

Computer Networks

LAB 3a

Author:
Tran Dinh Dang Khoa
2211649

Date: October 5, 2024

Contents

| | | |
|----------|--|-----------|
| 1 | The Basic HTTP GET/response interaction | 2 |
| 2 | The HTTP CONDITIONAL GET/response interaction | 5 |
| 3 | Retrieving Long Documents | 7 |
| 4 | HTML Documents with Embedded Objects | 9 |
| 5 | HTTP Authentication | 10 |

1 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?

```
Transmission Control Protocol, Src Port: 80, Dst Port: 50532, Seq: 1, Len: 427, Ecn: 0
  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
      Date: Sat, 05 Oct 2024 02:31:16 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1
```

The server is running HTTP version 1.1

```
Transmission Control Protocol, Src Port: 50532, Dst Port: 80, Seq: 1, Len: 100
  Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
      Host: gaia.cs.umass.edu\r\n
```

My browser is running HTTP version 1.1

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

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ir
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
```

The language that my browser accepts is "English - US"

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

```

Internet Protocol Version 4, Src: 10.128.129.179, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 491
    Identification: 0x0000 (0)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3756 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.128.129.179
    Destination Address: 128.119.245.12
    [Stream index: 9]
  > Transmission Control Protocol, Src Port: 56352, Dst Port: 80, Seq: 1, Ack: 1, Len: 451
  > Hypertext Transfer Protocol
    > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1

```

The "Source Address" is the IP address of my computer, the "Destination Address" is the address of the server

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

```

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
    Date: Sat, 05 Oct 2024 02:31:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1
    Last-Modified: Fri, 04 Oct 2024 05:59:02 GMT\r\n
    ETag: "80-623a05e32a06e"\r\n

```

The status code returned is 200

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

```

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
    Date: Sat, 05 Oct 2024 02:31:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5
    Last-Modified: Fri, 04 Oct 2024 05:59:02 GMT\r\n
    ETag: "80-623a05e32a06e"\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

```

Last modified on Fri, 04 Oct 2024 05:59:02 GMT

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

```

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
    Date: Sat, 05 Oct 2024 02:31:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.1
    Last-Modified: Fri, 04 Oct 2024 05:59:02 GMT\r\n
    ETag: "80-623a05e32a06e"\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
  [Request in frame: 299]
  [Time since request: 1.055316000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes

```

128 bytes

- 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.

```

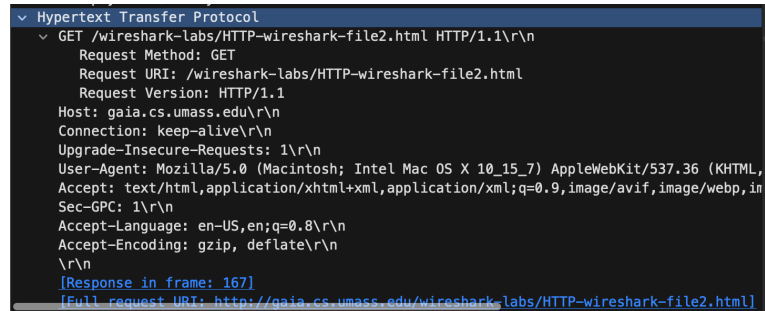
> Frame 344: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0
> Ethernet II, Src: Hewlett-Packard:44:44:44:44:44:44, Dst: Apple:77:77:77:77:77:77 (b0:be:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.128.129.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 56352, Seq: 1, Ack: 452, Len: 486
> Hypertext Transfer Protocol
  Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations. You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n

```

There are no headers in the raw data file

2 The HTTP CONDITIONAL GET/response interaction

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?



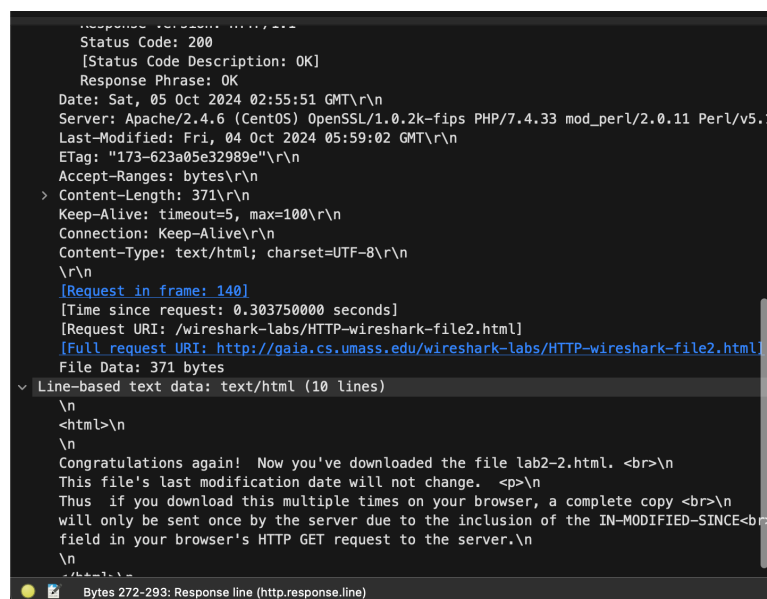
```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    \r\n
    [Response in frame: 167]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

There are no “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?



```

Response: 200 OK
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Sat, 05 Oct 2024 02:55:51 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.
  Last-Modified: Fri, 04 Oct 2024 05:59:02 GMT\r\n
  ETag: "173-623a05e32989e"\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
  [Request in frame: 140]
  [Time since request: 0.303750000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
  [Full 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 IF-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
  Bytes 272-293: Response line (http.response.line)

```

The server explicitly returned the contents

Because:

- The status code is 200
- HTML 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?

```

Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
    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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,in
    Sec-GPC: 1\r\n
    Accept-Language: en-US,en;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    If-None-Match: "173-623a05e32989e"\r\n
    If-Modified-Since: Fri, 04 Oct 2024 05:59:02 GMT\r\n
  \r\n
  [Response in frame: 220]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

```

The information follows the header: Fri, 04 Oct 2024 05:59:02 GMT

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.

```

Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
    Date: Sat, 05 Oct 2024 02:55:53 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.3
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-623a05e32989e"\r\n
  \r\n
  [Request in frame: 211]
  [Time since request: 0.298722000 seconds]
  [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

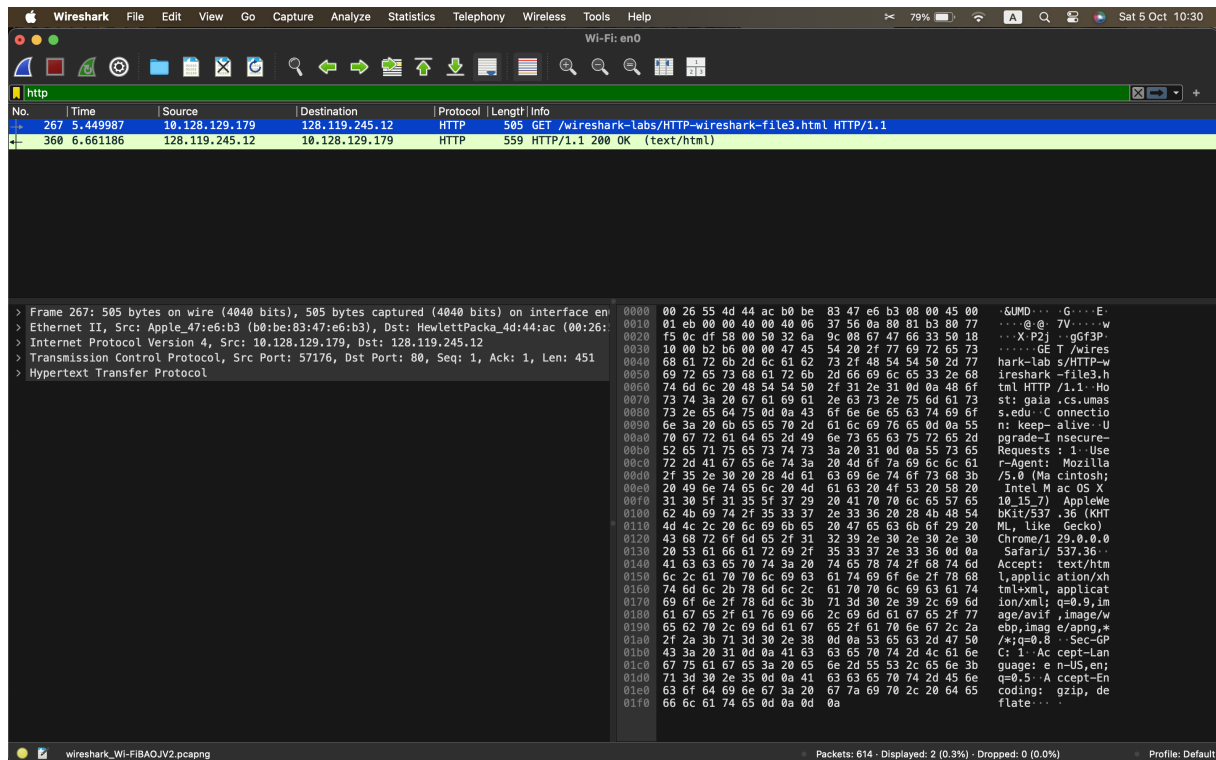
```

The status code on the second return is 304

The server did not explicitly return the contents this time. Because: My computer sent the "IF-MODIFIED-SINCE" header to the server, when inspect that header the server knows that the requested content hasn't changed since the last time my computer has fetched it. So instead of returning the content again, the server tells my computer to use the cached version that it already has.

3 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?



My browser sent 1 request message

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

Too old cant answer.

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


```

> Frame 360: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface en0
> Ethernet II, Src: HewlettPackard_4d:44:ac (00:26:55:4d:44:ac), Dst: Apple_47:e6:b3 (b0:be:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.128.129.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 57176, Seq: 4357, Ack: 452, Len:
> [4 Reassembled TCP Segments (4861 bytes): #299(1452), #300(1452), #301(1452), #360(505)]
√ 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
    Date: Sat, 05 Oct 2024 03:29:03 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.
    Last-Modified: Fri, 04 Oct 2024 05:59:02 GMT\r\n
    ETag: "1194-623a05e3261ee"\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
    [Request in frame: 267]
    [Time since request: 1.211199000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file3.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
  > Line-based text data: text/html (98 lines)

```

Status code: 200, Response 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?
One.

4 HTML Documents with Embedded Objects

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

| Destination | Protocol | Length | Info |
|----------------|----------|--------|--------------------------------------|
| 128.119.245.12 | HTTP | 505 | GET /wireshark-labs/HTTP-wireshark-f |
| 10.128.129.179 | HTTP | 1355 | HTTP/1.1 200 OK (text/html) |
| 128.119.245.12 | HTTP | 490 | GET /pearson.png HTTP/1.1 |
| 178.79.137.164 | HTTP | 469 | GET /8E_cover_small.jpg HTTP/1.1 |

My browser sent 3 GET request messages

The GET requests were sent to:

- 128.119.245.12: gaia.cs.umass.edu
- 178.79.137.164: kurose.cslash.net

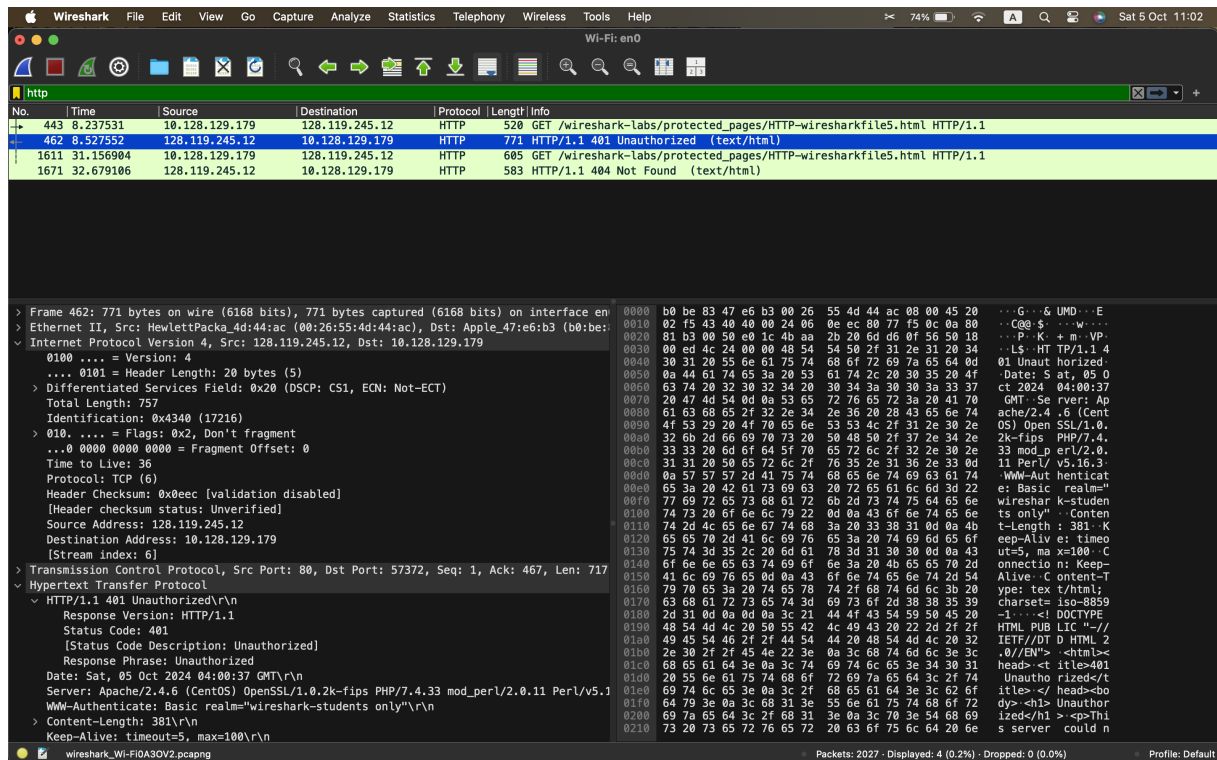
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|----------------|----------------|----------|--------|--------------------------------------|
| 421 | 6.583416 | 10.128.129.179 | 128.119.245.12 | HTTP | 505 | GET /wireshark-labs/HTTP-wireshark-f |
| 442 | 6.862720 | 128.119.245.12 | 10.128.129.179 | HTTP | 1355 | HTTP/1.1 200 OK (text/html) |
| 445 | 6.986780 | 10.128.129.179 | 128.119.245.12 | HTTP | 490 | GET /pearson.png HTTP/1.1 |
| 652 | 10.304943 | 10.128.129.179 | 178.79.137.164 | HTTP | 469 | GET /8E_cover_small.jpg HTTP/1.1 |

My browser downloaded two images serially because there are noticeable time gap between the requests

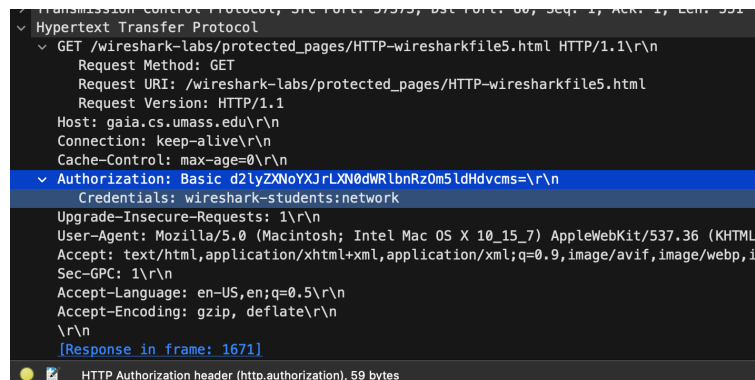
5 HTTP Authentication

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



The server response to my first request 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 included field is Authorization