CSP334: Computer Networks
Lab Assignment No 4
Http Wireshark Assignment

Abhishek Gupta 2016UCS0012

September 27, 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.

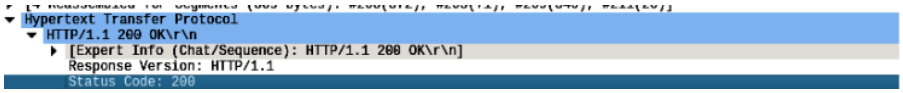

Figure 1: Screenshot of http Get file

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

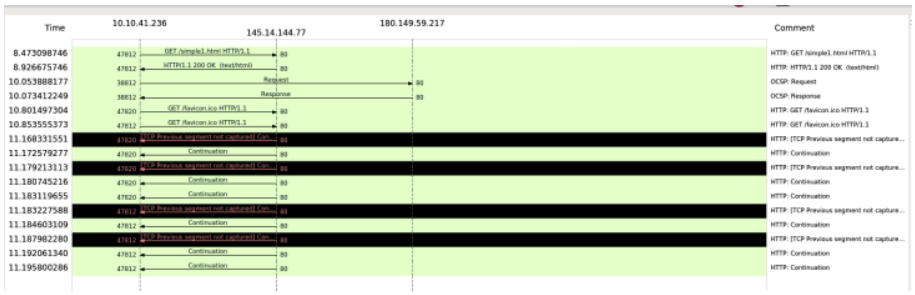

Figure 4: Screenshot of http Get file

1.10 Q10

Last-Modified: Fri, 03 Jun 2016 13:32:18 GMT. This last modified field is for gif image.
No. of bytes for html file = 868 bytes
No. of bytes for image = 9601 bytes
Therefore total bytes returned to browser = 10469 bytes.
Total of 7 http requests were sent and 7 responses were registered from server.

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burs
HTTP Requests by HTTP Host	7				0.0000	100%	0.0100	508
ocsp.sca1b.amazontrust.com	5				0.0000	71.43%	0.0100	102
/	5				0.0000	100.00%	0.0100	102
gifgifs.com	1				0.0000	14.29%	0.0100	509
/animations/nature/waterfalls/Waterfall_4.gif	1				0.0000	100.00%	0.0100	509
cncourse.000webhostapp.com	1				0.0000	14.29%	0.0100	508
/simple2.html	1				0.0000	100.00%	0.0100	508

Figure 13: Question 10

3elow is the http traffic flow graph :

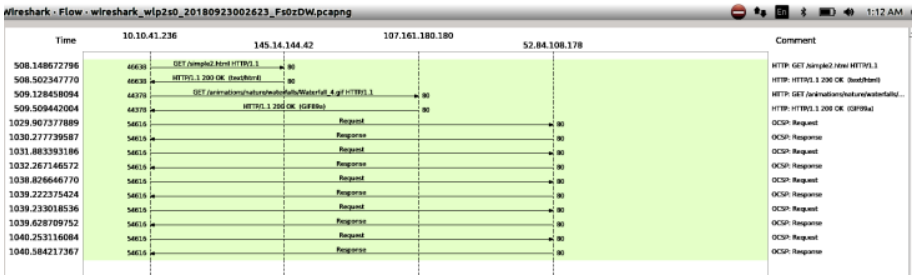

Figure 5: Screenshot of http Get file

1.11 Q11

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sat, 22 Sep 2018 20:16:23 GMT\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  Server: awex\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Request-ID: 1059d4167cd5bdf3bc5bfc63e3cb7b73\r\n
  Content-Encoding: gzip\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.356977795 seconds]
  [Request in frame: 22182]
  [Next request in frame: 22299]
  HTTP chunked response
  Content-encoded entity body (gzip): 572 bytes -> 868 bytes
  File Data: 868 bytes
```

Figure 6: Screenshot of http Get file

1.12 Q12

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sat, 22 Sep 2018 21:54:12 GMT\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  Transfer-Encoding: chunked\r\n
  Connection: keep-alive\r\n
  Server: awex\r\n
  X-Xss-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  X-Request-ID: 8a00483ed244f2a3778358f93faa5feb\r\n
  Content-Encoding: gzip\r\n
  \r\n
```

Figure 7: Screenshot of http Get file

Below is the http traffic flow graph :

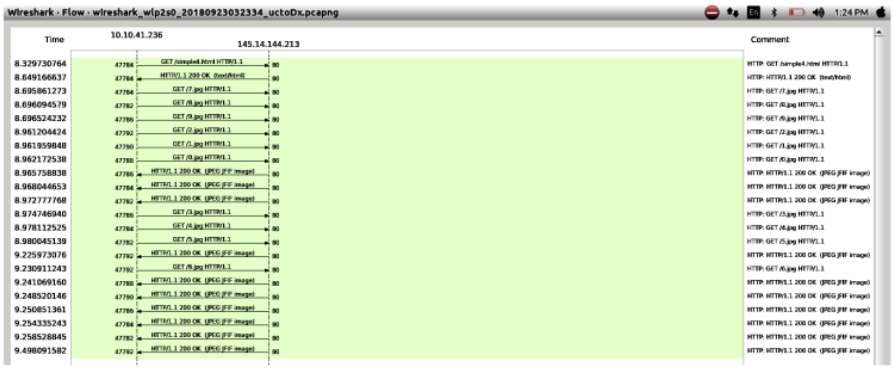

Figure 8: Screenshot of http Get file

1.13 Q13

The time required to access the file is 2.754 - 1.952 = 0.802 seconds or 802 ms.

1.14 Q14

File Value
Source Port No.23
DestinationPort 47360
No.Header Length 32 bytes
Acknowledgement 119
No.Reserved 0(Not set)
Flags 24
Window Size 227
TCP Checksum 62287
Urgent Pointer 0
Options 12 bytes
Data1 byte, 61

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.

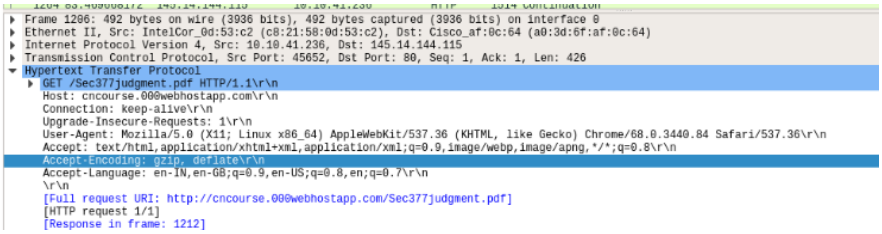

Figure 9: Screenshot of http Get file

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.

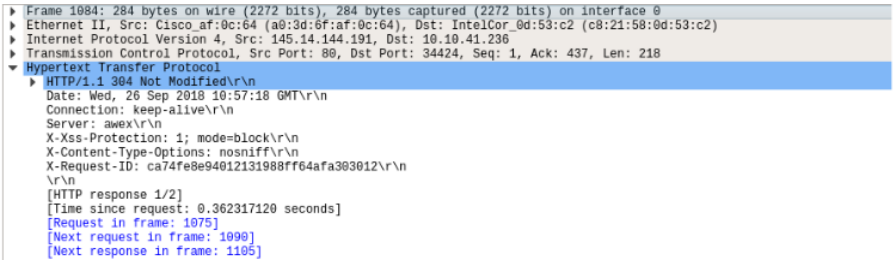

Figure 10: Screenshot of http Get file

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.

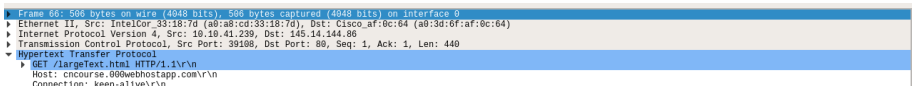

Figure 11: Screenshot of http Get file

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

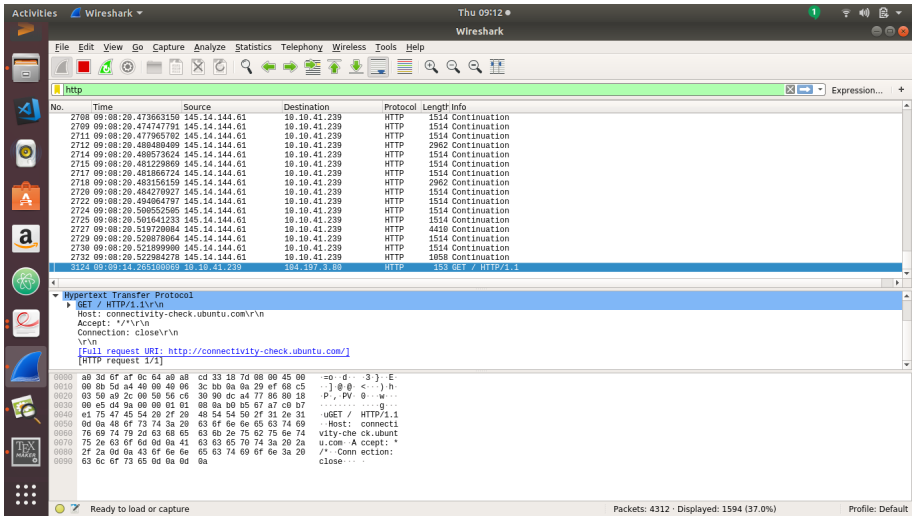

Figure 12: Screenshot of http Get file

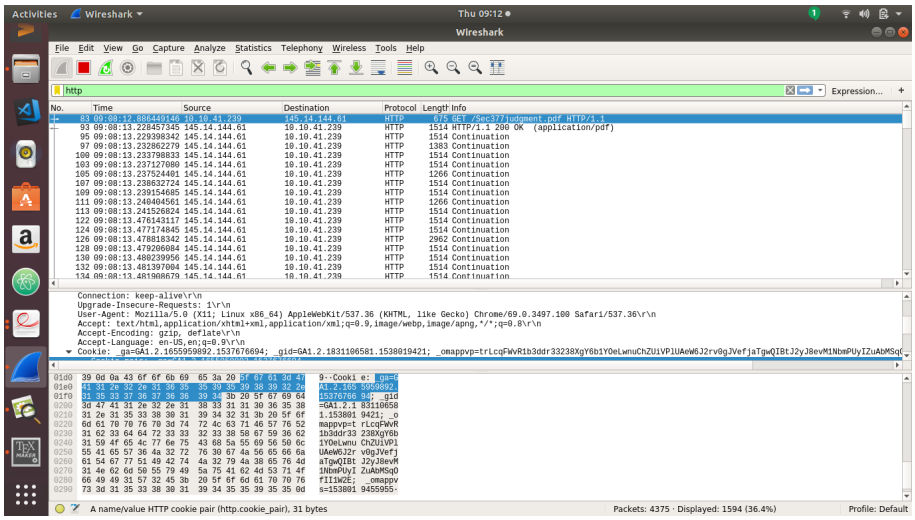

Figure 13: Screenshot of http Get file

3.2 Q2

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

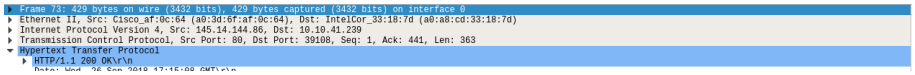

Figure 14: Screenshot of http Get file

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

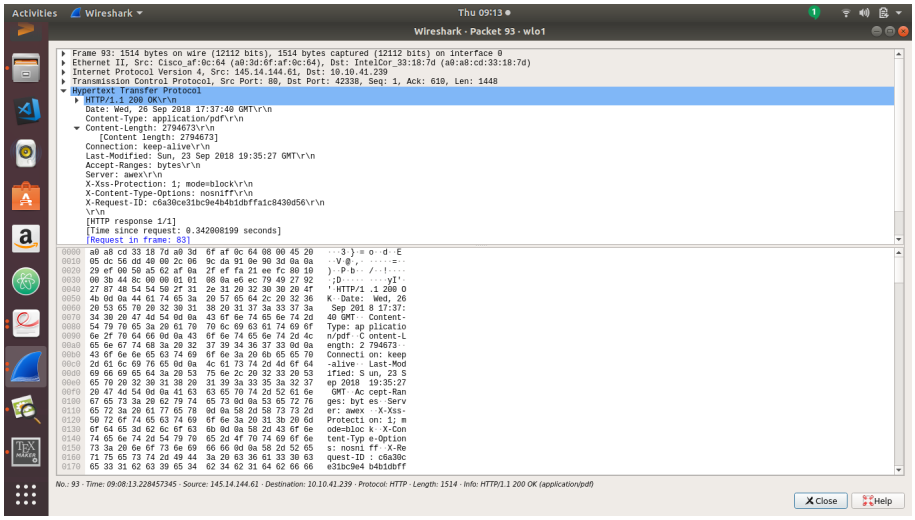

Figure 15: Screenshot of http Get file

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.

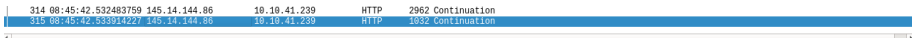

Figure 16: Screenshot of http Get file

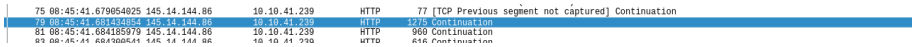

Figure 17: Screenshot of http Get file

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.

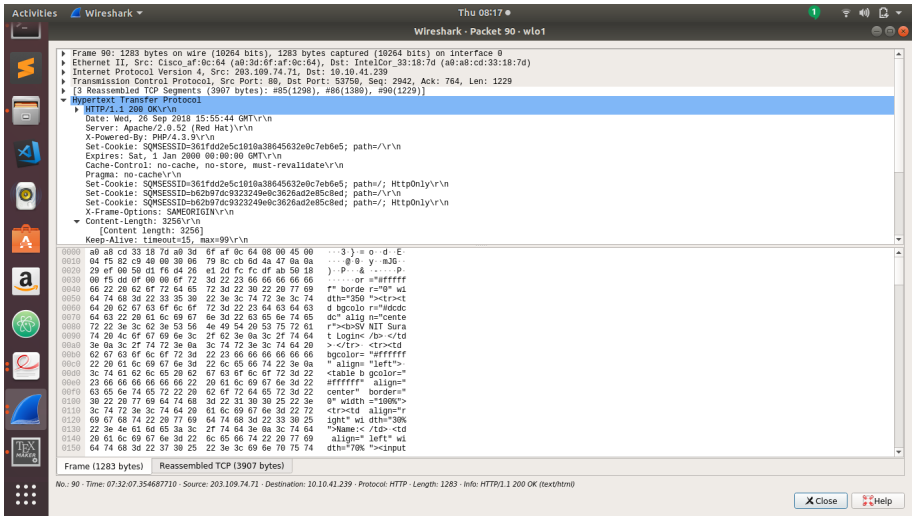

Figure 18: Screenshot of tcpdump file

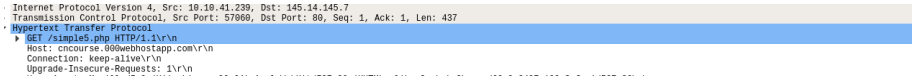

Figure 19: Screenshot of http Get file

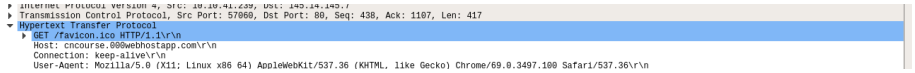

Figure 20: Screenshot of http Get favicon

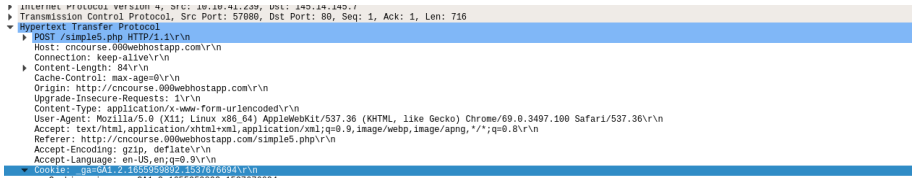

Figure 21: Screenshot of http Post

Figure 22: 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.

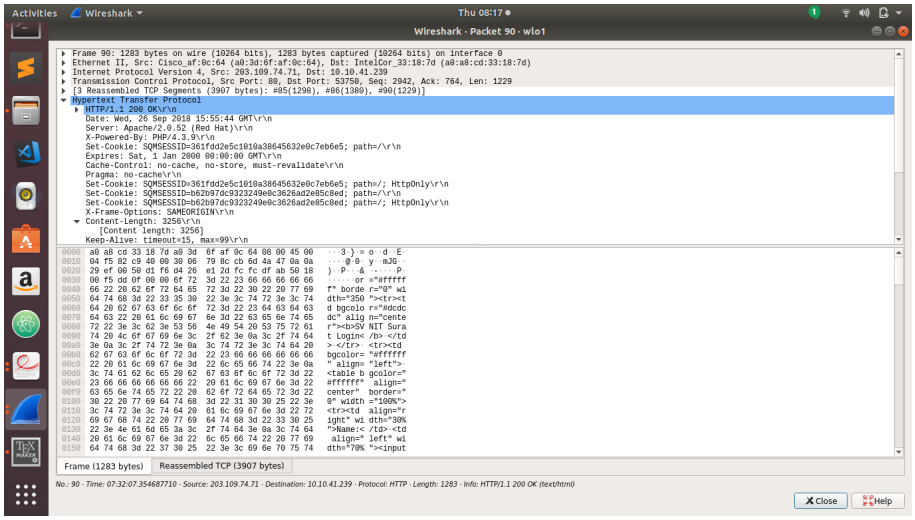

Figure 23: Screenshot of tcpdump file

5.2 Q2

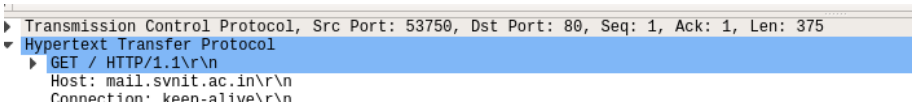

Figure 24: previous http get request

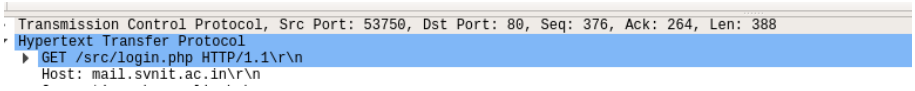

Figure 25: New http get request

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 26: Screenshot of cookie

5.3 Q3

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

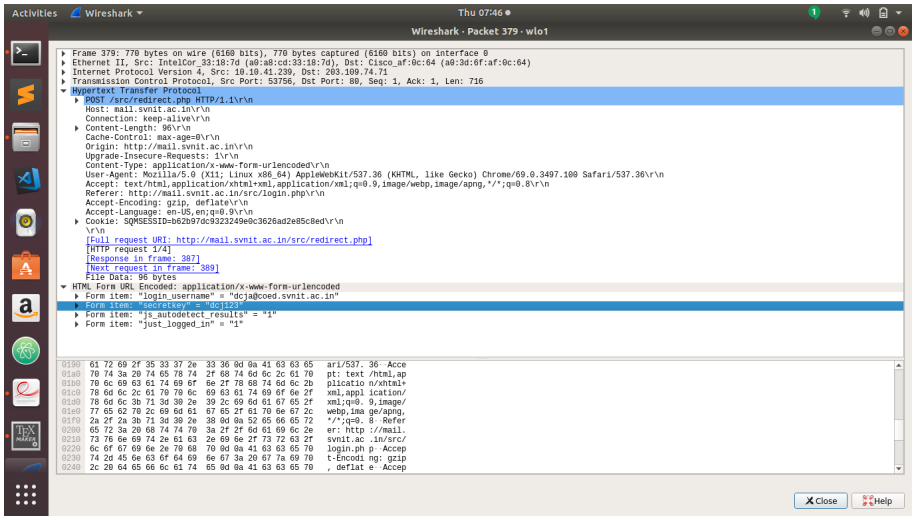

Figure 27: Screenshot of tcpdump file