WIRESHARK

Pranay Gupta 20161088
Shubh Maheshwari 20161170

Part 1 (HTTP)

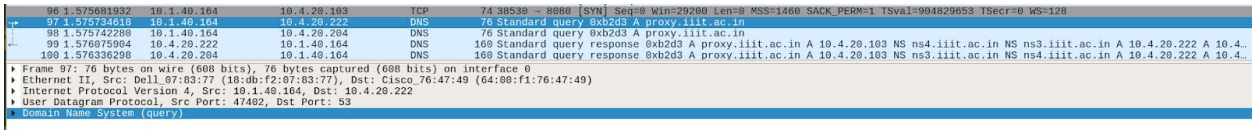
Part A :

1) Browser - HTTP 1.1; Server - HTTP 1.1; Accept Language en-US,en;q=0.5
2) Computer IP - 10.1.40.164 ; Server IP - 10.4.20.103
3) 200 OK
4) Last Modified : Mon, 26 Feb 2018 06:59:01 GMT
5) 128

Part B.

1) No.
2) Yes. All the contents are available in the Line-Based text data field
3) Yes it contains the if-modified since flag. If-Modified-Since : If-Modified-Since: If-Modified-Since: Mon, 26 Feb 2018 06:59:01 GMT. This contains the time and date of the last modification of the file from the previous GET request.
4) The status code returned is 304 Not Modified. This does not explicitly return the contents of the file because its loaded from the cache.

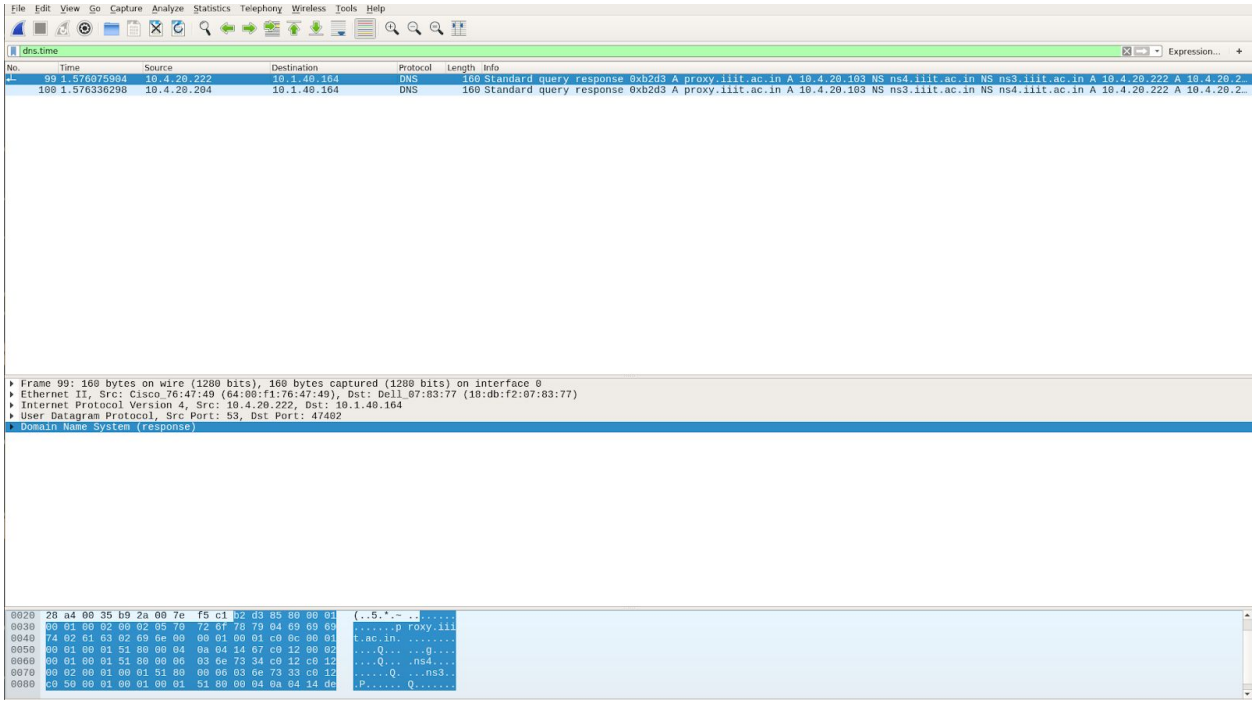
Part 2(DNS)



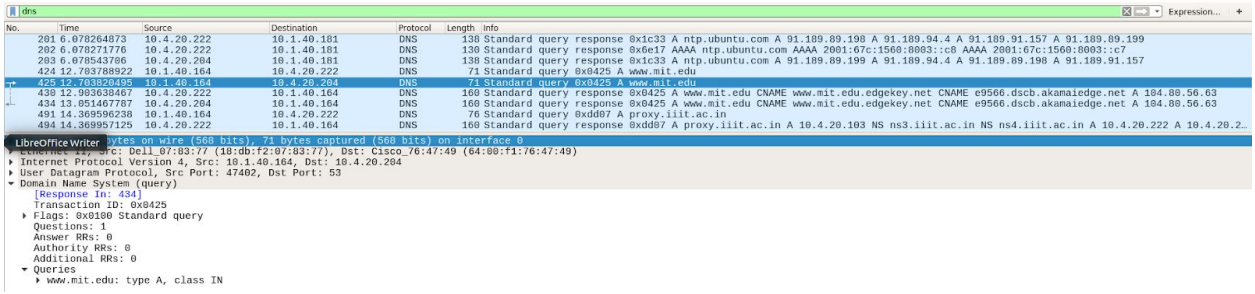
1) UDP
2) I received 1 answer in each of the response messages.

```
▼ 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
      Data length: 4
      Address: 10.4.20.103
```

3) Yes. They both have the ip address of 10.4.20.103. Which was the provided in the answers of the dns response messages.
4) No.

5) 

6) Destination port of DNS query message is 53. Source port of DNS query message is also 53.
7) The DNS query message is of type A. It does not contain any answers.



8) The response message contains 3 answers. One answer is of type A and the other two are of type CNAME.3
9) The DNS query is sent to the 10.4.20.222.Yes.
10) The query message is of type NS and it does not contain any answers.
11) The dns response message provides several MIT nameservers.
    a) use2.akam.net
    b) asia2.akam.net
    c) use5.akam.net
    d) usw2.akam.net
    e) ns1-173.akam.net
    f) asia1.akam.net
    g) ns1-37.akam.net
    h) eur5.akam.net

    Their IP addresses can be found under the additional records header

Part 3(TCP)

1) Source - IP address: 192.168.1.102, Port Number: 1161
   Destination - IP address 128.119.245.12, Port Number: 80
2) The IP address of gaia.cs.umass.edu is 128.119.245.12 (todo).
3) Sequence number of the TCP SYN segment is used to initiate the TCP connection between the client computer and gaia.cs.umass.edu. The value is 0 in the given trace. The syn flag bit is used to identify the syn segment.
4) The sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN is 0. The value of the ACKnowledgement field in the SYNACK segment is 1. The value of the ACKnowledgement field in the SYNACK segment is determined by adding 1 to the initial sequence number of SYN segment from the client computer. Here, the initial sequence number of the SYN segment from the client computer is 0, thus the value of the acknowledgement field in the SYN_ACK segment is 1. The SYN flag and Acknowledgement flag in the segment are set to 1 (Set) and they indicate that this segment is a SYNACK segment.
5) The sequence number of this segment has the value of 1.
6) Length of 1st TCP segment is 565 bytes and length of other 5 TCP segments is 1460 bytes.
7) The minimum amount of buffer space (receiver window) advertised at gaia.cs.umass.edu for the entire trace is 5840 byte. No, the sender is not throttled due to lacking of receiver buffer space.
8) No, there are no retransmitted segments in the trace file. This can verified by checking whether the sequence numbers of the TCP segments in the given trace are monotonically increasing or not.

Part 4(UDP)

1) There are 4 fields in the UDP header
   a) Source Port
   b) Destination Port
   c) Length
   d) Checksum
2) The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next. The length is 36. (28 data bytes + 8 bytes of header).

3) Yes, The source address is same as my ip address.

4) The destination address is 255.255.255.255
5) (2^16)-1-8(header size) = 65527
6) 2^16 -1 = 65535
7) The IP protocol number for UDP is 0x11 hex system. (17 in decimal system)
8) It's also a 16-bit field of one's complement of one's complement sum of a pseudo UDP header + UDP datagram. The Pseudo UDP header also consists of 5 fields,
    - source address: 32 bits/4 bytes, taken from IP header
    - destination address: 32 bits/4 bytes, taken from IP header
    - reserved: 8 bits/1 byte, set to all 0s.
    - protocol: 8 bits/1 byte, taken from IP header
    - length
9) The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.