CSP334: Computer Networks
Lab Assignment No 4
Http Wireshark Assignment

Abhishek Gupta 2016UCS0012

October 4, 2018

1 SET 1

1.1 Q1

My browser is running HTTP version 1.1. Server is also running HTTP version 1.1

1.2 Q2

My browser indicates that it can accept en-GB (English, Great Britain) to the server

1.3 Q3

IP Address of my computer is 10.10.41.239. IP Address of cncourse web server is 145.14.144.77. You can see it in request message from my computer to cncourse web server

1.4 Q4

Status code returned from the server was 200.
Status Message was OK.

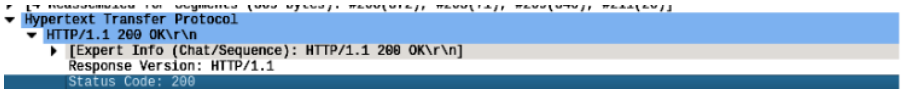

Figure 1: Screenshot of http Get file

1.5 Q5

We can filter messages by http.last-modified and we see that the HTTP response I received for the html file doesn't show this field. However as seen in screenshot my ocsp responce has a last modified field with value of :
Last-Modified: Sun, 16 Sep 2018 01:08:55 GMT

Figure 2: Screenshot of http Get file

1.6 Q6

HTML file sent by cncourse server is of 680 bytes

1.7 Q7

No.The raw data appears to match up exactly with what is shown in thepacket-listing window.

1.8 Q8

A total of 4 requests were sent by my browser as shown in screenshot. Server responded with 2 responses.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP Requests by HTTP Host	4				0.0015	100%	0.0200	10.801
ocsp.comodoca.com	1				0.0004	25.00%	0.0100	10.054
/	1				0.0004	100.00%	0.0100	10.054
cncourse.000webhostapp.com	3				0.0011	75.00%	0.0200	10.801
/simple1.html	1				0.0004	33.33%	0.0100	8.473
/favicon.ico	2				0.0007	66.67%	0.0200	10.801

Figure 3: Screenshot of http Get file

1.9 Q9

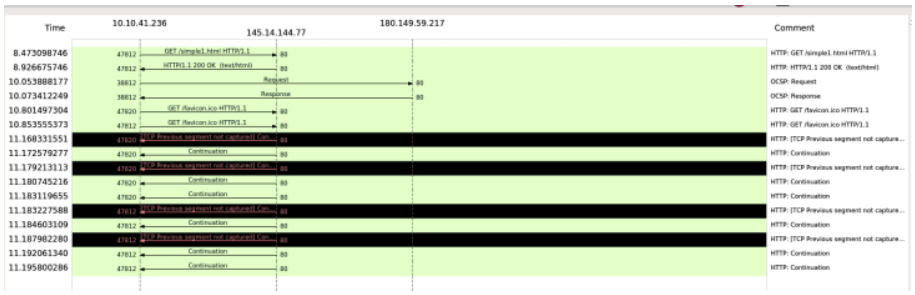

Figure 4: Screenshot of http Get file

2 SET 2

2.1 Q1

No I don't see any IF-MODIFIED-SINCE line in http GET request as you can see in the following screenshot.

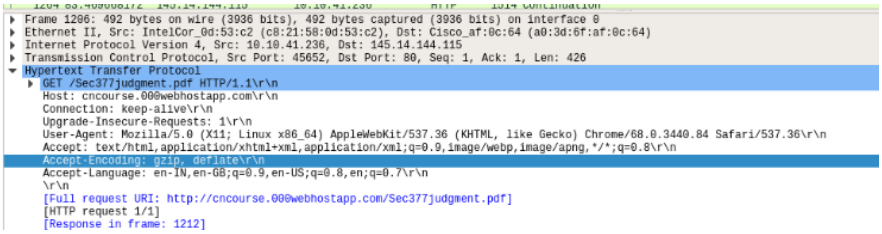

Figure 5: Screenshot of http Get file

2.2 Q2

The server did not explicitly send teh contents of the file as I was requesting a pdf file in my request. However it sents that media type teht it is going to send is of type pdf as you can see in screenshot.

2.3 Q3

Yes,I see an IF-MODIFIED-SINCE: line in the HTTP GET request header.

2.4 Q4

HTTP status code and message sent by server in response to this is 304 Not Modified. Server did not explicitly return anything in response of teh GET message.
It's because there is a proxy server which has this information already stored.In GET request browser asks if the file requested has been modified since a particular date, if not modified do not return anything to the server as this information is already with us.

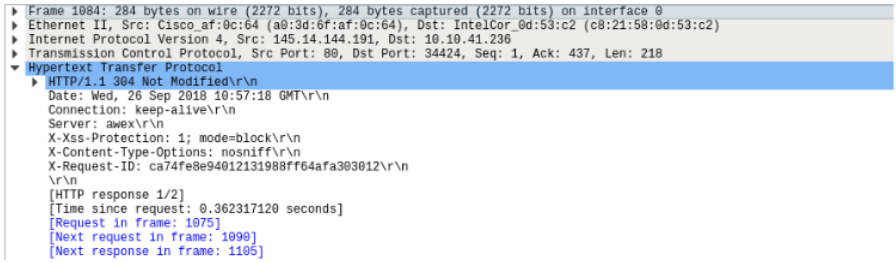

Figure 6: Screenshot of http Get file

3 SET 3

3.1 Q1

Long File:
1 http GET request was sent by my browser to cncourse server. Packet Number 66 is the GET request message.

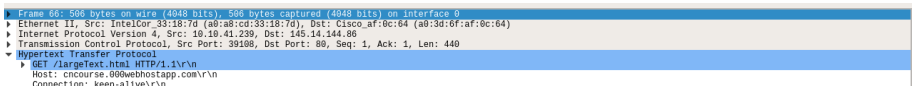

Figure 7: Screenshot of http Get file

PDF File:
2 http GET request messages were sent by my browser. Packet numbers 83 and 3124 are the two

GET requests.

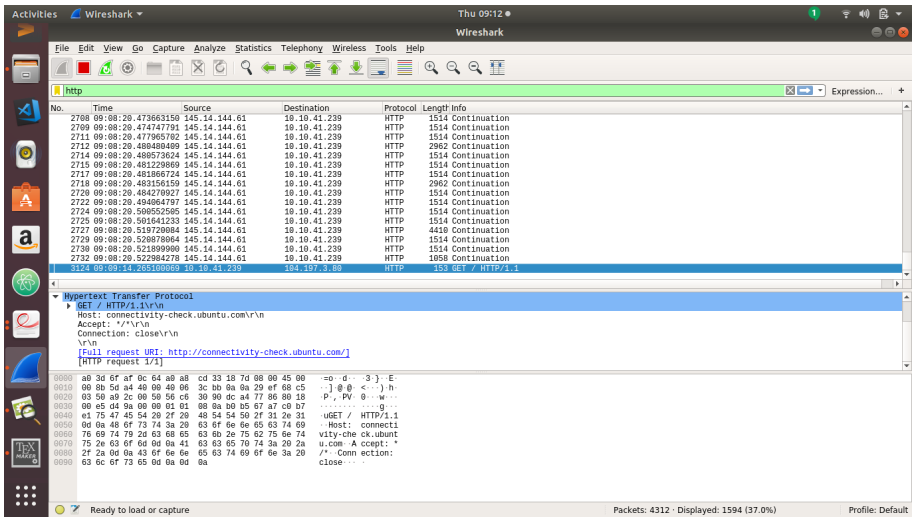

Figure 8: Screenshot of http Get file

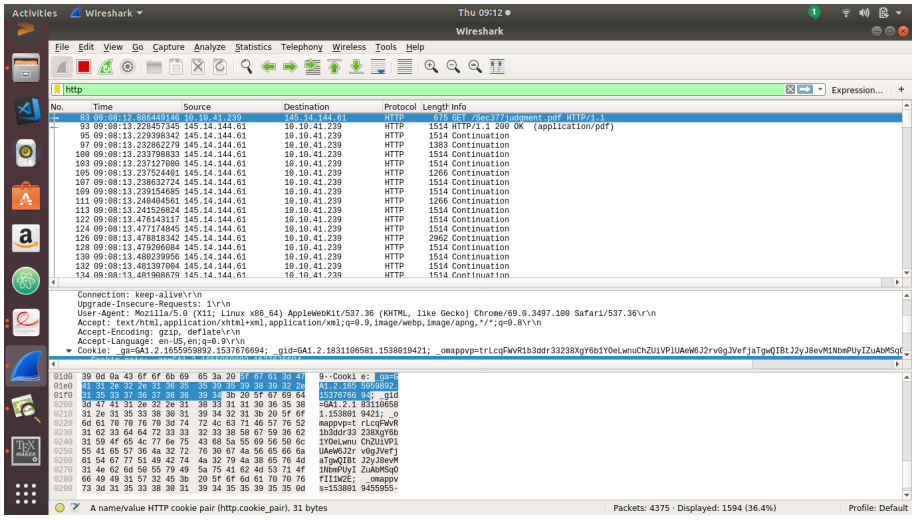

Figure 9: Screenshot of http Get file

3.2 Q2

Long File:
Packet number 73 contains the stauts code 200 and phrase associated with it that is OK.

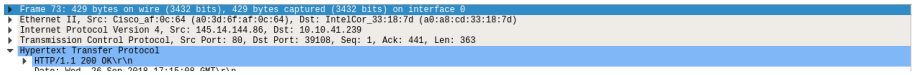

Figure 10: Screenshot of http Get file

Long File:
Packet number 93 contains the stauts code 200 and phrase associated with it that is OK.

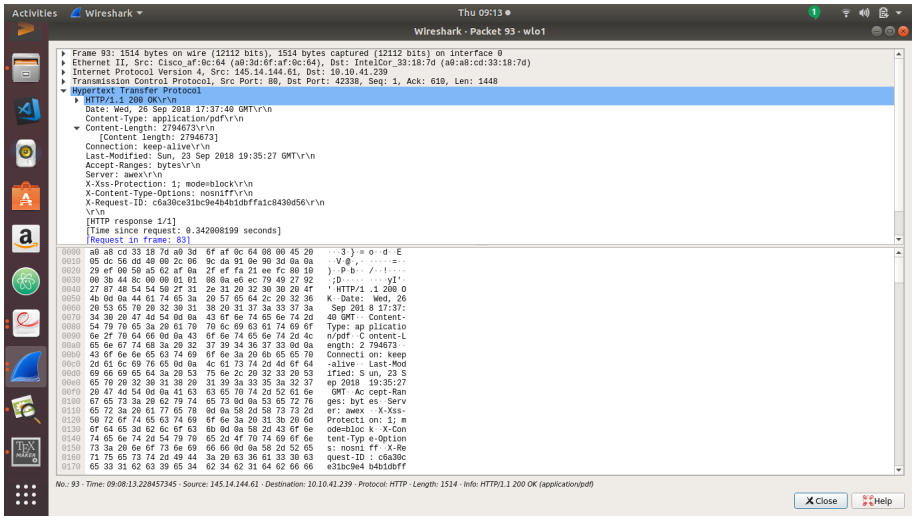

Figure 11: Screenshot of http Get file

3.3 Q3

Long File:
Status Code : 200
Phrase : OK

Pdf File:
Status Code : 200
Phrase : OK

3.4 Q4

In my case, HTTP Continuation responses carried the long text file on the server. I tried to change the same as demostrated on internet by going on ”edit” option in wireshark and select ”preferences option”, then selecting ”tcp” and checking some boxes but that didn’t worked out for me. A total of 246 continuation responses were registered in case of content from wikipedia page.

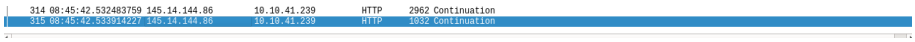

Figure 12: Screenshot of http Get file

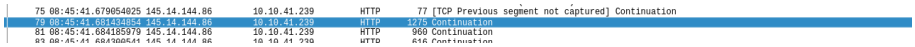

Figure 13: Screenshot of http Get file

As in above case, there are also many continuations http response messages.

4 SET 4

4.1 Q1

Three HTTP messages were sent by my browser. First one is HTTP GET request to open the the html page.Second one is also HTTP GET request to get favicon. Third one was HTTP POST message to post the form that we just filled.You can see these requests in the given screenshot.

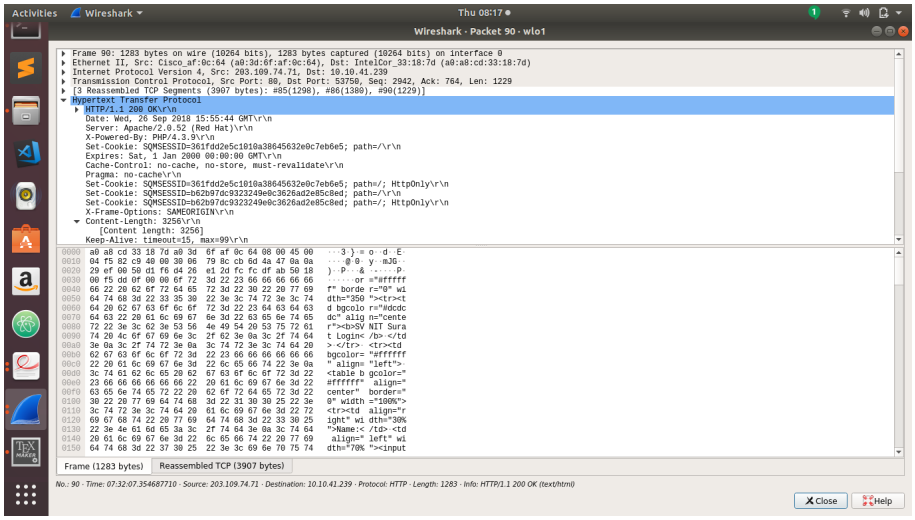

Figure 14: Screenshot of tcpdump file

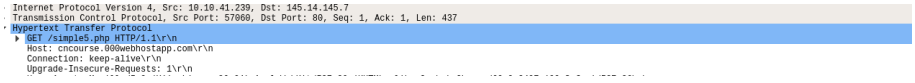

Figure 15: Screenshot of http Get file

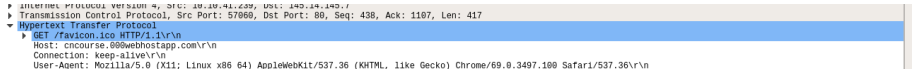

Figure 16: Screenshot of http Get favicon

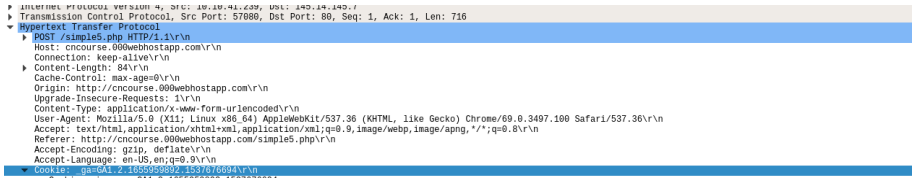

Figure 17: Screenshot of http Post

Figure 18: Screenshot of Form

The requests were sent to cncourse web server (145.14.145.7)

5 SET 5

5.1 Q1

In response to the initial HTTP GET message from my browser, server's re- sponse was 200 OK. You can see this in the screenshot above.

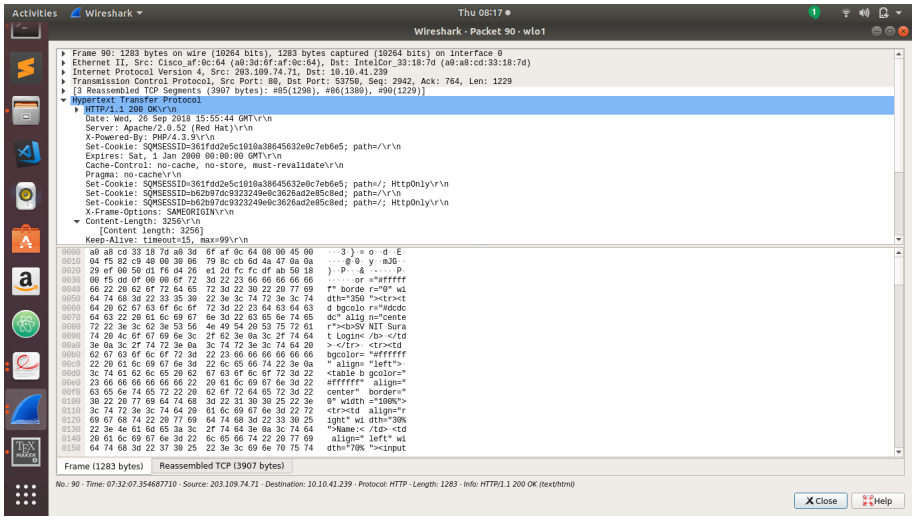

Figure 19: Screenshot of tcpdump file

5.2 Q2

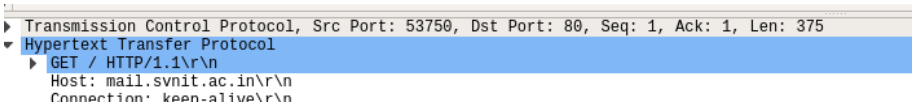

Figure 20: previous http get request

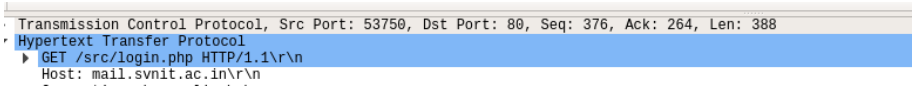

Figure 21: New http get request

When my browser sends the HTTP GET message for the second time, the new field added is Cookie. Cookie: SQMSESSID=b62b97dc9323249e0c3626ad2e85c8ed You can see this highlighted in the below given screenshot:

Figure 22: Screenshot of cookie

5.3 Q3

You can see the highlighted password which I found in POST request

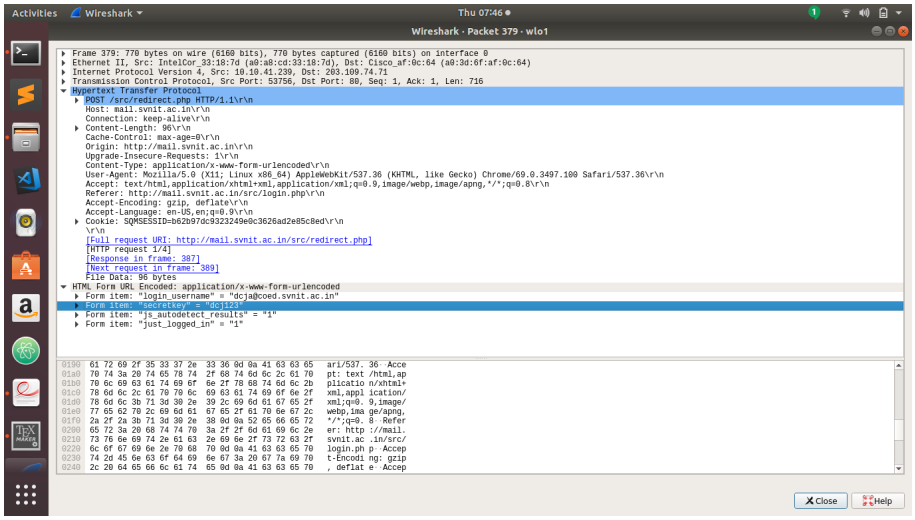

Figure 23: Screenshot of tcpdump file