CSP334: Computer Networks, Lab Assignment No 4,HTTP

Rahul Byas Sherwan
Entry No. : 2016UCS0028

1: SET 1: The Basic HTTP GET/response interaction :

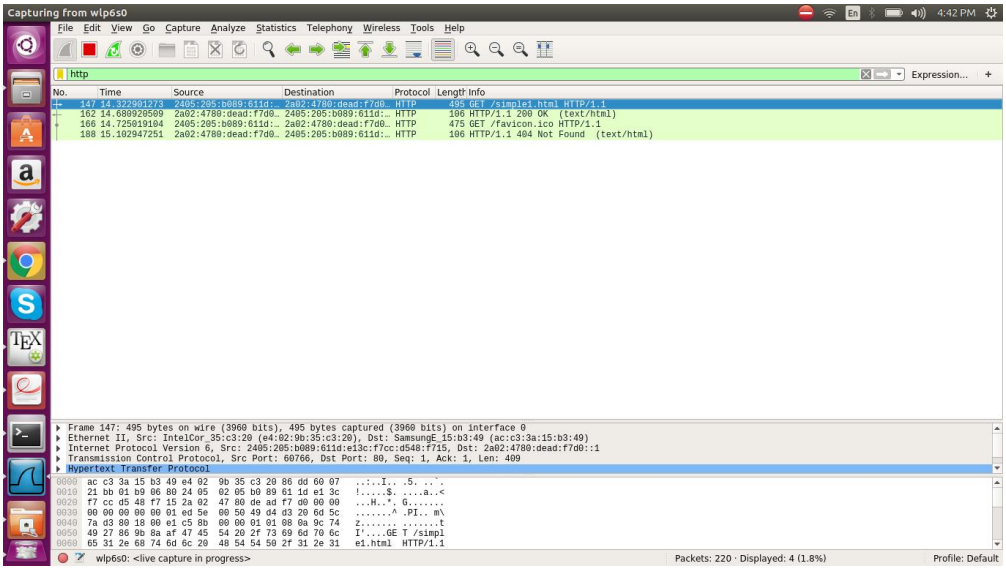

Figure 1: HTTP capture

(1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running 1.1 . Server is also running 1.1 ,we can verify by the images below.

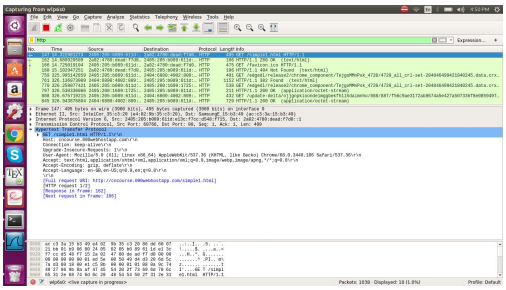

Figure 2: browser

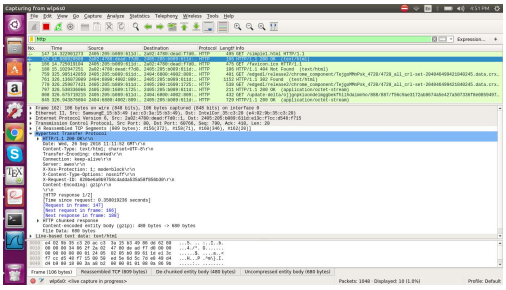

Figure 3: server

(2) What languages (if any) does your browser indicate that it can accept to the server?

It accepts the following language
en-GB : British English
en-US : American English

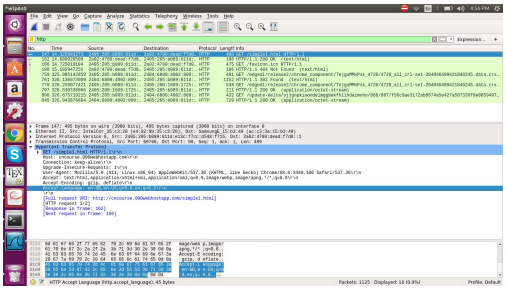

Figure 4: language

(3) What is the IP address of your computer? Of the cncourse web server?

IPA of my computer : 2405:205:b089:611d:e13c:f7cc:d548:f715 IPA of the server : 2a02:4780:dead:f7d0::1

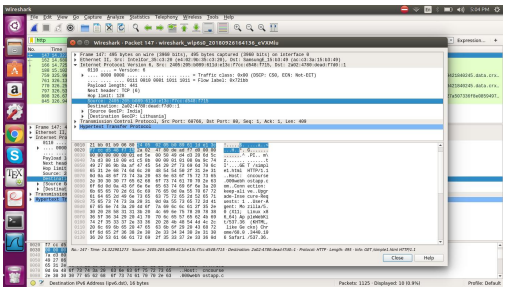

Figure 5: IPv6 IPA

(4) What is the status code returned from the server to your browser?

Status Code : 200

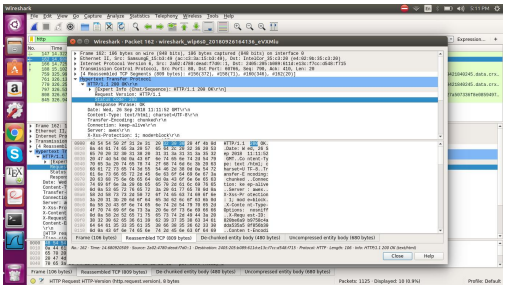

Figure 6: status code

(5) When was the HTML file that you are retrieving last modified at the server?

It doesnot show anything shown in the figure:

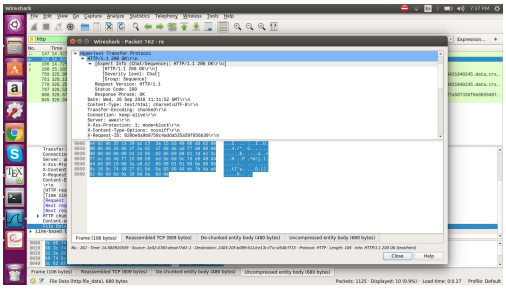

Figure 7: returned data

(6) How many bytes of content are being returned to your browser?

Bytes of content that returned are : 480 -¿ 680 bytes. That is 480 bytes of actual data are returned by the server excluding excluding headers which ultimately transforms it into 680 bytes. Thus , 680 bytes of content are recieved to my browser.

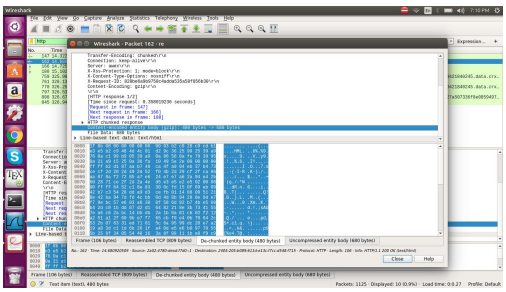

Figure 8: returned data

(7) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
No, we don't see any header within the data that are not displayed in the packet-listing.

(8) Click the following command on Wireshark menu: Statistics http Requests.

Find out how many requests were sent by your browser and how many did the server respond, with ?
Total HTTP packets : 30 HTTP request packets : 25 HTTP response packet : 5

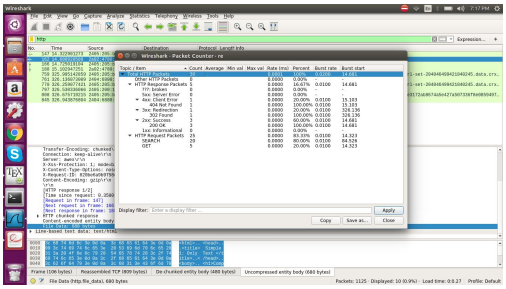

Figure 9: Statistics

(9) Find out how to obtain the http traffic flow graph showing the packet exchanges between the client and the server and take a dump of the flow graph for http packets and paste in your answer sheet after all the questions above are answered.

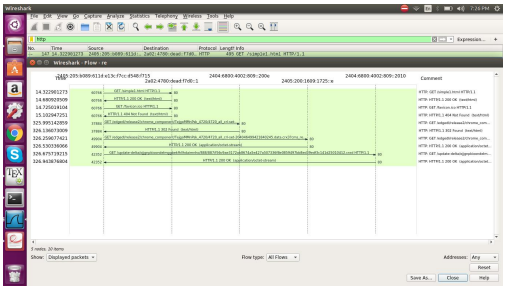

Figure 10: graphflow

(10) Now, enter the following URL to your browser, and answer the questions 5,6, 8 and 9 for the following file : http://cncourse.000webhostapp.com/simple2.html

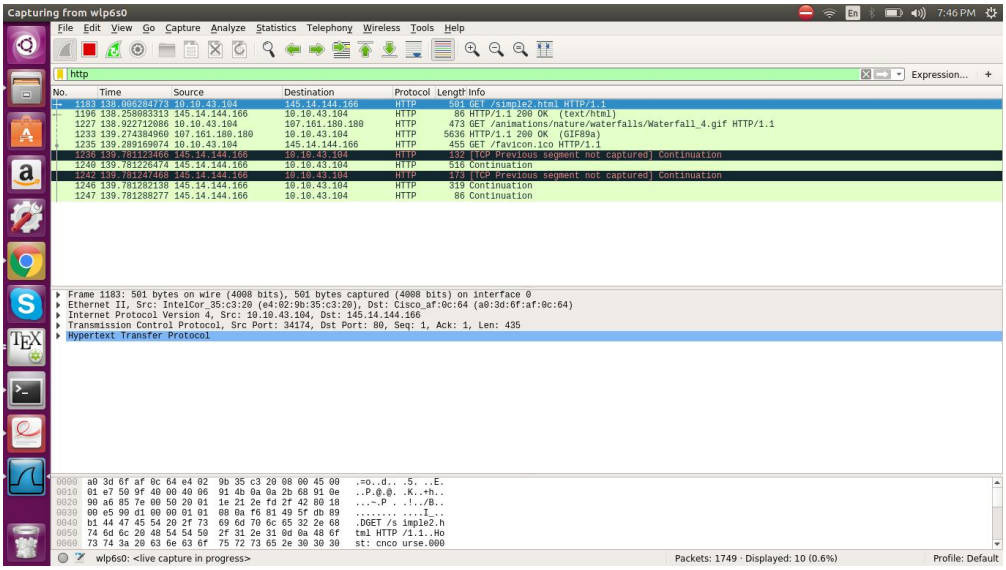

Figure 11: simple2.html

Following are the answer for part 10 for :

(a) question 5:

It doesnot show anything shown in the figure:

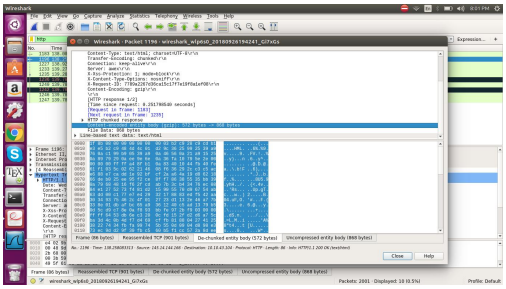

Figure 12: last modified

(b) question 6:

Bytes of content that returned are : 572 to 868 bytes.That is 572 bytes of actual data are returned by the server excluding headers which ultimately transforms it into 868 bytes. Thus , 868 bytes of content are recieved to my browser. There were two responses from the server but the other response has no size written on it.

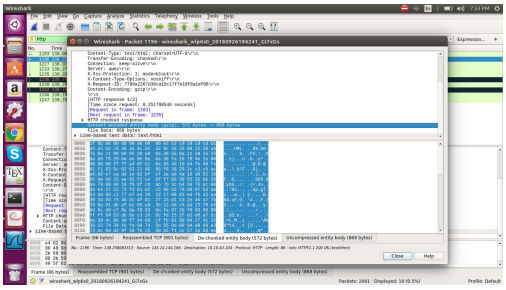

Figure 13: bytes of data returned for first OK

(c) question 8:

Total HTTP packets : 17
HTTP request packets : 11
HTTP response packet : 2

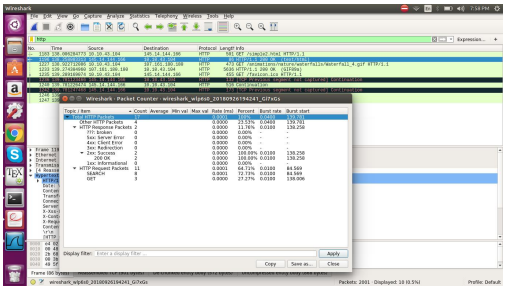

Figure 14: Statistics

(d) question 9:

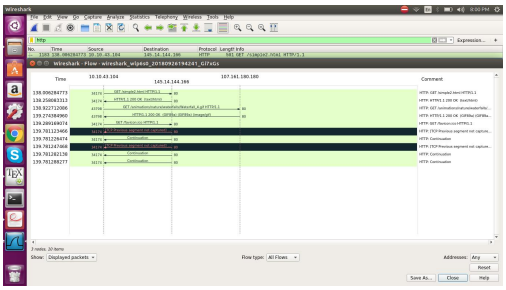

Figure 15: graphflow

(11) Now, enter the following URL to your browser, and answer the questions 5,6, 8 and 9 for the following file : http://cncourse.000webhostapp.com/simple3.html

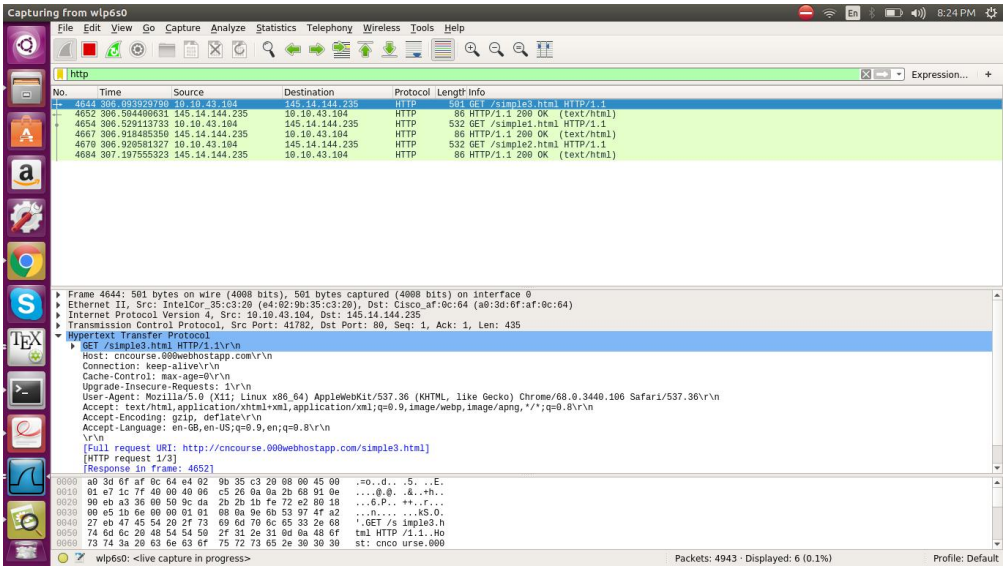

Figure 16: simple2.html

Following are the answer for part 11 for :

(a) question 5:

It doesnot show anything shown in the figure:

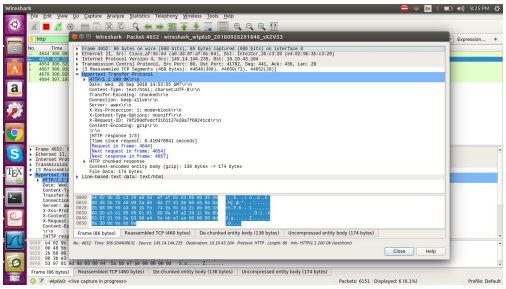

Figure 17: last modified

(b) question 6:

Bytes of content that returned are : 138 to 174 bytes.That is 138 bytes of actual data are returned by the server excluding headers which ultimately transforms it into 174 bytes. Thus , 174 bytes of content are recieved to my browser. Please note that i have written a single packet's bytes returned to the browser. Since there are three such reponses we will add their respective bytes , and that are 174 + 680 + 868 bytes returned to the browser as a whole. I have one such packets screendump below

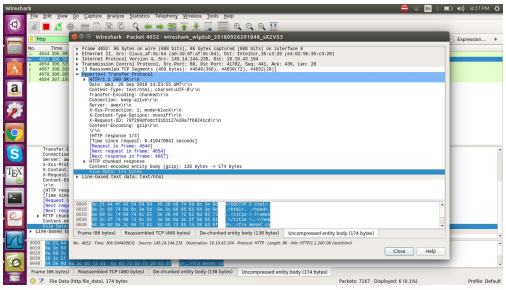

Figure 18: bytes of data returned for first OK

(c) question 8:

Total HTTP packets : 46
HTTP request packets : 43
HTTP response packet : 3

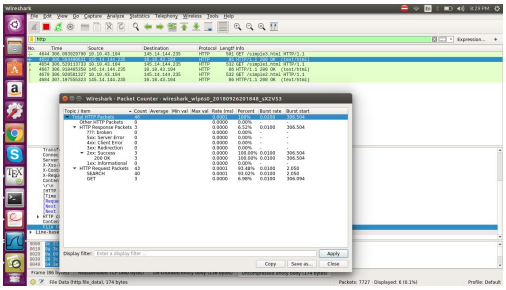

Figure 19: Statistics

(d) question 9:

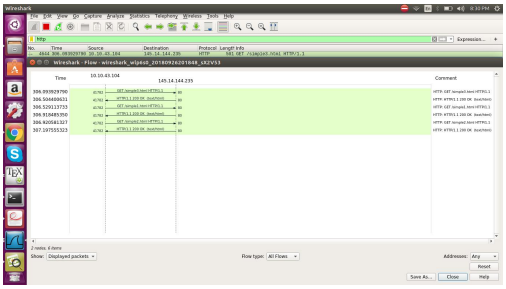

Figure 20: graphflow

(12) Now, enter the following URL to your browser, and answer the questions 5,6, 8 and 9 for the following file : http://cncourse.000webhostapp.com/simple4.html. Can you tell whether your browser downloaded the ten images serially, or whether they were downloaded from the two web sites in parallel? Explain.

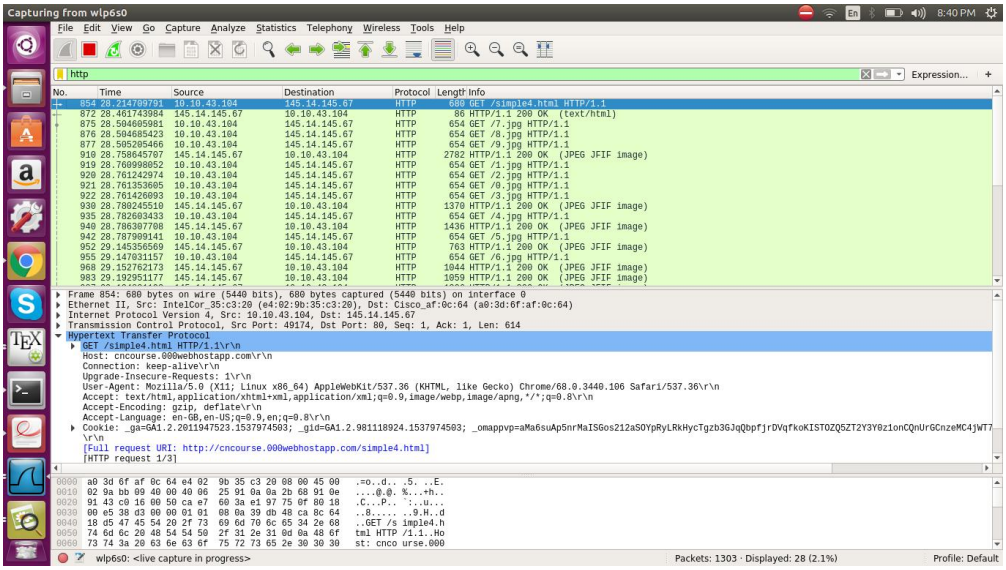

Figure 21: simple2.html

Following are the answer for part 12 for :

(a) question 5:

It doesnot show anything shown in the figure:

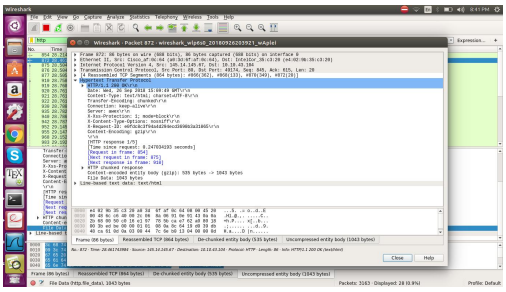

Figure 22: last modified

(b) question 6:

Bytes of content that returned are : 535 to 1043 bytes.That is 535 bytes of actual data are returned by the server excluding headers which ultimately transforms it into 1043 bytes. Thus , 1043 bytes of content are recieved to my browser. Please note that i have written a single packet's bytes returned to the browser. Since there are three such reponses we will add their respective bytes , and that many bytes returned to the browser as a whole. I have one such packets screendump below

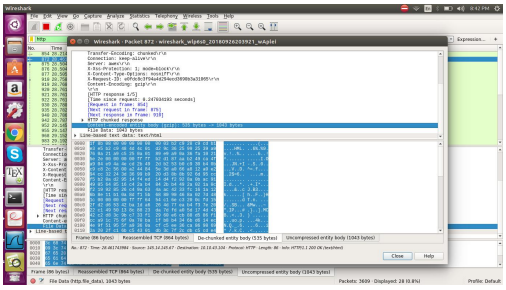

Figure 23: bytes of data returned for first OK

(c) question 8:

Total HTTP packets : 47
HTTP request packets : 32
HTTP response packet : 11

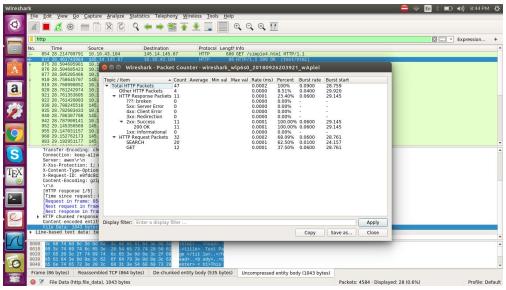

Figure 24: Statistics

(d) question 9:

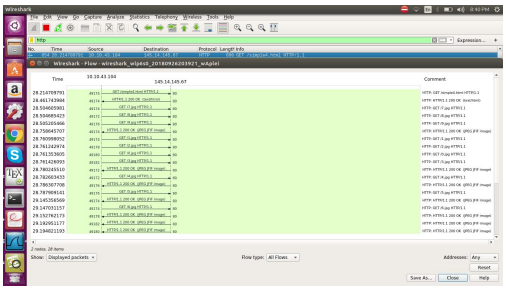

Figure 25: graphflow

(13) the thirteenth question

The time required to access this file : 22.345261520 - 22.151745278 = 0.193516242 seconds.
Note: the packet is highlighted in blue , we can verify the time from it.

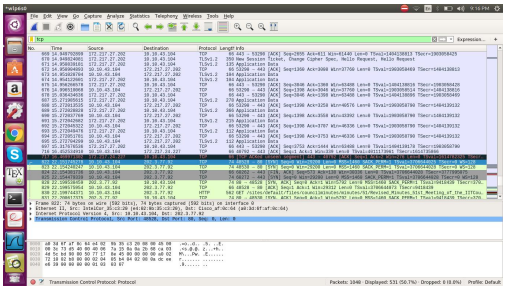

Figure 26: first tcp packet's time

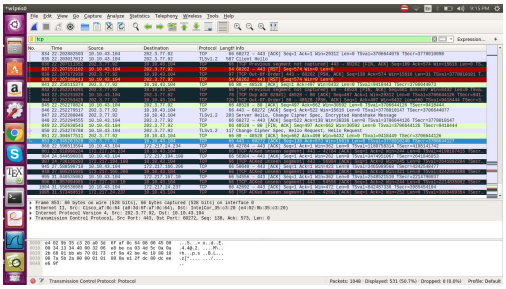

Figure 27: last tcp packet's time

(14) the forteenth question

We can do the same thing for each question as we have done in question 13.

2: SET 2: The HTTP CONDITIONAL GET/response interaction :

I am taking url of questions 12 i.e. http://cncourse.000webhostapp.com/simple4.html for answering this set.

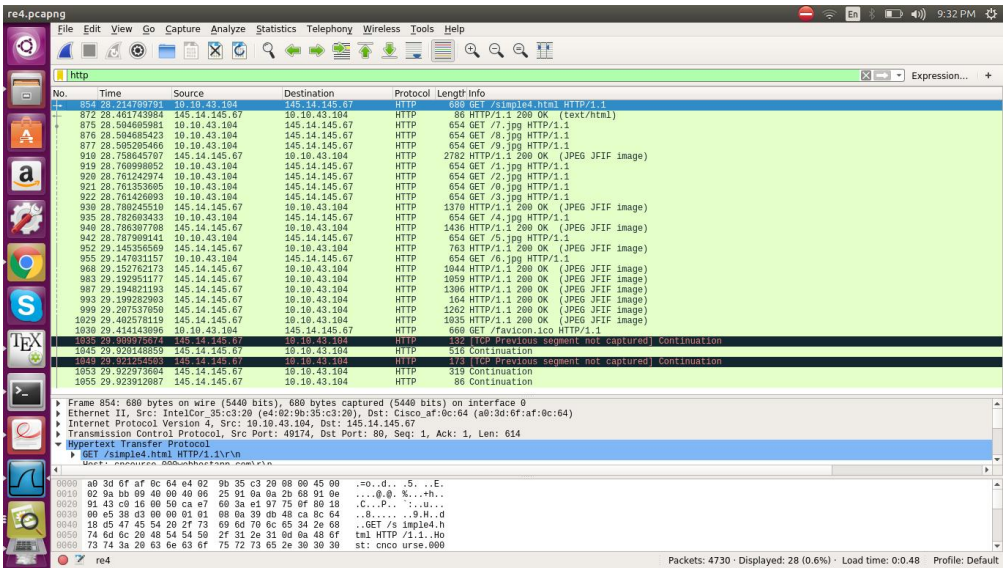

Figure 28: Packages for answering set 2

(1) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an IF-MODIFIED-SINCE line in the HTTP GET?

No, I didn't saw any IF-MODIFIED-SINCE line in the HTTP GET.

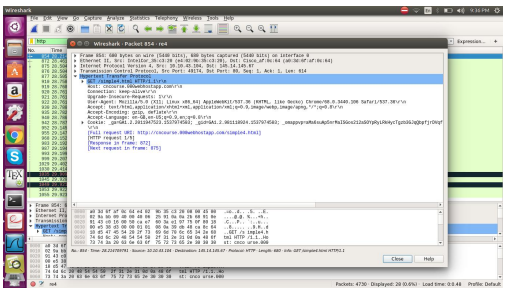

Figure 29: GET package

(2) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes,the server explicitly return the contents of the file. As we can see in the screenshot below that the html file is there in the Link-based text data. Details of all the objects (the various images location) are written in the html file as we can see it.

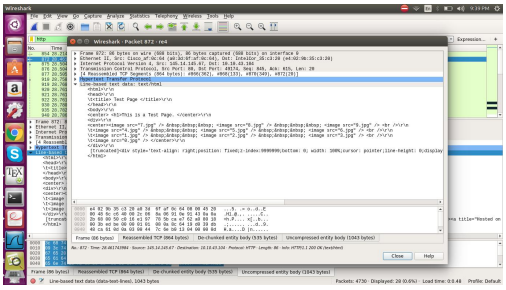

Figure 30: contents of the file

(3) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an IF-MODIFIED-SINCE: line in the HTTP GET? If so, what information follows the IF-MODIFIED-SINCE: header?
No, I didn't saw any IF-MODIFIED-SINCE line in the second HTTP GET also.

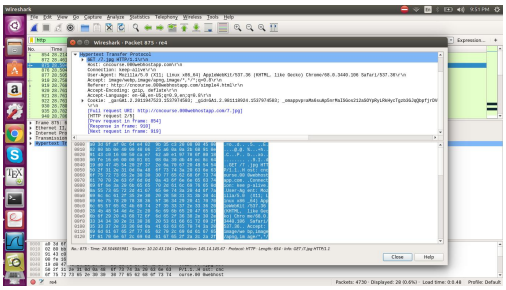

Figure 31: GET package

(4) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Yes,the server explicitly return the contents of the file. As we can see in the screenshot below that the html file is there in the Link-based text data.It shows the details of the image which was requested by the browser when the browser received the first base file(as shown in part 2 screendump content of base file).

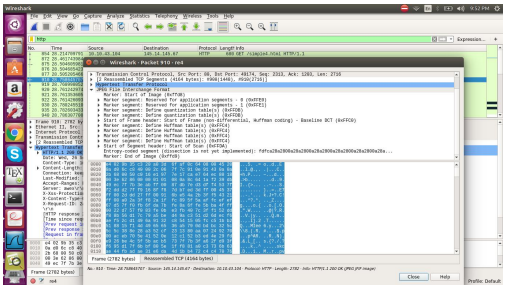

Figure 32: content of the image

3: SET 3: Retrieving Long Documents :

(1) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message ?

(a)For first site i.e. http://cncourse.000webhostapp.com/largeText.html:

The browser send 2 GET request. packet numbers are 11384 and 12015.

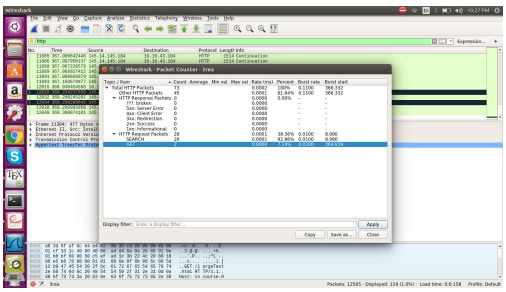

Figure 33: GET count

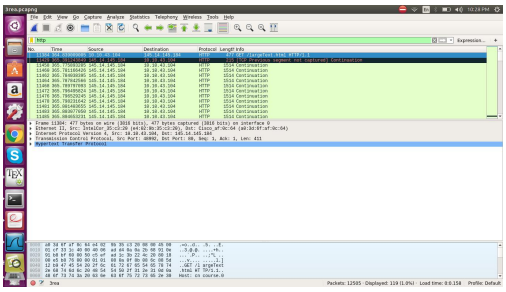

Figure 34: GET package number

(b)For second site i.e.http://cncourse.000webhostapp.com/Sec377judgment.pdf:

The browser send 1 GET request. packet numbers is 588.

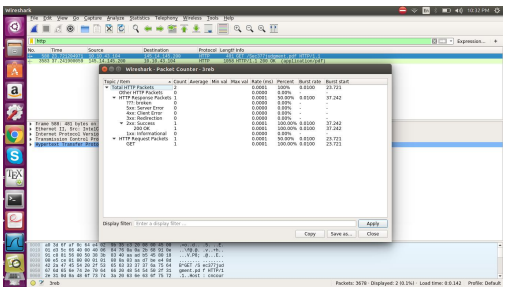

Figure 35: GET count

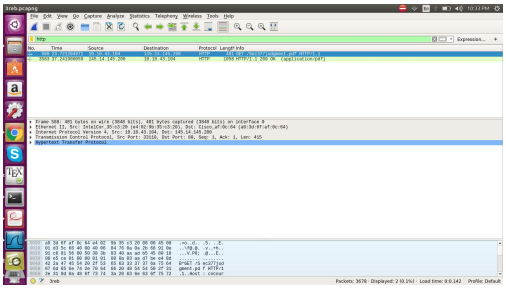

Figure 36: GET package number

(2) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request??

(a)For first site i.e. http://cncourse.000webhostapp.com/largeText.html:

For this i didn't get any status code and phrase associated as we can see below.

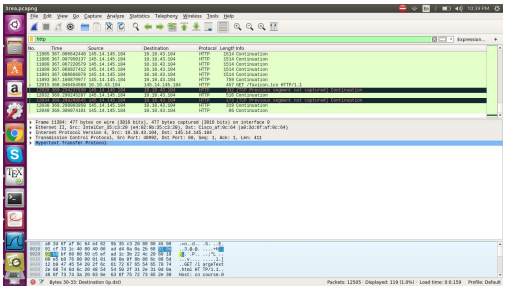

Figure 37: Status code

(b)For second site i.e.http://cncourse.000webhostapp.com/Sec377judgment.pdf:

The packet number is : 3583. **(3) What is the status code and phrase in the response?**

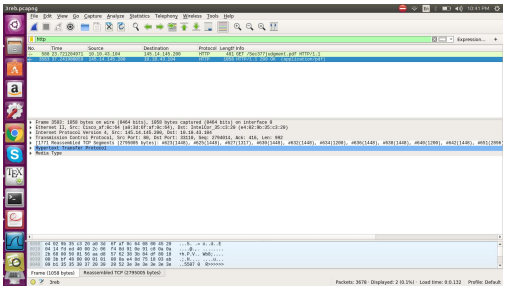

Figure 38: Status code

(a)For first site i.e. http://cncourse.000webhostapp.com/largeText.html:

No, response for this site from the server.

(b)For second site i.e.http://cncourse.000webhostapp.com/Sec377judgment.pdf:

Status code is :200. And the phrase associated is : OK as we can see above.For this screendump is already there in part 2.We can verify it from there.

(4) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the file ?

(a)For first site i.e. http://cncourse.000webhostapp.com/largeText.html:

TCP segments : 75

(b)For second site i.e.http://cncourse.000webhostapp.com/Sec377judgment.pdf:

TCP segments : 3

4: SET 4 - HTML Documents with CGI Script :

(1)What is the method used in your HTTP message ? How many HTTP request messages did your browser send? To which Internet addresses were these requests sent?

Method Used are : GET and POST.
HTTP request send by the browser are : 2 (Get and Post)
IPA to which the request are sent are: 145.14.145.161

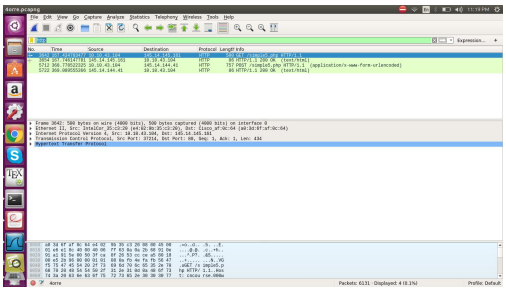

Figure 39: GET AND POST

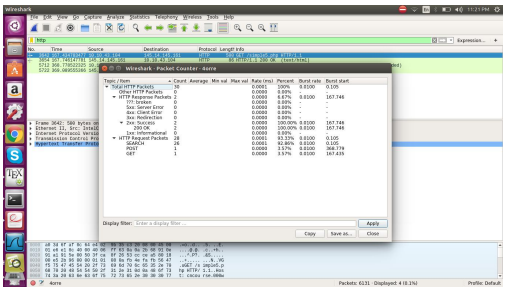

Figure 40: HTTP request by the browser

5: SET 5 - HTTP Authentication :

(1)What is the servers response (status code and phrase) in response to the initial HTTP GET message from your browser?

Status Code : 302
Status Phrase : Found

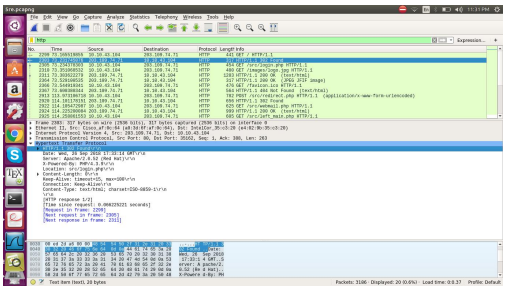

Figure 41: HTTP request by the browser

(2)When your browsers sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

It remains the same , there is no extra field included in the HTTP GET message as we can see in the figure below.

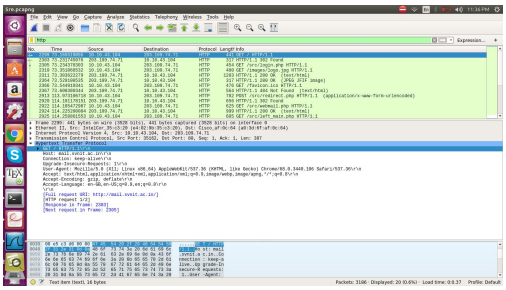

Figure 42: HTTP first GET

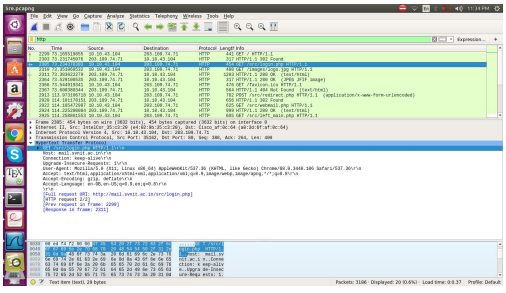

Figure 43: HTTP second GET

(3)Highlight the content of that packet in Wireshark, where the password field is

actually displayed in clear.It must be the same password as you entered while logging in.

Below is the screenshot from where we can verfy the password.

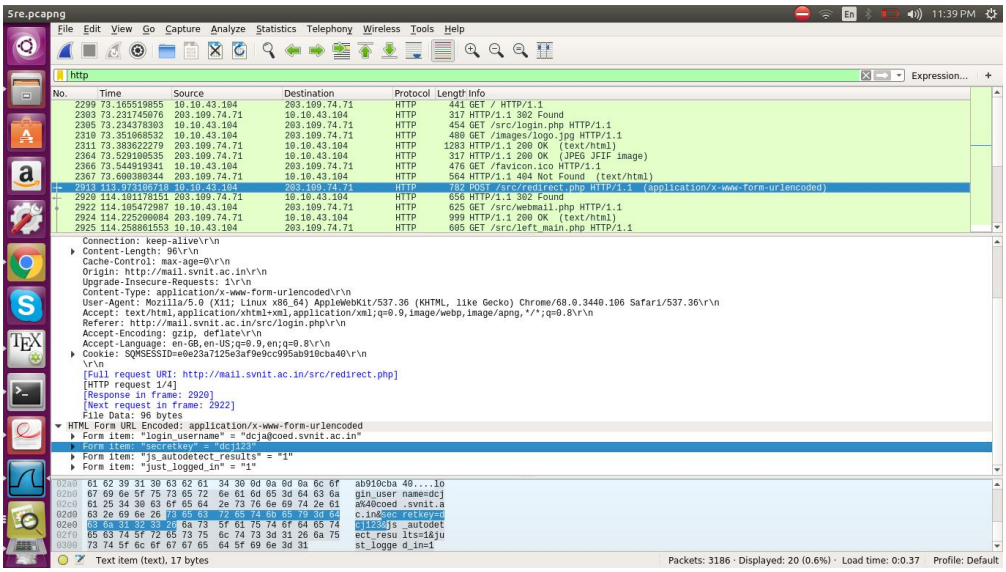

Figure 44: password chunk