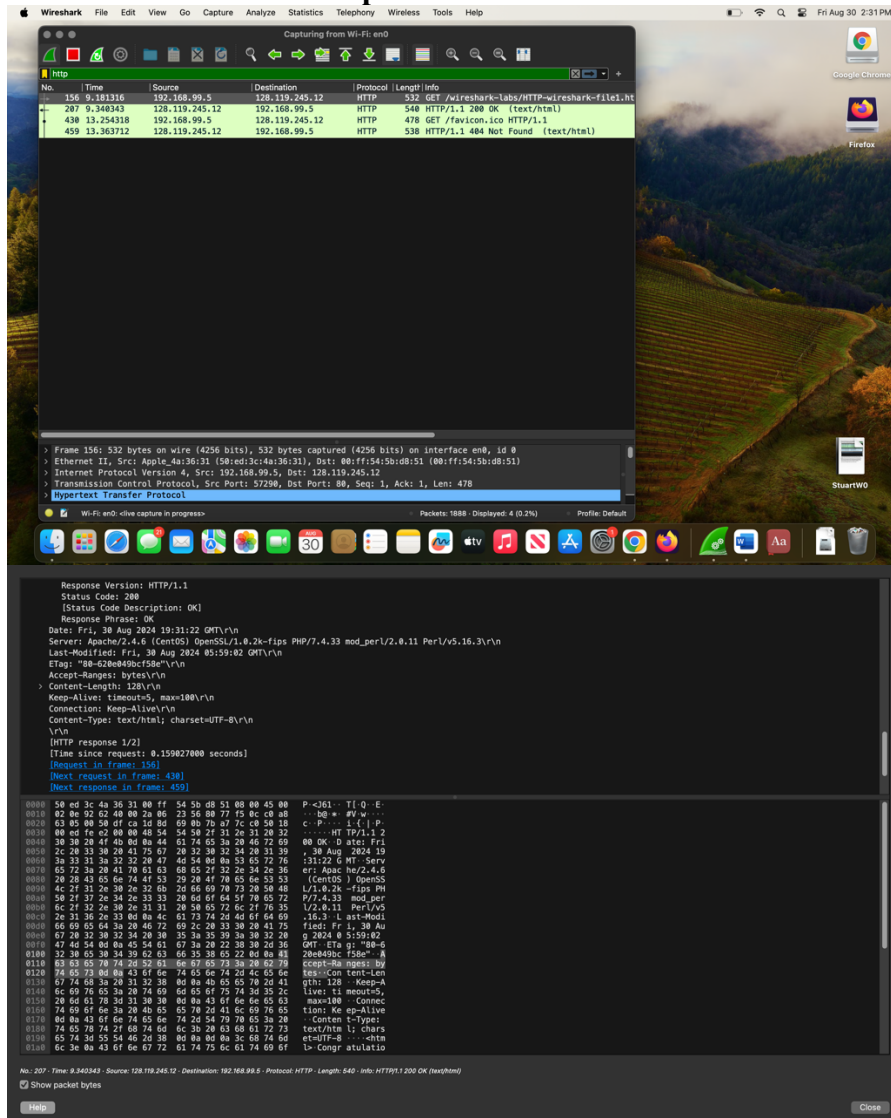


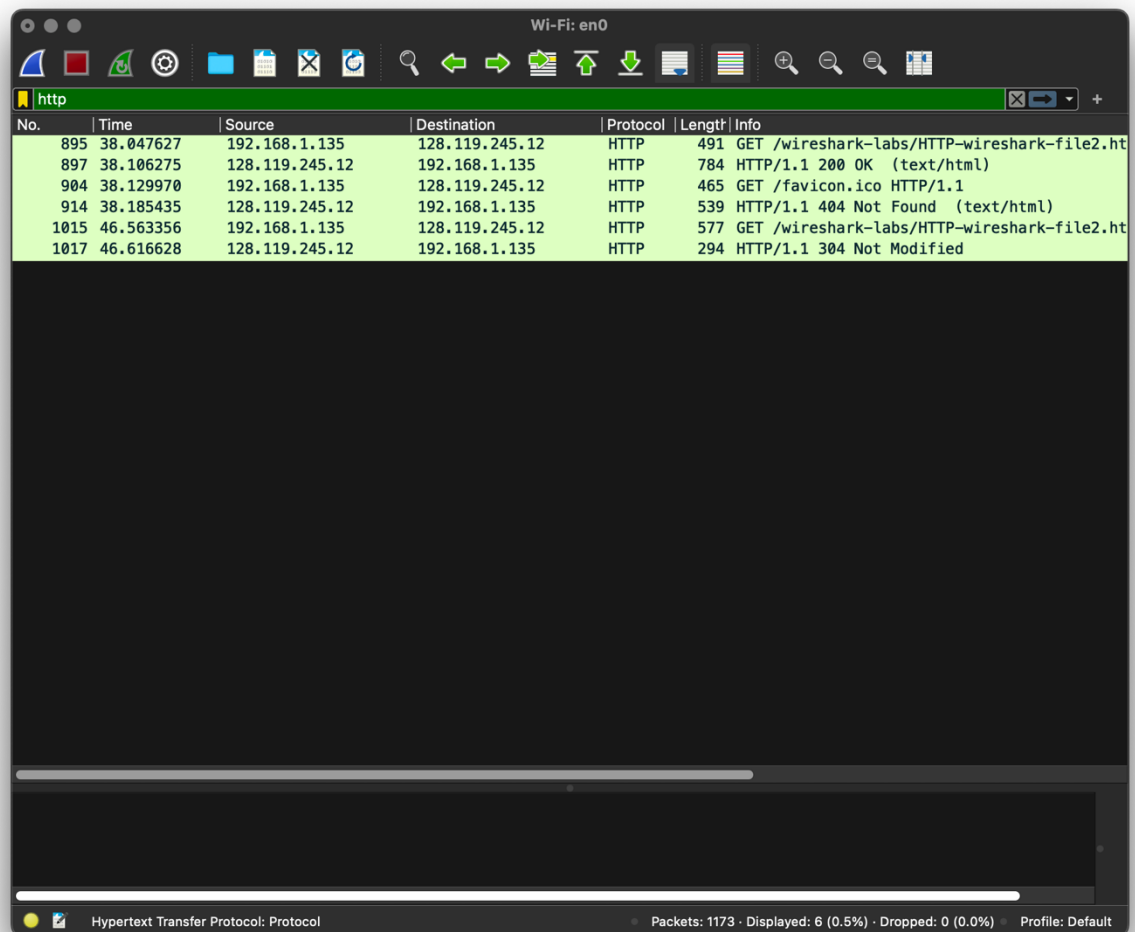
The Basic HTTP GET/response interaction



1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
The browser is running HTTP version 1.1 as indicated by the GET request in the "Protocol" column (HTTP/1.1).
The server is also running **HTTP version 1.1** as shown in the server response (HTTP/1.1 200 OK)
2. What languages (if any) does your browser indicate that it can accept to the server?
Accept-Language: en-US,en;q=0.9\r\n
3. What is the IP address of your computer? Of the **gaia.cs.umass.edu** server?
192.168.99.5 (as seen in the "Source" column of the packets captured)
128.119.245.12 (as seen in the "Destination" column of the packets captured).
4. What is the status code returned from the server to your browser?
The status code returned from the server is 200 OK (as seen in the "Info" column for packet number 207)

5. **When was the HTML file that you are retrieving last modified at the server?**The Last-Modified header shows that the HTML file was last modified on Fri, 30 Aug 2024 05:59:02 GMT.
6. **How many bytes of content are being returned to your browser?**
The Content-Length header indicates that 128 bytes of content are being returned to browser.
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 header found in packet content window

The HTTP CONDITIONAL GET/response interaction



No.	Time	Source	Destination	Protocol	Length	Info
895	38.047627	192.168.1.135	128.119.245.12	HTTP	491	GET /wireshark-labs/HTTP-wireshark-file2.ht
897	38.106275	128.119.245.12	192.168.1.135	HTTP	784	HTTP/1.1 200 OK (text/html)
904	38.129970	192.168.1.135	128.119.245.12	HTTP	465	GET /favicon.ico HTTP/1.1
914	38.185435	128.119.245.12	192.168.1.135	HTTP	539	HTTP/1.1 404 Not Found (text/html)
1015	46.563356	192.168.1.135	128.119.245.12	HTTP	577	GET /wireshark-labs/HTTP-wireshark-file2.ht
1017	46.616628	128.119.245.12	192.168.1.135	HTTP	294	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol: Protocol Packets: 1173 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%) · Profile: Default

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 the browser has no cached copy.
9. **Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?**
Yes, the status code is 200 OK, the server returned the full content.

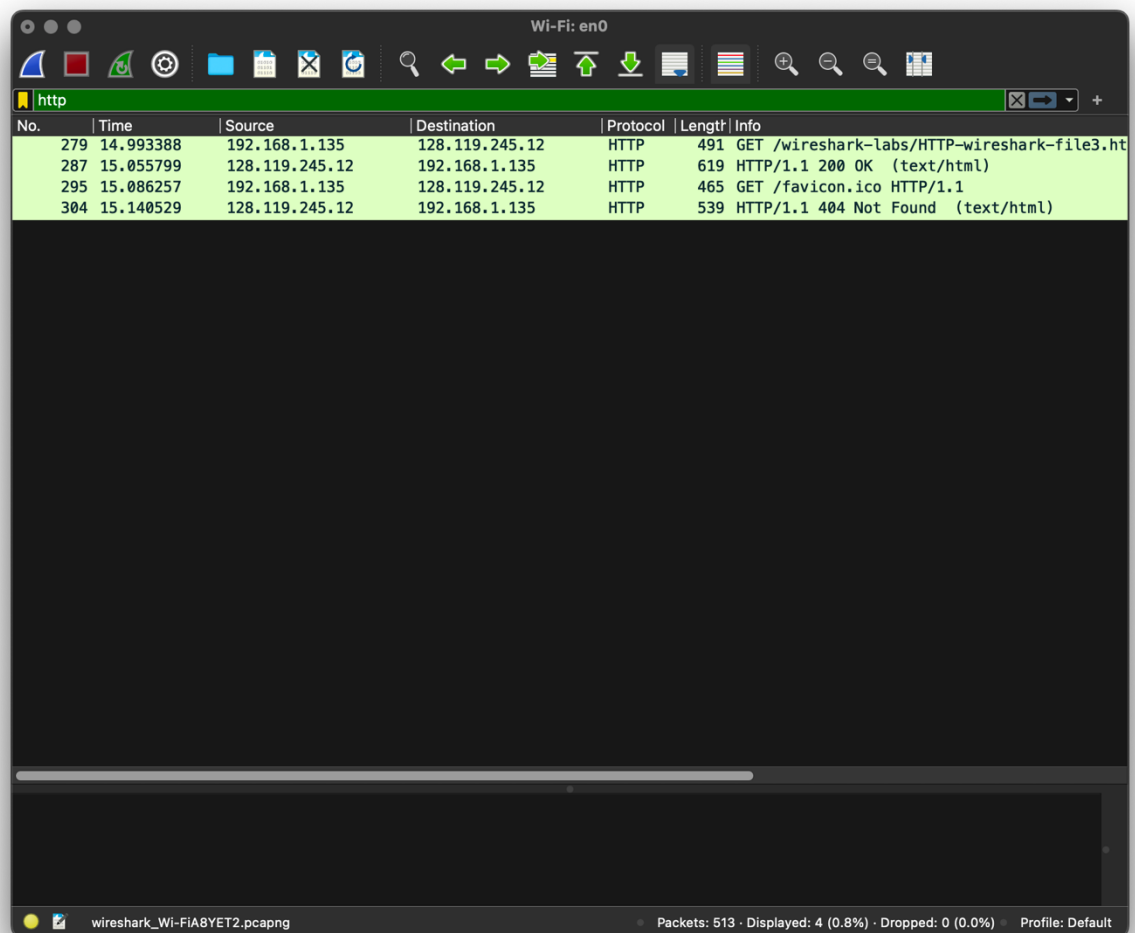
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

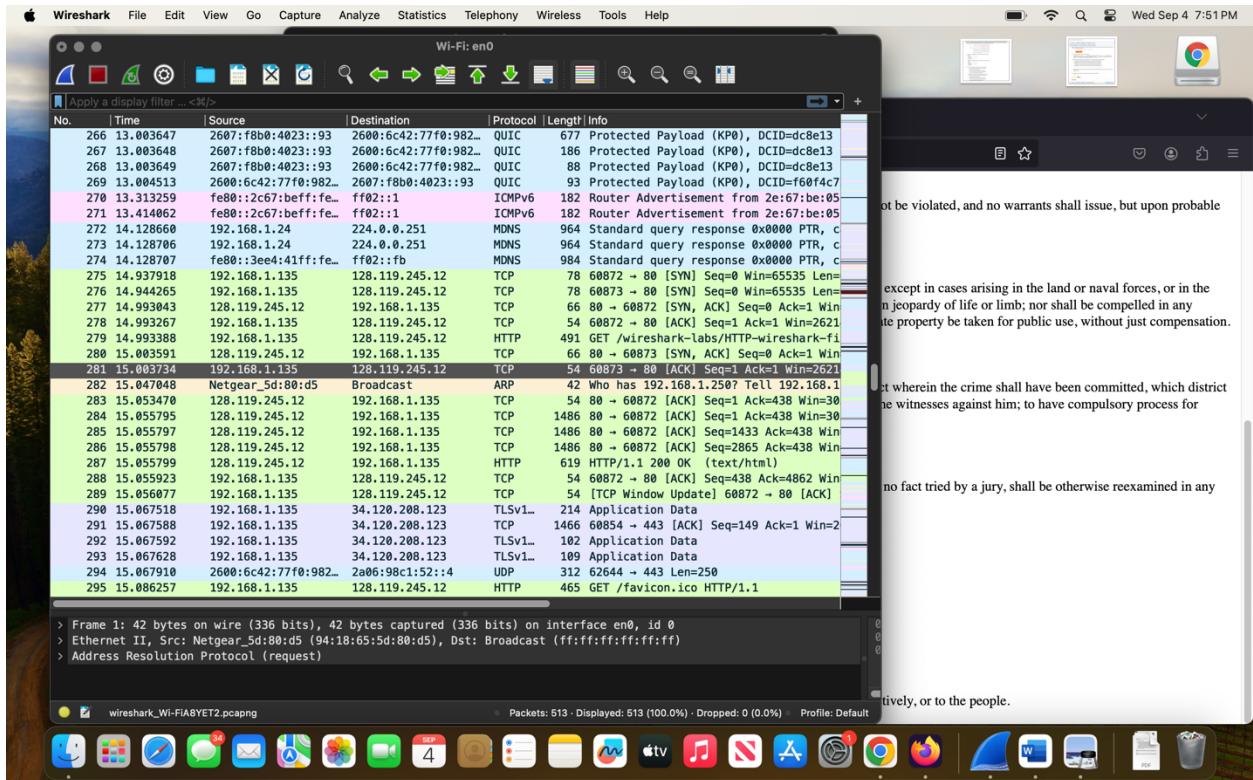
Yes, If-Modified-Since: Wed, 04 Sep 2024 05:59:02 GMT\r\n

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.

No, The status code is 304 Not Modified, the server did not return the file content because it has not changed.

Retrieving Long Documents





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?

I only see one GET request for the long document because the cache was properly cleared and no network issues occurred.

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

The packet number 279 contains the GET message for the Bill of Rights. This is indicated in the "Info" column where it says GET /wireshark-labs/HTTP-wireshark-file3.html.

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

The packet number 287 contains the response to the HTTP GET request, indicated by HTTP/1.1 200 OK

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

In total, there are 6 TCP segments (287, 288, 289, 290, 291, and 292) used to carry the complete HTTP response and the text of the Bill of Rights.

HTML Documents with Embedded Objects

No.	Time	Source	Destination	Protocol	Length	Info
128	5.897915	192.168.1.135	128.119.245.12	HTTP	491	GET /wireshark-labs/HTTP-wireshark-file4.ht
131	5.954547	128.119.245.12	192.168.1.135	HTTP	1355	HTTP/1.1 200 OK (text/html)
133	6.002104	192.168.1.135	128.119.245.12	HTTP	468	GET /pearson.png HTTP/1.1
144	6.055249	128.119.245.12	192.168.1.135	HTTP	801	HTTP/1.1 200 OK (PNG)
147	6.161713	192.168.1.135	128.119.245.12	HTTP	465	GET /favicon.ico HTTP/1.1
150	6.211127	128.119.245.12	192.168.1.135	HTTP	538	HTTP/1.1 404 Not Found (text/html)
156	6.316872	192.168.1.135	178.79.137.164	HTTP	447	GET /8E_cover_small.jpg HTTP/1.1
161	6.455349	178.79.137.164	192.168.1.135	HTTP	240	HTTP/1.1 302 Found

> Frame 161: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits) on interface en0, id 0 > Ethernet II, Src: 2e:67:be:05:95:c5 (2e:67:be:05:95:c5), Dst: Apple_4a:36:31 (50:ed:3c:4a:36:31) > Internet Protocol Version 4, Src: 178.79.137.164, Dst: 192.168.1.135 > Transmission Control Protocol, Src Port: 80, Dst Port: 60904, Seq: 1, Ack: 382, Len: 186 > Hypertext Transfer Protocol	
--	--

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

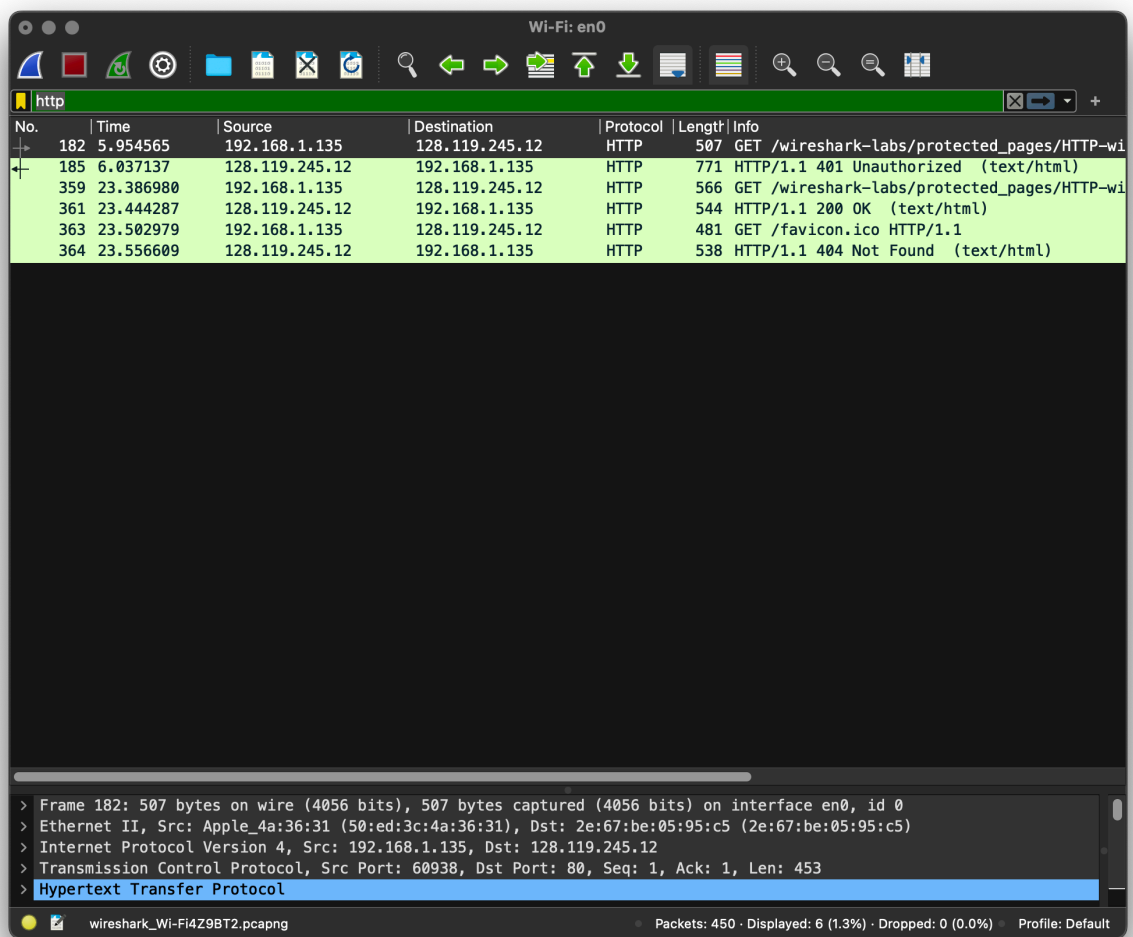
The browser sent five HTTP GET requests: one for the main HTML document (/wireshark-labs/HTTP-wireshark-file4.html), one for an image (/pearson.png), one for a favicon (/favicon.ico), and two for another image (/DE_cover_small.jpg).

The GET requests were sent to two different IP addresses: 128.119.245.12 for the main HTML document, pearson.png, and favicon.ico, and 178.79.137.164 for DE_cover_small.jpg.

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 images were downloaded in parallel, as indicated by the close timestamps of the GET requests for pearson.png (6.021040 seconds) and DE_cover_small.jpg (6.316872 seconds).

HTTP Authentication



```
> Internet Protocol Version 4, Src: 192.168.1.135, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60939, Dst Port: 80, Seq: 1, Ack: 1, Len: 512
> Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/2]
  [Response in frame: 361]
  [Next request in frame: 363]
00b0 4d 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 65 6c Macintosh h; Intel
00c0 20 4d 61 63 20 4f 53 20 58 20 31 30 2e 31 35 3b Mac OS X 10.15;
00d0 20 72 76 3a 31 32 39 2e 30 29 20 47 65 63 6b 6f rv:129.0) Gecko
00e0 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 6f /20100101 Firefo
00f0 70 2f 31 32 39 2e 30 0d 0a 41 63 63 65 70 74 3a x/129.0) Accept:
0100 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 text/html,appli
0110 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c cation/xhtml+xml
0120 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c ,applica tion/xml
0130 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 ;q=0.9,i mage/avi
0140 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 f,image/ webp,ima
0150 67 65 2f 70 6e 67 2c 69 6d 61 67 65 2f 73 76 67 ge/png,i mage/svg
0160 2b 78 6d 6c 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a +xml,*/*; q=0.8-
0170 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a Accept-L anguage:
0180 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 35 0d en-US,e n;q=0.5-
0190 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 -Accept- Encoding
01a0 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d : gzip, deflate
01b0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 -Connect ion: kee
01c0 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 p-alive- -Upgrade
01d0 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 65 73 -Insecur e-Reques
01e0 74 73 3a 20 31 0d 0a 50 72 69 6f 72 69 74 79 3a ts: 1-P riority:
01f0 20 75 3d 30 2c 20 69 0d 0a 41 75 74 68 6f 72 69 u=0, i- Authori
0200 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 64 32 zation: Basic d2
0210 6c 79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 30 64 57 lyZXNoYXJrLXN0dW
0220 52 6c 62 6e 52 7a 4f 6d 35 6c 64 48 64 76 63 6d RlbnRzM5ldHdvcms=
0230 73 3d 0d 0a 0d 0a
```

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

The server’s response to the initial HTTP GET request is 401 Unauthorized. This is seen in packet 185. The 401 Unauthorized status code indicates that the server requires authentication before allowing access to the requested resource.

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

When the browser sends the HTTP GET message for the second time (packet 359), the new field included is the Authorization header. This header contains the credentials (wireshark-students:network) encoded in Base64 format. The Authorization header value shown is Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=.