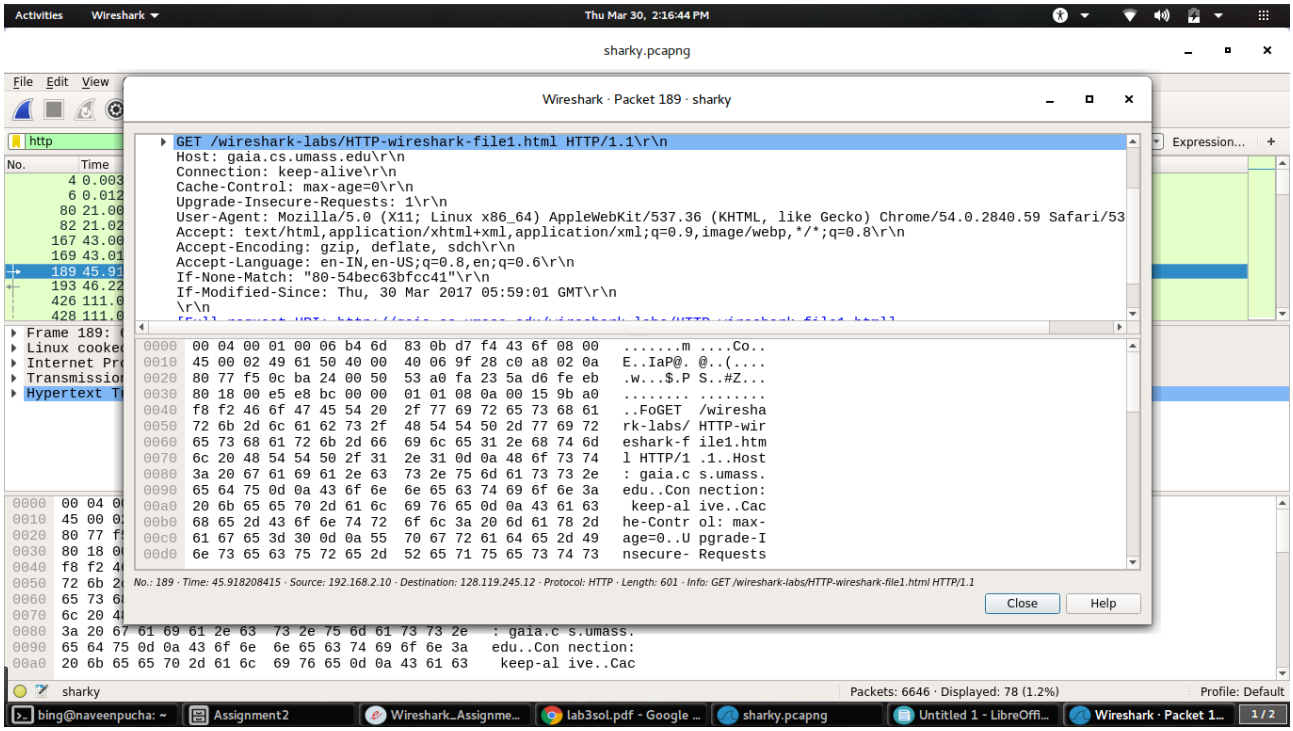
WIRESHARK ASSIGNMENT
Computer Networks
Sai Naveen Pucha
201502013

PART 1

A

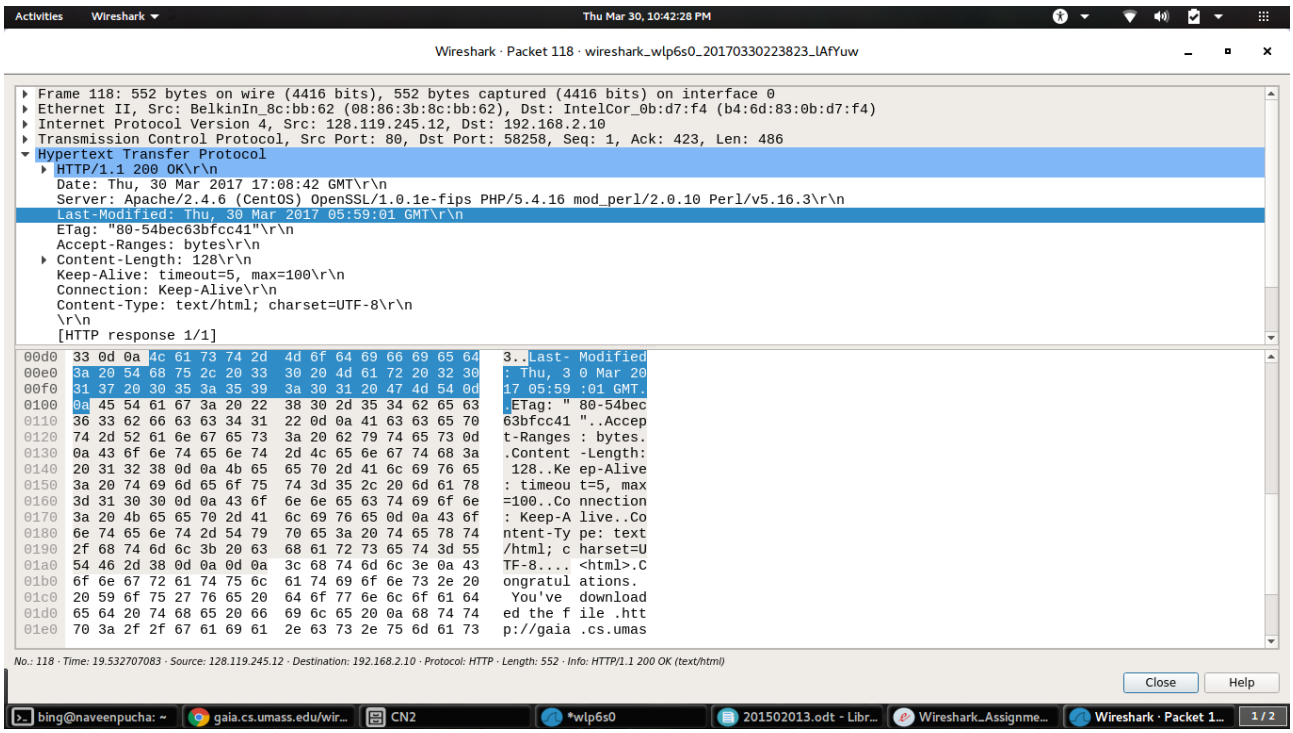
1) My browser is running http version 1.1. My server is running http 1.1 .
Accept-Language : en-IN, en-US; q=0.8,en; q=0.6\r\n



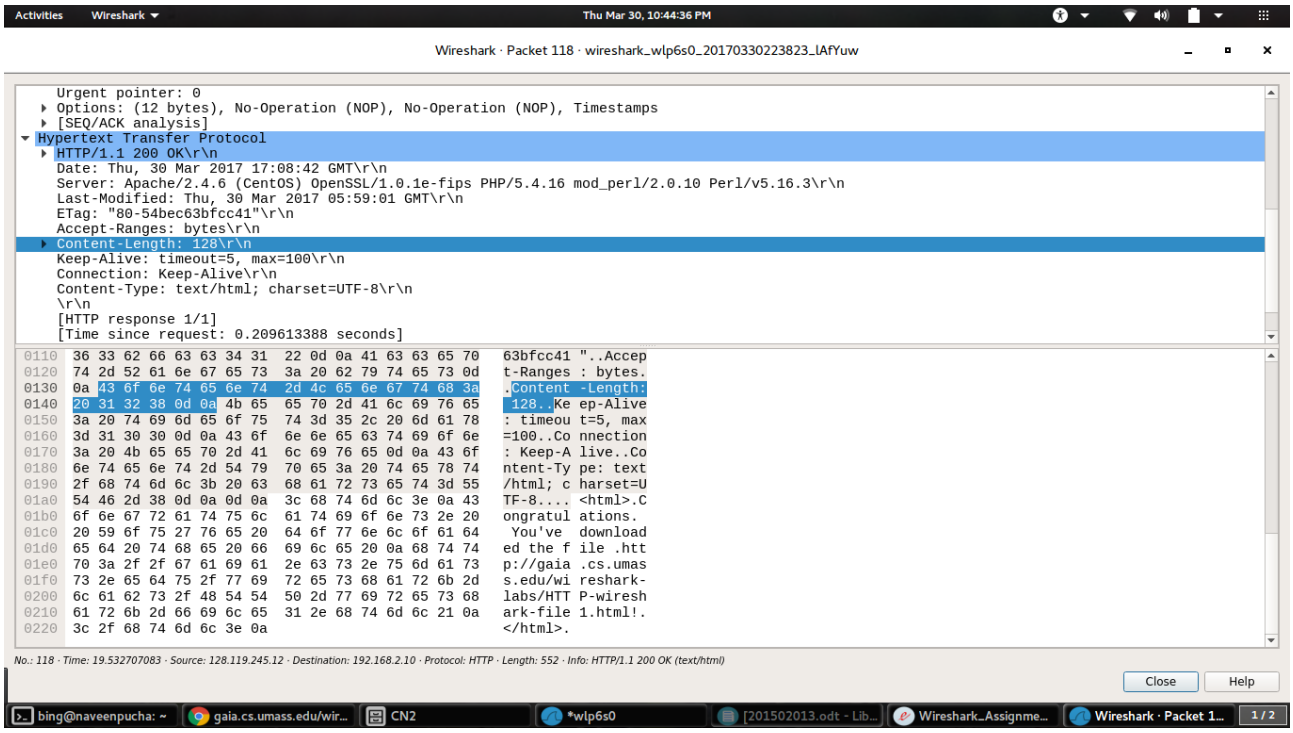
2) The IP address of my computer is 192.168.2.10(this is a virtual address assigned)
The IP address of the gaia.cs.umass.edu server is 128.119.245.12

3) 200 is the status code returned from the server to my browser

4) The file is last modified on Thu, 30 Mar 2017 05:59:01 GMT\r\n



5) The content length is 128 bytes

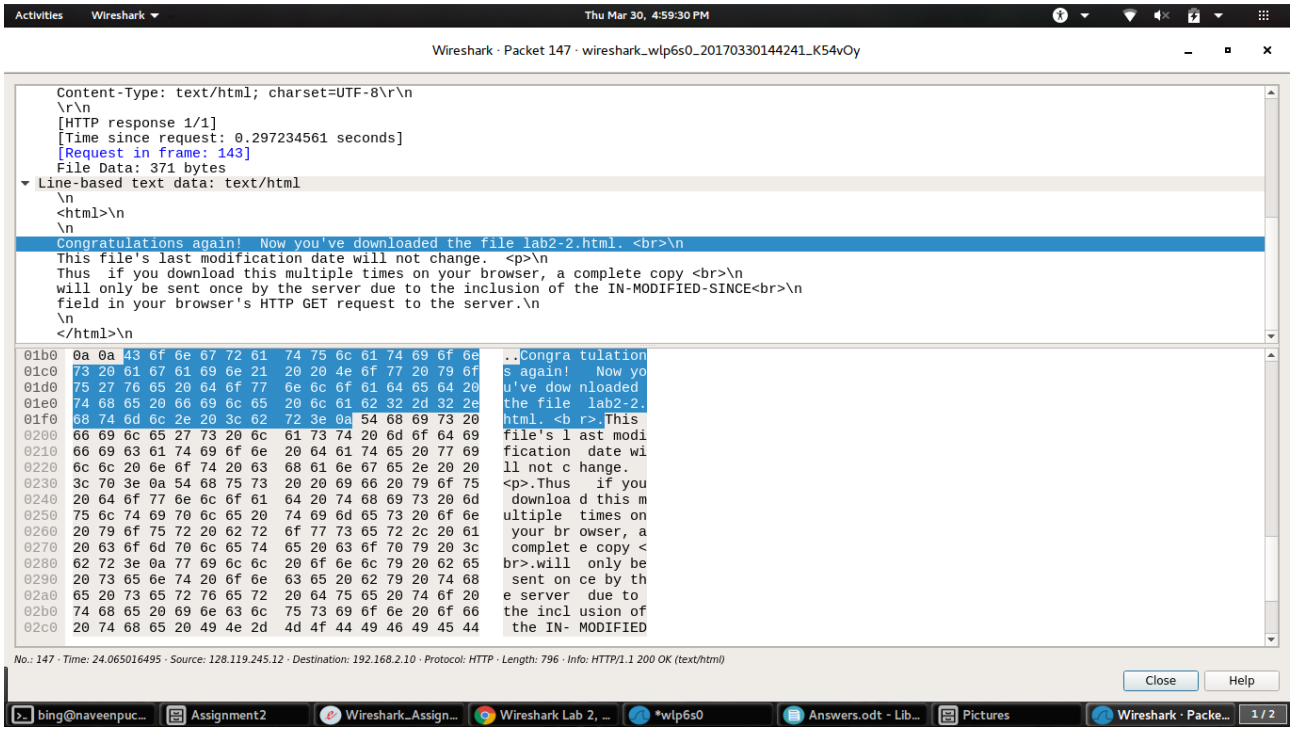


6) No, the raw data appears to match up exactly with what is shown in the packet-listing window.

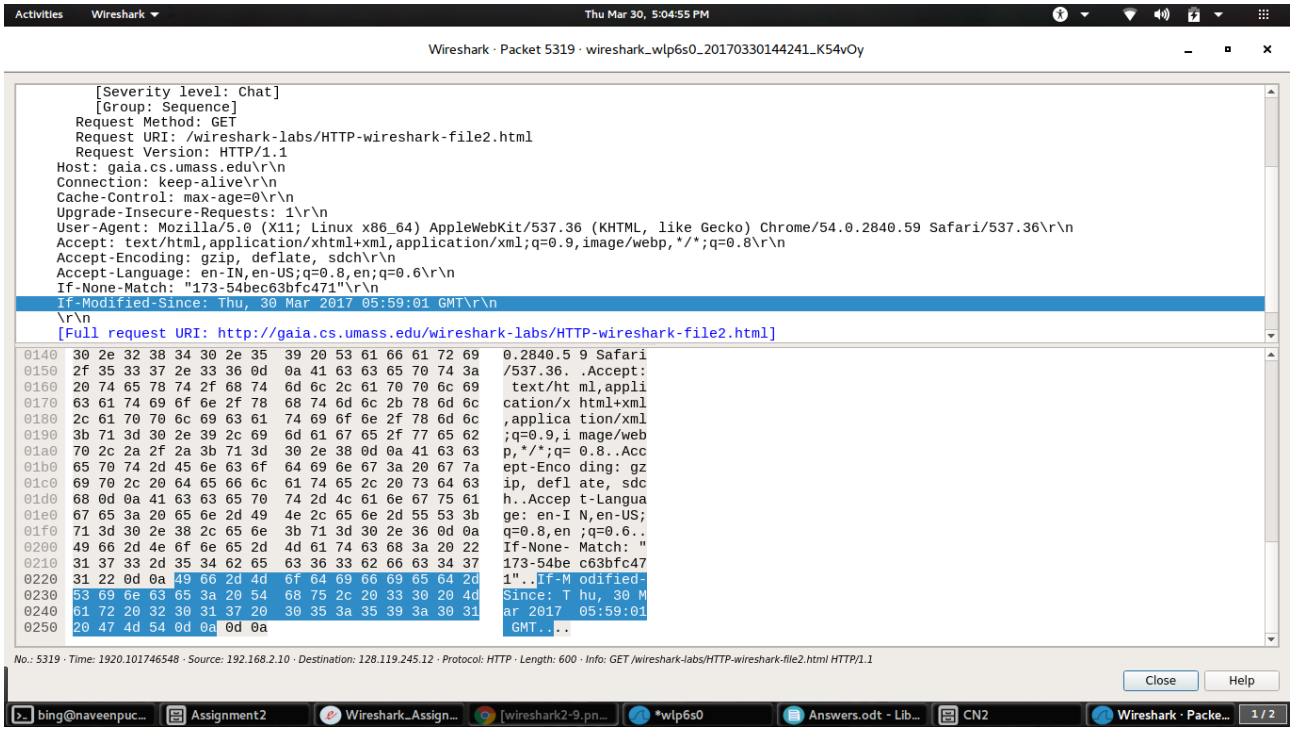
B

7) There is no IF-MODIFIED-SINCE line in the HTTP GET in the GET message.

8) The server did return the contents of the file. There is section “Line-Based Text Data” which has what the server has sent back to the browser as shown in the screenshot.

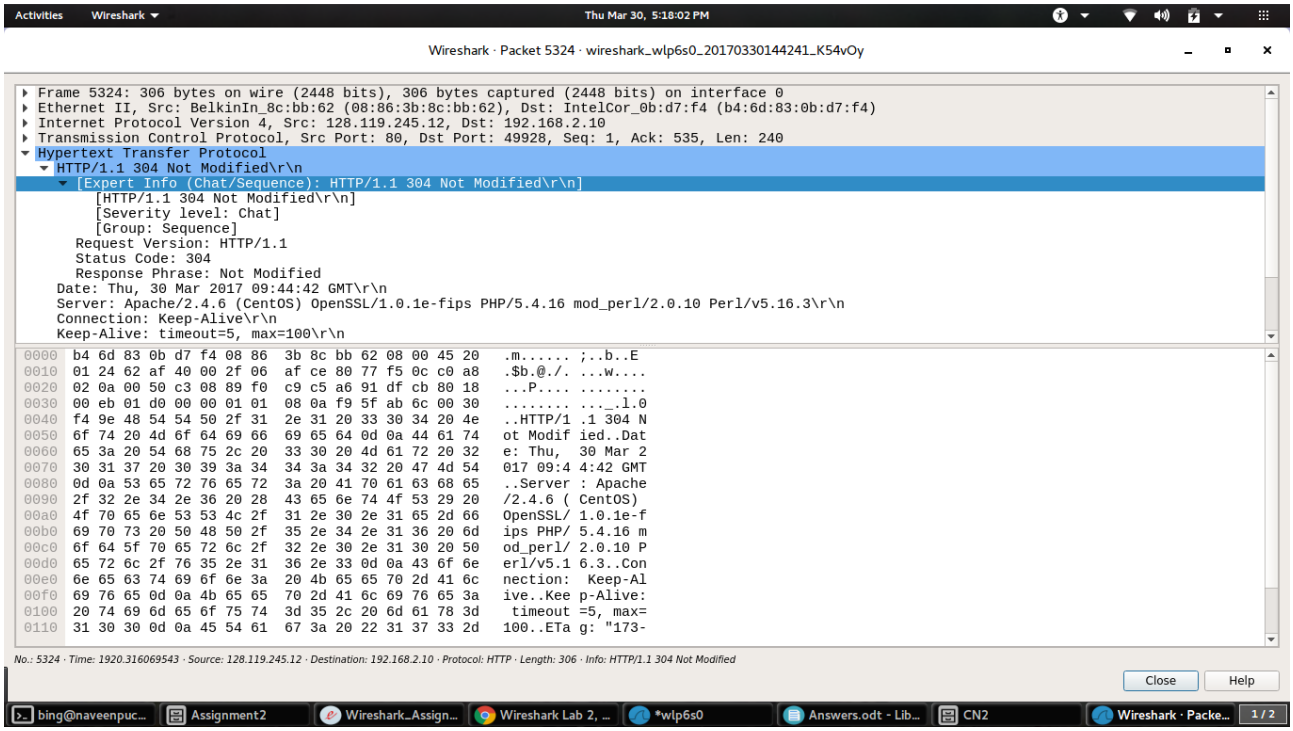


9) Yes
If-Modified-Since: Thu, 30 Mar 2017 05:59:01 GMT\r\n



10) The http status code for this is 304: Not Modified

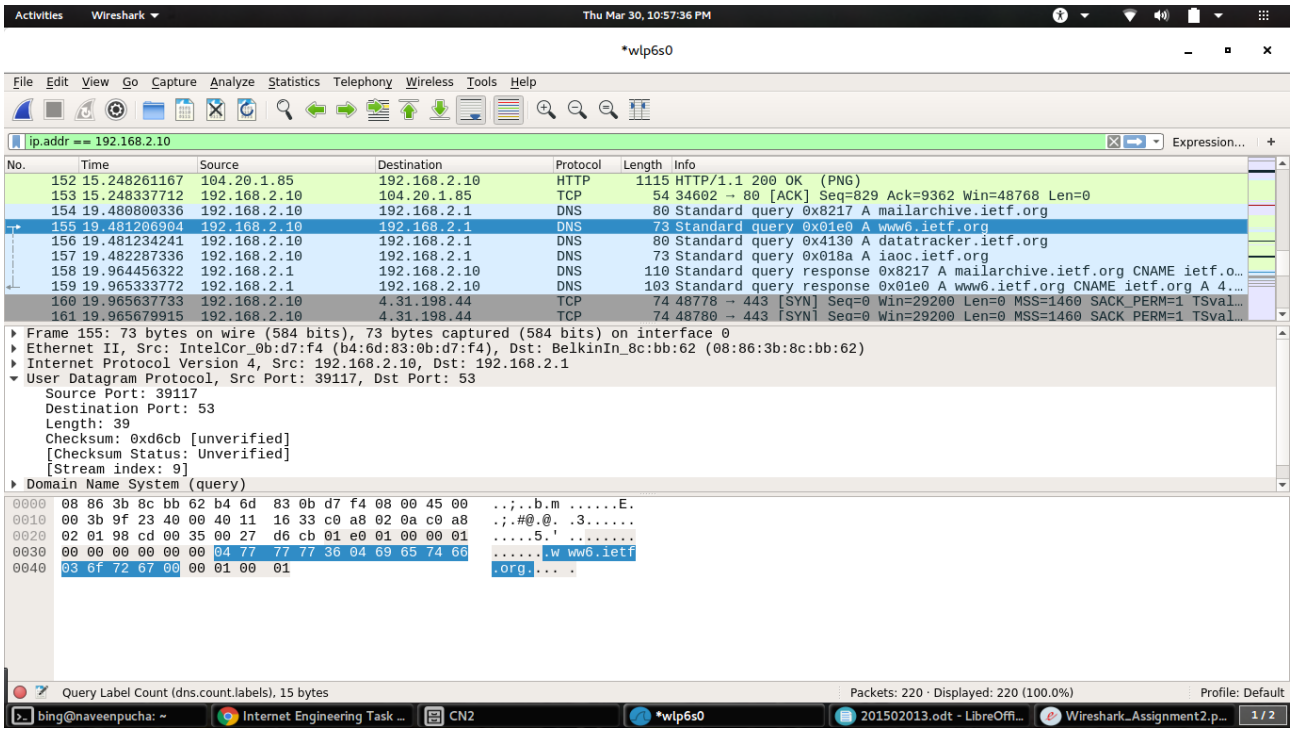
The server did not return the contents of the file because the browser simply retrieved the contents from its cache. If the file had been modified since it was last accessed, it might have returned the contents of the file. Check the below screenshot for reference.



PART 2

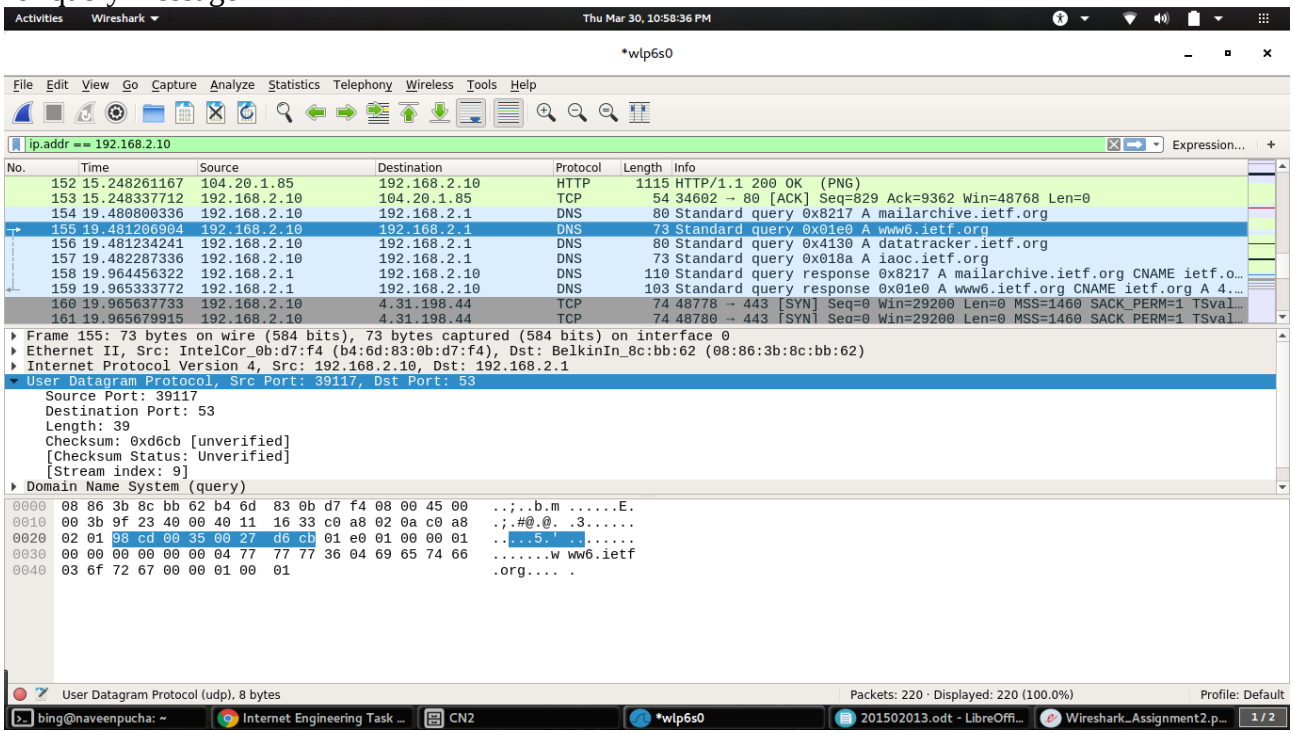
A

1) Related to the DNS query the response messages are sent over UDP

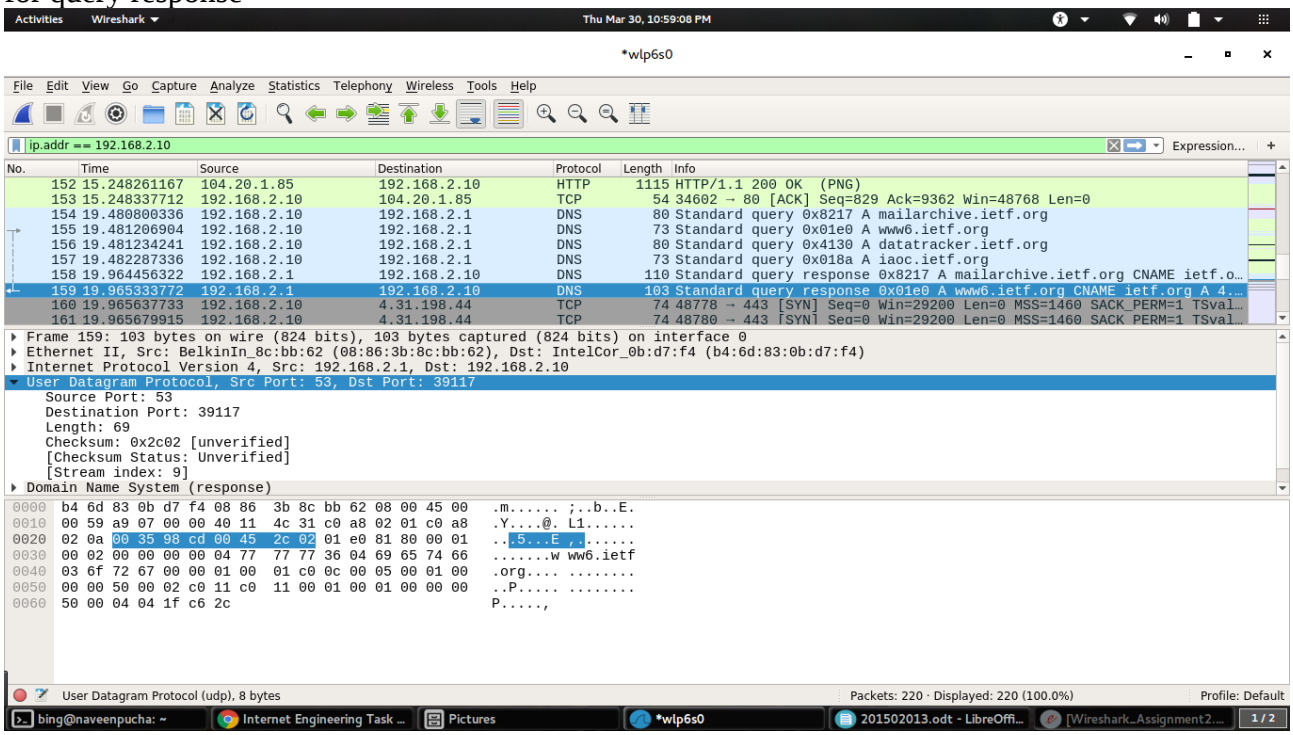


2) Destination Port : 53 for query message Source Port : 53 for query response Check below screenshots for reference.

for query message

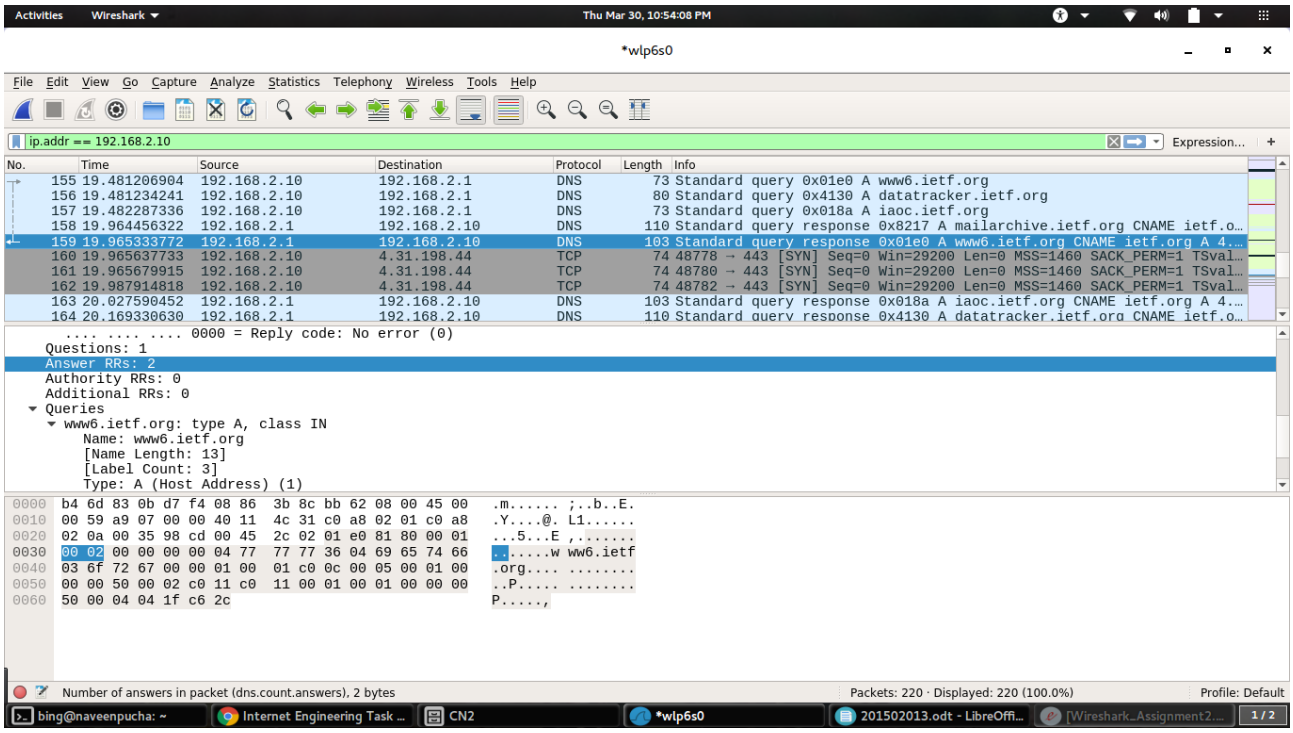


for query response



3) The IP address of the local DNS server is 192.168.2.1 and the IP address of the to which the DNS query message is sent to is also 192.168.2.1. Yes, as we can see that the IP addresses are the same. As we can see the IP address of the destination in the screenshot of the 2nd question of part 2.

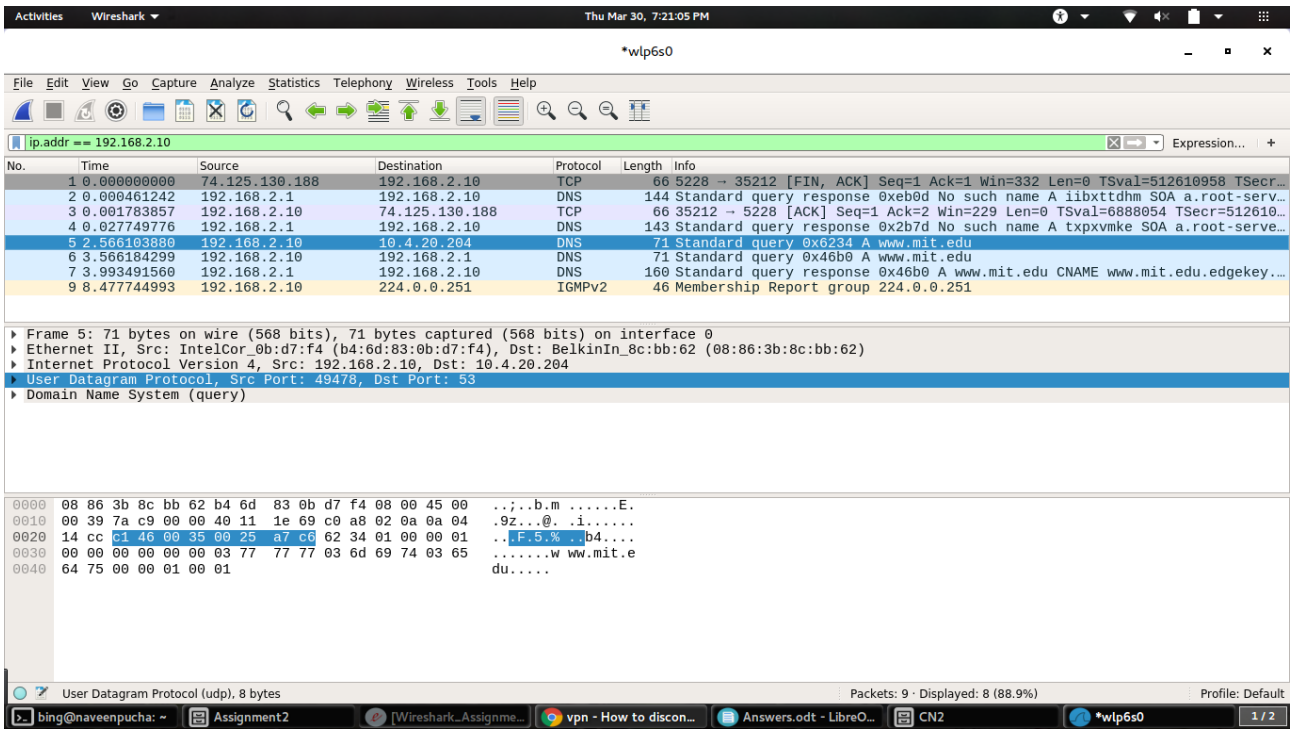
4) There are 2 answers in the response. The answer has 1 type CNAME and 1 type A queries, containing the website name and host address respectively.



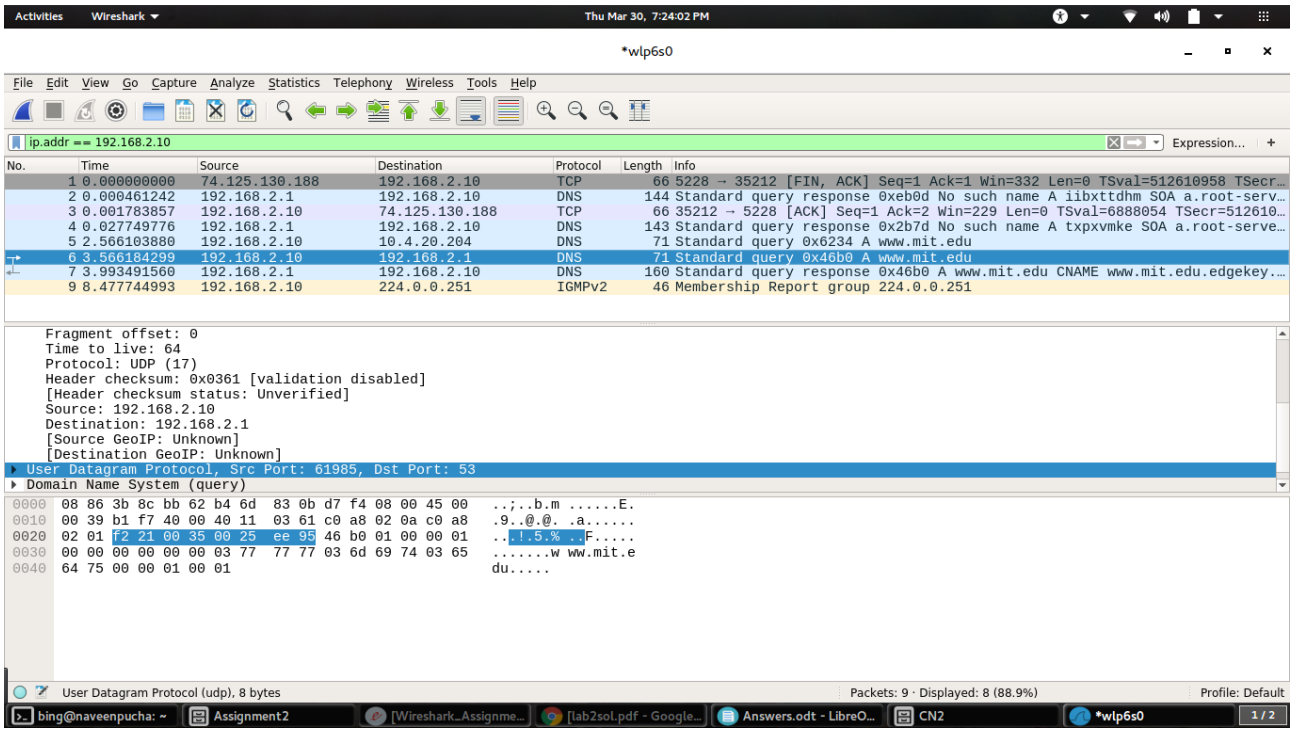
5) As shown in the above screenshot the destination address is 212.110.167.151 This is address provided by the DNS server.

6) No all the images are loaded from the website. So no additional DNS queries are necessary.

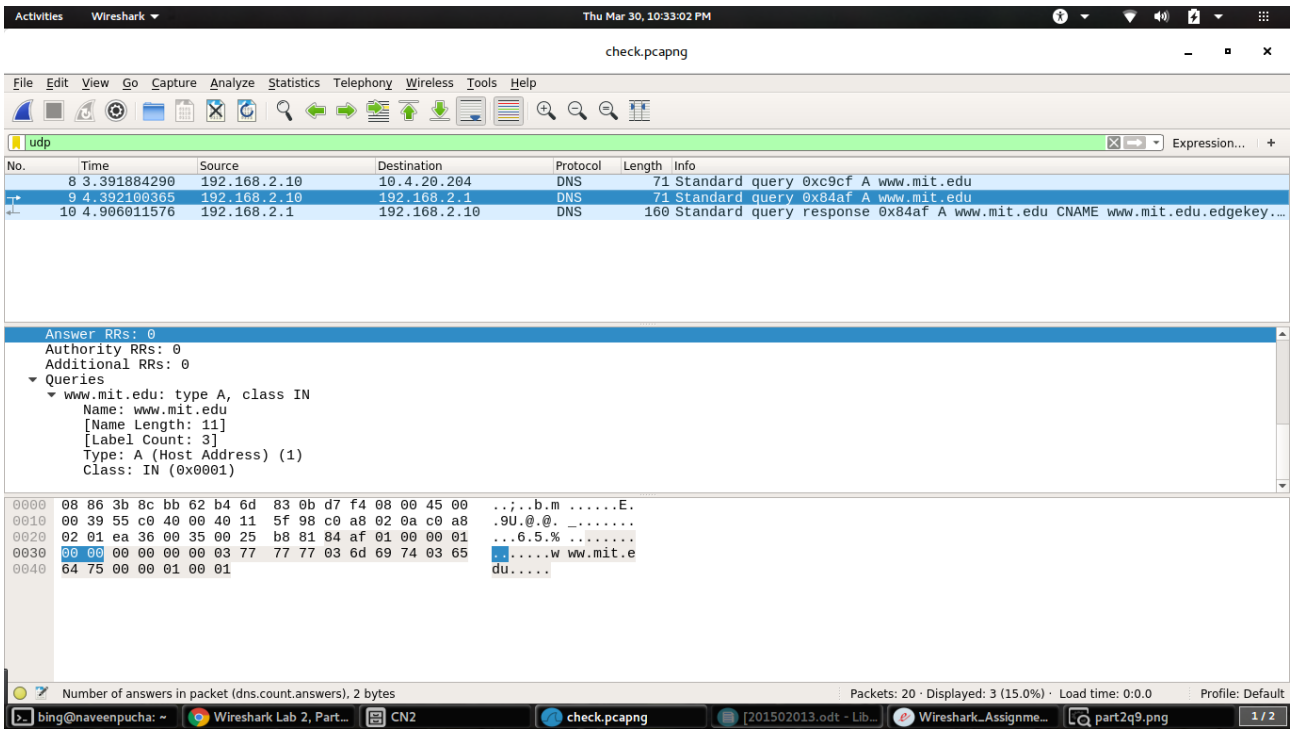
7) The destination port is 53 and the source port is 49478



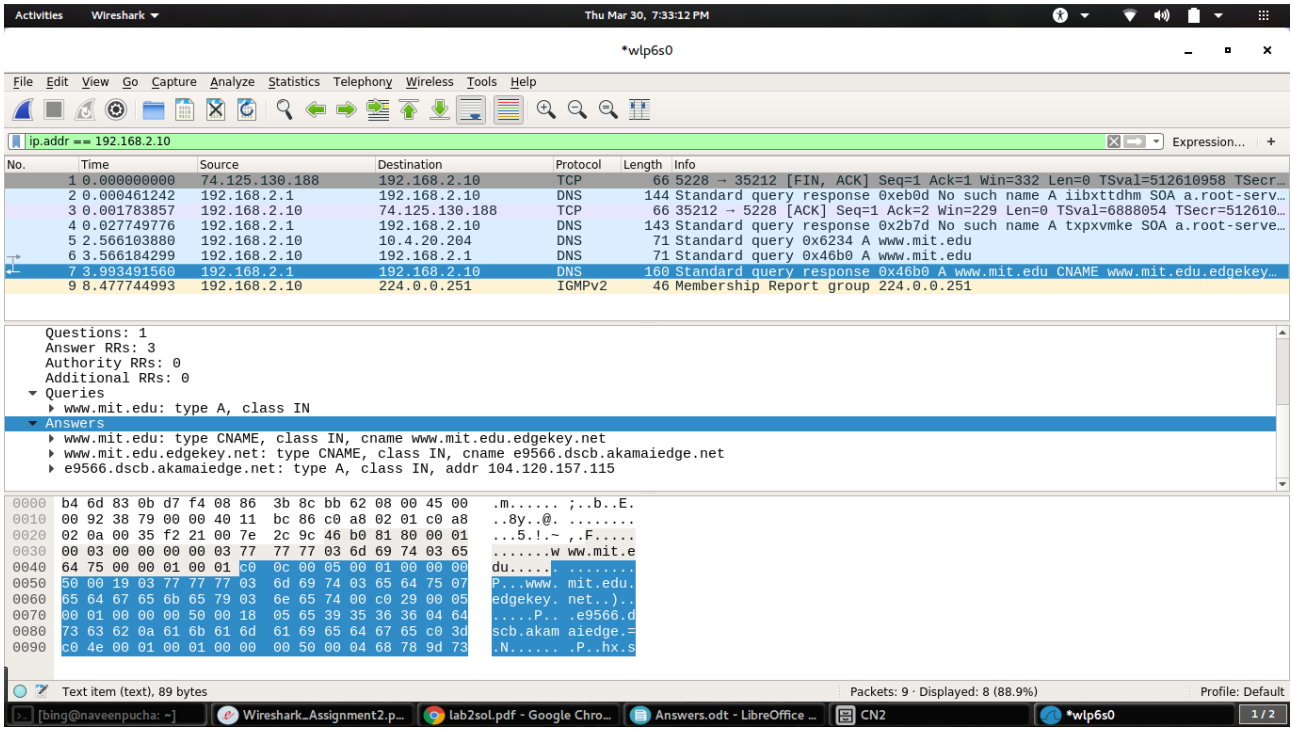
8) It is being sent to 192.168.2.1. Yes it is the IP address of the default local DNS server.



9) It is a Type A query. Yes the query contains answers.

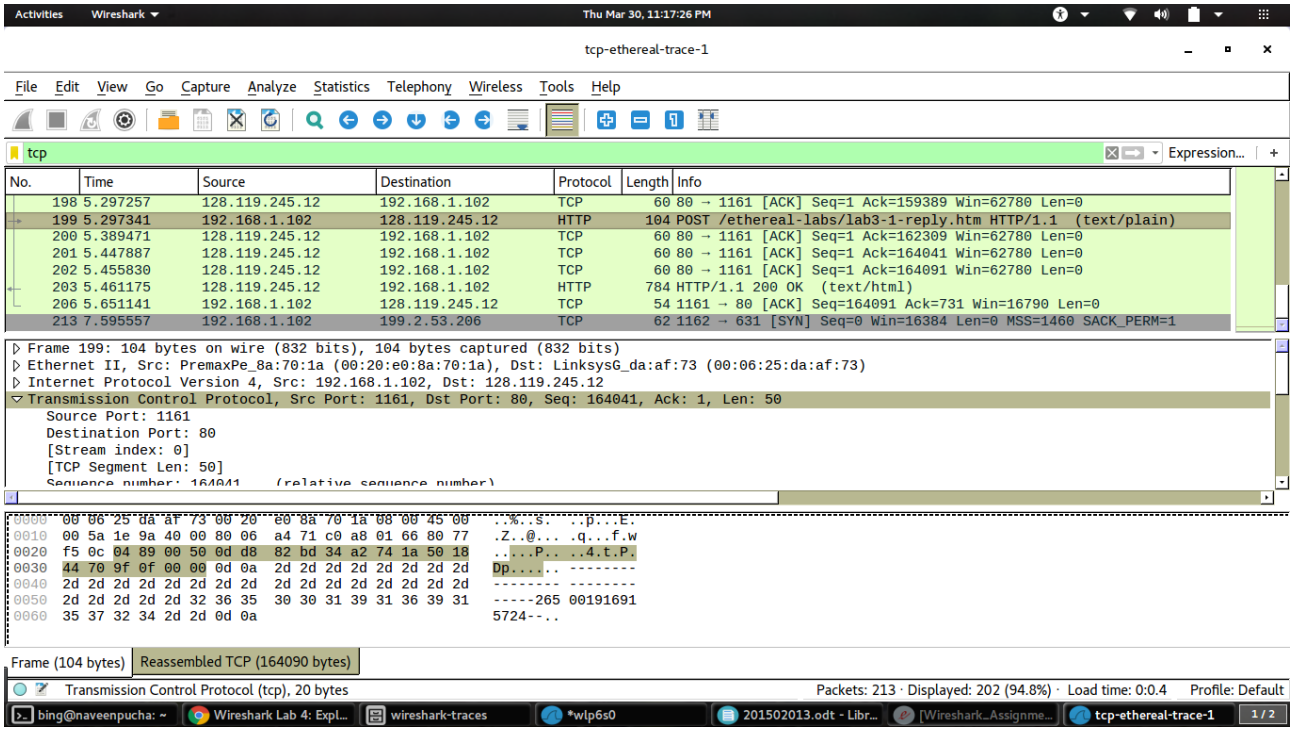


10) There are “Three” answers provided. Two answers are of type CNAME and one is a host address.

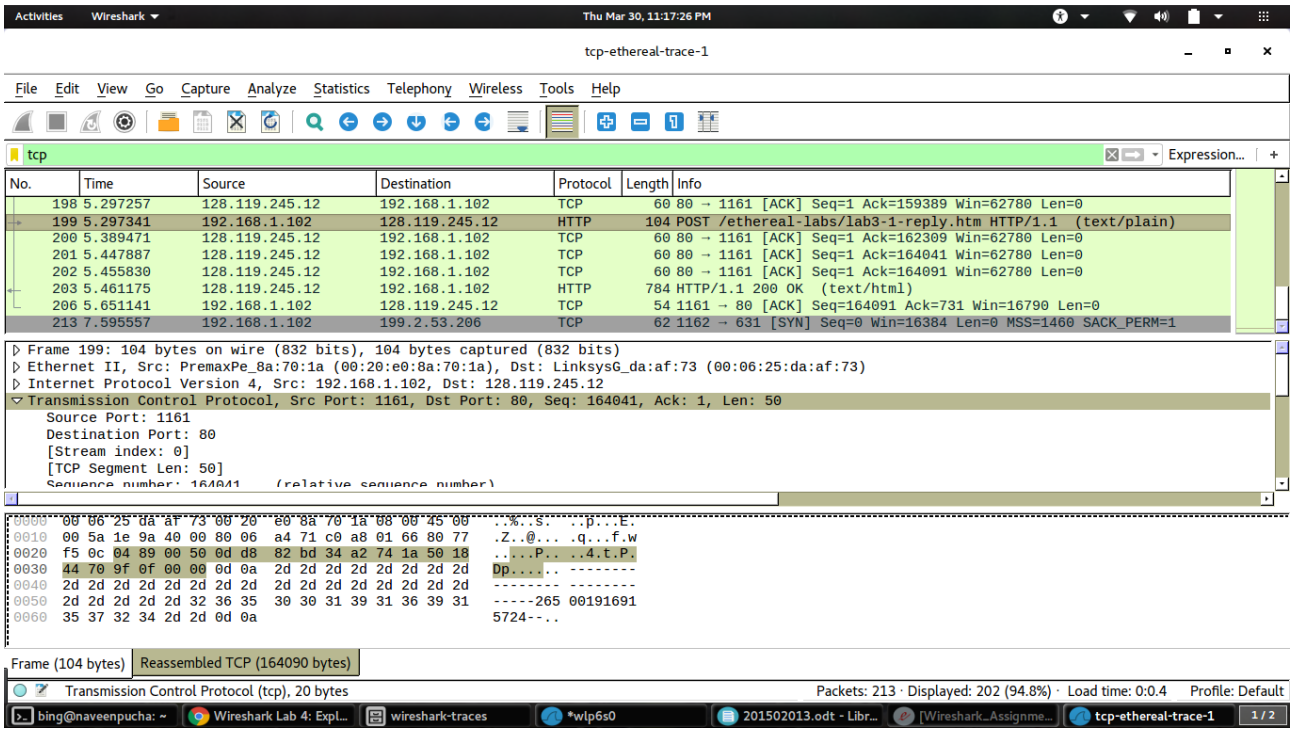


PART 3

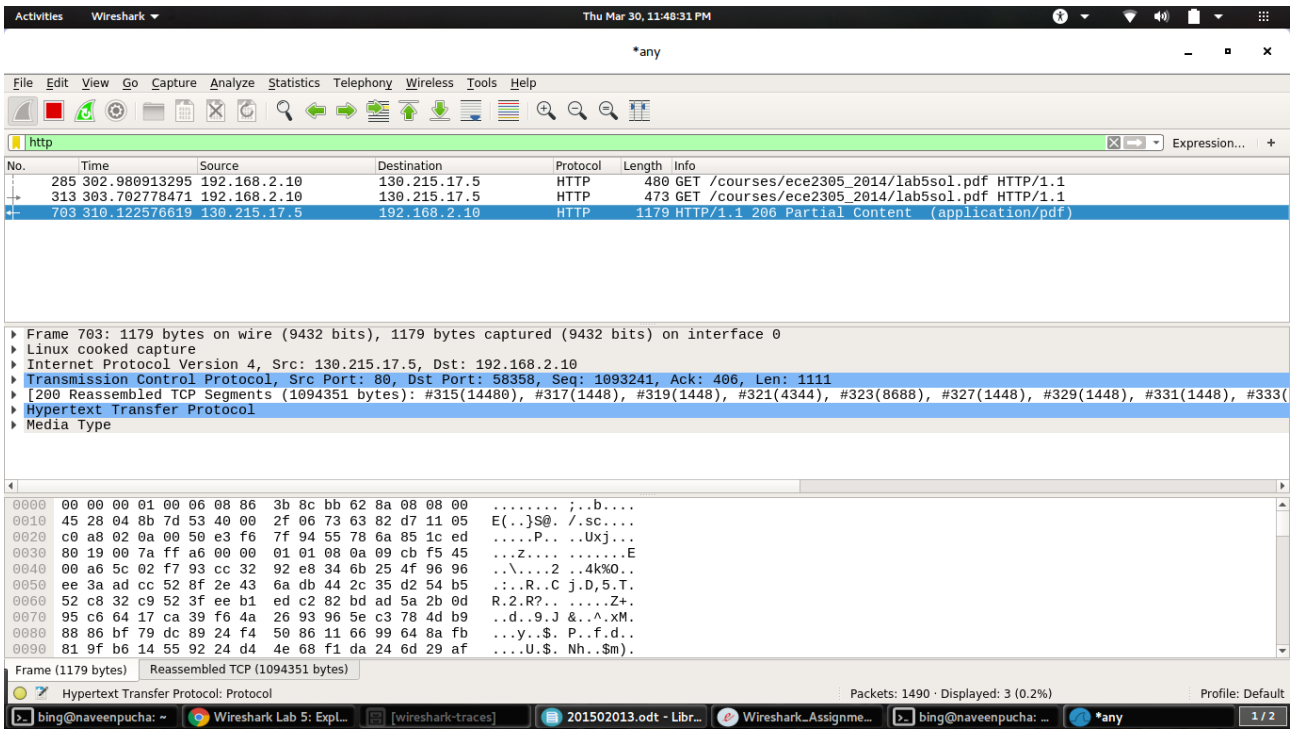
1) The source IP address is 192.168.1.102 using port 1161



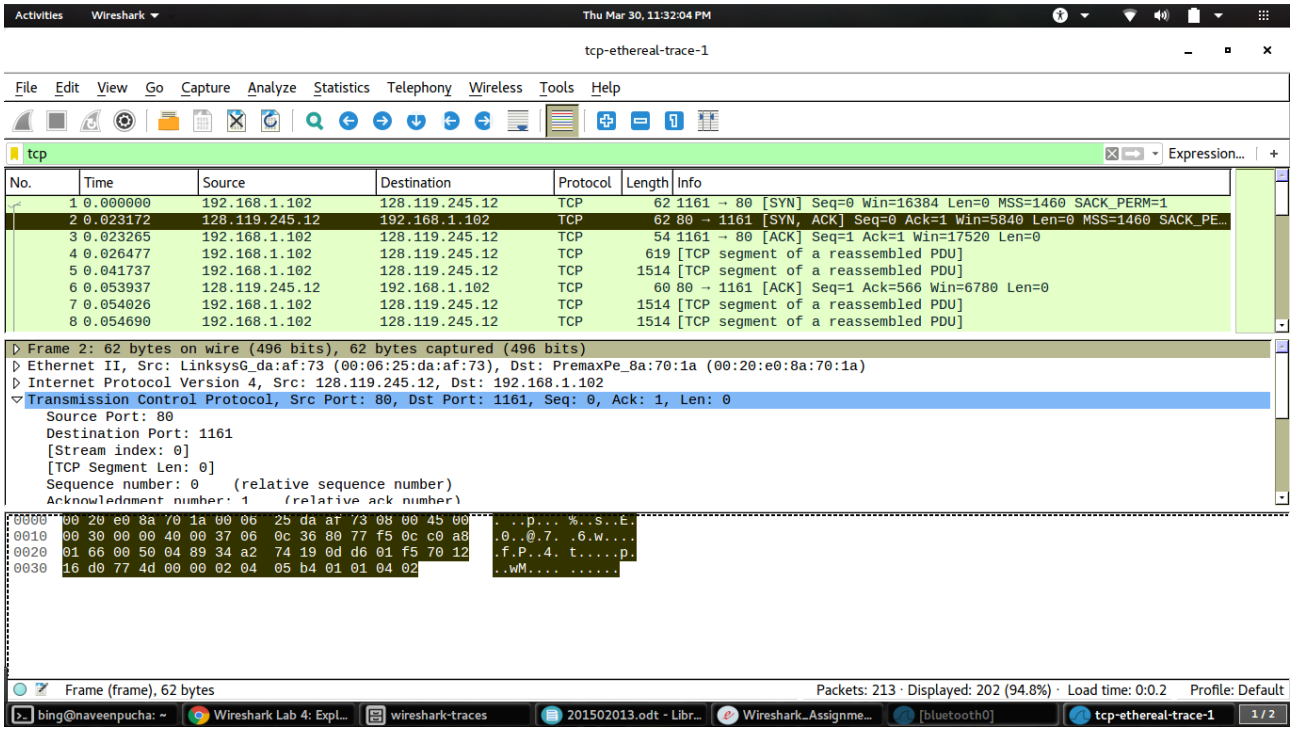
2) The destination IP address is 128.119.245.12 using port 80



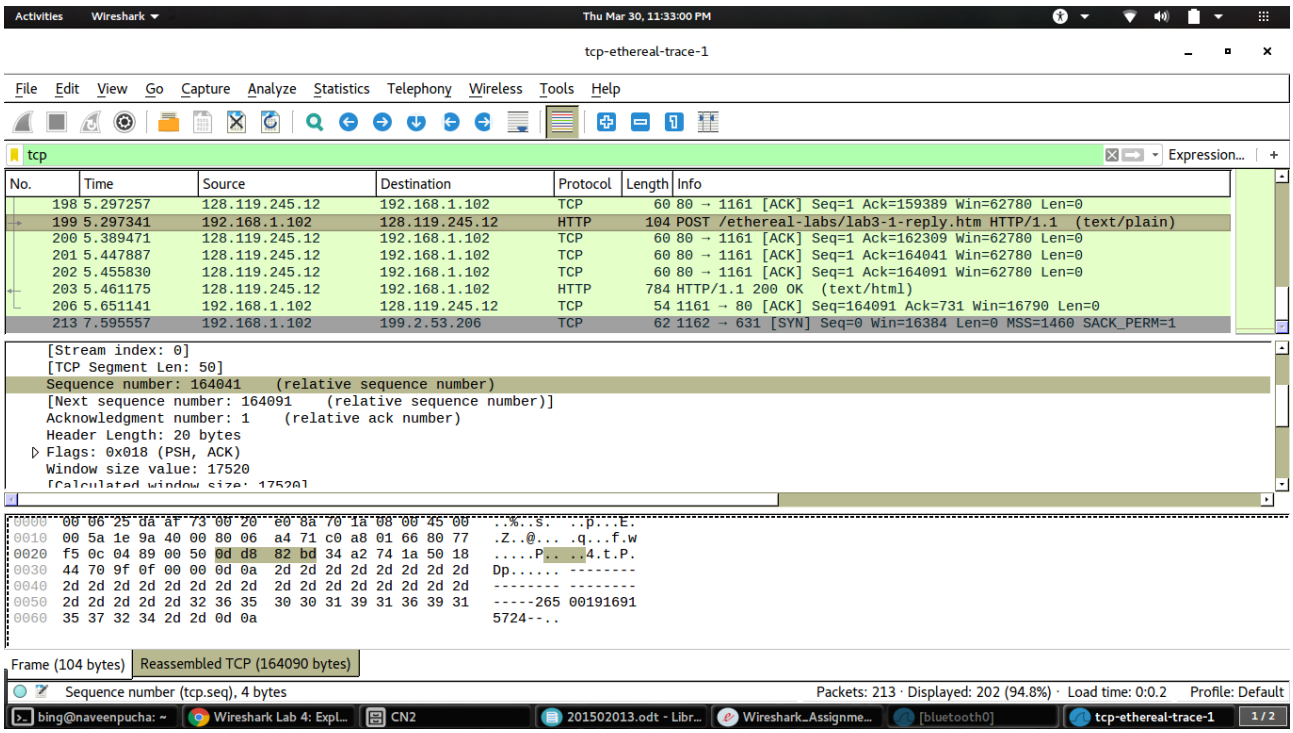
3) The source IP address is 130.215.17.5 using port 80



4) The sequence number of the segment which will be used to initiate the TCP connection is 0. That is Seq=0. This contains a SYN flag which identifies the segment as a SYN segment.

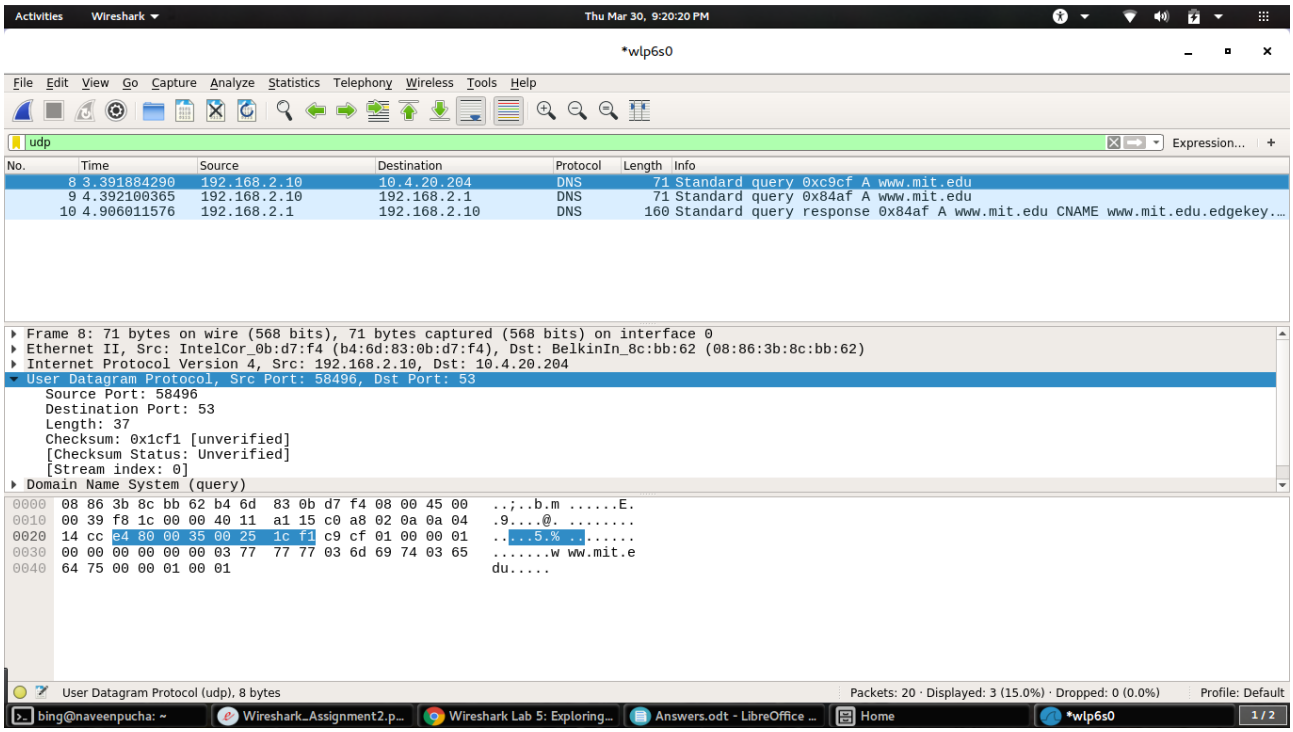


5) The sequence number of the TCP segment containing the HTTP post command is 164041



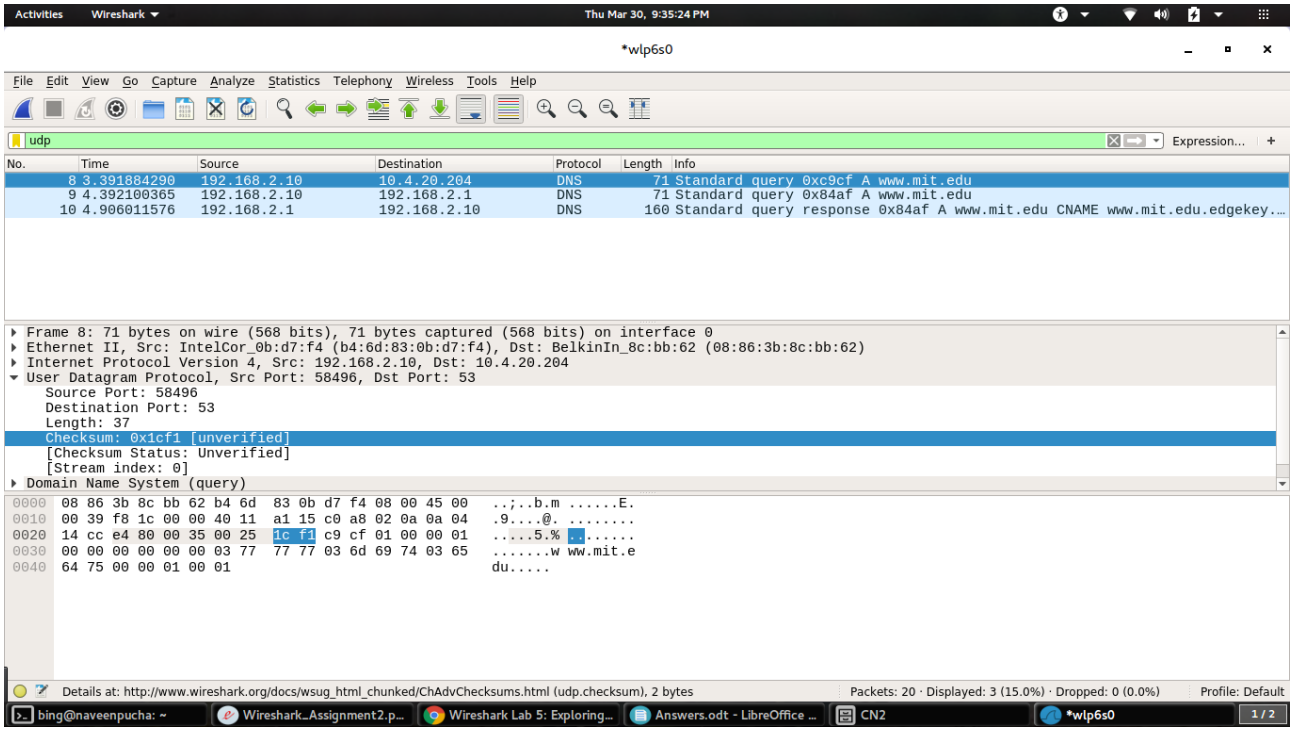
PART 4

1) There are 4 fields in the header. These are the Source Port, Destination Port, Length and Checksum



2) In the above case the length is 37. It's the count of the bytes that were captured for that particular frame, it'll match the number of bytes of raw data in the bottom section of the wireshark window.

3) The each of the UDP header files is 2 bytes long as shown below.



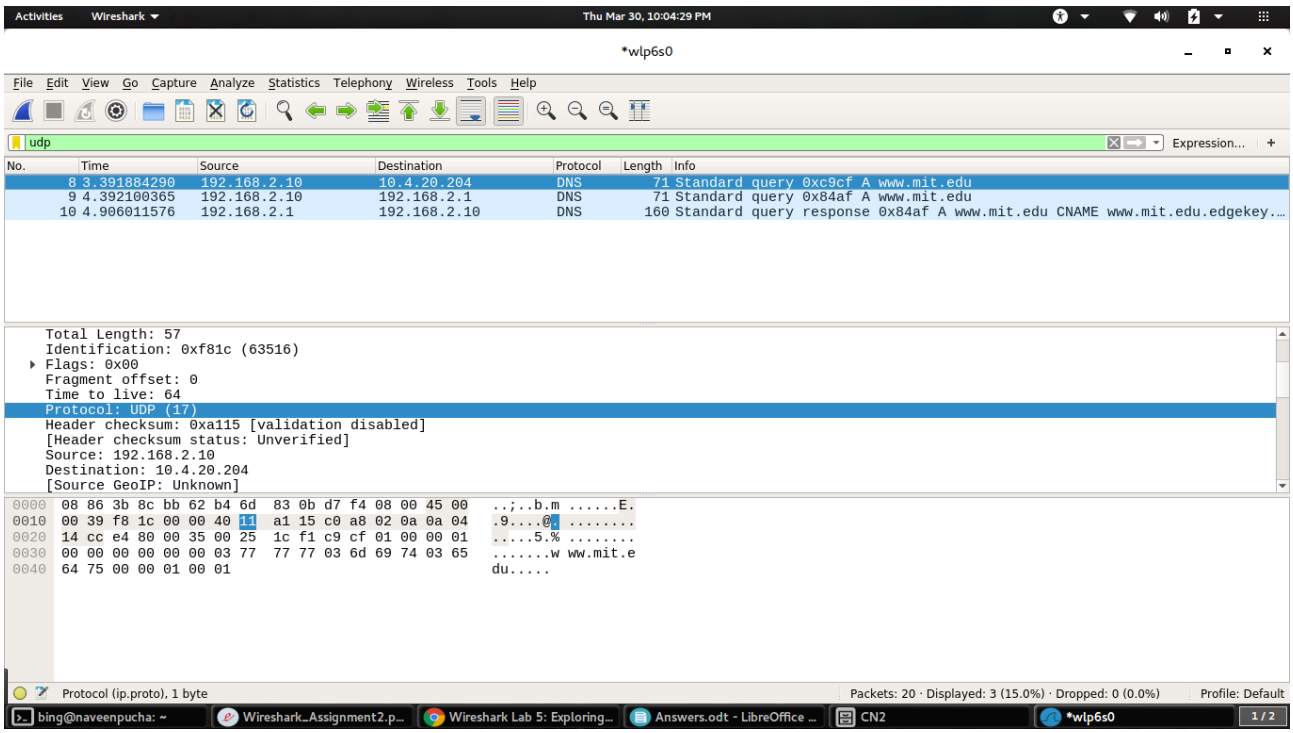
The maximum number of bytees that can be the payload is 2^16 – the bytes already being used by the header file

There are 4 header files, and each has 2 bytes , so in total there will be 8 header bytes.

Therefore the answer for this will be 65535 – 8 = 65527.

Largest possible is 65535

4) The protocol number for UDP is 17 in decimal and in hexadecimal notation it is 0x11.



5) It is a 16-bit field of one's complement of one's complement sum of a psuedo UDP header + UDP datagram.

The Psuedo UDP header 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 0's in the beginning.

Protocol : 8 bits / 1 byte, taken from IP header.

Length : because UDP header has a length field that indicates the length of the entire datagram, including UDP header and data, the value from UDP header used.

This UDP checksum is optional. If it's not computed, it is set to all 0's.