Computer Assignment-3
Wireshark

Part-I (HTTP)

1. The browser and the server is running on HTTP 1.1 .
   Languages-used : **en-US(US English)**

2. The IP address of my computer is : 10.1.40.17
   The IP address of server is : 10.4.20.103

3. The status code returned is : 200

4. **Last-Modified: Mon, 26 Feb 2018 06:19:02 GMT.**

5. **128** bytes were transferred from server to browser.

7. No, we do not get a "IF-MODIFIED-SINCE" in first GET request

8. Yes, the server returned the contents of file.

9. Yes, there is a "IF-MODIFIED-SINCE" in second GET request
   If-Modified-Since: Mon, 26 Feb 2018 06:59:01 GMT

10. The HTTP status code is : 304

    The phrase is : **HTTP/1.1 304 Not Modified**

    The server did not return the contents of file as the file was not modified so the proxy server directly returned the file.

PART-II (DNS)

1. DNS queries and responses are sent over UDP

2. There is 2 answer provided.

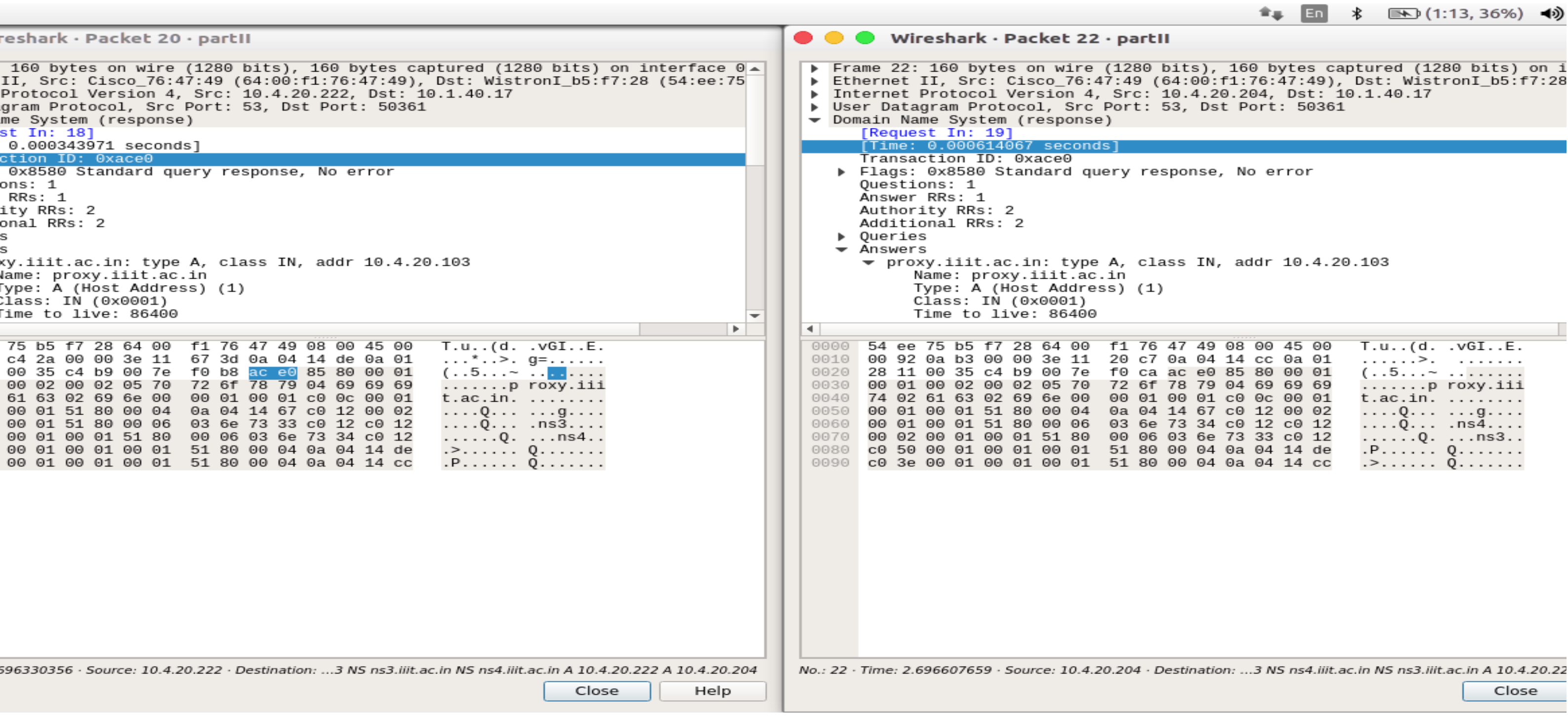
The answer contains the name of the proxy server, its type , class and address.

proxy.iiit.ac.in: type A, class IN, addr 10.4.20.103

3. Yes, the destination IP address of the SYN packet correspond to one of the IP addresses provided in the DNS response message.

4. No, the DNS queries are made only for retrieving the IP address of the server. So number of DNS queries made were 4.

5.



```
 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: WistronI_b5:f7:28 (54:ee:75
Protocol Version 4, Src: 10.4.20.222, Dst: 10.1.40.17
gram Protocol, Src Port: 53, Dst Port: 50361
me System (response)
st In: 18]
 0.000343971 seconds]
ction ID: 0xace0
 0x8580 Standard query response, No error
ons: 1
 RRs: 1
ity RRs: 2
onal RRs: 2
s
s
xy.iiit.ac.in: type A, class IN, addr 10.4.20.103
Name: proxy.iiit.ac.in
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 86400
```

```
 75 b5 f7 28 64 00  f1 76 47 49 08 00 45 00   T.u..(d. .vGI..E.
 c4 2a 00 00 3e 11  67 3d 0a 04 14 de 0a 01   ...*..>. g=......
 00 35 c4 b9 00 7e  f0 b8 ac e0 85 80 00 01   (..5...~ ........
 00 02 00 02 05 70  72 6f 78 79 04 69 69 69   .......p roxy.iii
 61 63 02 69 6e 00  00 01 00 01 c0 0c 00 01   t.ac.in. ........
 00 01 51 80 00 04  0a 04 14 67 c0 12 00 02   ....Q... ...g....
 00 01 51 80 00 06  03 6e 73 33 c0 12 c0 12   ....Q... .ns3....
 00 01 00 01 51 80  00 06 03 6e 73 34 c0 12   ......Q. ...ns4..
 00 01 00 01 00 01  51 80 00 04 0a 04 14 de   .>...... Q.......
 00 01 00 01 00 01  51 80 00 04 0a 04 14 cc   .P...... Q.......
```

596330356 · Source: 10.4.20.222 · Destination: ...3 NS ns3.iiit.ac.in NS ns4.iiit.ac.in A 10.4.20.222 A 10.4.20.204

```
▶ Frame 22: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on i
▶ Ethernet II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: WistronI_b5:f7:28
▶ Internet Protocol Version 4, Src: 10.4.20.204, Dst: 10.1.40.17
▶ User Datagram Protocol, Src Port: 53, Dst Port: 50361
▼ Domain Name System (response)
    [Request In: 19]
    [Time: 0.000614067 seconds]
    Transaction ID: 0xace0
  ▶ Flags: 0x8580 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 2
  ▶ Queries
  ▼ Answers
    ▼ proxy.iiit.ac.in: type A, class IN, addr 10.4.20.103
          Name: proxy.iiit.ac.in
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 86400
```

```
0000  54 ee 75 b5 f7 28 64 00  f1 76 47 49 08 00 45 00   T.u..(d. .vGI..E.
0010  00 92 0a b3 00 00 3e 11  20 c7 0a 04 14 cc 0a 01   ......>.  .......
0020  28 11 00 35 c4 b9 00 7e  f0 ca ac e0 85 80 00 01   (..5...~ ........
0030  00 01 00 02 00 02 05 70  72 6f 78 79 04 69 69 69   .......p roxy.iii
0040  74 02 61 63 02 69 6e 00  00 01 00 01 c0 0c 00 01   t.ac.in. ........
0050  00 01 00 01 51 80 00 04  0a 04 14 67 c0 12 00 02   ....Q... ...g....
0060  00 01 00 01 51 80 00 06  03 6e 73 34 c0 12 c0 12   ....Q... .ns4....
0070  00 02 00 01 00 01 51 80  00 06 03 6e 73 33 c0 12   ......Q. ...ns3..
0080  c0 50 00 01 00 01 00 01  51 80 00 04 0a 04 14 de   .P...... Q.......
0090  c0 3e 00 01 00 01 00 01  51 80 00 04 0a 04 14 cc   .>...... Q.......
```

No.: 22 · Time: 2.696607659 · Source: 10.4.20.204 · Destination: ...3 NS ns4.iiit.ac.in NS ns3.iiit.ac.in A 10.4.20.22

6. I have two destination port: **10.4.20.222** and **10.4.20.204** and these are also the source ports for their respective responses.

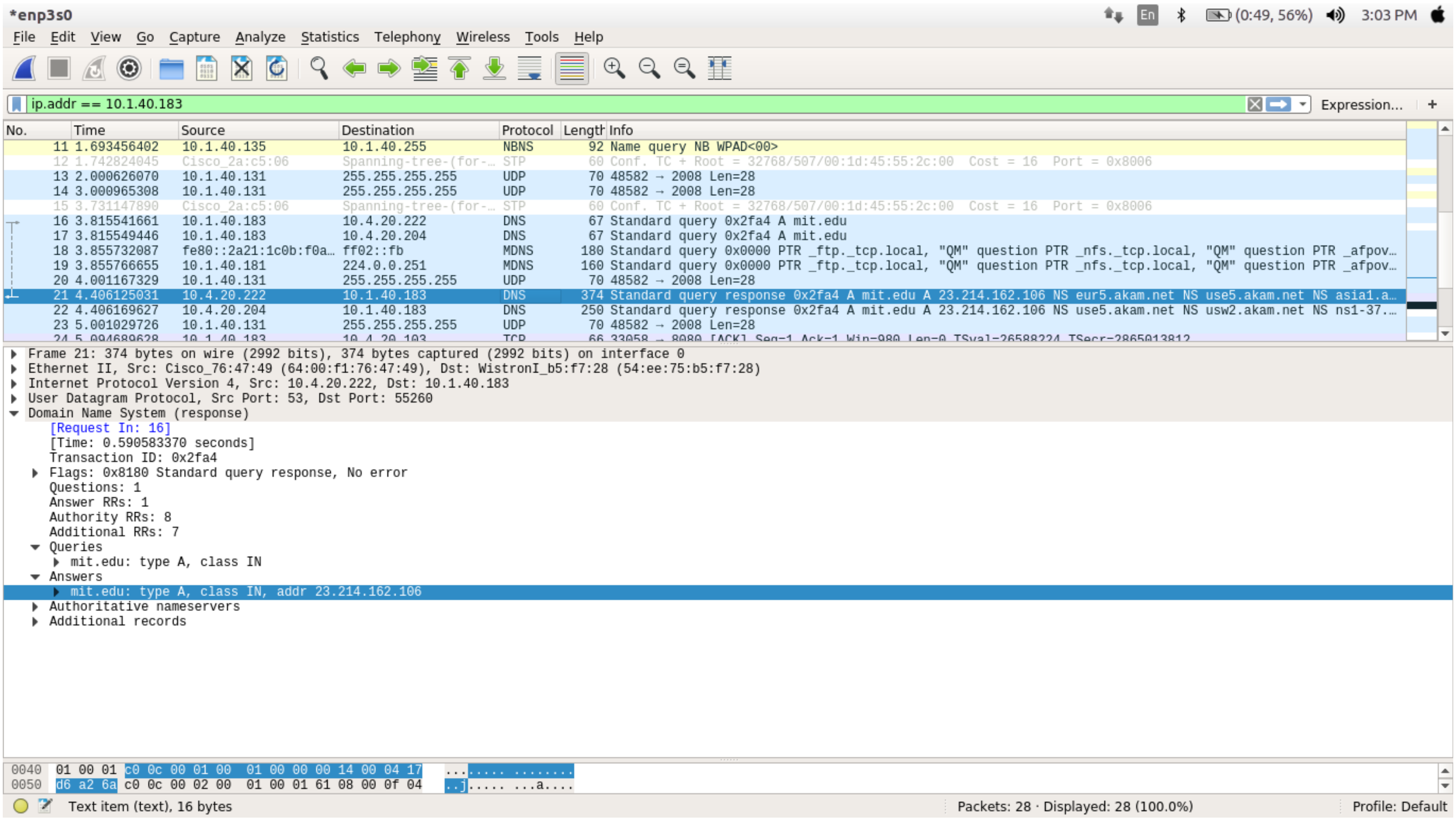
7. DNS query is of **Type:’A’**

No, there are no answers in query messages.

8. DNS response is of **Type:'A'**

Yes the response message contains one answer that is:

mit.edu: type A, class IN, addr 23.214.162.106



*enp3s0
(0:49, 56%)
3:03 PM
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
ip.addr == 10.1.40.183
```

```
No.  Time         Source                Destination           Protocol Length Info
  11 1.693456402  10.1.40.135           10.1.40.255           NBNS       92 Name query NB WPAD<00>
  12 1.742824045  Cisco_2a:c5:06        Spanning-tree-(for-…  STP        60 Conf. TC + Root = 32768/507/00:1d:45:55:2c:00  Cost = 16  Port = 0x8006
  13 2.000626070  10.1.40.131           255.255.255.255       UDP        70 48582 → 2008 Len=28
  14 3.000965308  10.1.40.131           255.255.255.255       UDP        70 48582 → 2008 Len=28
  15 3.731147890  Cisco_2a:c5:06        Spanning-tree-(for-…  STP        60 Conf. TC + Root = 32768/507/00:1d:45:55:2c:00  Cost = 16  Port = 0x8006
  16 3.815541661  10.1.40.183           10.4.20.222           DNS        67 Standard query 0x2fa4 A mit.edu
  17 3.815549446  10.1.40.183           10.4.20.204           DNS        67 Standard query 0x2fa4 A mit.edu
  18 3.855732087  fe80::2a21:1c0b:f0a…  ff02::fb              MDNS      180 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _afpov…
  19 3.855766655  10.1.40.181           224.0.0.251           MDNS      160 Standard query 0x0000 PTR _ftp._tcp.local, "QM" question PTR _nfs._tcp.local, "QM" question PTR _afpov…
  20 4.001167329  10.1.40.131           255.255.255.255       UDP        70 48582 → 2008 Len=28
  21 4.406125031  10.4.20.222           10.1.40.183           DNS       374 Standard query response 0x2fa4 A mit.edu A 23.214.162.106 NS eur5.akam.net NS use5.akam.net NS asia1.a…
  22 4.406169627  10.4.20.204           10.1.40.183           DNS       250 Standard query response 0x2fa4 A mit.edu A 23.214.162.106 NS use5.akam.net NS usw2.akam.net NS ns1-37.…
  23 5.001029726  10.1.40.131           255.255.255.255       UDP        70 48582 → 2008 Len=28
  24 5.094689628  10.1.40.183           10.4.20.103           TCP        66 33058 → 8080 [ACK] Seq=1 Ack=1 Win=980 Len=0 TSval=26588224 TSecr=2865013812
```

```
▸ Frame 21: 374 bytes on wire (2992 bits), 374 bytes captured (2992 bits) on interface 0
▸ Ethernet II, Src: Cisco_76:47:49 (64:00:f1:76:47:49), Dst: WistronI_b5:f7:28 (54:ee:75:b5:f7:28)
▸ Internet Protocol Version 4, Src: 10.4.20.222, Dst: 10.1.40.183
▸ User Datagram Protocol, Src Port: 53, Dst Port: 55260
▾ Domain Name System (response)
    [Request In: 16]
    [Time: 0.590583370 seconds]
    Transaction ID: 0x2fa4
  ▸ Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 8
    Additional RRs: 7
  ▾ Queries
    ▸ mit.edu: type A, class IN
  ▾ Answers
    ▸ mit.edu: type A, class IN, addr 23.214.162.106
  ▸ Authoritative nameservers
  ▸ Additional records
```

```
0040  01 00 01 c0 0c 00 01 00  01 00 00 00 14 00 04 17   ...........·....
0050  d6 a2 6a c0 0c 00 02 00  01 00 01 61 08 00 0f 04   ..j..... ...a....
```

```
Text item (text), 16 bytes          Packets: 28 · Displayed: 28 (100.0%)          Profile: Default
```

9. DNS queries are sent to two IP addresses: **10.4.20.222 and 10.4.20.204**

Yes, it is the IP address of default DNS server.

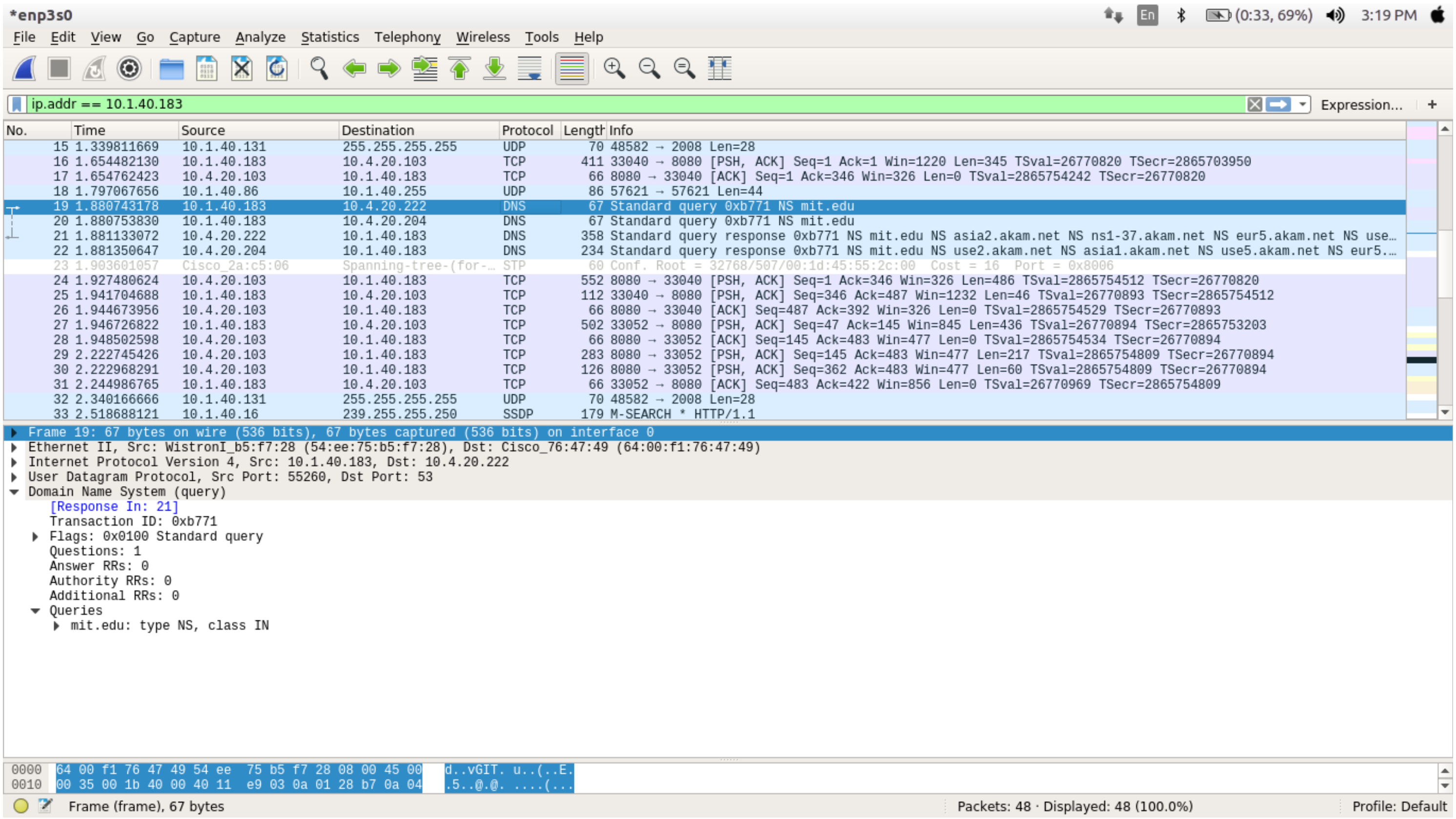
10. The type of DNS query is : **"NS"**

No, the DNS query message does not contain any answers.

11. The response message provides 8 DNS name servers:

1. **asia2.akam.net**
2. **ns1-37.akam.net**
3. **eur5.akam.net**
4. **use2.akam.net**
5. **usw2.akam.net**
6. **asia1.akam.net**
7. **use5.akam.net**
8. **ns1-173.akam.net**

No, the response message does not provide the IP addresses of DNS name servers.



ip.addr == 10.1.40.183

```
No.    Time         Source            Destination          Protocol  Length Info
    15 1.339811669  10.1.40.131       255.255.255.255      UDP           70 48582 → 2008 Len=28
    16 1.654482130  10.1.40.183       10.4.20.103          TCP          411 33040 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=1220 Len=345 TSval=26770820 TSecr=2865703950
    17 1.654762423  10.4.20.103       10.1.40.183          TCP           66 8080 → 33040 [ACK] Seq=1 Ack=346 Win=326 Len=0 TSval=2865754242 TSecr=26770820
    18 1.797067656  10.1.40.86        10.1.40.255          UDP           86 57621 → 57621 Len=44
    19 1.880743178  10.1.40.183       10.4.20.222          DNS           67 Standard query 0xb771 NS mit.edu
    20 1.880753830  10.1.40.183       10.4.20.204          DNS           67 Standard query 0xb771 NS mit.edu
    21 1.881133072  10.4.20.222       10.1.40.183          DNS          358 Standard query response 0xb771 NS mit.edu NS asia2.akam.net NS ns1-37.akam.net NS eur5.akam.net NS use…
    22 1.881350647  10.4.20.204       10.1.40.183          DNS          234 Standard query response 0xb771 NS mit.edu NS use2.akam.net NS asia1.akam.net NS use5.akam.net NS eur5.…
    23 1.903601057  Cisco_2a:c5:06    Spanning-tree-(for-… STP           60 Conf. Root = 32768/507/00:1d:45:55:2c:00  Cost = 16  Port = 0x8006
    24 1.927480624  10.4.20.103       10.1.40.183          TCP          552 8080 → 33040 [PSH, ACK] Seq=1 Ack=346 Win=326 Len=486 TSval=2865754512 TSecr=26770820
    25 1.941704688  10.1.40.183       10.4.20.103          TCP          112 33040 → 8080 [PSH, ACK] Seq=346 Ack=487 Win=1232 Len=46 TSval=26770893 TSecr=2865754512
    26 1.944673956  10.4.20.103       10.1.40.183          TCP           66 8080 → 33040 [ACK] Seq=487 Ack=392 Win=326 Len=0 TSval=2865754529 TSecr=26770893
    27 1.946726822  10.1.40.183       10.4.20.103          TCP          502 33052 → 8080 [PSH, ACK] Seq=47 Ack=145 Win=845 Len=436 TSval=26770894 TSecr=2865753203
    28 1.948502598  10.4.20.103       10.1.40.183          TCP           66 8080 → 33052 [ACK] Seq=145 Ack=483 Win=477 Len=0 TSval=2865754534 TSecr=26770894
    29 2.222745426  10.4.20.103       10.1.40.183          TCP          283 8080 → 33052 [PSH, ACK] Seq=145 Ack=483 Win=477 Len=217 TSval=2865754809 TSecr=26770894
    30 2.222968291  10.4.20.103       10.1.40.183          TCP          126 8080 → 33052 [PSH, ACK] Seq=362 Ack=483 Win=477 Len=60 TSval=2865754809 TSecr=26770894
    31 2.244986765  10.1.40.183       10.4.20.103          TCP           66 33052 → 8080 [ACK] Seq=483 Ack=422 Win=856 Len=0 TSval=26770969 TSecr=2865754809
    32 2.340166666  10.1.40.131       255.255.255.255      UDP           70 48582 → 2008 Len=28
    33 2.518688121  10.1.40.16        239.255.255.250      SSDP         179 M-SEARCH * HTTP/1.1
```

```
▶ Frame 19: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▶ Ethernet II, Src: WistronI_b5:f7:28 (54:ee:75:b5:f7:28), Dst: Cisco_76:47:49 (64:00:f1:76:47:49)
▶ Internet Protocol Version 4, Src: 10.1.40.183, Dst: 10.4.20.222
▶ User Datagram Protocol, Src Port: 55260, Dst Port: 53
▼ Domain Name System (query)
    [Response In: 21]
    Transaction ID: 0xb771
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ mit.edu: type NS, class IN
```

```
0000  64 00 f1 76 47 49 54 ee  75 b5 f7 28 08 00 45 00   d..vGIT. u..(..E.
0010  00 35 00 1b 40 00 40 11  e9 03 0a 01 28 b7 0a 04   .5..@.@. ....(...
```

Frame (frame), 67 bytes   Packets: 48 · Displayed: 48 (100.0%)   Profile: Default

PART-III (TCP)

Part-A

1. IP address: **192.168.1.102**
   Port Number: **1161**

2. IP address of server : **128.119.245.12**
   It is **receiving and sending** at port number **80**

Part-B

1. The sequence number is : **0** (relative sequence number)

   The SYN bit identifies that the segment is SYN segment as the SYN bit is **1**
   Flags: 0x002 (SYN)

2. The sequence number of SYNACK is : **0** (relative sequence number)

   Value of acknowledgment field : **1**

   Acknowledgement field contains value of sequence number of last successfully received packet.

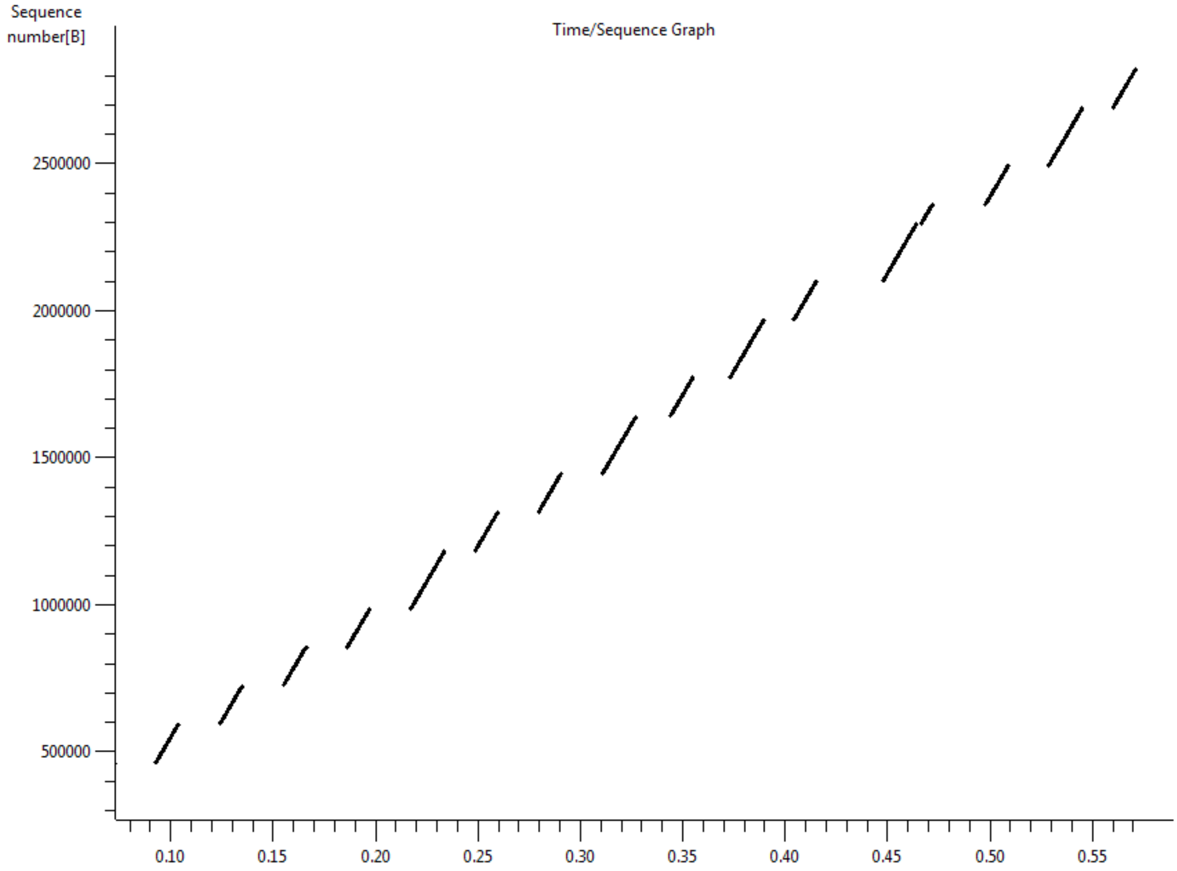
   SYN and ACK bit is set to 1 on an SYNACK segment
   Flags: 0x012 (SYN, ACK)

3. The sequence number is : **1** (relative sequence number)

4. The length of first 6 TCP segments is:
   a. 565
   b. 1460
   c. 1460
   d. 1460
   e. 1460
   f. 1460

5. The minimum amount of buffer available is **5840 bytes** which is the window size of first ACK

6. There are no retransmitted segments in the trace file. As we can see in the diagram that all sequence numbers from source to destination are increasing monotonically w.r.t. time. If there is retransmitted segment , the sequence number of this segment should be smaller than those of its neighboring segments.



Part-IV (UDP)

1. It contains 4 fields :

    a. Source Port
    b. Destination Port
    c. Length
    d. Checksum

2. The length field indicates the length in bytes of **UDP header** and **UDP data.** The value in the length field is the sum of the 8 header bytes, plus the 42 encapsulated data bytes.

3. Yes, the source address is my IP address : **“10.1.40.162”**

4. The destination address is : **“10.4.20.204”**

5. **65527** is the maximum number of bytes that can be included in a UDP payload

6. **65535** is the maximum port number available.

7. The protocol number is : **17**

8. The UDP checksum is calculated as the 16-bit one’s complement of the one’s complement sum of a pseudo header of information from the IP header, the UDP header, and the data. This is padded as needed with zero bytes at the end to make a multiple of two bytes. If the checksum is
computed to be 0, it must be set to 0xFFFF

9. The port numbers just gets interchanged. The source port in first packet becomes the destination port of response to first packet and similar case for destination port of destination port of first packet.