COMPUTER-NETWORKS

ASSIGNMENT-2

NAME:B.VISHAL REDDY
ROLLNO:201501173

PART-1 (WIRESHARK HTTP):

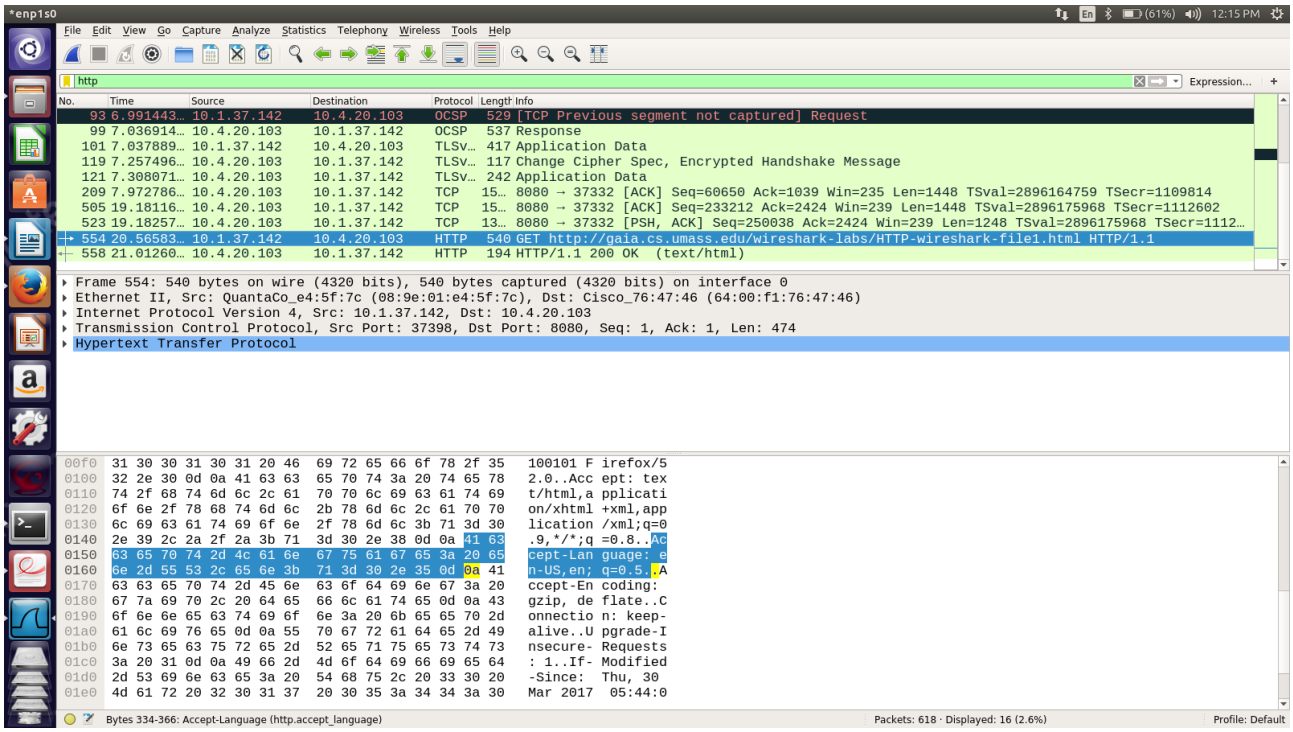
<u>The GET message is</u> :

GET http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

<u>The Response message is:</u>

HTTP/1.1 200 OK (text/html)

1. From the above messages HTTP version is 1.1



From the above screenshot the accepted languages are ‘ en-Us,en ’

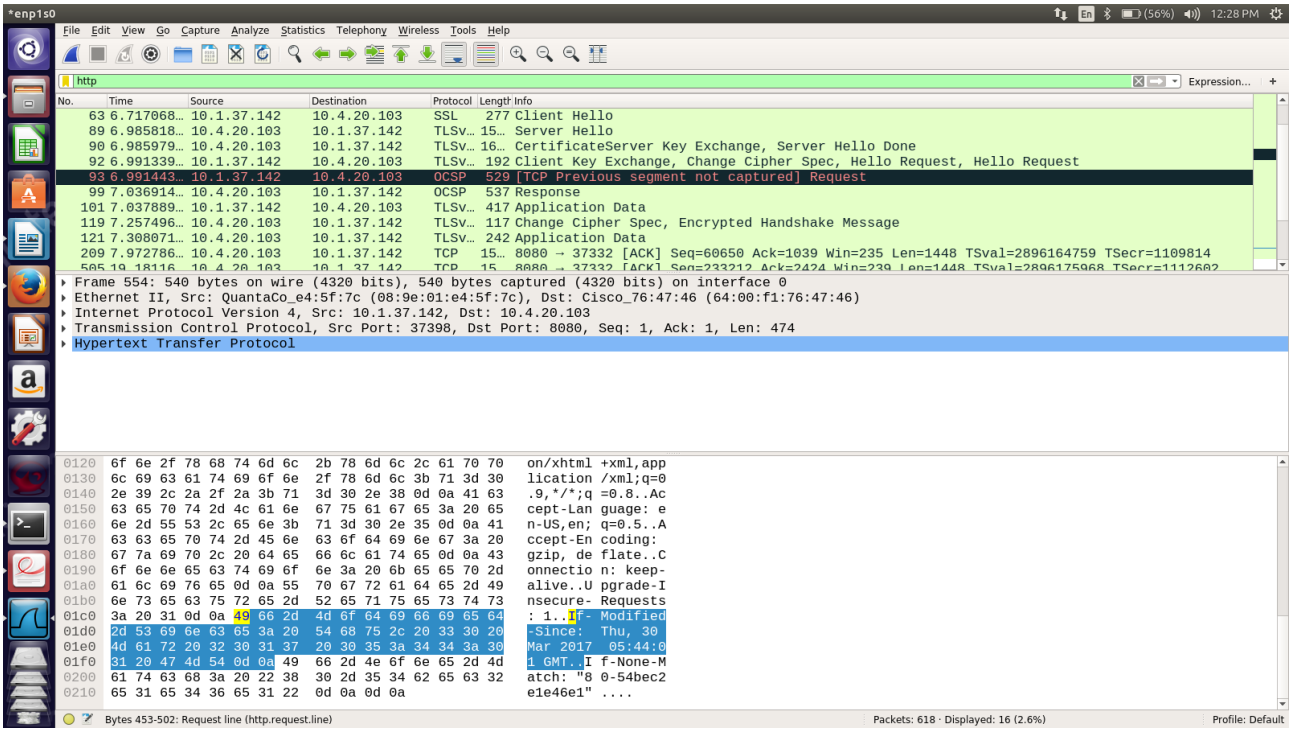
2. From the above screenshot the source ip that is my computer ip address is 10.1.37.142 and the destination ip address is 10.4.20.103

3. <u>The Response message is:</u>

HTTP/1.1 200 OK (text/html)

Hence the status code returned is '200 OK'

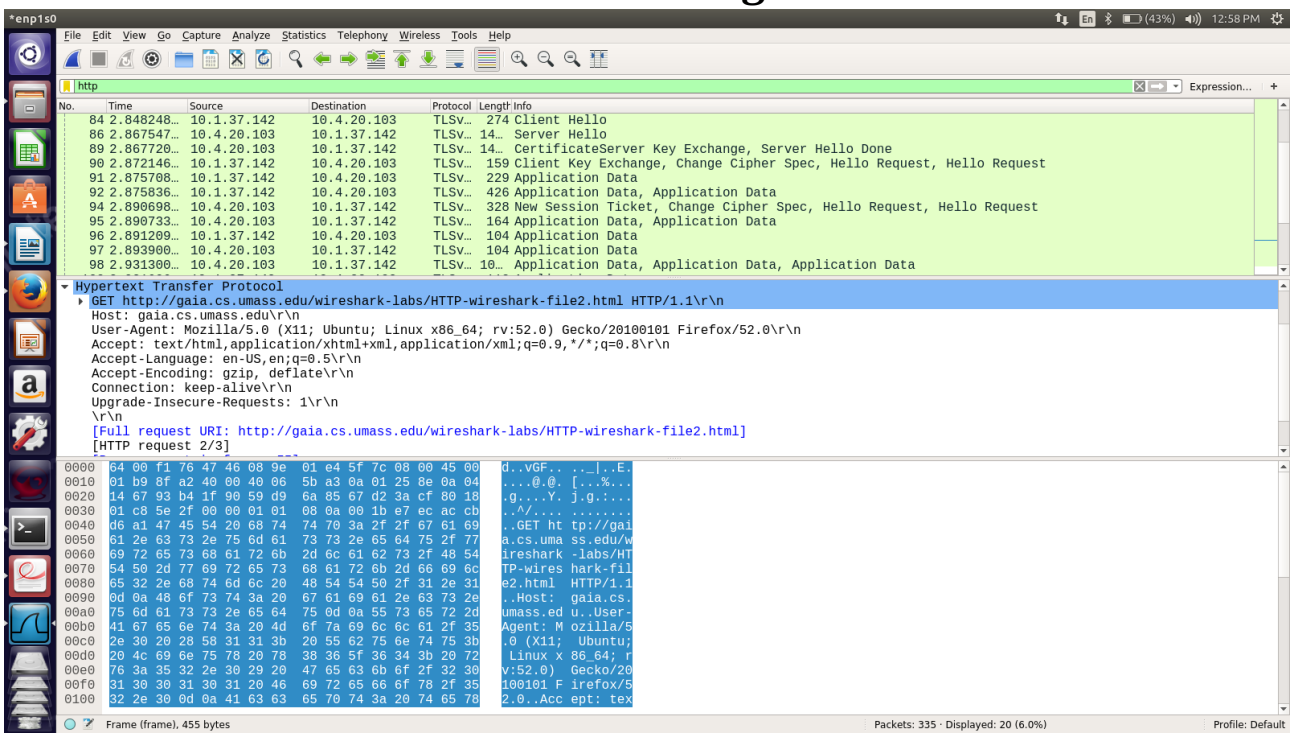
4. From the below screenshot last modified time is Thu,30 Mar 2017 05:44:01 GMT



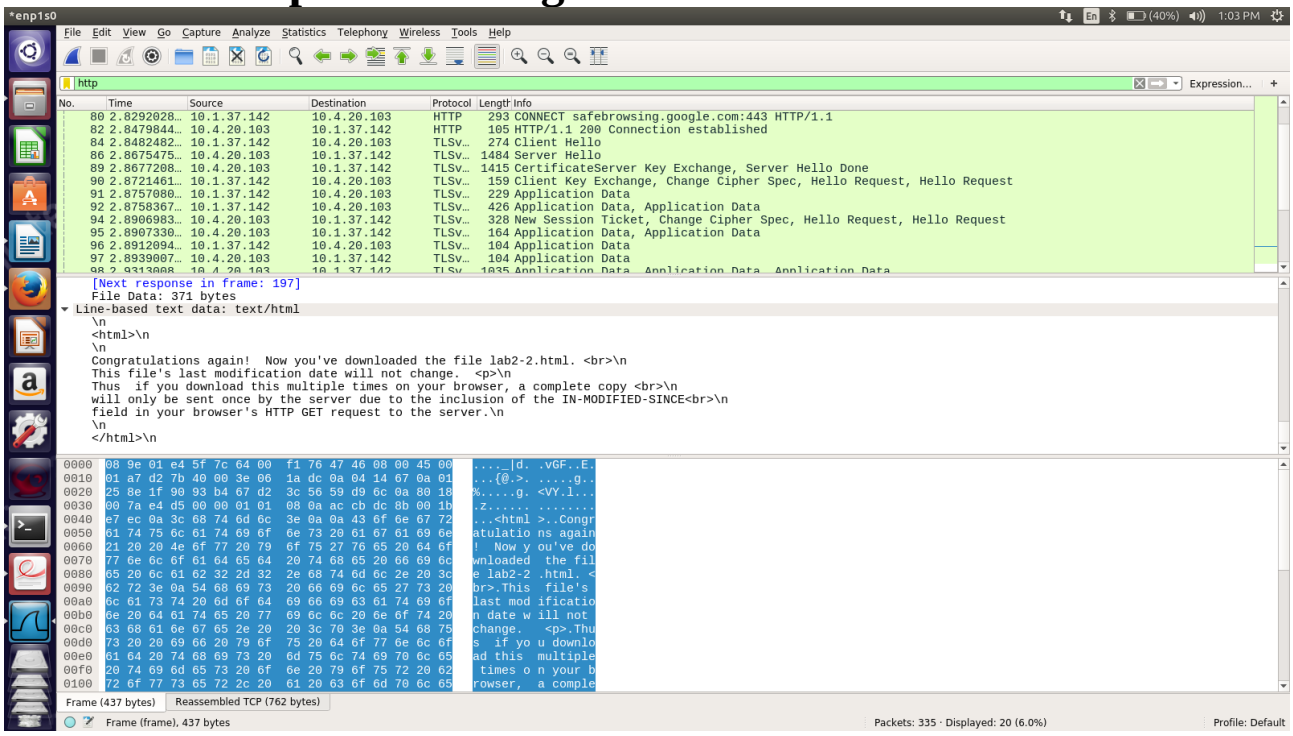
5. Content-length is 128 bytes.

6. By clicking each word in raw data it gets highlighted in packet-listing window .So all the headers are present in rawdata .

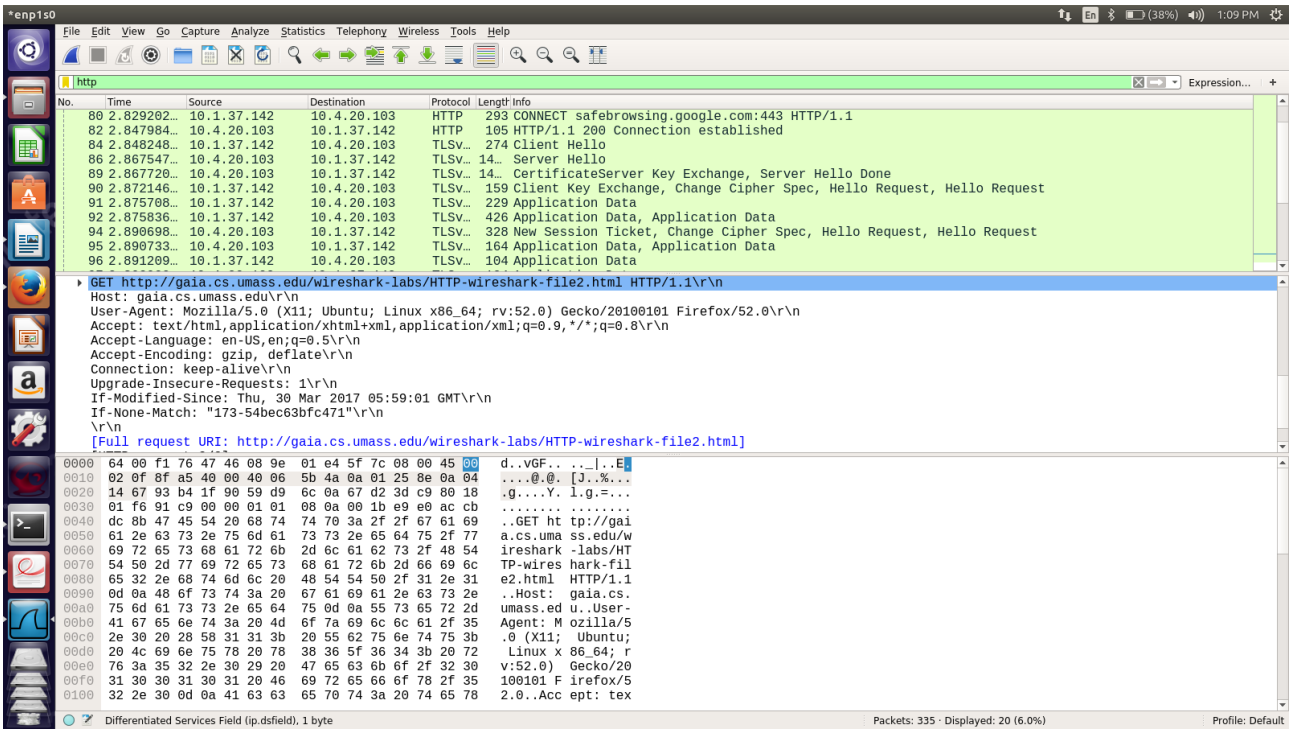
7. From the below screenshot there is no ‘IF-MODIFIED SINCE’ line in the HTTP GET message.



8. From the below screenshot server explicitly returned contents of file via line-based text data field in packet listing window of response message.



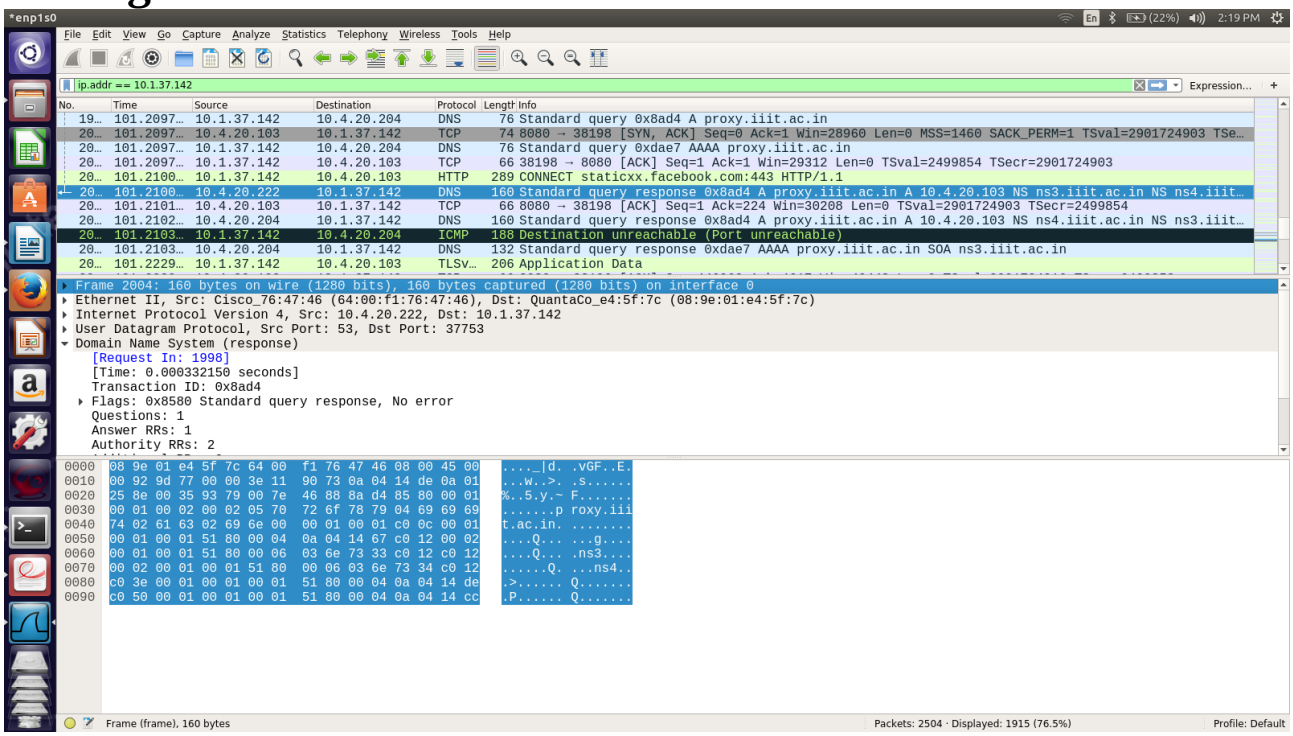
9. Yes, i can see ‘IF-MODIFIED SINCE’ line in the HTTP GET request from the below screenshot.The information followed is Thu, 30 Mar 2017 05:59:01 GMT which is same modified time of the last GET request to the server. Here Modified time doesnt change.



10. The HTTP status code and phrase returned from server is HTTP/1.1 304 Not Modified . In the second HTTP GET request server didnt explicitly return the contents since it is loaded from the browser cache.

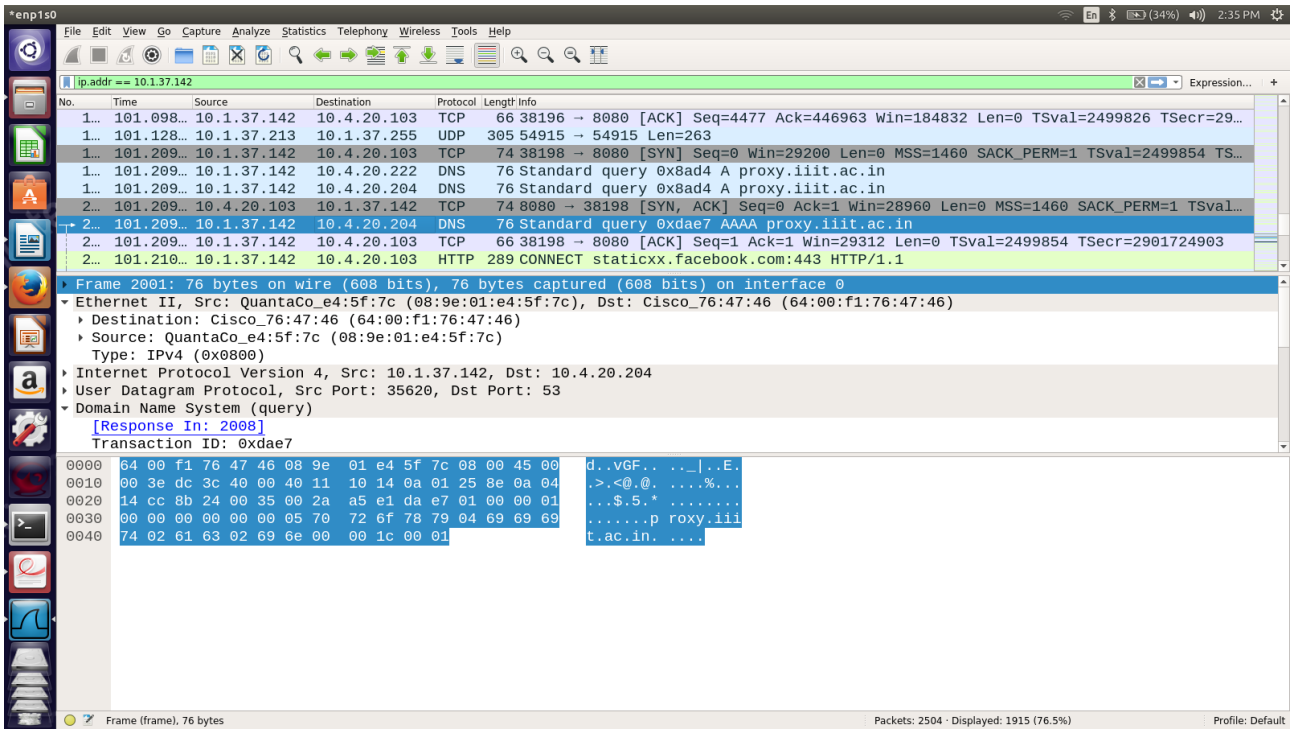
PART-2 (WIRESHARK DNS):

1. From the below screen shot DNS query and response messages are sent over UDP.



2. The destination port for DNS query message is 53 and the source port of DNS response message is 53.

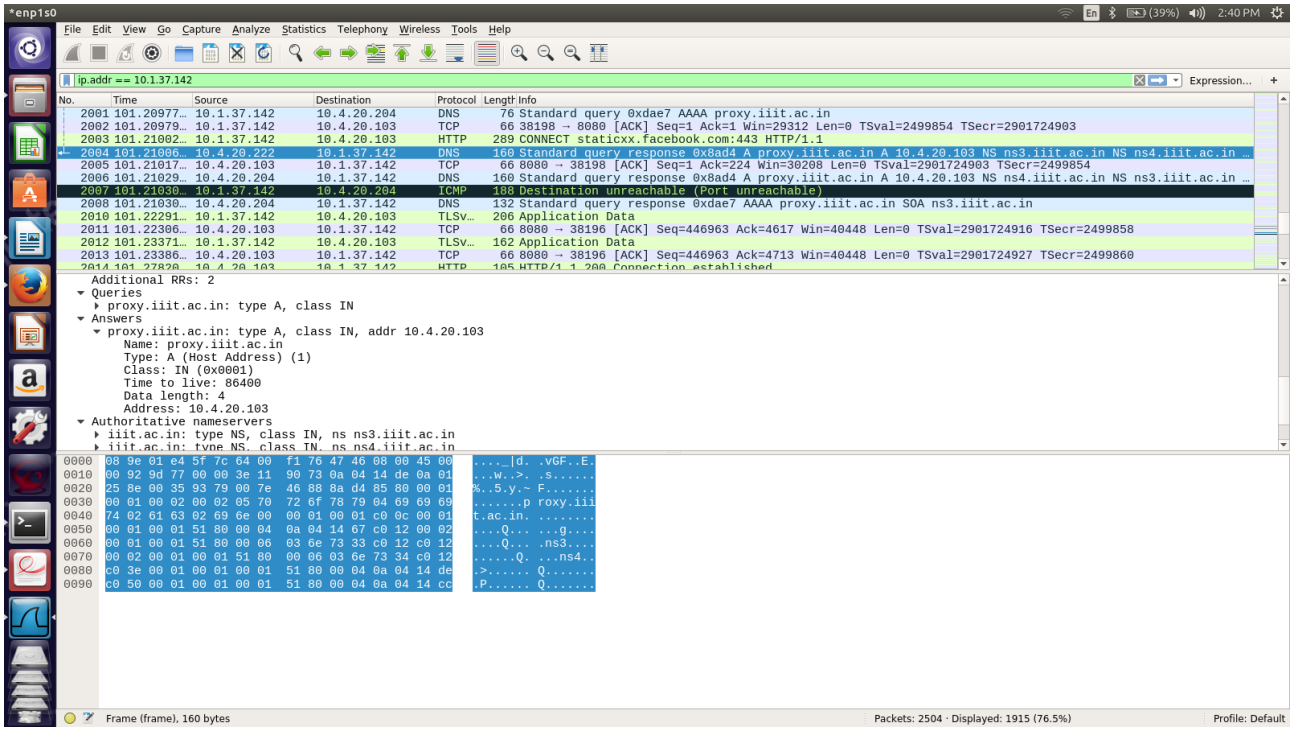
3.



Primary DNS: 10.4.20.222
Secondary DNS: 10.4.20.204

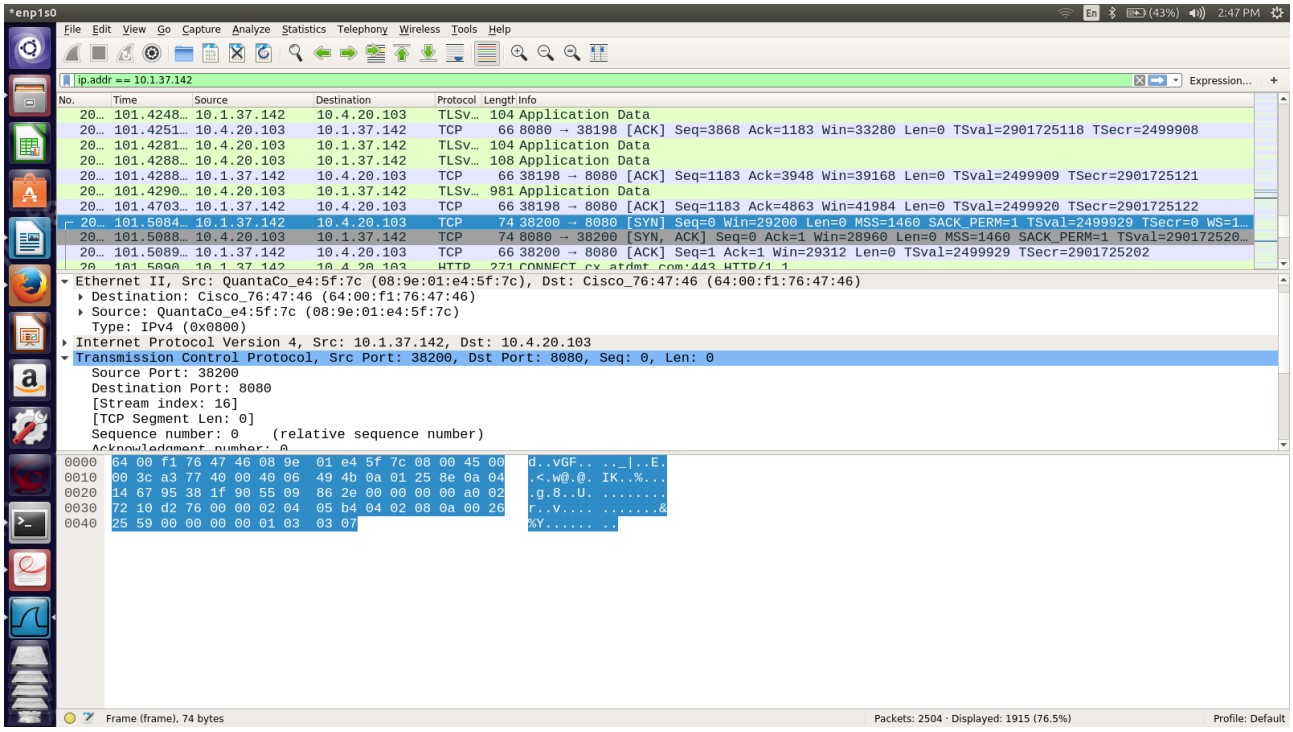
It is sent to above DNS servers which is same as my DNS server ip address.

4.



There is only one answer containing information about Name,Type,Class,Time to live,Data length,Address.

5.



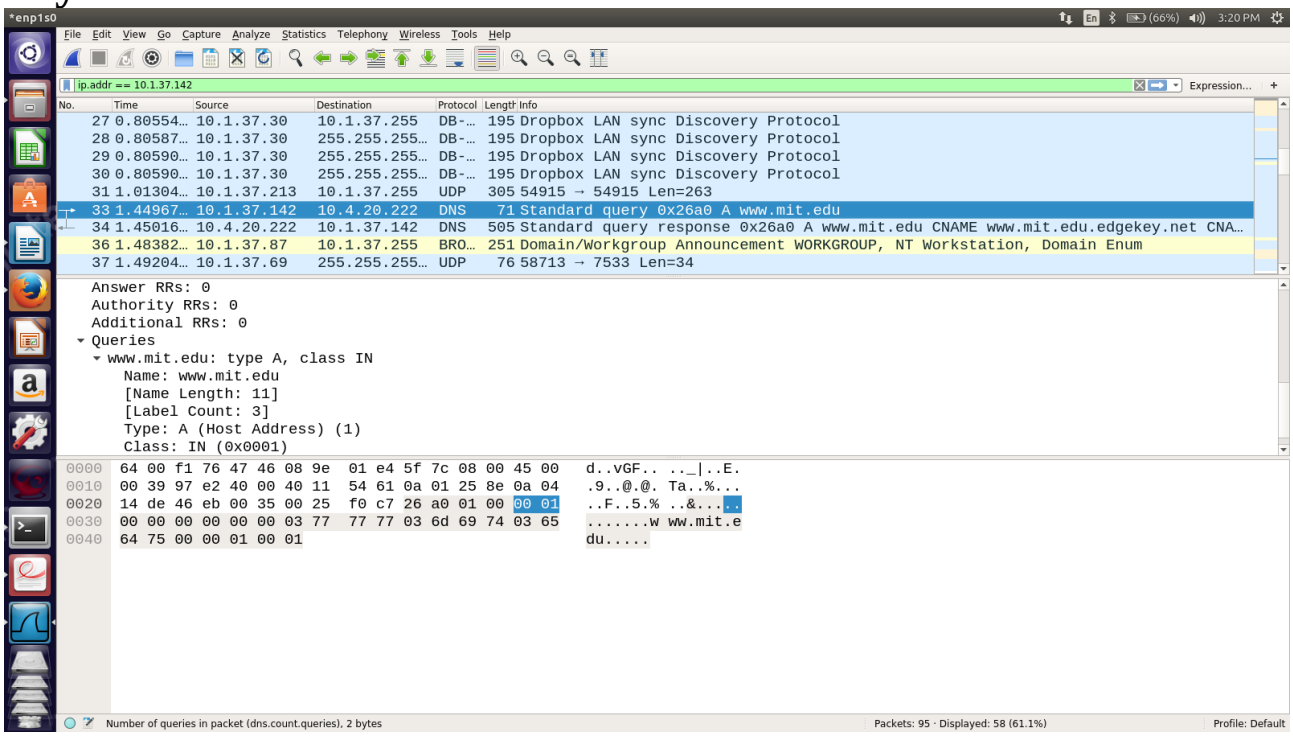
Yes ,(first syn packet) the ip 10.4.20.103 corresponds to the ip address in the DNS response message.

6. No ,Host doesnt issue any DNS queries before retrieving each image.

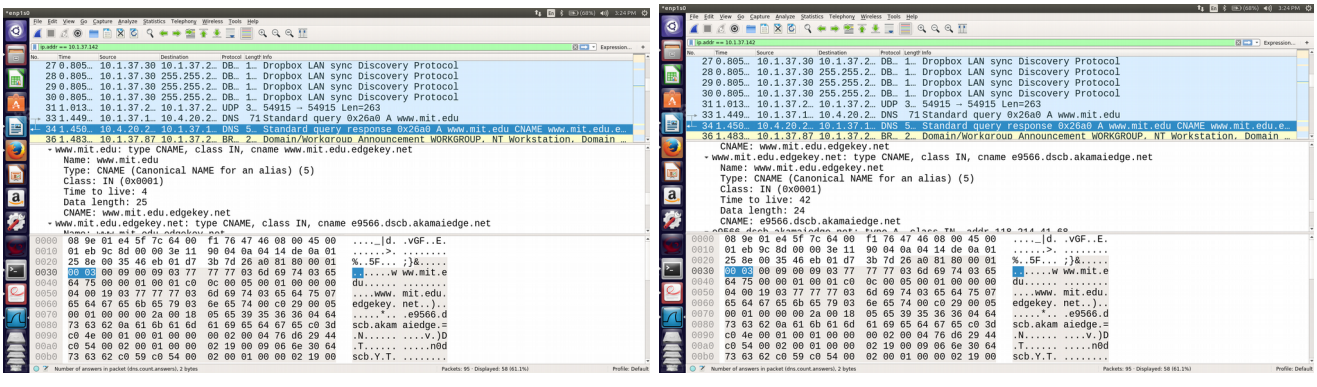
7. The destination port for DNS query message is 53 and source port of DNS response message is 53.

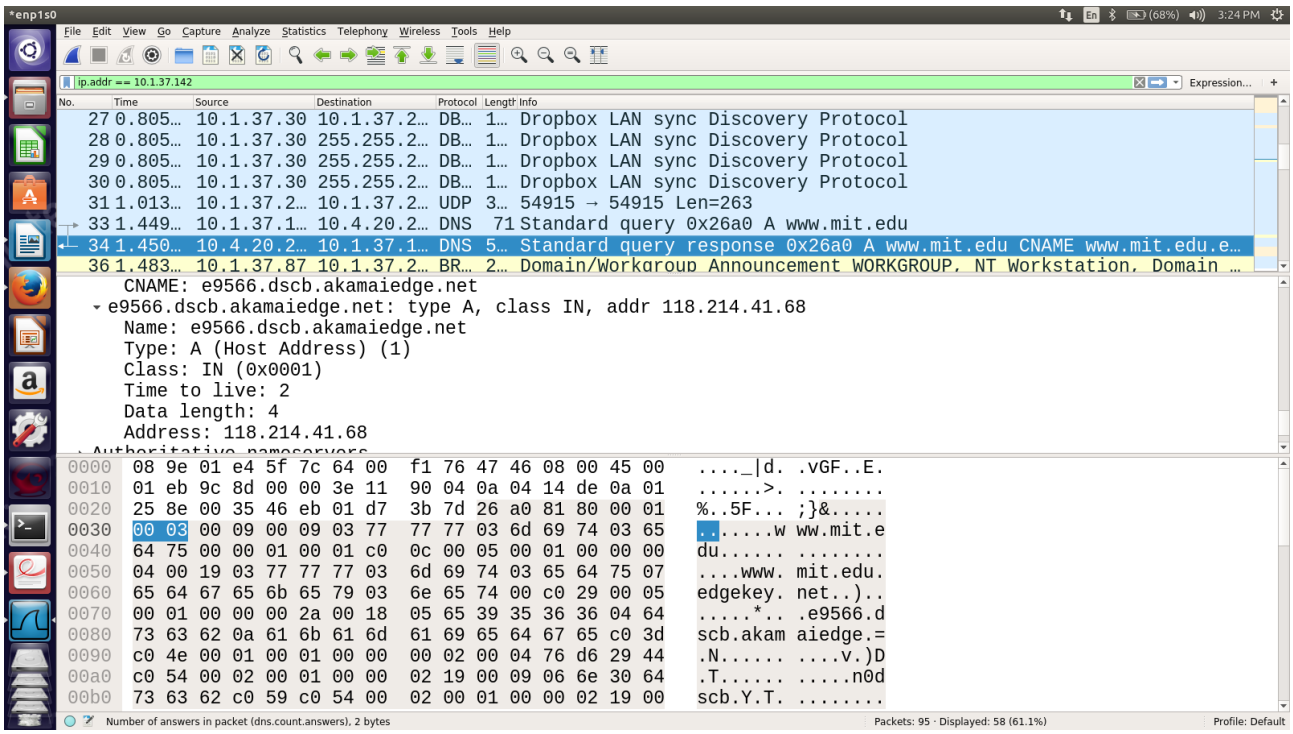
8. The DNS query message is sent to 10.4.20.222 which is the ip of one of my DNS servers (default / primary).

9. The DNS query message is of Type-A and doesnt contain any answers.



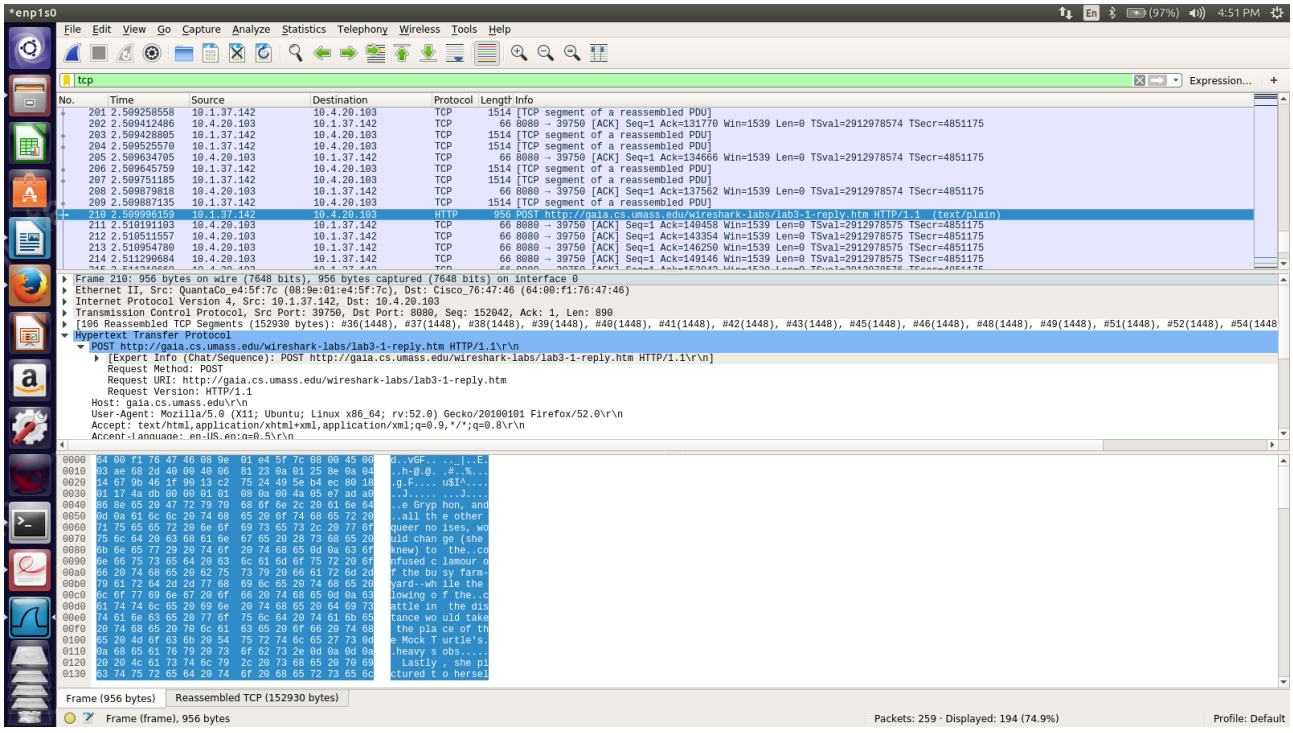
10. The response DNS message consists of 3 answers which consists of Name,Type,Class,Time to live,Data length,Address





PART-3 (WIRESHARK TCP):

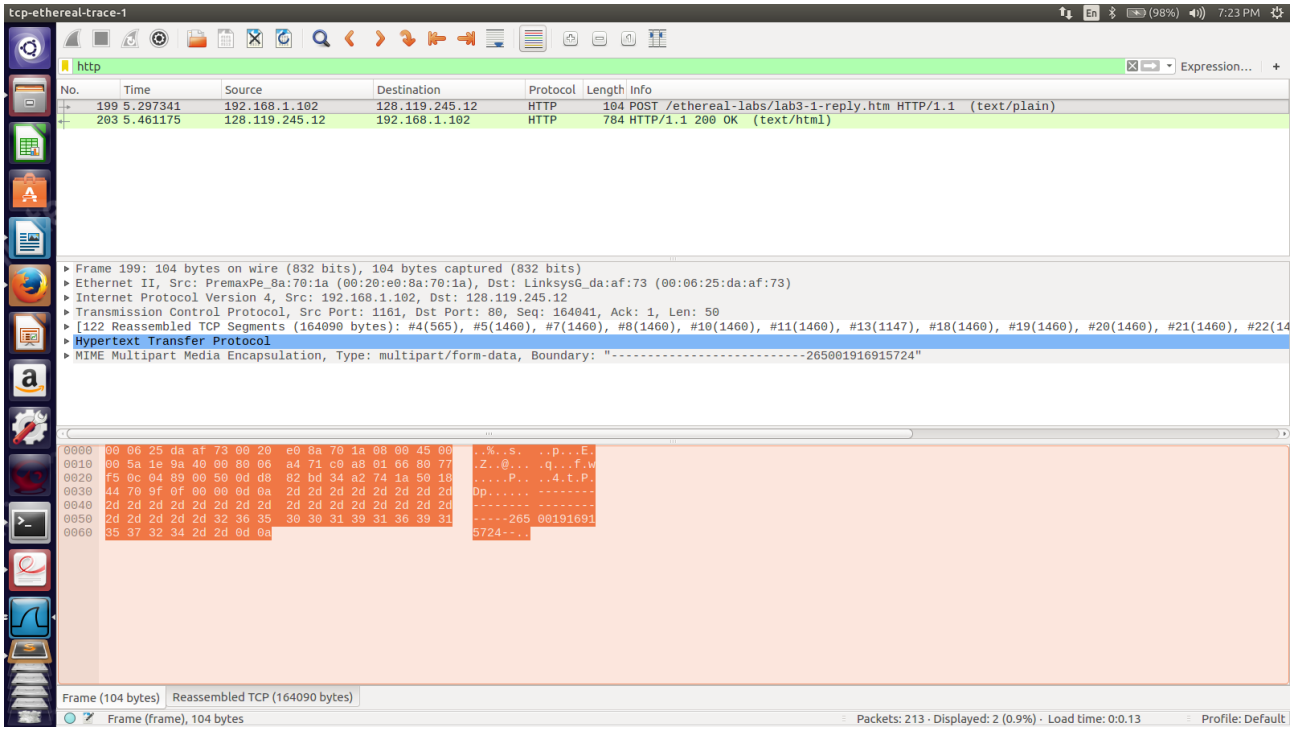
1.



From the above screenshot the source ip address is 10.1.37.142 and the source tcp port is 39750

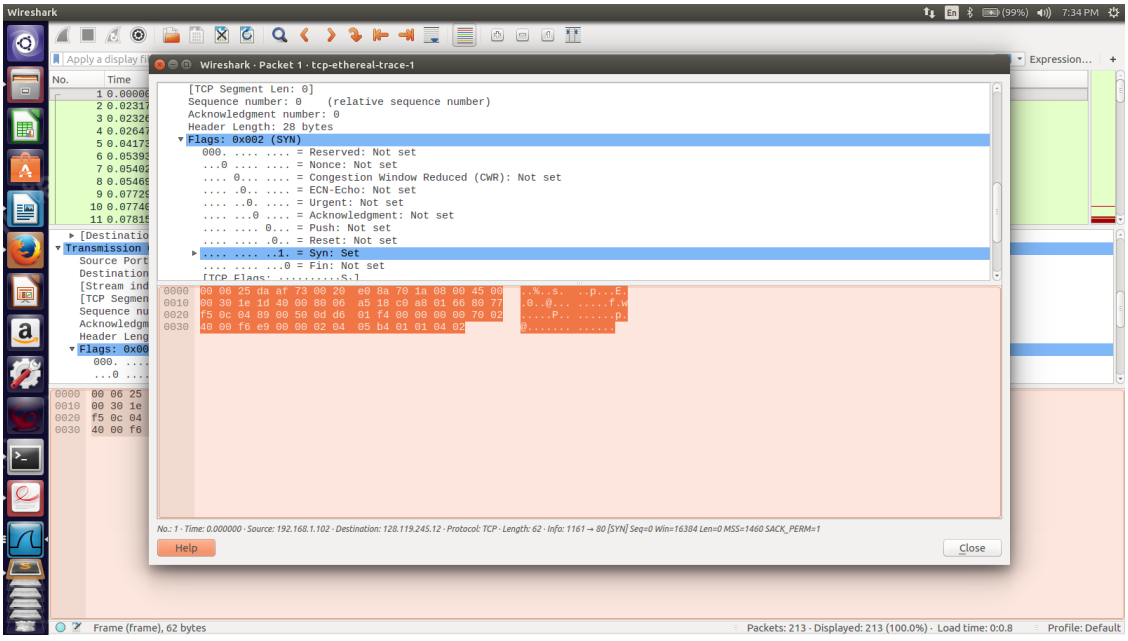
2. IP address of gaia.cs.umass.edu and the port number is 8080 for sending and receiving through 39750 port TCP segments.

3.



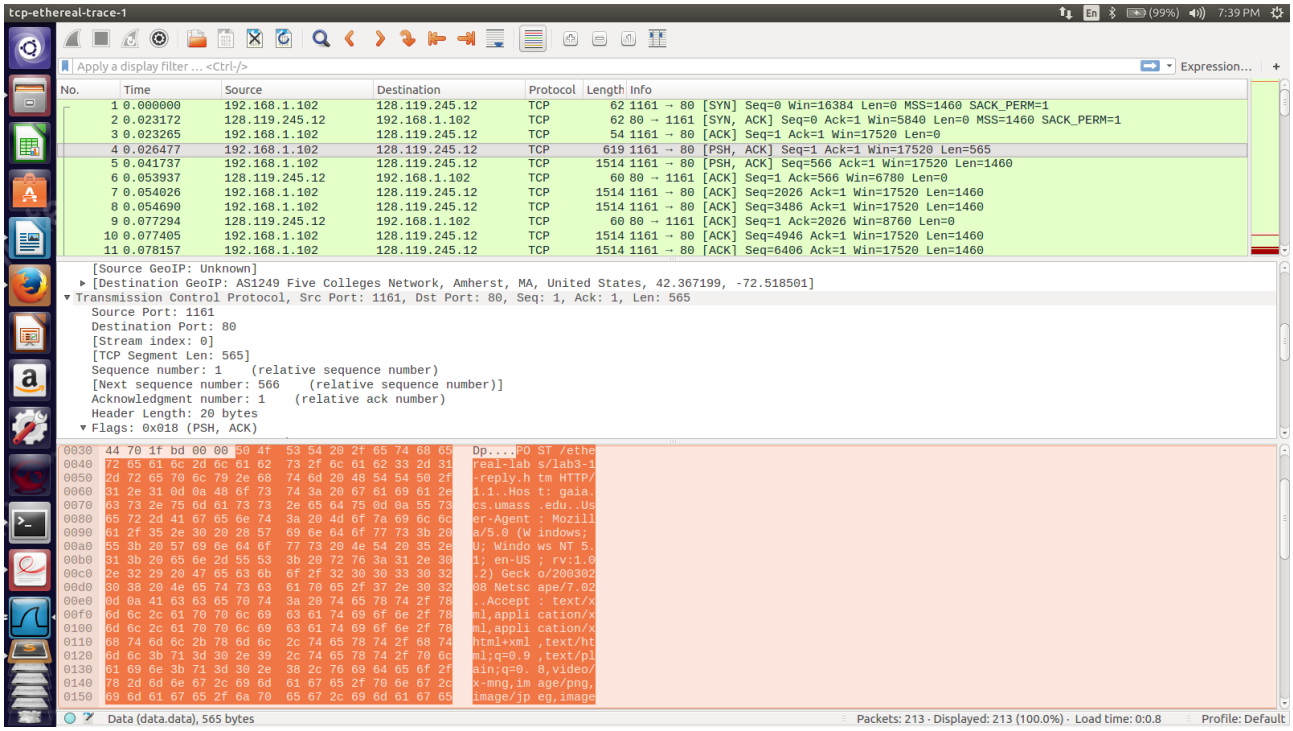
IP address used by client computer(source) is 192.168.1.102 and TCP port is 1161

4.



The sequence number is 0 TCP SYN segment . The SYN flag is 1 from the above screenshot so it indicates it as a syn segment.

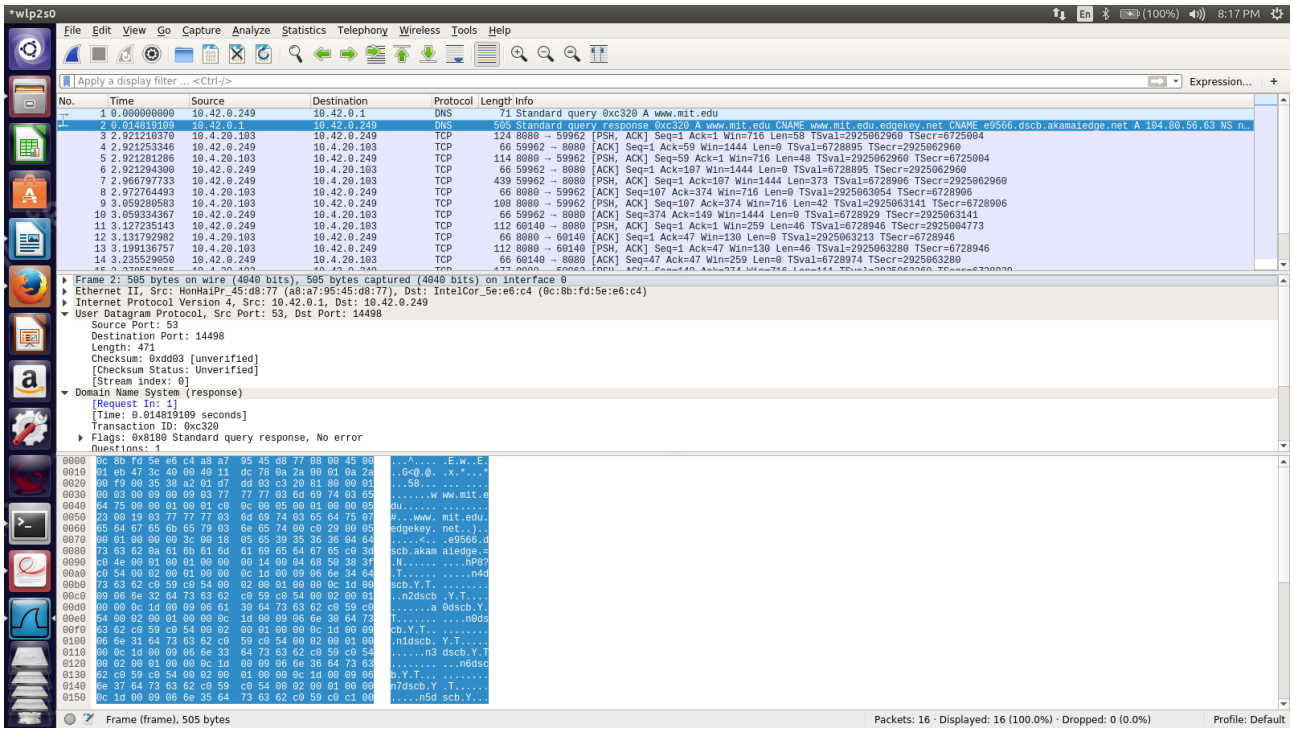
5.



Segment no 4 is the tcp segment containign http post . The sequence number for this segment is 1.

PART-4 (WIRESHARK UDP):

1.



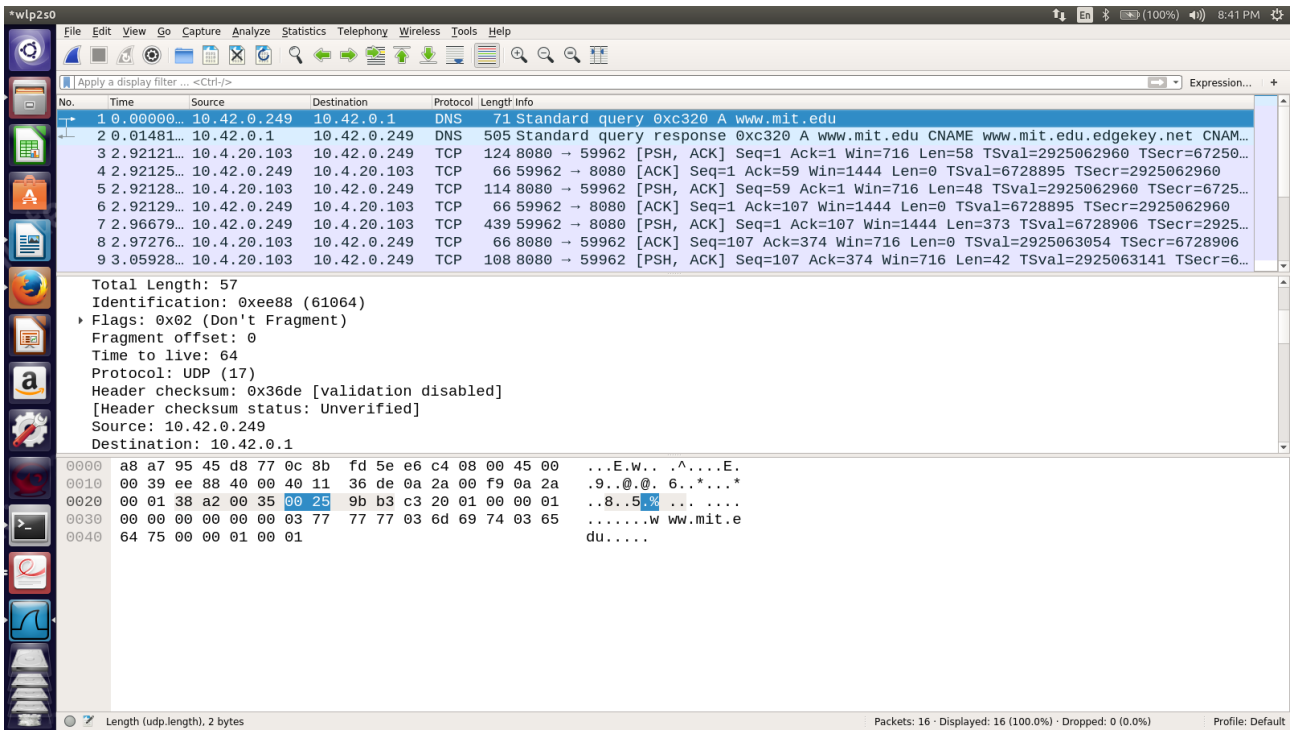
The four fields in the UDP header are source port,destination port,length,checksum.

2. 8 bytes of UDP packet header + 29 bytes of payload fron application layer=37

3. Maximum number of bytes used that can be included in payload is 2^16-1 – header bytes => 65535-8 = 65527

Largest possible source port number is unsigned 16 bit number => 65536-1 = 65535

4. Protocol number for UDP is 17(decimal) or 11(hexadecimal) from the below screenshot



5. The UDP checksum is performed over the entire payload, and the other fields in the header, and some fields from the IP header. A pseudo-header is constructed from the IP header in order to perform the calculation (which is done over this pseudo-header, the UDP header and the payload).