IMRAN KHAN(1802035)

Computer Networks

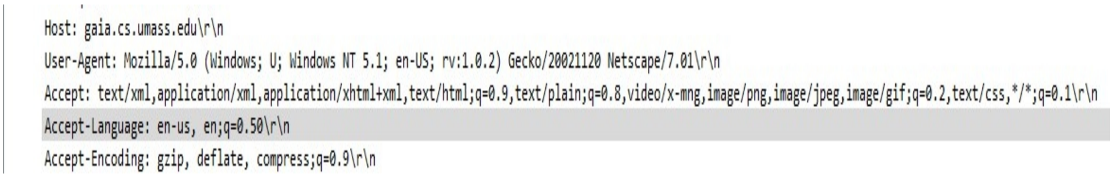
Lab#1(Wire shark)

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

Browser:1.1

Server:1.1

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



```
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
Accept-Language: en-us, en;q=0.50\r\n
Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
```

3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Source:192.168.1.102

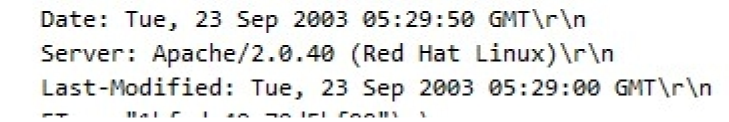
Destination:128.119.245.12

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

I) 200 ok

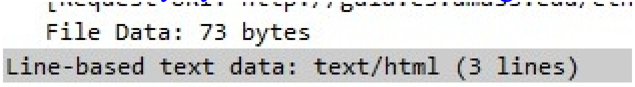
II) 404 Not found

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



```
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
```

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



```
 File Data: 73 bytes
Line-based text data: text/html (3 lines)
```

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.

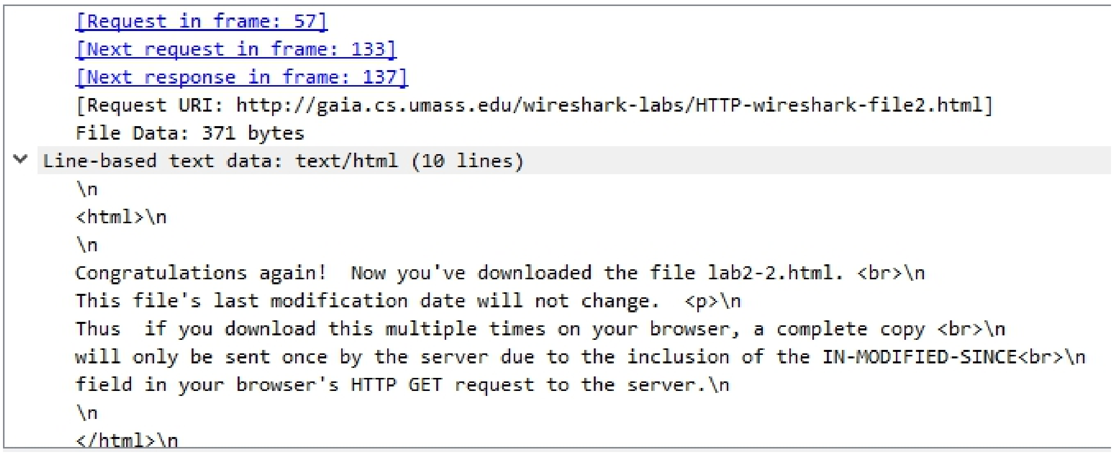
……..Ignored

8. 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 there is not any “IF-MODIFIED-SINCE” line in the HTTP GET.

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

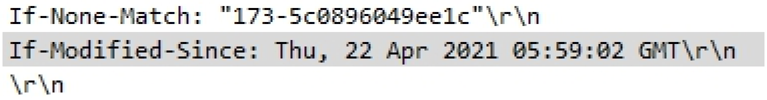
Yes the server explicitly returned the contents of the file.From the screenshot below its obvious that the server returned the file explicitly as there is 371 bytes data we received.



```
    [Request in frame: 57]
    [Next request in frame: 133]
    [Next response in frame: 137]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    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
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

10. 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?

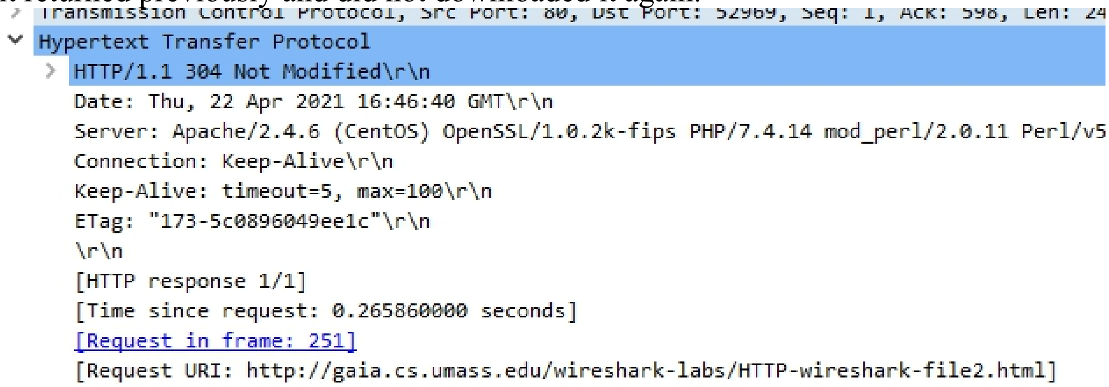
Yes there is “IF-MODIFIED-SINCE:” line in the HTTP GET.The server did not modified the file after we accessed it before and it shows time at which last time the file was modified.



```
If-None-Match: "173-5c0896049ee1c"\r\n
If-Modified-Since: Thu, 22 Apr 2021 05:59:02 GMT\r\n
\r\n
```

11. 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.

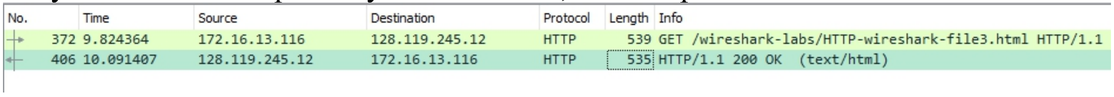
In res ponce to the second HTTP Get request status code was 304 and phrase was Not Modified.No the server did not explicitly return the contents of the file as upon our second request the was no modification in the file ,the browser returned the same file it returned previously and did not downloaded it again.



```
> Transmission Control Protocol, Src Port: 80, Dst Port: 52969, Seq: 1, Ack: 598, Len: 24
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 22 Apr 2021 16:46:40 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5c0896049ee1c"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.265860000 seconds]
    [Request in frame: 251]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

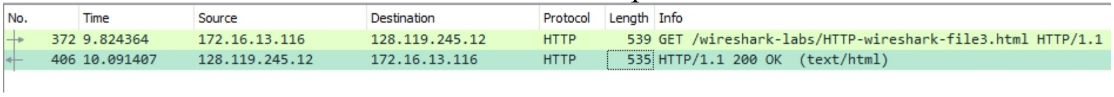
Only 1 HTTP Get request my browser send,with the packet number 372.



```
No.     Time        Source           Destination      Protocol  Length  Info
  372   9.824364    172.16.13.116    128.119.245.12   HTTP         539  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  406   10.091407   128.119.245.12   172.16.13.116    HTTP         535  HTTP/1.1 200 OK  (text/html)
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Packet No 406 contains the status code 200 with phrase “OK”.



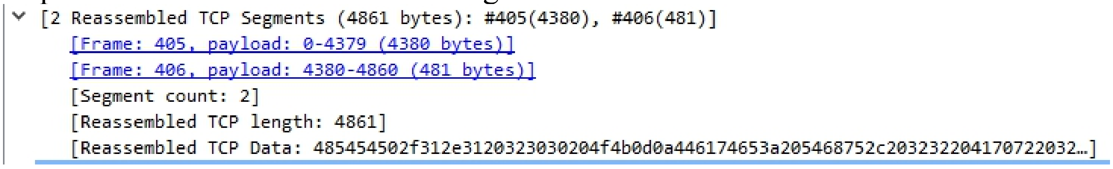
```
No.     Time        Source           Destination      Protocol  Length  Info
  372   9.824364    172.16.13.116    128.119.245.12   HTTP         539  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  406   10.091407   128.119.245.12   172.16.13.116    HTTP         535  HTTP/1.1 200 OK  (text/html)
```

14. What is the status code and phrase in the response?

The status code 200 with phrase “OK”

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

There were 2 TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.

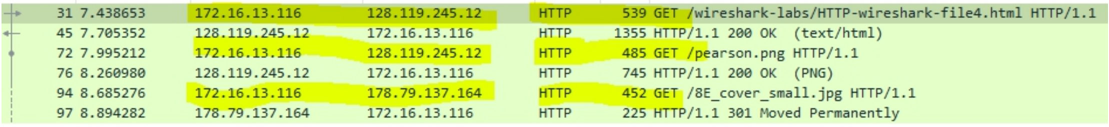


```
v [2 Reassembled TCP Segments (4861 bytes): #405(4380), #406(481)]
    [Frame: 405, payload: 0-4379 (4380 bytes)]
    [Frame: 406, payload: 4380-4860 (481 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a205468752c203232204170722032…]
```

16. How many HTTP GET request messages did your browser send? To which

Internet addresses were these GET requests sent?

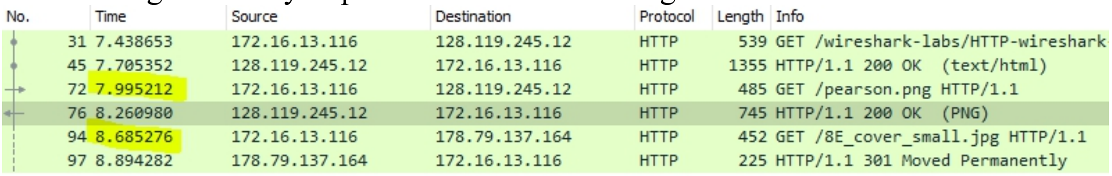
3 HTTP GET requets were send by the browsers.



```
31 7.438653  172.16.13.116   128.119.245.12  HTTP   539 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
45 7.705352  128.119.245.12  172.16.13.116   HTTP  1355 HTTP/1.1 200 OK  (text/html)
72 7.995212  172.16.13.116   128.119.245.12  HTTP   485 GET /pearson.png HTTP/1.1
76 8.260980  128.119.245.12  172.16.13.116   HTTP   745 HTTP/1.1 200 OK  (PNG)
94 8.685276  172.16.13.116   178.79.137.164  HTTP   452 GET /8E_cover_small.jpg HTTP/1.1
97 8.894282  178.79.137.164  172.16.13.116   HTTP   225 HTTP/1.1 301 Moved Permanently
```

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

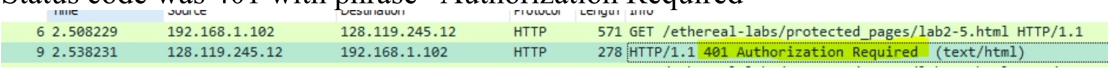
The browser downloaded the two images in serially,because the first image was requested and sent before the second image was requested by the browser. I they were requested at the same time been running in parallel, both files would have been requested then would have returned in the same time period. In this case however, the second image was only requested after the first image came back.



```
No.  Time         Source           Destination      Protocol  Length  Info
 31  7.438653     172.16.13.116    128.119.245.12   HTTP       539   GET /wireshark-labs/HTTP-wireshark
 45  7.705352     128.119.245.12   172.16.13.116    HTTP      1355   HTTP/1.1 200 OK  (text/html)
 72  7.995212     172.16.13.116    128.119.245.12   HTTP       485   GET /pearson.png HTTP/1.1
 76  8.260980     128.119.245.12   172.16.13.116    HTTP       745   HTTP/1.1 200 OK  (PNG)
 94  8.685276     172.16.13.116    178.79.137.164   HTTP       452   GET /8E_cover_small.jpg HTTP/1.1
 97  8.894282     178.79.137.164   172.16.13.116    HTTP       225   HTTP/1.1 301 Moved Permanently
```

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

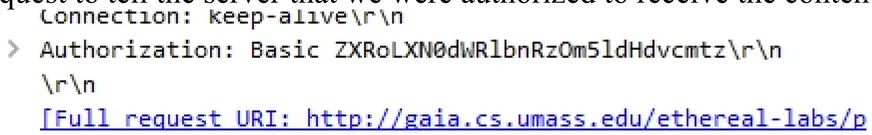
Status code was 401 with phrase "Authorization Required"



```
   Time        Source          Destination     Protocol  Length  Info
 6 2.508229    192.168.1.102   128.119.245.12  HTTP       571    GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
 9 2.538231    128.119.245.12  192.168.1.102   HTTP       278    HTTP/1.1 401 Authorization Required  (text/html)
```

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The new field that is now included is the authorization field.Username and password(encoded in a format known as Base64 format.) were send along with our request to tell the server that we were authorized to receive the content.



```
  Connection: keep-alive\r\n
> Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/p
```