COMP 535 Assignment 3

Jingyuan Wang 260860682

April 9, 2019

Exercise 1

a. Maximum window size is $\frac{10Mbps \times 150msec}{1500 \times 8bit} = 125$

b. Average window size is $125 \times \frac{3}{4} = 93.75$

Average throughput is $\frac{0.75 \times W}{RTT} = \frac{0.75 \times 125 \times 1500 \times 8b}{150msec} = 7.5Mbps$

c. In a Reno TCP schema considering fast recovery, the window size will drop to $\frac{1}{2} \times cwnd + 3 = 65$ and thus need $(125 - 65) \times 150msec = 9\,\text{sec}$ to grow linearly to the maximum window size of 125.

If we do not consider the fast recovery mechanism, which means the window size drops to $\frac{1}{2} \times cwnd$, then we need $125 \times (1 - 0.5) \times 150msec = 9.375\,\text{sec}$.

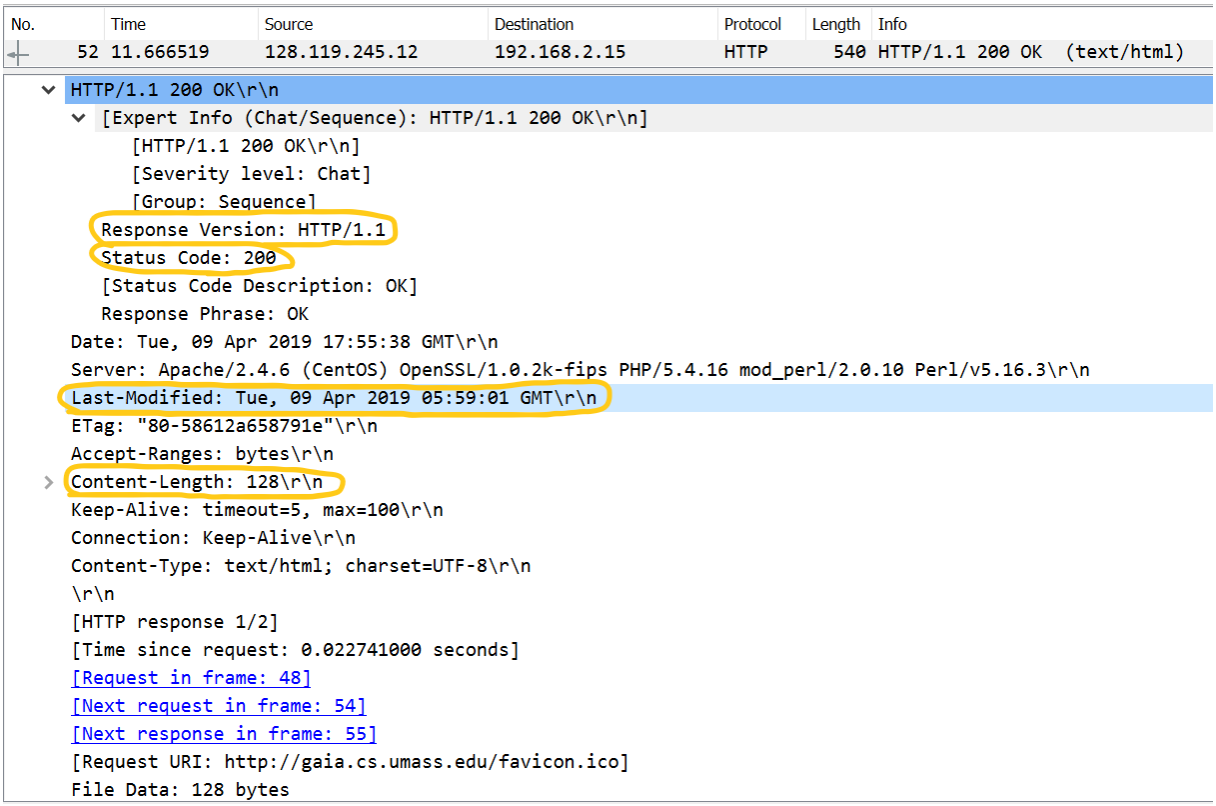
Exercise 2

Part I

```
No.   Time        Source          Destination     Protocol  Length  Info
   48 11.643778   192.168.2.15    128.119.245.12  HTTP       513 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

> Frame 48: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: IntelCor_c6:2a:eb (04:d3:b0:c6:2a:eb), Dst: Sagemcom_49:3d:06 (f0:82:61:49:3d:06)
> Internet Protocol Version 4, Src: 192.168.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52570, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 52]
    [Next request in frame: 54]
```

HTTP GET message from my computer to the server is shown above.



No.	Time	Source	Destination	Protocol	Length	Info
52	11.666519	128.119.245.12	192.168.2.15	HTTP	540	HTTP/1.1 200 OK (text/html)

```
HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
     [HTTP/1.1 200 OK\r\n]
     [Severity level: Chat]
     [Group: Sequence]
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
Date: Tue, 09 Apr 2019 17:55:38 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
Last-Modified: Tue, 09 Apr 2019 05:59:01 GMT\r\n
ETag: "80-58612a658791e"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.022741000 seconds]
[Request in frame: 48]
[Next request in frame: 54]
[Next response in frame: 55]
[Request URI: http://gaia.cs.umass.edu/favicon.ico]
File Data: 128 bytes
```

HTTP response message sent by the server is shown above.

1. My browser is with HTTP version 1.1 as **Request Version:HTTP/1.1** field suggested in the first snapshot.

The server also runs with version 1.1 as **Response Version:HTTP/1.1**

2. Through **Accept-Language: en-Us, en;0.9**, it is indicated that my browser accept both US English and English. It prefer US English but also accept general English with a preference quality value of 0.9.

3. My computer's IP address is 192.168.2.15 while server's IP address is 128.119.245.12

4. **Status Code** is 200.

5. **Last-Modified** is on Tue, 09 Apr 2019 05:59:01 GMT.

6. **Content-Length** is 128.

7. No.

Part II

8. No.

No.	Time	Source	Destination	Protocol	Length	Info
34	2.639883	192.168.2.15	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
38	2.662528	128.119.245.12	192.168.2.15	HTTP	784	HTTP/1.1 200 OK (text/html)
40	2.706632	192.168.2.15	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
41	2.728696	128.119.245.12	192.168.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
64	15.607464	192.168.2.15	128.119.245.12	HTTP	625	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
70	15.629735	128.119.245.12	192.168.2.15	HTTP	294	HTTP/1.1 304 Not Modified

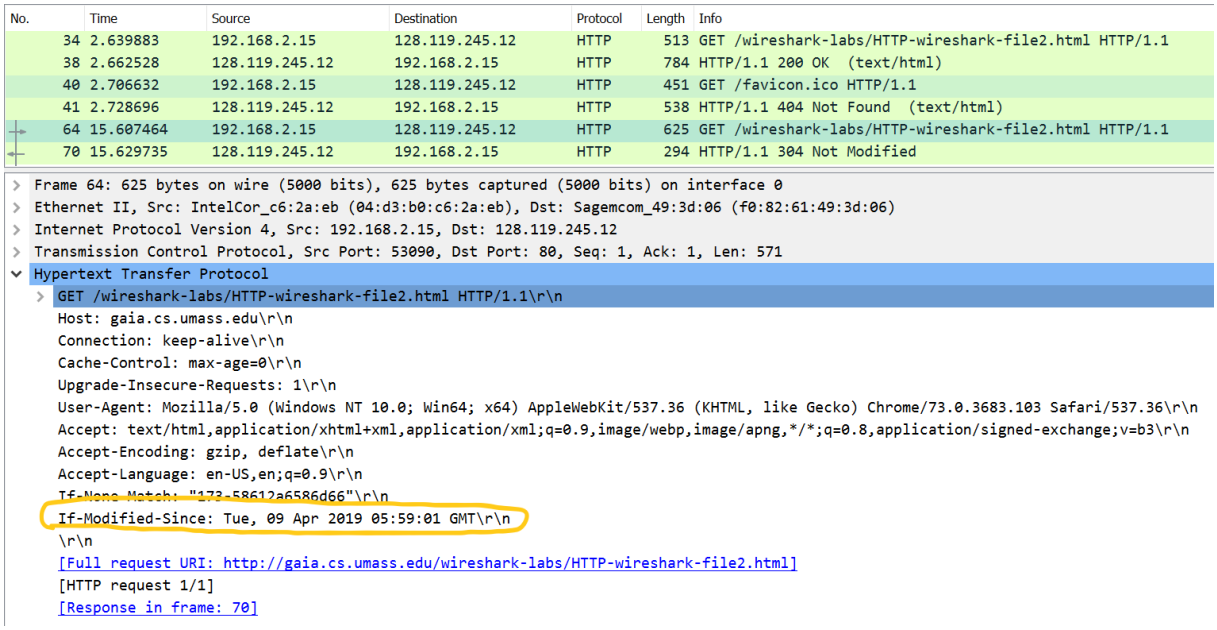
```
Frame 34: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
Ethernet II, Src: IntelCor_c6:2a:eb (04:d3:b0:c6:2a:eb), Dst: Sagemcom_49:3d:06 (f0:82:61:49:3d:06)
Internet Protocol Version 4, Src: 192.168.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53088, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/2]
  [Response in frame: 38]
  [Next request in frame: 40]
```

9. Yes. It is shown in the **Line-based text data** field.

No.	Time	Source	Destination	Protocol	Length	Info
34	2.639883	192.168.2.15	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
38	2.662528	128.119.245.12	192.168.2.15	HTTP	784	HTTP/1.1 200 OK (text/html)

```
  HTTP/1.1 200 OK\r\n
  Date: Tue, 09 Apr 2019 19:06:03 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Last-Modified: Tue, 09 Apr 2019 05:59:01 GMT\r\n
  ETag: "173-58612a6586d66"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.022645000 seconds]
  [Request in frame: 34]
  [Next request in frame: 40]
  [Next response in frame: 41]
  [Request URI: http://gaia.cs.umass.edu/favicon.ico]
  File Data: 371 bytes
Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change.  <p>\n
  Thus  if you download this multiple times on your browser, a complete copy <br>\n
```

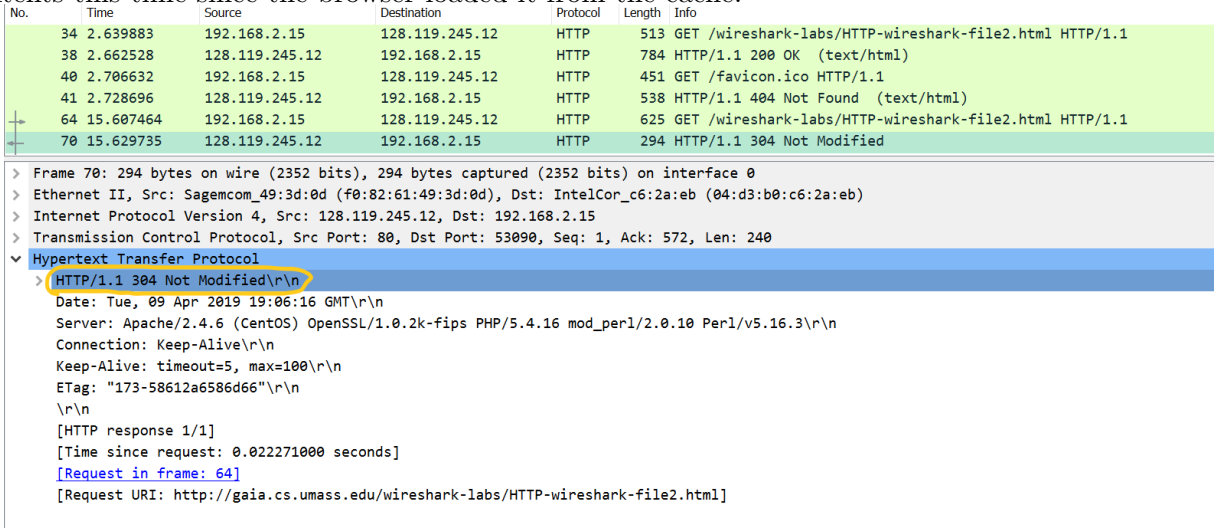
10. Yes. **If-Modified-Since: Tue, 09 Apr 2019 05:59:01 GMT** is the time of last modification field of the previous response message I received in the first part.



No.	Time	Source	Destination	Protocol	Length	Info
34	2.639883	192.168.2.15	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
38	2.662528	128.119.245.12	192.168.2.15	HTTP	784	HTTP/1.1 200 OK (text/html)
40	2.706632	192.168.2.15	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
41	2.728696	128.119.245.12	192.168.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
64	15.607464	192.168.2.15	128.119.245.12	HTTP	625	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
70	15.629735	128.119.245.12	192.168.2.15	HTTP	294	HTTP/1.1 304 Not Modified

```
Frame 64: 625 bytes on wire (5000 bits), 625 bytes captured (5000 bits) on interface 0
Ethernet II, Src: IntelCor_c6:2a:eb (04:d3:b0:c6:2a:eb), Dst: Sagemcom_49:3d:06 (f0:82:61:49:3d:06)
Internet Protocol Version 4, Src: 192.168.2.15, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53090, Dst Port: 80, Seq: 1, Ack: 1, Len: 571
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-58612a6586d66"\r\n
  If-Modified-Since: Tue, 09 Apr 2019 05:59:01 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/1]
  [Response in frame: 70]
```

11. HTTP Status Code and Phase is **304: Not Modified**. The server did not return contents this time since the browser loaded it from the cache.

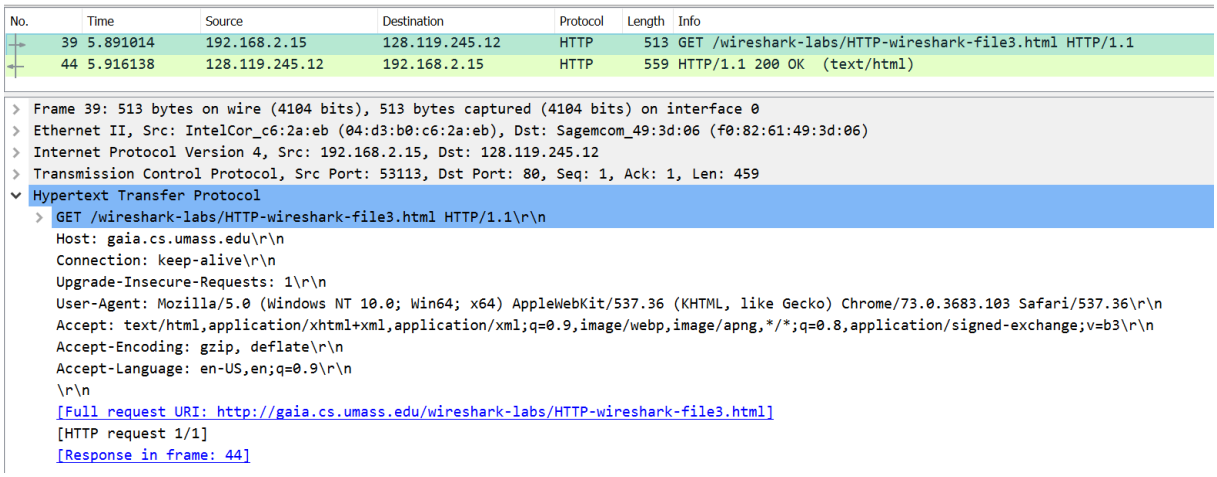


No.	Time	Source	Destination	Protocol	Length	Info
34	2.639883	192.168.2.15	128.119.245.12	HTTP	513	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
38	2.662528	128.119.245.12	192.168.2.15	HTTP	784	HTTP/1.1 200 OK (text/html)
40	2.706632	192.168.2.15	128.119.245.12	HTTP	451	GET /favicon.ico HTTP/1.1
41	2.728696	128.119.245.12	192.168.2.15	HTTP	538	HTTP/1.1 404 Not Found (text/html)
64	15.607464	192.168.2.15	128.119.245.12	HTTP	625	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
70	15.629735	128.119.245.12	192.168.2.15	HTTP	294	HTTP/1.1 304 Not Modified

```
Frame 70: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
Ethernet II, Src: Sagemcom_49:3d:0d (f0:82:61:49:3d:0d), Dst: IntelCor_c6:2a:eb (04:d3:b0:c6:2a:eb)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 53090, Seq: 1, Ack: 572, Len: 240
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
  Date: Tue, 09 Apr 2019 19:06:16 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-58612a6586d66"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.022271000 seconds]
  [Request in frame: 64]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Part III

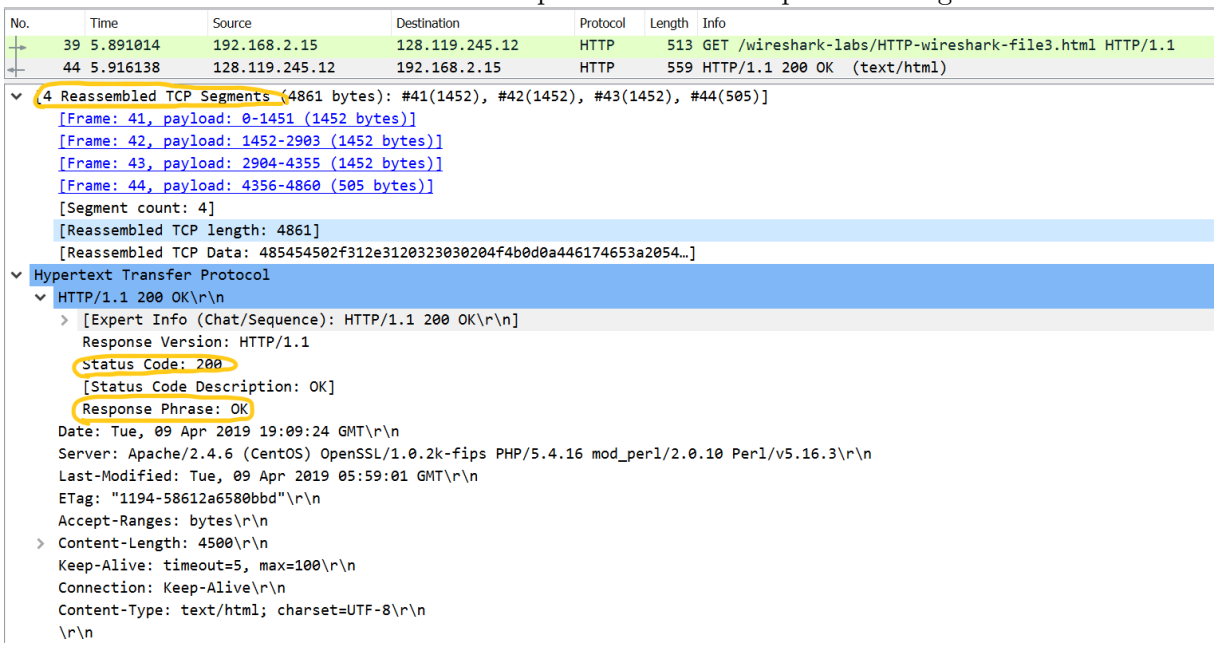
12. My browser sent one HTTP GET request whose packet number is 39.



```
No.  Time      Source          Destination     Protocol  Length  Info
  39 5.891014  192.168.2.15    128.119.245.12  HTTP         513  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 5.916138  128.119.245.12  192.168.2.15    HTTP         559  HTTP/1.1 200 OK  (text/html)

> Frame 39: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface 0
> Ethernet II, Src: IntelCor_c6:2a:eb (04:d3:b0:c6:2a:eb), Dst: Sagemcom_49:3d:06 (f0:82:61:49:3d:06)
> Internet Protocol Version 4, Src: 192.168.2.15, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53113, Dst Port: 80, Seq: 1, Ack: 1, Len: 459
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    [HTTP request 1/1]
    [Response in frame: 44]
```

13. Packet 44 contains the status code and phrase with the response message.



```
No.  Time      Source          Destination     Protocol  Length  Info
  39 5.891014  192.168.2.15    128.119.245.12  HTTP         513  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 5.916138  128.119.245.12  192.168.2.15    HTTP         559  HTTP/1.1 200 OK  (text/html)

v [4 Reassembled TCP Segments (4861 bytes): #41(1452), #42(1452), #43(1452), #44(505)]
    [Frame: 41, payload: 0-1451 (1452 bytes)]
    [Frame: 42, payload: 1452-2903 (1452 bytes)]
    [Frame: 43, payload: 2904-4355 (1452 bytes)]
    [Frame: 44, payload: 4356-4860 (505 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2054…]
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 09 Apr 2019 19:09:24 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Tue, 09 Apr 2019 05:59:01 GMT\r\n
    ETag: "1194-58612a6580bbd"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
```

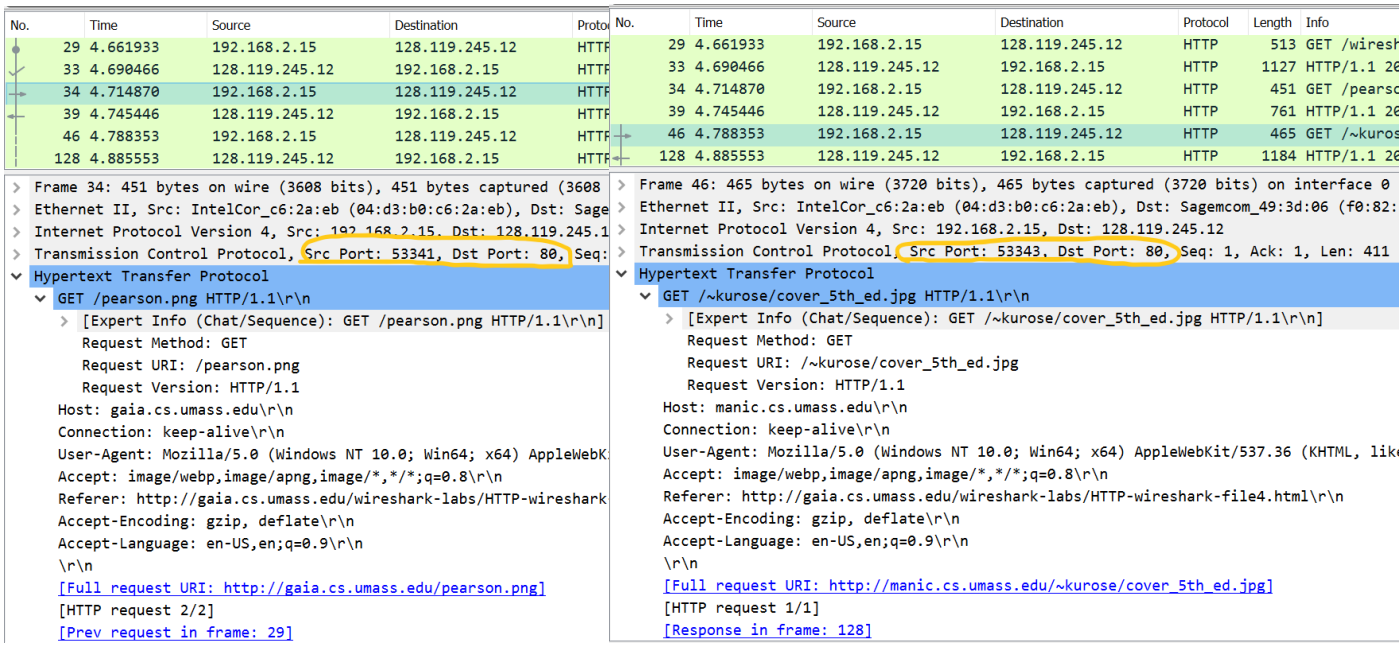
14. **Status Code** is 200. **Response Phrase** is OK.

15. Four TCP segments were needed.

Part IV

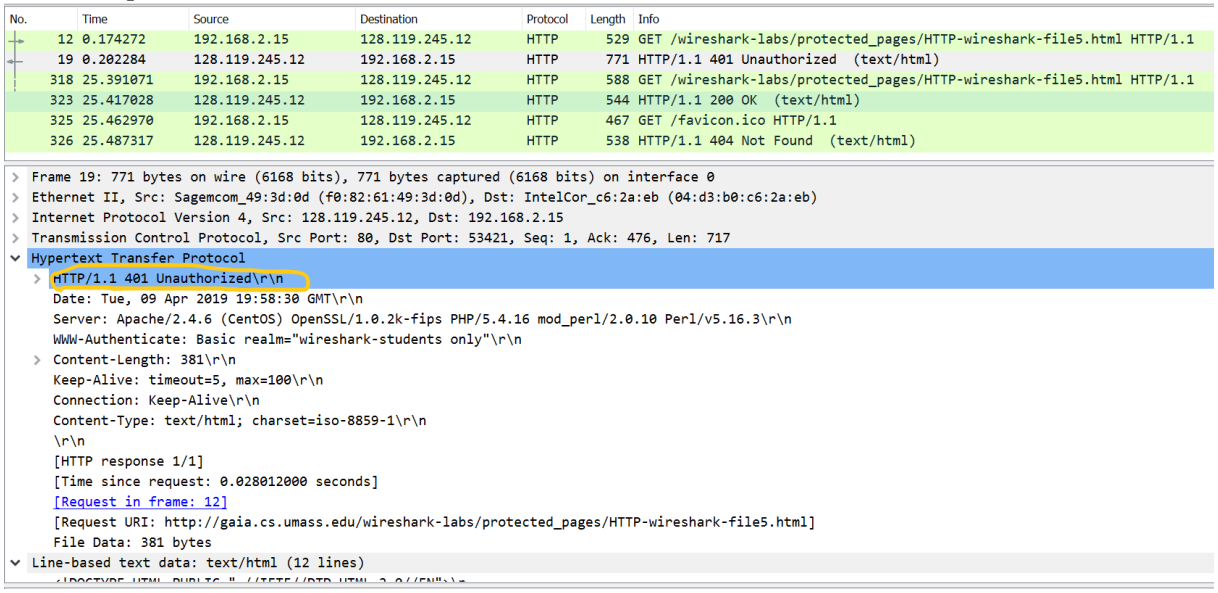
16. My browser sent 3 HTTP GET request messages. They were sent to IP address 128.119.245.12 as in the snapshots of the next question.

17. The two images were downloaded in parallel. As marked in the snapshots, the source port of the TCP messages are different indicating my browser established one TCP connection for getting each image data separately.

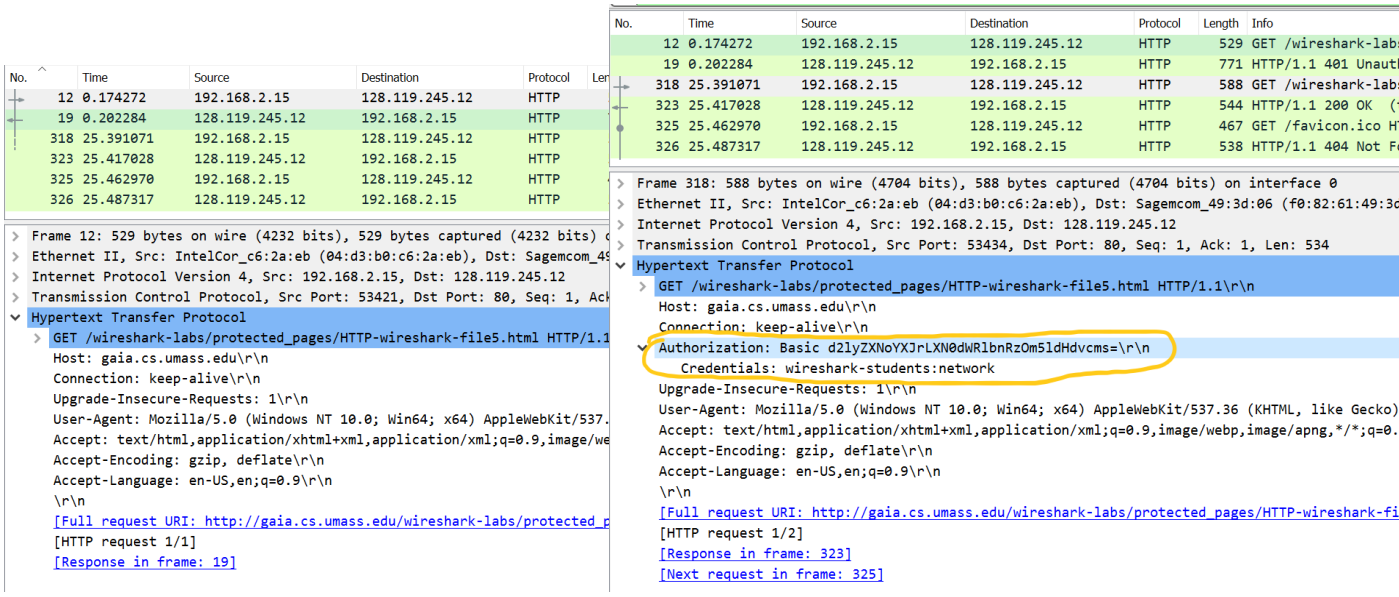


Part V

18. The response is **401 Unauthorized**



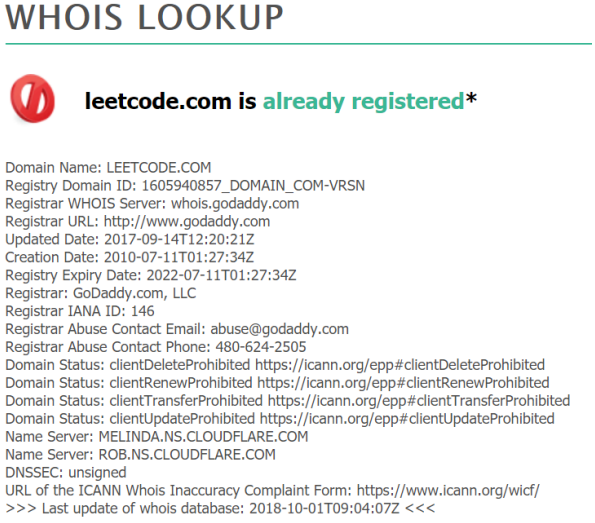
19. After comparing those two messages, we can easily discover that the second response included **Authorization** field, decoded as "wireshark-students:network", which is the combination of our username and password.



Exercise 3

a. **WHOIS** is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.

b. I used *https://whois.net/* to search for dns server names.
bilibili.com: NS3.DNSV5.COM NS4.DNSV5.COM
leetcode.com: MELINDA.NS.CLOUDFLARE.COM ROB.NS.CLOUDFLARE.COM



c. **bilibili.com:**

```
> set type=mx
> bilibili.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
bilibili.com    MX preference = 5, mail exchanger = mxbiz1.qq.com
bilibili.com    MX preference = 10, mail exchanger = mxbiz2.qq.com

bilibili.com    nameserver = ns3.dnsv5.com
bilibili.com    nameserver = ns4.dnsv5.com
> set type=ns
> bilibili.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
bilibili.com    nameserver = ns4.dnsv5.com
bilibili.com    nameserver = ns3.dnsv5.com
> set type=a
> bilibili.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
Name:    bilibili.com
Address:  61.244.33.181
```

leetcode.com:

```
> set type=mx
> leetcode.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
leetcode.com    MX preference = 1, mail exchanger = aspmx.l.google.com
leetcode.com    MX preference = 10, mail exchanger = alt3.aspmx.l.google.com
leetcode.com    MX preference = 10, mail exchanger = alt4.aspmx.l.google.com
leetcode.com    MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
leetcode.com    MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
> set type=ns
> leetcode.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
leetcode.com    nameserver = melinda.ns.cloudflare.com
leetcode.com    nameserver = rob.ns.cloudflare.com
> set type=a
> leetcode.com
Server:  mynetwork
Address:  192.168.2.1

Non-authoritative answer:
Name:    leetcode.com
Addresses:  104.24.125.31
          104.24.124.31
```

d. In the *leetcode.com* nslookup figure, it is shown that there are 2 IP address in *Non-authoritative answer* section and it has multiple IP addresses. Mcgill Web Server does not have multiple IP addresses.

e. 108.170.192.0 - 108.170.255.255 108.177.0.0 - 108.177.127.255 142.250.0.0 - 142.251.255.255
172.217.0.0 - 172.217.255.255 172.253.0.0 - 172.253.255.255 173.194.0.0 - 173.194.255.255
192.178.0.0 - 192.179.255.255 199.87.241.32 - 199.87.241.63 199.88.130.0 - 199.88.130.255
199.89.220.0 - 199.89.220.255 207.223.160.0 - 207.223.175.255 209.170.110.128 - 209.170.110.255
209.170.119.128 - 209.170.119.255 209.170.120.64 - 209.170.120.127 209.170.91.128 - 209.170.91.191
209.85.128.0 - 209.85.255.255 216.239.32.0 - 216.239.63.255 216.58.192.0 - 216.58.223.255
64.233.160.0 - 64.233.191.255 66.102.0.0 - 66.102.15.255 66.249.64.0 - 66.249.95.255
70.32.128.0 - 70.32.159.255 70.90.219.48 - 70.90.219.55 70.90.219.72 - 70.90.219.79
72.14.192.0 - 72.14.255.255 74.114.24.0 - 74.114.31.255 74.125.0.0 - 74.125.255.255

f. *Whois database* and *nslookup* tool can be easily used to search for IP addresses and domain information which would be needed to perform SYN flooding or other kinds of attacks.

g. Whois databases should be publicly available because they are used to find out registration and IP information about domains and are really helpful for those who wants to set up new websites or search for some particular IP or domain informations.