38:a9:8b:f1)
▸ Internet Protocol Version 4, Src: 192.168.103.165, Dst: 104.20.0.85
▸ Transmission Control Protocol, Src Port: 54656, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security
```

   As we can see it is indeed 103.20.0.85

10. No (this is by checking the whole packet list, didnt attach screenshot as too many packets to show)

11.

| No. | Time | Source | Destination | Protoc | Length | Info |
|---|---|---|---|---|---|---|
| 99 | 1.868368… | 192.168.103.1… | 192.168.36.53 | DNS | 82 | Standard query 0xd34c A www.mit.edu OPT |
| 100 | 1.923264… | 192.168.36.53 | 192.168.103.165 | DNS | 171 | Standard query response 0xd34c A www.mit.e |
| 101 | 1.924913… | 192.168.103.1… | 192.168.36.53 | DNS | 96 | Standard query 0xc37c AAAA e9566.dscb.akar |
| 107 | 1.979359… | 192.168.36.53 | 192.168.103.165 | DNS | 152 | Standard query response 0xc37c AAAA e9566. |
| 181 | 3.475341… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0xf328 A zagent495.hola.org |
| 182 | 3.475396… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0xddcb AAAA zagent495.hola. |
| 183 | 3.475441… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0xf5ab A zagent875.hola.org |
| 184 | 3.475485… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0x1aa1 AAAA zagent875.hola. |
| 185 | 3.480161… | 192.168.36.53 | 192.168.103.165 | DNS | 105 | Standard query response 0xf5ab A zagent875 |
| 186 | 3.480342… | 192.168.36.53 | 192.168.103.165 | DNS | 105 | Standard query response 0xf328 A zagent495 |

```
▸ Frame 99: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▸ Ethernet II, Src: Dell_c1:60:2f (50:9a:4c:c1:60:2f), Dst: HewlettP_a9:8b:f1 (5c:8a:38:a9:8b:f1)
▸ Internet Protocol Version 4, Src: 192.168.103.165, Dst: 192.168.36.53
▸ User Datagram Protocol, Src Port: 56564, Dst Port: 53
```

destination port of DNS query is 53.
source port of DNS response is 53.

```
▸ User Datagram Protocol, Src Port: 53, Dst Port: 56564
```

12. In above screenshot, we can see that it is being sent to 192.168.36.53 which is our dns server as we have shown in earlier question using appropriate command.

13.

```
▾ Domain Name System (query)
    Transaction ID: 0xd34c
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ www.mit.edu: type A, class IN
```

Type A and no answers.

14.

```
▾ Answers
  ▾ www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
      Name: www.mit.edu
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 270
      Data length: 25
      CNAME: www.mit.edu.edgekey.net
  ▾ www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
      Name: www.mit.edu.edgekey.net
      Type: CNAME (Canonical NAME for an alias) (5)
      Class: IN (0x0001)
      Time to live: 36
      Data length: 24
      CNAME: e9566.dscb.akamaiedge.net
  ▾ e9566.dscb.akamaiedge.net: type A, class IN, addr 23.57.254.82
      Name: e9566.dscb.akamaiedge.net
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 20
      Data length: 4
      Address: 23.57.254.82
```

3 answers as shown.

It has host, type, class, ip address.

On elongating it, we also find TTL and data length.

15. All necessary screenshots have

16.

```
archelaus@archelaus  ~  nslookup www.mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.mit.edu     canonical name = www.mit.edu.edgekey.net.
www.mit.edu.edgekey.net canonical name = e9566.dscb.akamaiedge.net.
Name:   e9566.dscb.akamaiedge.net
Address: 23.57.254.82
Name:   e9566.dscb.akamaiedge.net
Address: 2600:140f:5:187::255e
Name:   e9566.dscb.akamaiedge.net
Address: 2600:140f:5:182::255e

archelaus@archelaus  ~  nslookup -type=NS mit.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
mit.edu nameserver = asia1.akam.net.
mit.edu nameserver = ns1-37.akam.net.
mit.edu nameserver = use2.akam.net.
mit.edu nameserver = ns1-173.akam.net.
mit.edu nameserver = usw2.akam.net.
mit.edu nameserver = asia2.akam.net.
mit.edu nameserver = use5.akam.net.
mit.edu nameserver = eur5.akam.net.

Authoritative answers can be found from:
```

ip.addr == 192.168.103.165

| No. | Time | Source | Destination | Protoc | Length | Info |
|---|---|---|---|---|---|---|
| 322 | 3.273713… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0x7c80 A zagent874.hola.org OPT |
| 323 | 3.273787… | 192.168.103.1… | 192.168.36.53 | DNS | 89 | Standard query 0xe86c AAAA zagent874.hola.org OPT |
| 324 | 3.273863… | 192.168.103.1… | 192.168.36.53 | DNS | 87 | Standard query 0xa381 A zagent3.hola.org OPT |
| 325 | 3.273937… | 192.168.103.1… | 192.168.36.53 | DNS | 87 | Standard query 0x0cc8 AAAA zagent3.hola.org OPT |
| 326 | 3.279314… | 192.168.36.53 | 192.168.103.165 | DNS | 103 | Standard query response 0xa381 A zagent3.hola.org A 66.85.185.71 OPT |
| 331 | 3.326309… | 192.168.36.53 | 192.168.103.165 | DNS | 168 | Standard query response 0x0cc8 AAAA zagent3.hola.org SOA ns-404.awsdns-50.com OPT |
| 334 | 3.336285… | 192.168.36.53 | 192.168.103.165 | DNS | 105 | Standard query response 0x7c80 A zagent874.hola.org A 108.170.8.170 OPT |
| 336 | 3.336892… | 192.168.36.53 | 192.168.103.165 | DNS | 170 | Standard query response 0xe86c AAAA zagent874.hola.org SOA ns-404.awsdns-50.com OPT |

Destination is 192.168.36.53 which is indeed out dns server as shown in earlier questions.

17. Somehow as shown, DNS query is of type A were sent instead of type NS as asked.This does not have any answers.

18.

```
▾ Domain Name System (query)
    Transaction ID: 0x7e81
  ▸ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▾ Queries
    ▸ zagent347.hola.org: type AAAA, class IN

  ▾ Domain Name System (response)
      Transaction ID: 0x0ba9
    ▸ Flags: 0x8180 Standard query response, No error
      Questions: 1
      Answer RRs: 1
      Authority RRs: 0
      Additional RRs: 1
    ▾ Queries
      ▸ zagent779.hola.org: type A, class IN
    ▾ Answers
      ▾ zagent779.hola.org: type A, class IN, addr 107.170.54.54
          Name: zagent779.hola.org
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 600
          Data length: 4
          Address: 107.170.54.54
```

Here as shown we can see the answers in response as well as the nameservers ip address.

19. required screenshots already attached

20.

```
archelaus@archelaus  ~  nslookup www.aiit.or.kr bitsy.mit.edu
;; connection timed out; no servers could be reached
```

also 21,22,23. We cant proceed as we cant reach bitsy.mit.edu. This might be because the server is updated and the time of assignment bitsy was the server being used. Hence, we cant complete rest of the questions with the given dns server.