

Computer Networks 1

Lab 2a

Wireshark Lab: HTTP v8.0

Student Name: Nguyễn Quý Hải

Student No.: 2052974

I. Objectives

In this lab, we'll explore several aspects of the HTTP protocol:

- The basic GET/response interaction
- HTTP message formats
- Retrieving large HTML files
- Retrieving HTML files with embedded objects
- HTTP authentication and security

II. Content

1. The Basic HTTP GET/response interaction

- Q1: Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Answer: Both my browser and server are running HTTP version 1.1

- Q2: What languages (if any) does your browser indicate that it can accept to the server?

Answer: en-US (English - United States)

- Q3: What is the IP address of your computer? Of the gaia.cs.umass.edu server?

Answer:

+IP address of my computer: 192.168.1.11

+IP address of gaia.cs.umass.edu server 128.119.245.12

- Q4: What is the status code returned from the server to your browser?

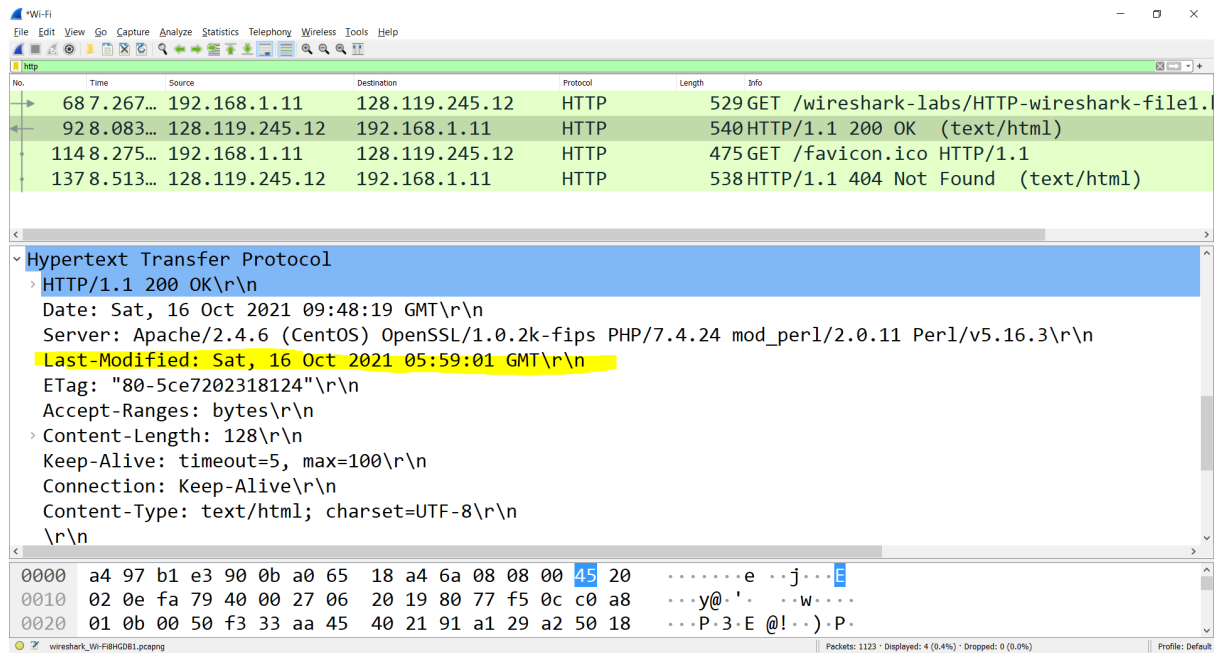
Answer:

+With getting .html request, server returns 200 (OK)

+With getting .ico request, server returns 404 (Not Found)

- Q5: When was the HTML file that you are retrieving last modified at the server?

Answer: Sat, 16 Oct 2021 09:48:19 GMT (Sat, 16 Oct 2021 16:48:19 in VietNam)



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 68 | 7.267... | 192.168.1.11 | 128.119.245.12 | HTTP | 529 | GET /wireshark-labs/HTTP-wireshark-file1. |
| 92 | 8.083... | 128.119.245.12 | 192.168.1.11 | HTTP | 540 | HTTP/1.1 200 OK (text/html) |
| 114 | 8.275... | 192.168.1.11 | 128.119.245.12 | HTTP | 475 | GET /favicon.ico HTTP/1.1 |
| 137 | 8.513... | 128.119.245.12 | 192.168.1.11 | HTTP | 538 | HTTP/1.1 404 Not Found (text/html) |

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sat, 16 Oct 2021 09:48:19 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sat, 16 Oct 2021 05:59:01 GMT\r\n

ETag: "80-5ce7202318124"\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

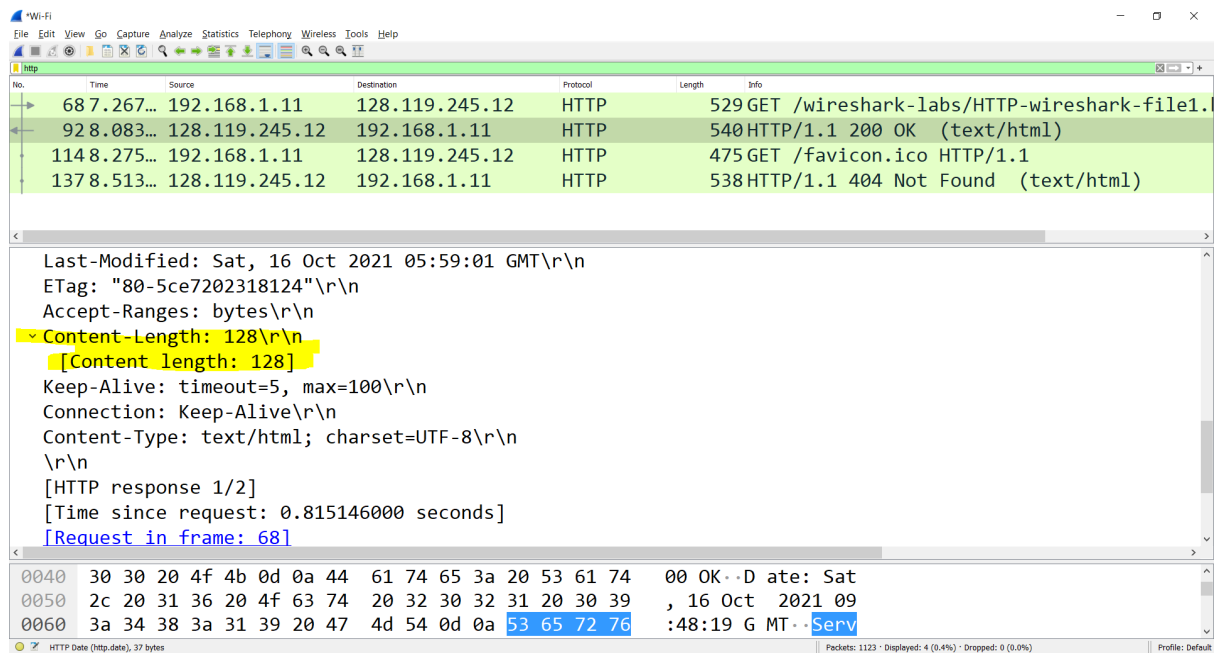
0000 a4 97 b1 e3 90 0b a0 65 18 a4 6a 08 08 00 45 20e..j...E

0010 02 0e fa 79 40 00 27 06 20 19 80 77 f5 0c c0 a8 ...y@.'...w...

0020 01 0b 00 50 f3 33 aa 45 40 21 91 a1 29 a2 50 18 ...P.3.E @!..).P.

- Q6: How many bytes of content are being returned to your browser?

Answer: 128



Last-Modified: Sat, 16 Oct 2021 05:59:01 GMT\r\n

ETag: "80-5ce7202318124"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

[Content length: 128]

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: 0.815146000 seconds]

[Request in frame: 68]

0040 30 20 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..D ate: Sat

0050 2c 20 31 36 20 4f 63 74 20 32 30 32 31 20 30 39 , 16 Oct 2021 09

0060 3a 34 38 3a 31 39 20 47 4d 54 0d 0a 53 65 72 76 :48:19 G MT..Serv

- Q7: 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.

Answer: No

2. The HTTP CONDITIONAL GET/response interaction

- Q8: 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?

Answer: No

- Q9: Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Answer: Yes

Line-based text data: text/html (10 lines)

\n

<html>\n

\n

Congratulations again! Now you've downloaded the file lab2-2.html.
\n

This file's last modification date will not change. <p>\n

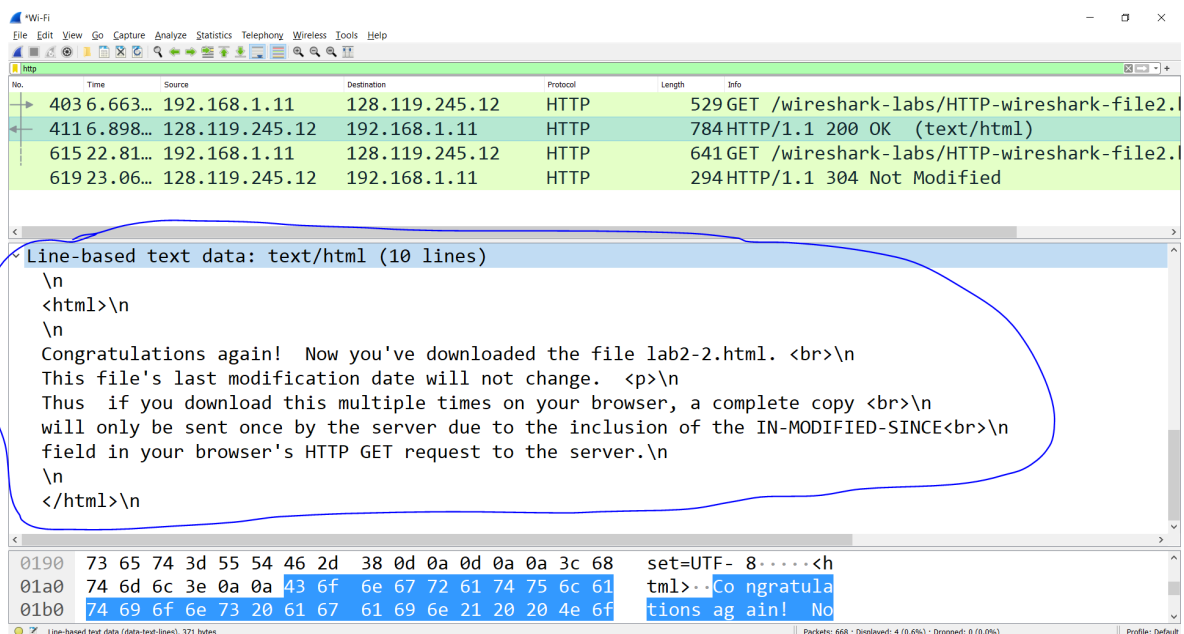
Thus if you download this multiple times on your browser, a complete copy
\n will only be sent once by the server due to the inclusion of the

IN-MODIFIED-SINCE
\n

field in your browser's HTTP GET request to the server.\n

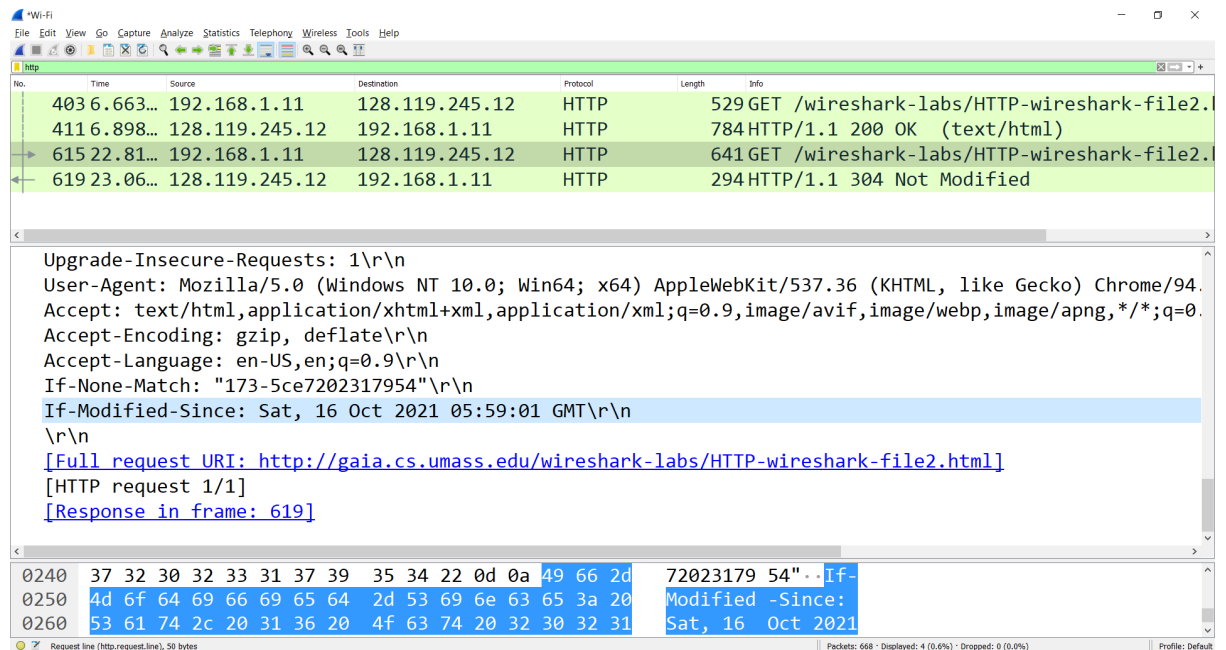
\n

</html>\n



- Q10: 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?

Answer: Yes, If-Modified-Since: Sat, 16 Oct 2021 05:59:01 GMT



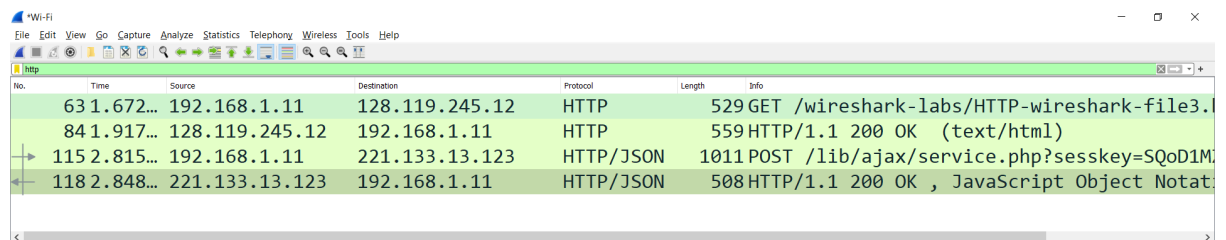
- Q11: What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Answer: 304 Not Modified. I think the server did not explicitly return the contents because it has been done on the first HTTP response and these contents might be stored somewhere in the browser.

3. Retrieving Long Documents

- Q12: 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?

Answer: Only 1. That number is 63.



- Q13: Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

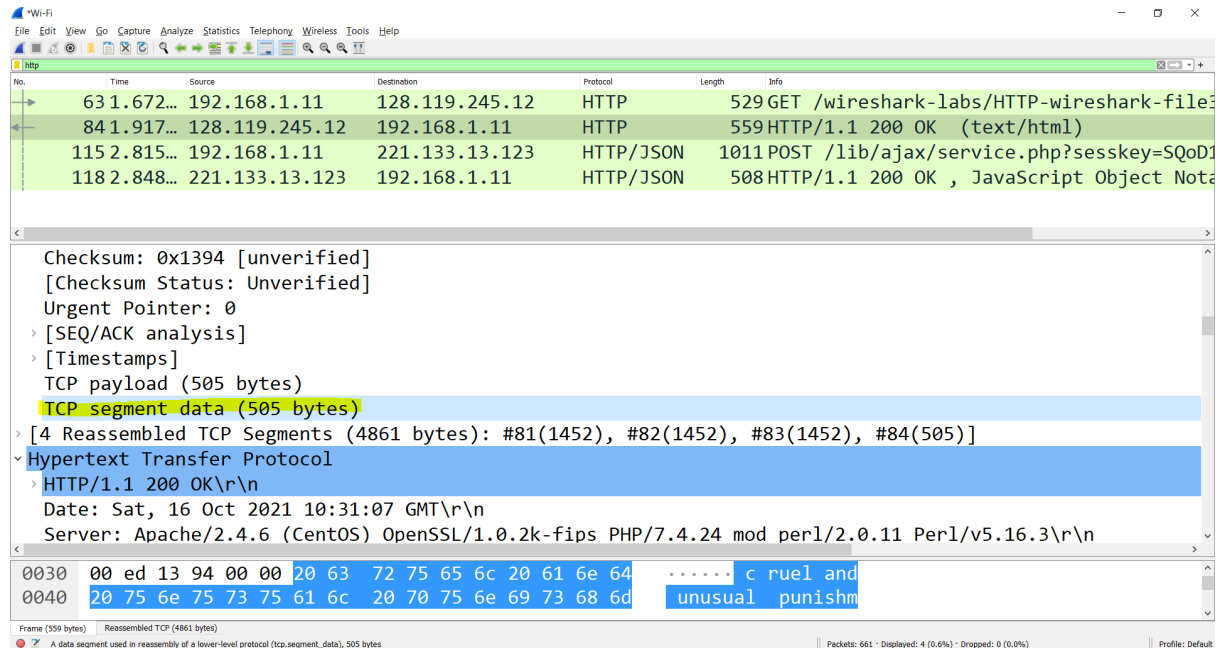
Answer: It is 84

- Q14: What is the status code and phrase in the response?

Answer: 200 (OK)

- Q15: How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

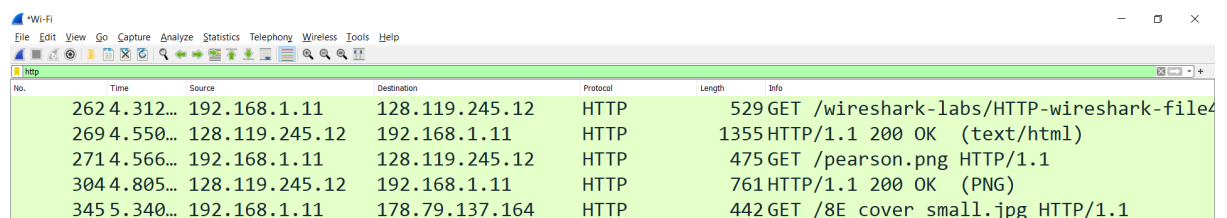
Answer: 505 bytes



4. HTML Documents with Embedded Objects

- Q16: How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: My browser sends 3 HTTP GET request messages to 128.119.245.12 and 178.79.137.164



- Q17: Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

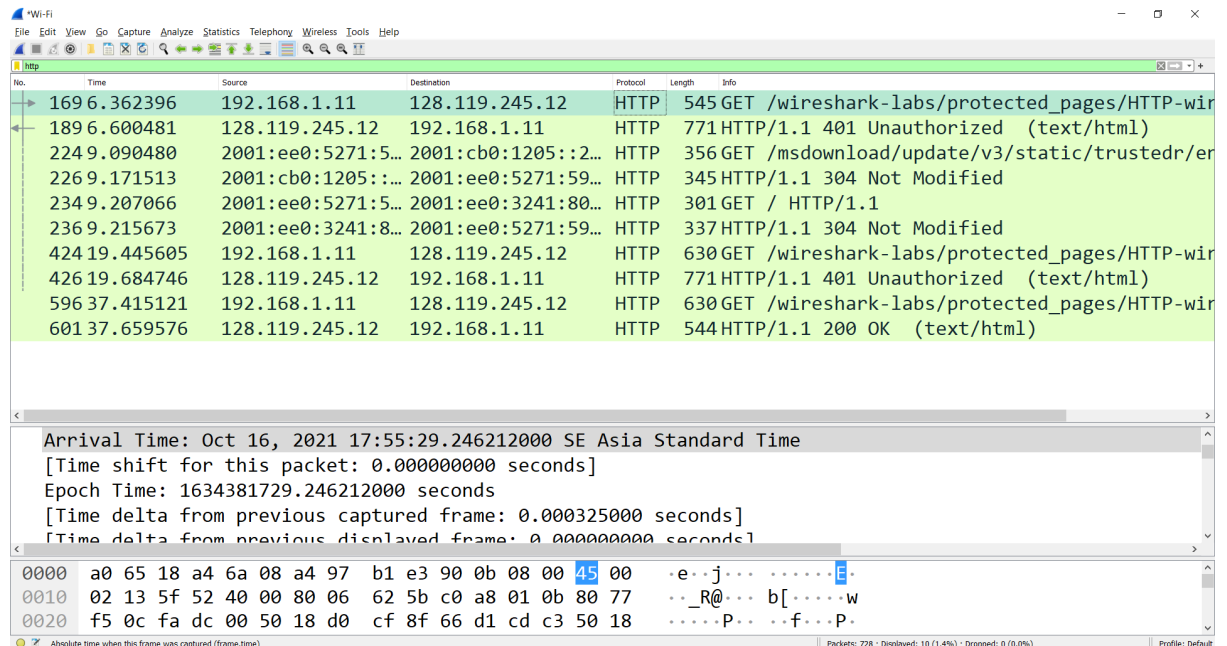
I think browser downloaded the two images serially, because:

- pearson.png arrival time: Oct 16, 2021 17:43:03.130610000 SE Asia Standard Time
- 8E_cover_small.jpg arrival time: Oct 16, 2021 17:43:03.904062000 SE Asia Standard Time, it is even after the time browser gets the first image.

5. HTTP Authentication

- Q18: What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

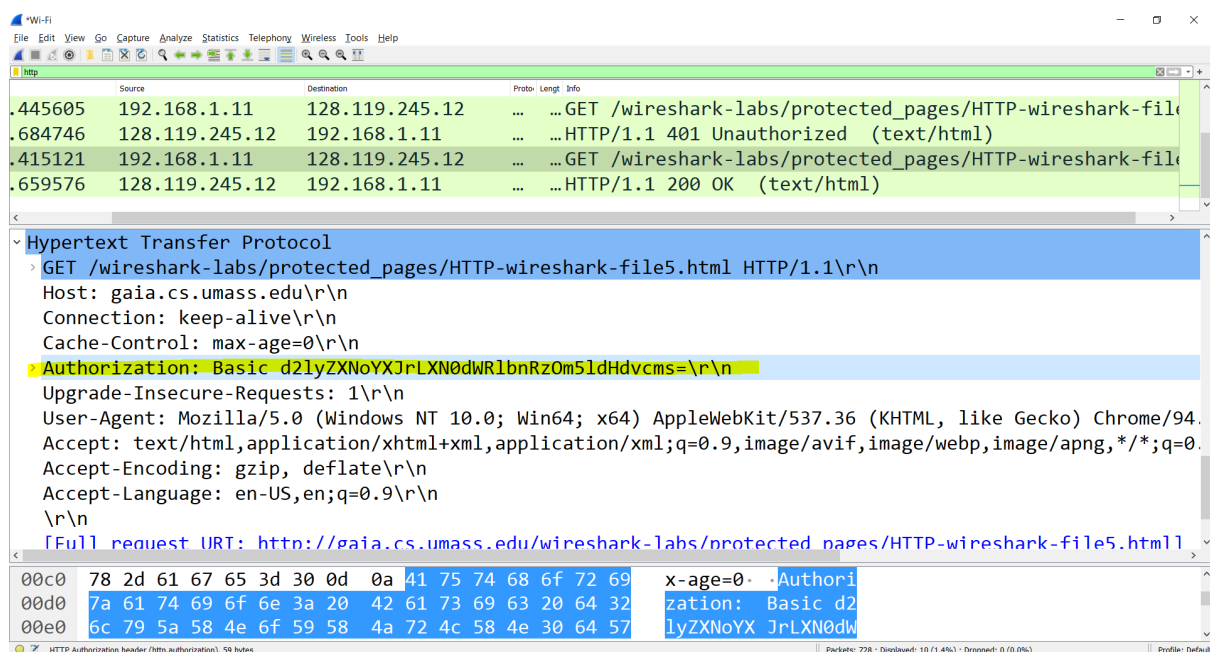
Answer: 401 Unauthorized.



The screenshot shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several packets, with the 189th packet (No. 189, Time 6.600481) being the response: HTTP/1.1 401 Unauthorized (text/html). The packet details pane on the right shows the 'Arrival Time: Oct 16, 2021 17:55:29.246212000 SE Asia Standard Time' and the 'Epoch Time: 1634381729.246212000 seconds'. The packet bytes pane at the bottom shows the raw data of the response, including the status line 'HTTP/1.1 401 Unauthorized' and the 'WWW-Authenticate: Basic' header.

- Q19: When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answer: I think Authorization.



The screenshot shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several packets, with the 415th packet (No. 415, Time 12.415121) being the second request: GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1. The packet details pane on the right shows the 'Hypertext Transfer Protocol' section expanded, displaying the request headers. The 'Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm5=' header is highlighted in yellow. The packet bytes pane at the bottom shows the raw data of the request, including the status line 'GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1' and the 'Authorization: Basic' header.