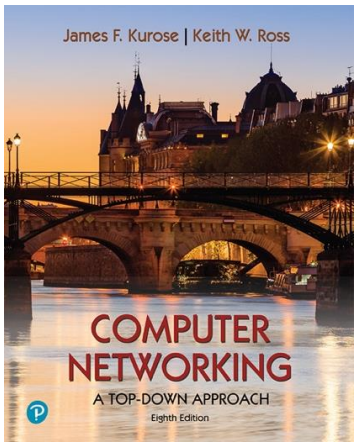
Wireshark Lab: HTTP v8.1

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross

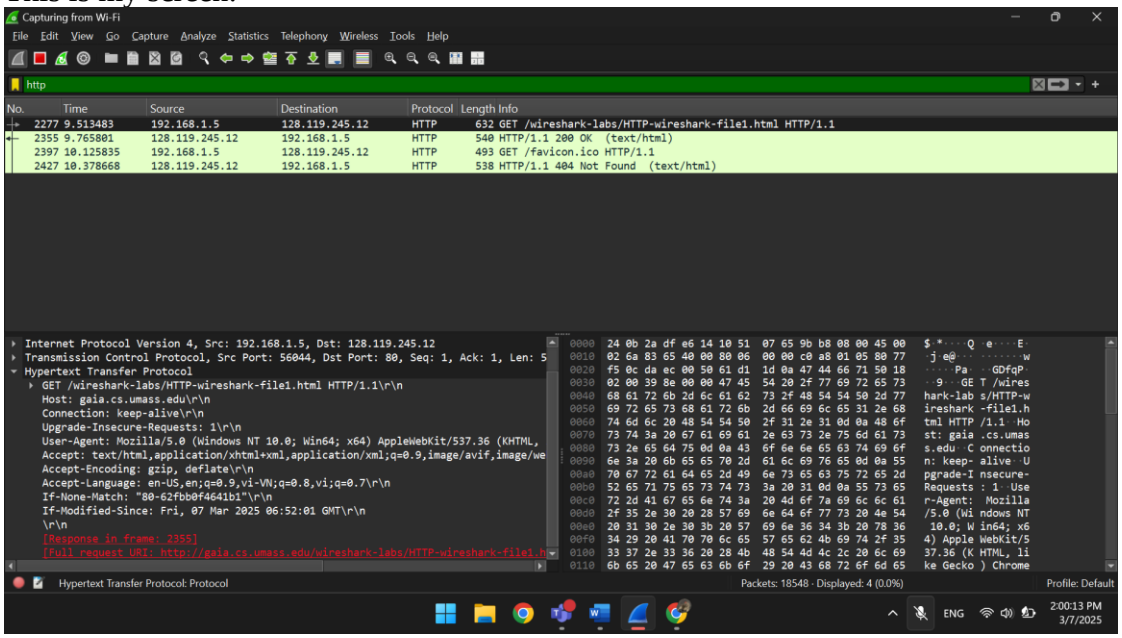


"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

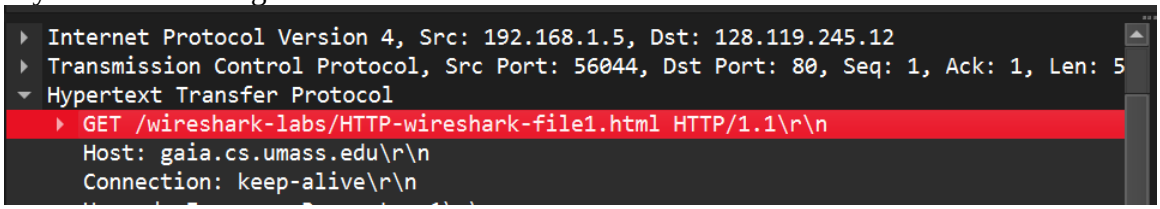
ITCSIU24092
Phạm Hoàng Tuấn Tú

1. The Basic HTTP GET/response interaction

This is my screen:



1. **Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?**
   My browser running HTTP version 1.1



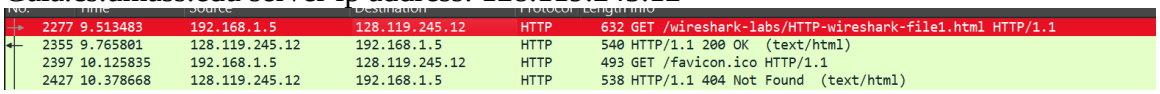
2. **What languages (if any) does your browser indicate that it can accept to the server?**

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,vi-VN;q=0.8,vi;q=0.7\r\n
If-None-Match: "80-62fbb0f4641b1"\r\n
If-Modified-Since: Fri, 07 Mar 2025 06:52:01 GMT\r\n
```

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

My computer IP address: 192.168.1.5

Gaia.cs.umass.edu server ip address: 128.119.245.12



No.	Time	Source	Destination	Protocol	Length/Info
2277	9.513483	192.168.1.5	128.119.245.12	HTTP	632 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2355	9.765801	128.119.245.12	192.168.1.5	HTTP	540 HTTP/1.1 200 OK (text/html)
2397	10.125835	192.168.1.5	128.119.245.12	HTTP	493 GET /favicon.ico HTTP/1.1
2427	10.378668	128.119.245.12	192.168.1.5	HTTP	538 HTTP/1.1 404 Not Found (text/html)

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

The status code is : 200 OK

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

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

The below picture shown the Last-Modified:

```
Date: Fri, 07 Mar 2025 07:07:37 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl
Last-Modified: Fri, 07 Mar 2025 06:59:01 GMT\r\n
ETag: "80-62fbb284868b1"\r\n
```

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

128 bytes of content are being returned to my browser

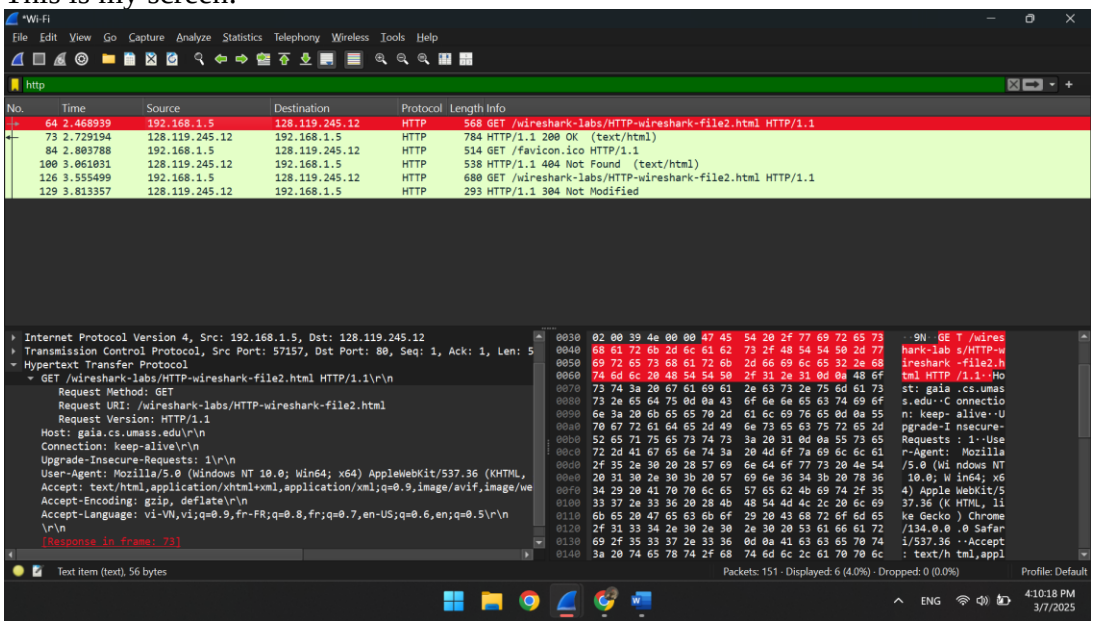
```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
    [Content length: 128]
Keep-Alive: timeout=5, max=100\r\n
```

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.**

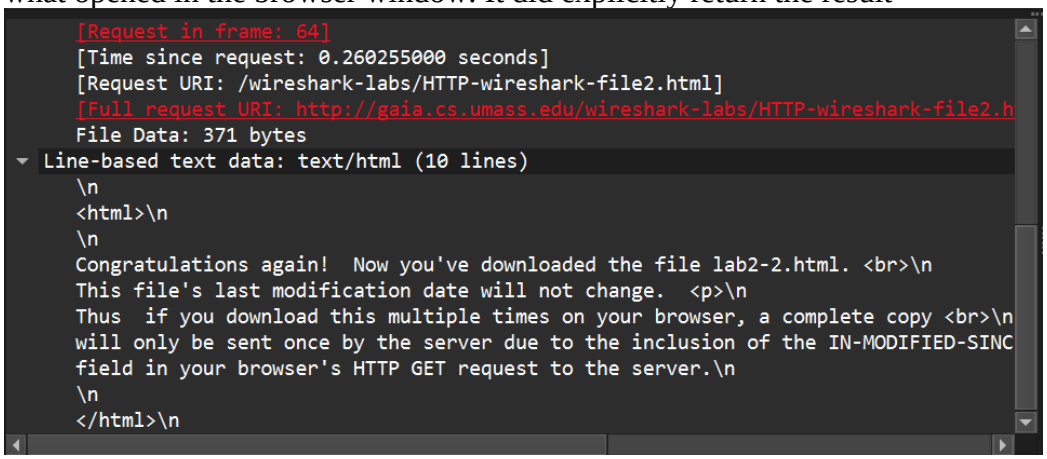
No headers not displayed in the packet-listing window

2. The HTTP CONDITIONAL GET/response interaction

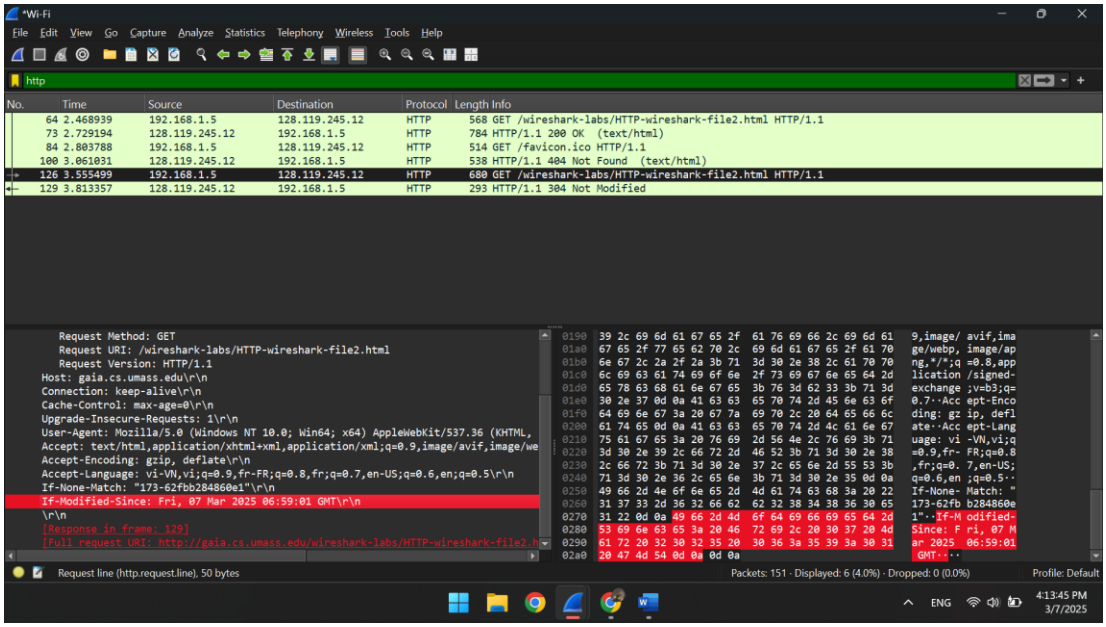
This is my screen:



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?**
   There is no such line that can be seen in the HTTP GET as the figure shown
9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**
   In the Line-based text data: text/html we can see the text/html returned which is what opened in the browser window. It did explicitly return the result

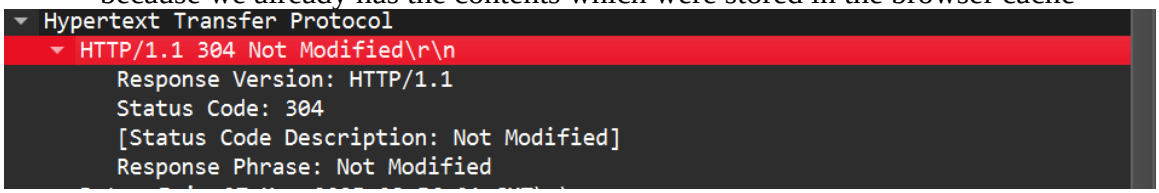


10. **Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET[1]? If so, what information follows the "IF-MODIFIED-SINCE:" header?**
    The information is: Fri, 07 Mar 2025 06:59:01 GMT\r\n



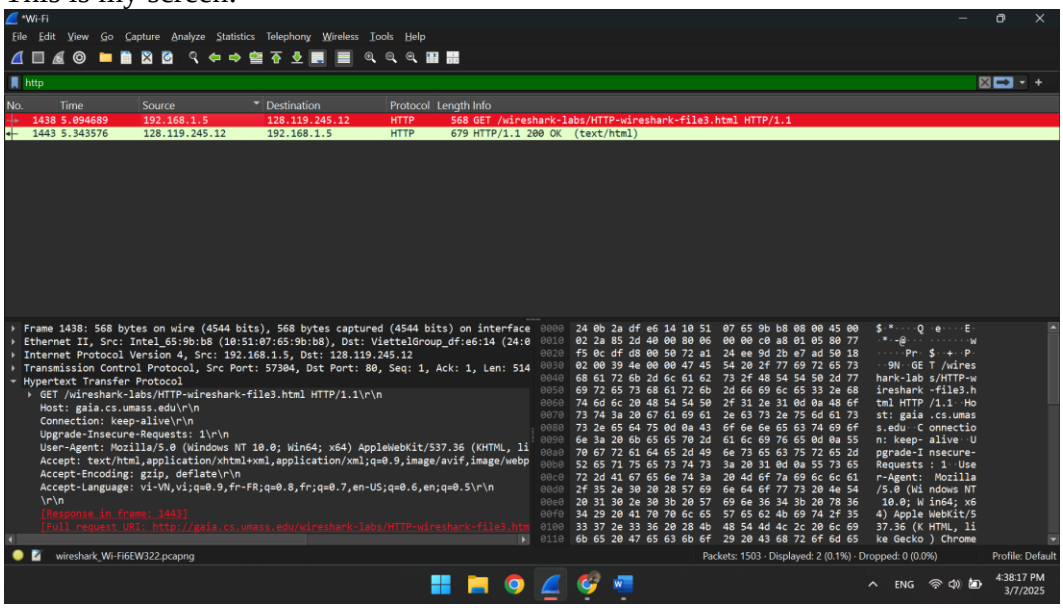
11. **What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.**

HTTP status code: 304 Not Modified, and does not return anything this time, because we already has the contents which were stored in the browser cache

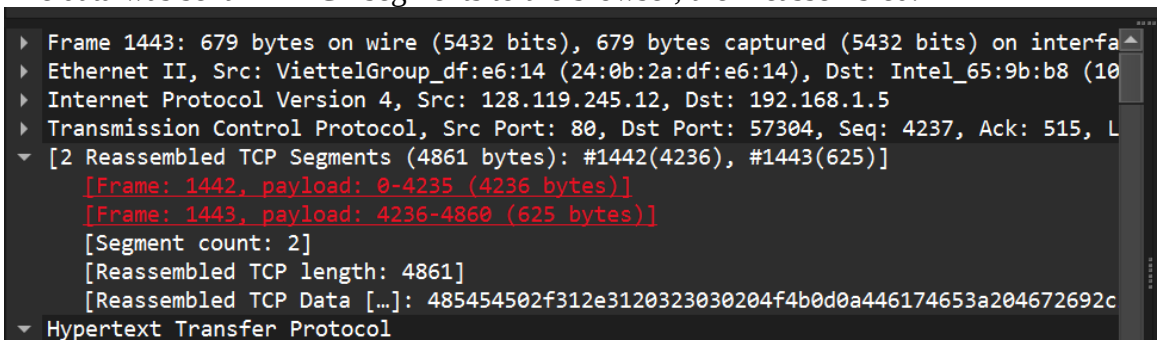


3. Retrieving Long Documents

This is my screen:

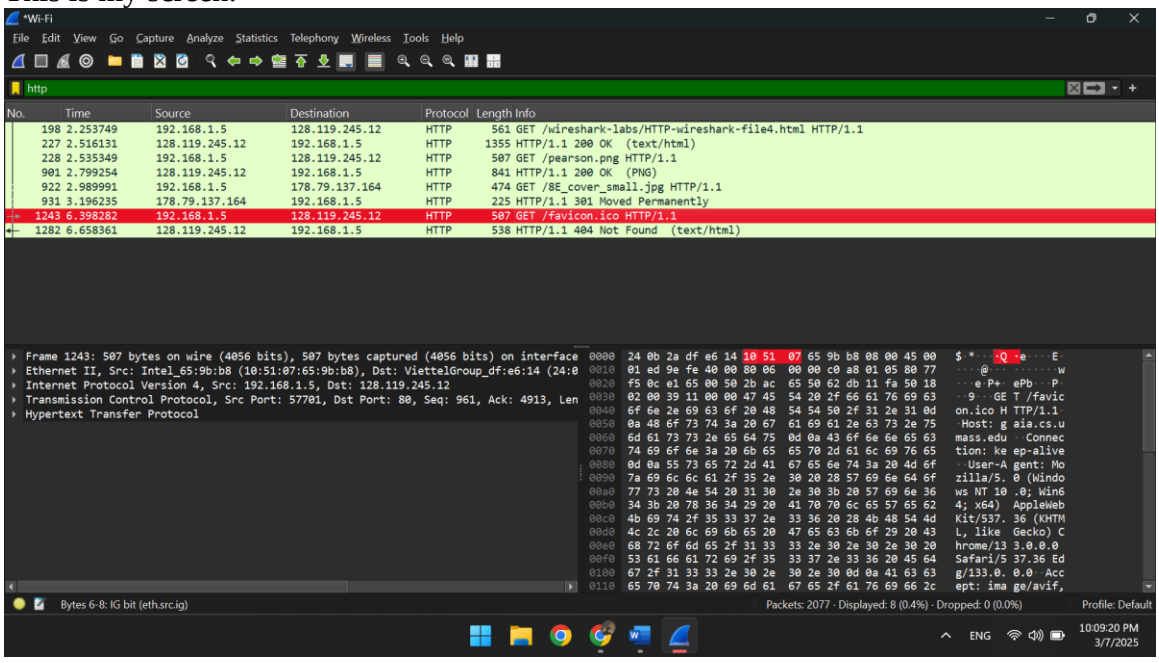


12. **How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**
    My browser sent one HTTP GET request messages. The packet that contained the GET messages was packet number 1438.
13. **Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?**
    The packet that contains the status code and phrase which the server sent in respone to the GET message was packet number 1443
14. **What is the status code and phrase in the response?**
    The status code and phrase in the respone was 200 OK
15. **How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**
    The data was sent in 2 TCP segments to the browser, then reassembled.



4. HTML Documents with Embedded Objects

This is my screen:



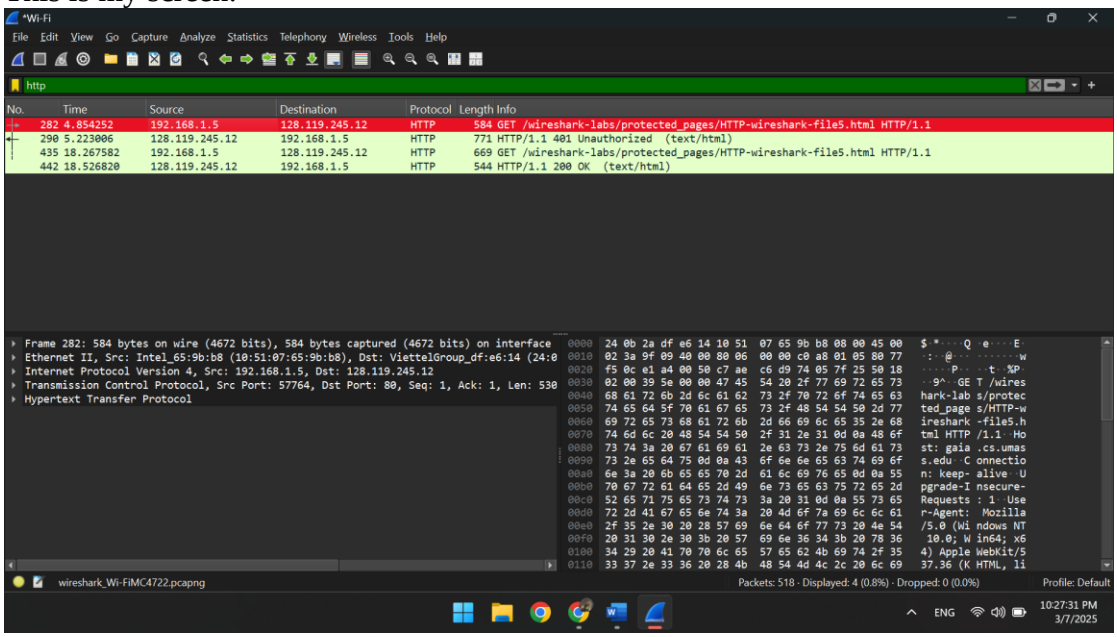
16. **How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**

My browser sent 4 HTTP GET request messages: The initial page, the Pearson logo, the image of the 8th edition book, and the favicon image.

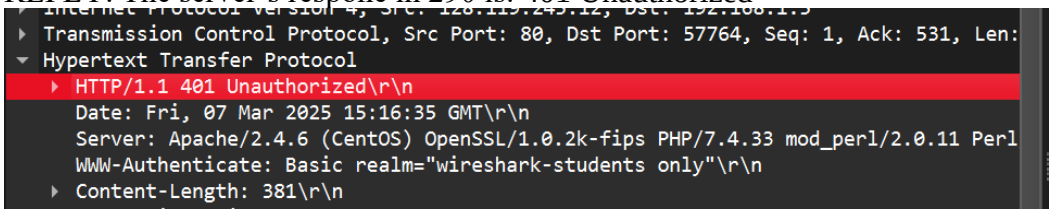
17. **Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.**
The browser downloaded the two images serially, because the first image was requested and sent before the second image was requested by the browser. If they were downloaded in parallel, it would have been returned in the same period.

5 HTTP Authentication

This is my screen:



18. **What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?**
Packet 282 in the trace contains the first GET and packet 290 contains the REPLY. The server's respone in 290 is: 401 Unauthorized



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 is Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n