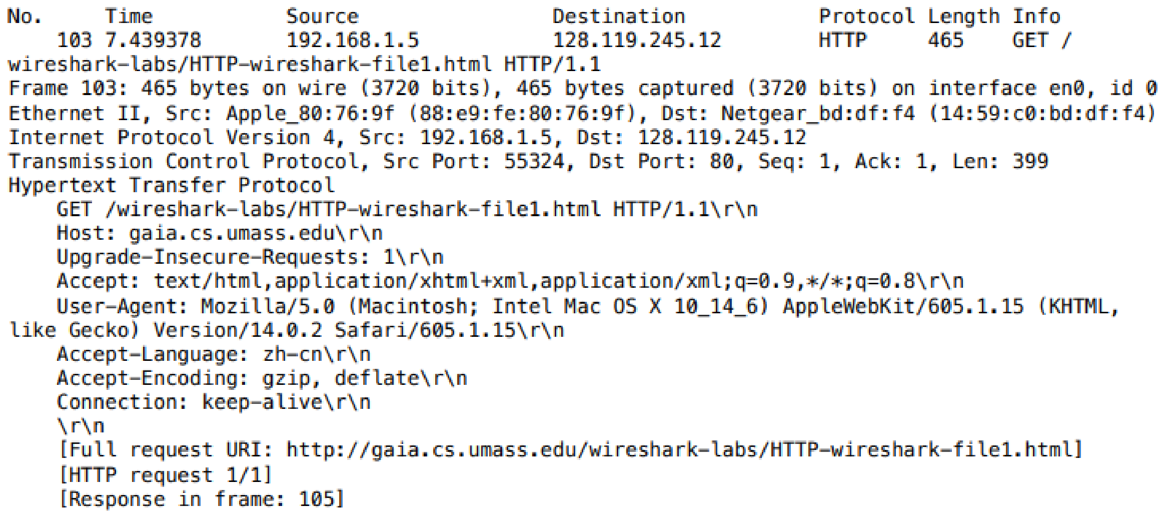
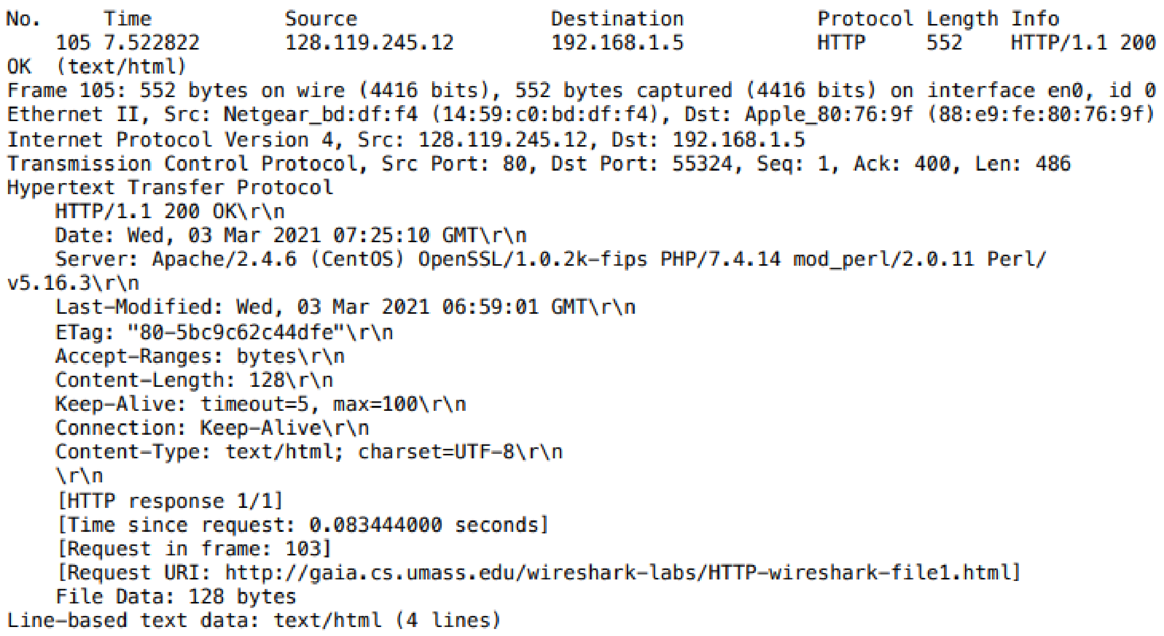
ECS 152A Programing 2

Part A

Q1:



```
No.      Time            Source                Destination           Protocol Length Info
    103 7.439378         192.168.1.5           128.119.245.12        HTTP     465    GET /
wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 103: 465 bytes on wire (3720 bits), 465 bytes captured (3720 bits) on interface en0, id 0
Ethernet II, Src: Apple_80:76:9f (88:e9:fe:80:76:9f), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55324, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML,
like Gecko) Version/14.0.2 Safari/605.1.15\r\n
    Accept-Language: zh-cn\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 105]
```



```
No.      Time            Source                Destination           Protocol Length Info
    105 7.522822         128.119.245.12        192.168.1.5           HTTP     552    HTTP/1.1 200
OK  (text/html)
Frame 105: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id 0
Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 55324, Seq: 1, Ack: 400, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Wed, 03 Mar 2021 07:25:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    Last-Modified: Wed, 03 Mar 2021 06:59:01 GMT\r\n
    ETag: "80-5bc9c62c44dfe"\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
    [HTTP response 1/1]
    [Time since request: 0.083444000 seconds]
    [Request in frame: 103]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

Questions:

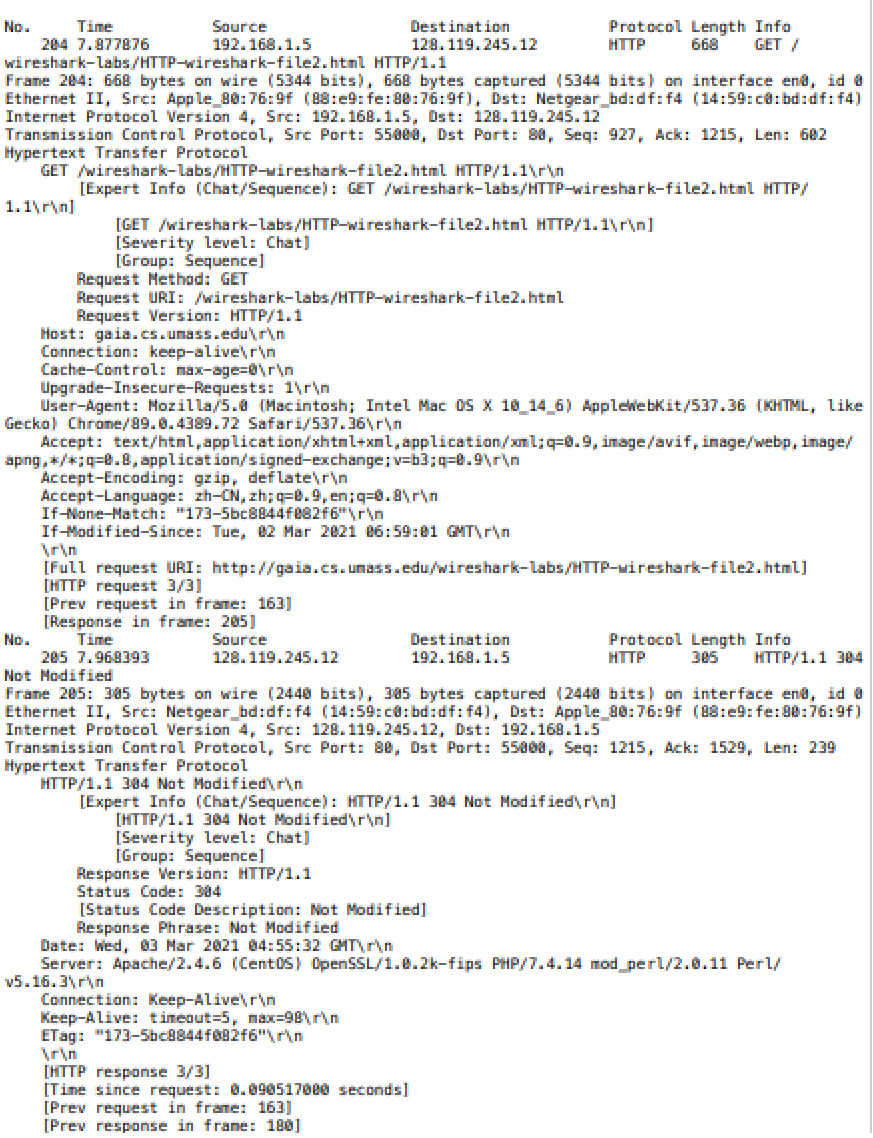
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What languages (if any) does your browser indicate that it can accept to the server?
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
4. What is the status code returned from the server to your browser?
5. When was the HTML file that you are retrieving last modified at the server?
6. How many bytes of content are being returned to your 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.

Answers:

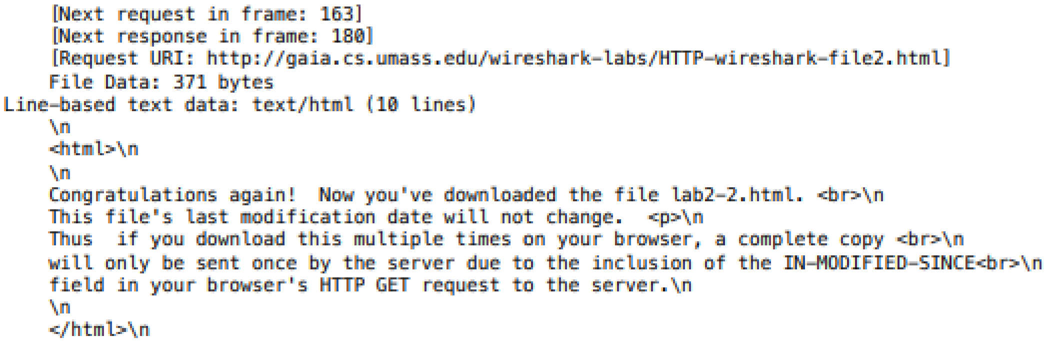
```
1. My browser is running **HTTP version 1.1**; the server also running **HTTP version 1.1**.
2. My browser accept **zh-CN**.
3. The IP address of my computer is **192.168.1.5**; the IP address of gaia.cs.umass.edu server is **128.119.245.12**.
4. The status code returned from the server to my browser is **200**.
5. The last modified time is **Wed, 03 Mar 2021 07:25:10 GMT**.
6. There are **128 bytes** being returned to my browser.
7. I did not see any headers within the data thar are not displayed in the packet-listing window.
```

Q2:

First Time:

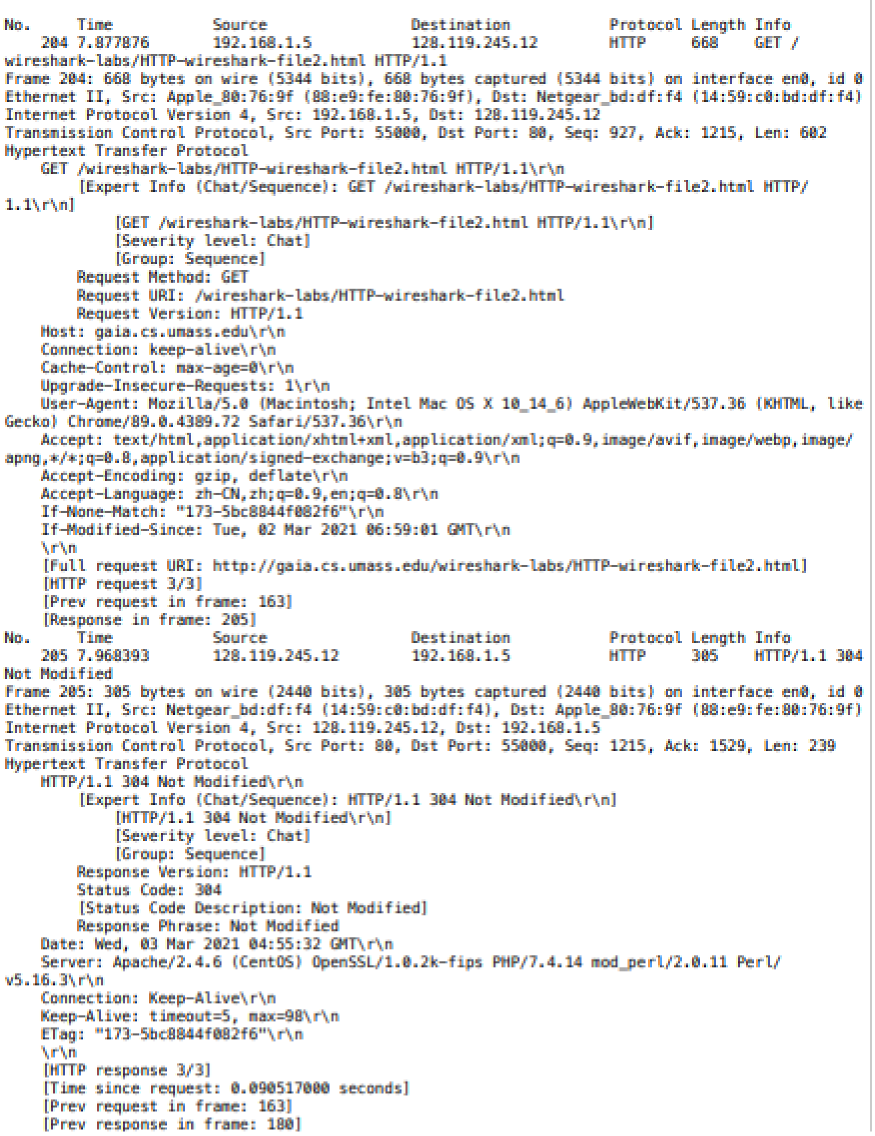


```
No.     Time           Source                Destination           Protocol Length Info
    204 7.877876       192.168.1.5           128.119.245.12        HTTP     668    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 204: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface en0, id 0
Ethernet II, Src: Apple_80:76:9f (88:e9:fe:80:76:9f), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55000, Dst Port: 80, Seq: 927, Ack: 1215, Len: 602
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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_14_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/89.0.4389.72 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    If-None-Match: "173-5bc8844f082f6"\r\n
    If-Modified-Since: Tue, 02 Mar 2021 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 163]
    [Response in frame: 205]
No.     Time           Source                Destination           Protocol Length Info
    205 7.968393       128.119.245.12        192.168.1.5           HTTP     305    HTTP/1.1 304
Not Modified
Frame 205: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface en0, id 0
Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 55000, Seq: 1215, Ack: 1529, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 03 Mar 2021 04:55:32 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-5bc8844f082f6"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.090517000 seconds]
    [Prev request in frame: 163]
    [Prev response in frame: 180]
```



```
        [Next request in frame: 163]
        [Next response in frame: 180]
        [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
```

Second Time:



```
No.     Time           Source                Destination           Protocol Length Info
    204 7.877876       192.168.1.5           128.119.245.12        HTTP     668    GET /
wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Frame 204: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface en0, id 0
Ethernet II, Src: Apple_80:76:9f (88:e9:fe:80:76:9f), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55000, Dst Port: 80, Seq: 927, Ack: 1215, Len: 602
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/
1.1\r\n]
            [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        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_14_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/89.0.4389.72 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    If-None-Match: "173-5bc8844f082f6"\r\n
    If-Modified-Since: Tue, 02 Mar 2021 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 3/3]
    [Prev request in frame: 163]
    [Response in frame: 205]
No.     Time           Source                Destination           Protocol Length Info
    205 7.968393       128.119.245.12        192.168.1.5           HTTP     305    HTTP/1.1 304
Not Modified
Frame 205: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface en0, id 0
Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 55000, Seq: 1215, Ack: 1529, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
            [HTTP/1.1 304 Not Modified\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 03 Mar 2021 04:55:32 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
    ETag: "173-5bc8844f082f6"\r\n
    \r\n
    [HTTP response 3/3]
    [Time since request: 0.090517000 seconds]
    [Prev request in frame: 163]
    [Prev response in frame: 180]
```

Questions:

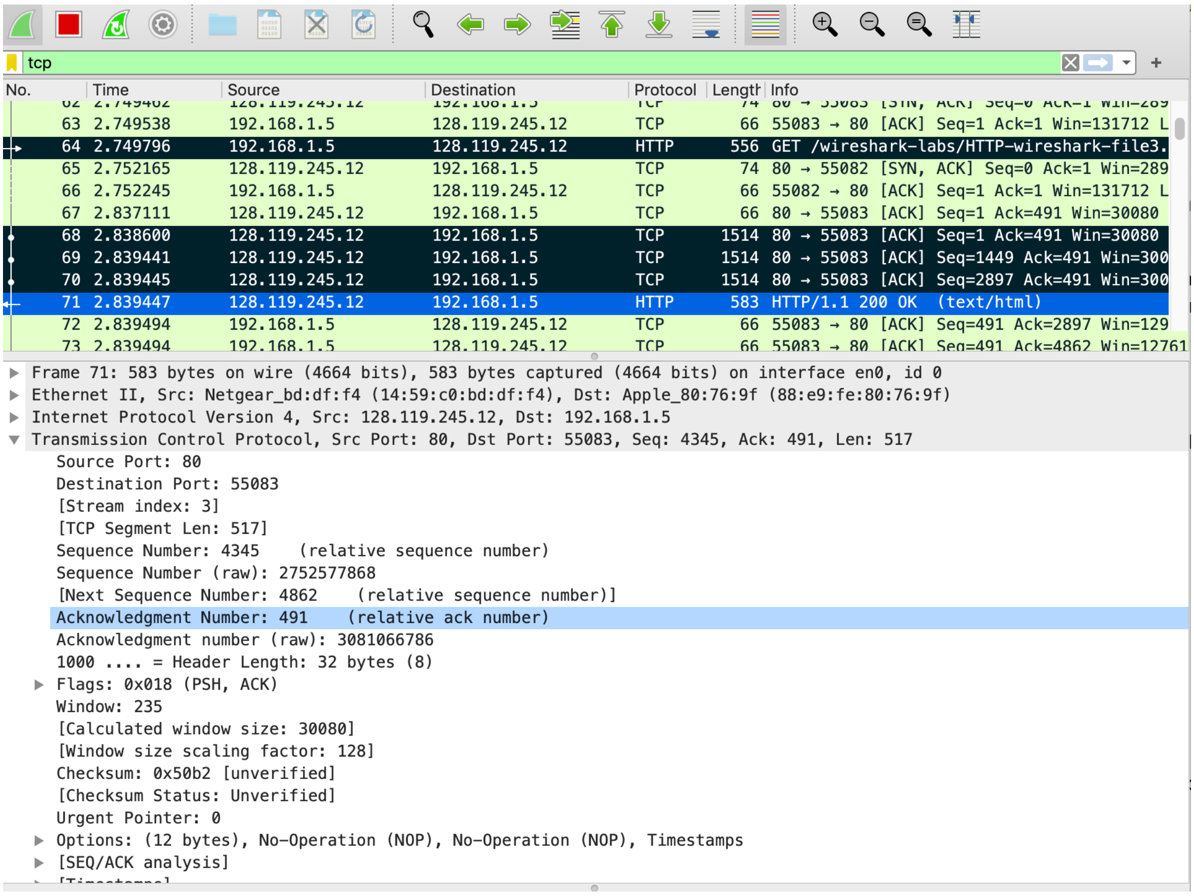
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
10. Now inspect the contents of the 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?

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.

Answers:

8. There is **No** “IF-MODIFIED-SINCE” line in the first HTTP GET.
9. **Yes, the server explicity return the contesnts fo the file.** Since we can see the full test of the file in the first response.
10. **Yes**, there is an “IF-MODIFIED-SINCE” line in the second HTTP GET. The information follows the “IF-MODIFIED-SINCE” header is a record of the time, which is **Tue, 02 Mar 2021 06:59:01 GMT**.
11. The status code returned from the server in response to the second HTTP GET is code **304**, which represents “not modified”. The server does **NOT** explicity return the contents of the file.

Q3:



tcp

```
No.   Time      Source           Destination      Protocol Length Info
62 2.749462  128.119.245.12   192.168.1.5      TCP        74 80 → 55083 [SYN, ACK] Seq=0 Ack=1 Win=289
63 2.749538  192.168.1.5      128.119.245.12   TCP        66 55083 → 80 [ACK] Seq=1 Ack=1 Win=131712 L
64 2.749796  192.168.1.5      128.119.245.12   HTTP      556 GET /wireshark-labs/HTTP-wireshark-file3.
65 2.752165  128.119.245.12   192.168.1.5      TCP        74 80 → 55082 [SYN, ACK] Seq=0 Ack=1 Win=289
66 2.752245  192.168.1.5      128.119.245.12   TCP        66 55082 → 80 [ACK] Seq=1 Ack=1 Win=131712 L
67 2.837111  128.119.245.12   192.168.1.5      TCP        66 80 → 55083 [ACK] Seq=1 Ack=491 Win=30080
68 2.838600  128.119.245.12   192.168.1.5      TCP      1514 80 → 55083 [ACK] Seq=1 Ack=491 Win=30080
69 2.839441  128.119.245.12   192.168.1.5      TCP      1514 80 → 55083 [ACK] Seq=1449 Ack=491 Win=300
70 2.839445  128.119.245.12   192.168.1.5      TCP      1514 80 → 55083 [ACK] Seq=2897 Ack=491 Win=300
71 2.839447  128.119.245.12   192.168.1.5      HTTP      583 HTTP/1.1 200 OK  (text/html)
72 2.839494  192.168.1.5      128.119.245.12   TCP        66 55083 → 80 [ACK] Seq=491 Ack=2897 Win=129
73 2.839494  192.168.1.5      128.119.245.12   TCP        66 55083 → 80 [ACK] Seq=491 Ack=4862 Win=12761
```

```
▶ Frame 71: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
▶ Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
▼ Transmission Control Protocol, Src Port: 80, Dst Port: 55083, Seq: 4345, Ack: 491, Len: 517
    Source Port: 80
    Destination Port: 55083
    [Stream index: 3]
    [TCP Segment Len: 517]
    Sequence Number: 4345    (relative sequence number)
    Sequence Number (raw): 2752577868
    [Next Sequence Number: 4862    (relative sequence number)]
    Acknowledgment Number: 491    (relative ack number)
    Acknowledgment number (raw): 3081066786
    1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
    Window: 235
    [Calculated window size: 30080]
    [Window size scaling factor: 128]
    Checksum: 0x50b2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▶ [SEQ/ACK analysis]
```

Questions:

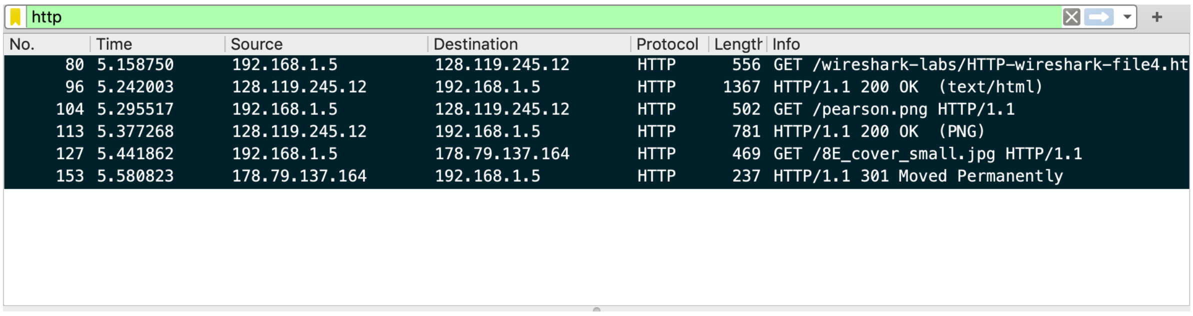
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
14. What is the status code and phrase in the response?
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Answers:

12. My browser only send **1** HTTP GET request message. The packet contains the GET message for the Bill or Rights is the packet with number **64**.

13. The packet that contians the status code and phrase associated with the response to the HTTP GET request is the packet number **68**.
14. The status code and phrase in the response is **200 OK**.
15. **3 packets** are needed to carry the single HTTp response and the text of the Bill of Rights. They are packet **68, 69, 70**.

Q4:



```
http
No.    Time      Source          Destination     Protocol Length Info
    80 5.158750  192.168.1.5     128.119.245.12  HTTP      556 GET /wireshark-labs/HTTP-wireshark-file4.ht
    96 5.242003  128.119.245.12  192.168.1.5     HTTP     1367 HTTP/1.1 200 OK  (text/html)
   104 5.295517  192.168.1.5     128.119.245.12  HTTP      502 GET /pearson.png HTTP/1.1
   113 5.377268  128.119.245.12  192.168.1.5     HTTP      781 HTTP/1.1 200 OK  (PNG)
   127 5.441862  192.168.1.5     178.79.137.164  HTTP      469 GET /8E_cover_small.jpg HTTP/1.1
   153 5.580823  178.79.137.164  192.168.1.5     HTTP      237 HTTP/1.1 301 Moved Permanently
```

Questions:

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

Answers:

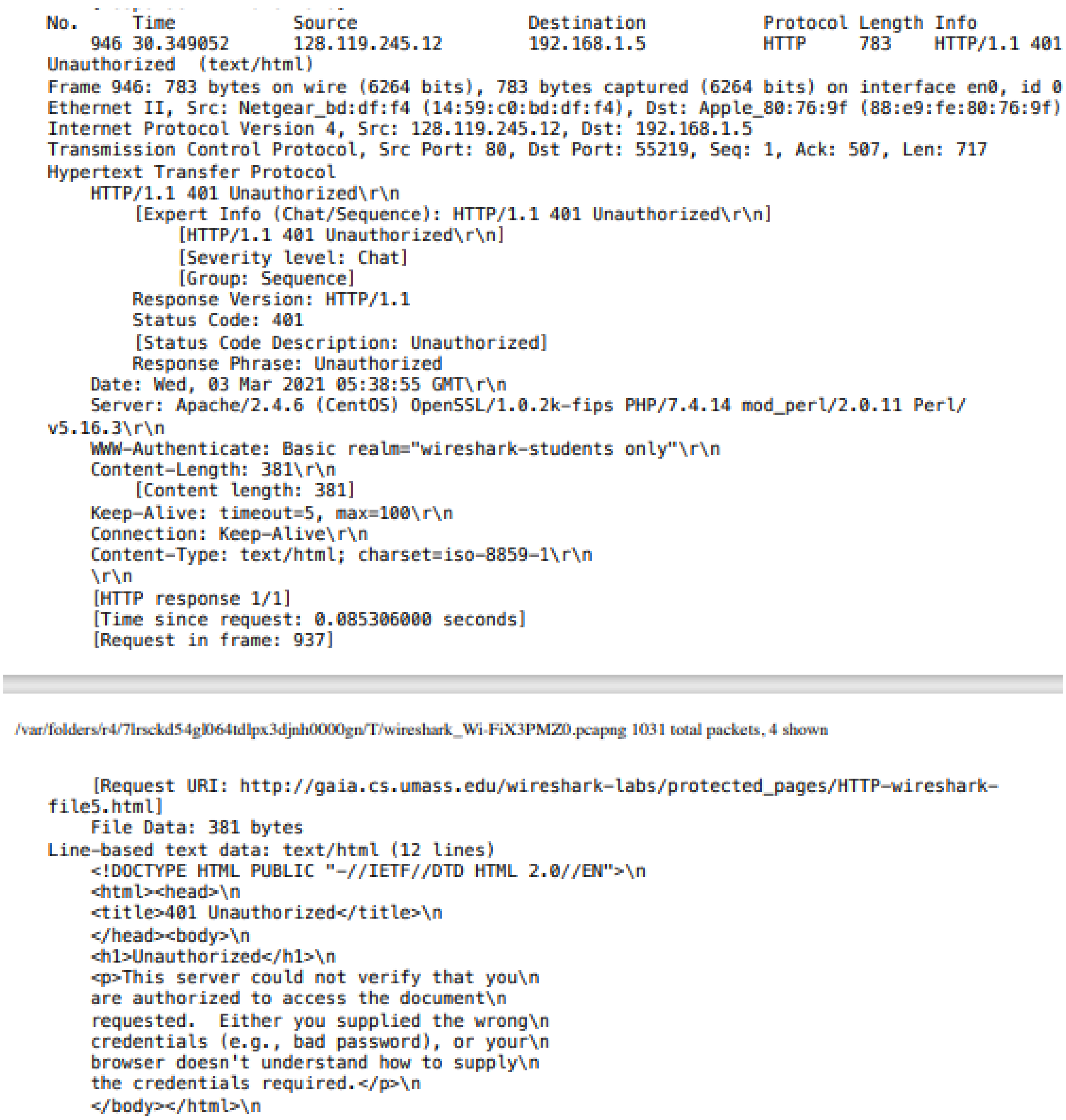
16. My browser send **3** HTTP Get request messages. The packet **80** sent to **128.119.245.12**; the packet **104** sent to **128.119.245.12**; the packet **127** sent to **178.79.137.164**.
17. My browser downloaded the two images **serially** since the GET requests were sent in packet NO.104 and NO.127, but the first respose was returned in packet NO.113 from the server. Thus, my browser downloaded the two images serially but not parallel.

Q5:

First Request

```
No.     Time           Source                Destination           Protocol Length Info
    937 30.263746      192.168.1.5           128.119.245.12        HTTP     572    GET /
wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Frame 937: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits) on interface en0, id 0
Ethernet II, Src: Apple_80:76:9f (88:e9:fe:80:76:9f), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55219, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-
file5.html HTTP/1.1\r\n]
            [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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_14_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/89.0.4389.72 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-
file5.html]
    [HTTP request 1/1]
    [Response in frame: 946]
```

First Response

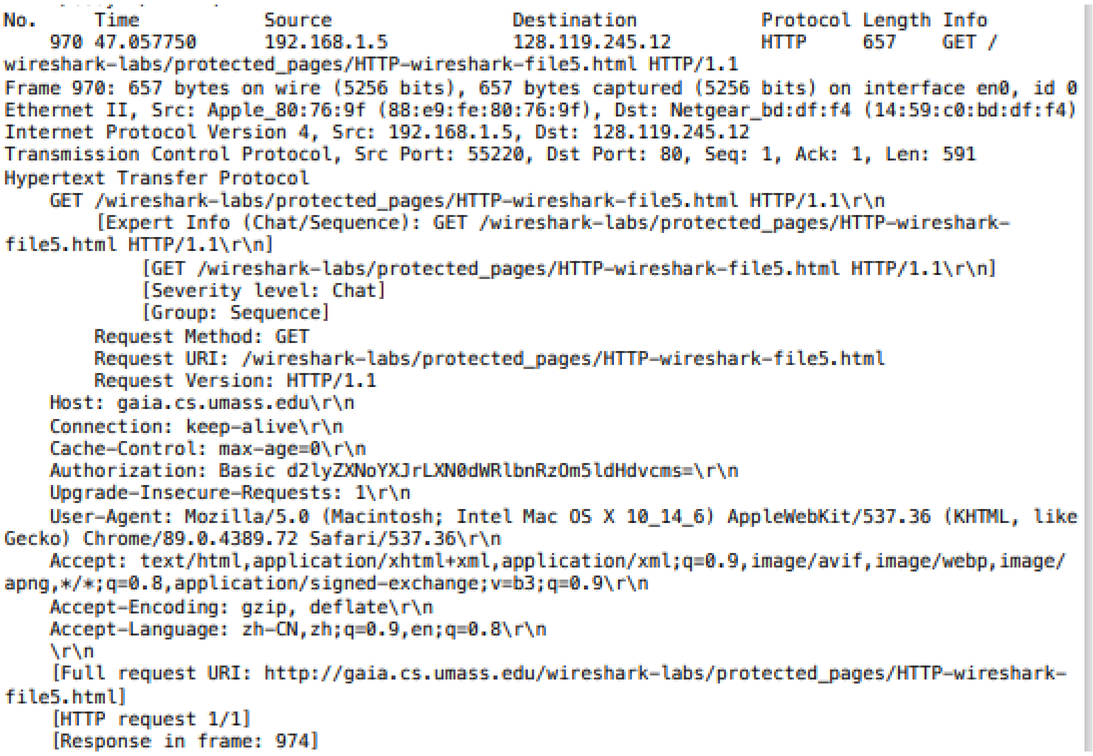


```
No.     Time           Source                Destination           Protocol Length Info
    946 30.349052      128.119.245.12        192.168.1.5           HTTP     783    HTTP/1.1 401
Unauthorized  (text/html)
Frame 946: 783 bytes on wire (6264 bits), 783 bytes captured (6264 bits) on interface en0, id 0
Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 55219, Seq: 1, Ack: 507, Len: 717
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
            [HTTP/1.1 401 Unauthorized\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Wed, 03 Mar 2021 05:38:55 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
        [Content length: 381]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.085306000 seconds]
    [Request in frame: 937]
```

/var/folders/r4/7lrsckd54gl064tdlpx3djnh0000gn/T/wireshark_Wi-FiX3PMZ0.pcapng 1031 total packets, 4 shown

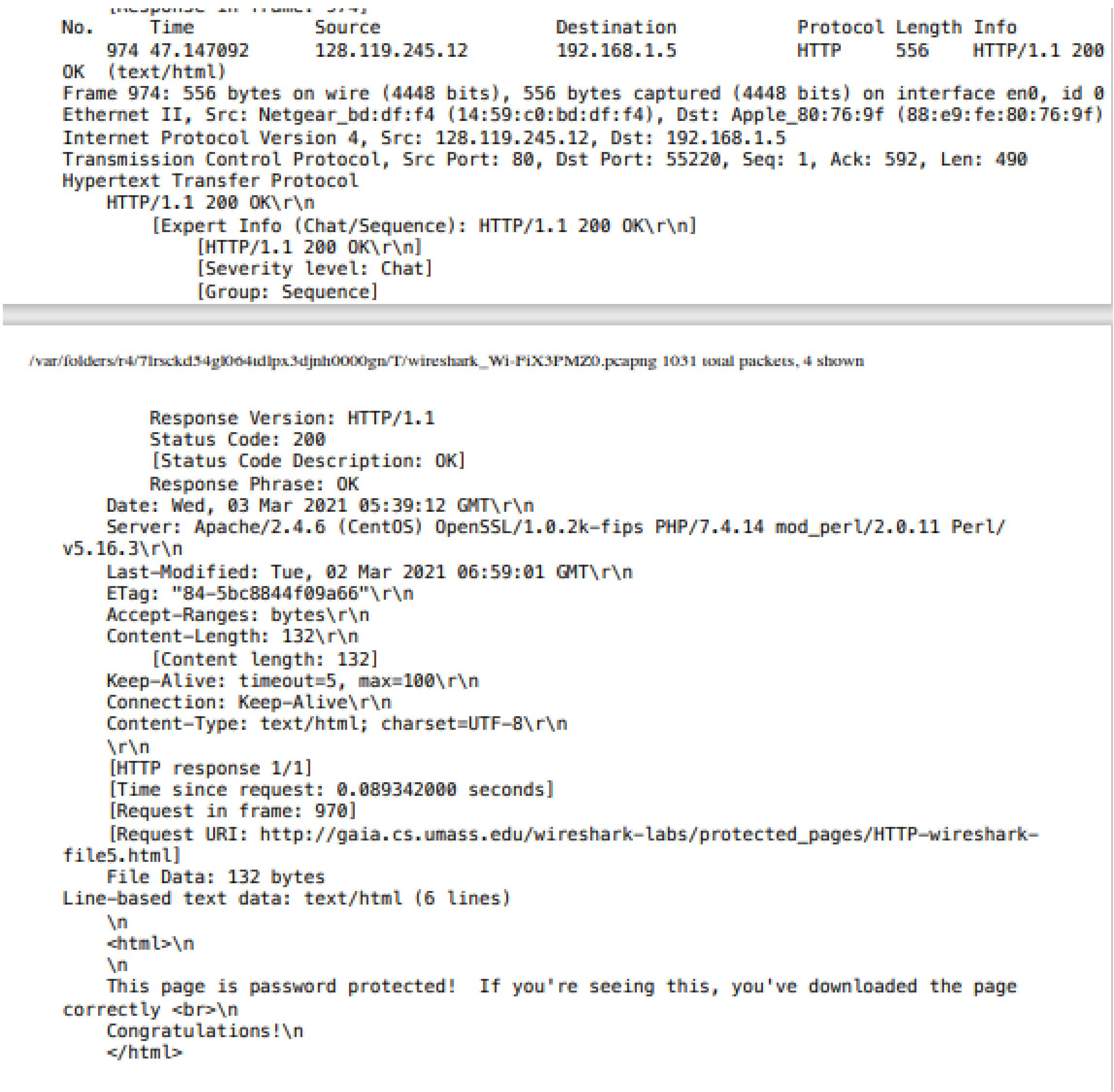
```
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-
file5.html]
    File Data: 381 bytes
Line-based text data: text/html (12 lines)
    <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
    <html><head>\n
    <title>401 Unauthorized</title>\n
    </head><body>\n
    <h1>Unauthorized</h1>\n
    <p>This server could not verify that you\n
    are authorized to access the document\n
    requested.  Either you supplied the wrong\n
    credentials (e.g., bad password), or your\n
    browser doesn't understand how to supply\n
    the credentials required.</p>\n
    </body></html>\n
```

Second Request



```
No.     Time           Source                Destination           Protocol Length Info
    970 47.057750      192.168.1.5           128.119.245.12        HTTP     657    GET /
wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Frame 970: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface en0, id 0
Ethernet II, Src: Apple_80:76:9f (88:e9:fe:80:76:9f), Dst: Netgear_bd:df:f4 (14:59:c0:bd:df:f4)
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55220, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-
file5.html HTTP/1.1\r\n]
            [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/89.0.4389.72 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-
file5.html]
    [HTTP request 1/1]
    [Response in frame: 974]
```

Second Response



```
    [Response in frame: 974]
No.     Time           Source                Destination           Protocol Length Info
    974 47.147092      128.119.245.12        192.168.1.5           HTTP     556    HTTP/1.1 200
OK  (text/html)
Frame 974: 556 bytes on wire (4448 bits), 556 bytes captured (4448 bits) on interface en0, id 0
Ethernet II, Src: Netgear_bd:df:f4 (14:59:c0:bd:df:f4), Dst: Apple_80:76:9f (88:e9:fe:80:76:9f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.5
Transmission Control Protocol, Src Port: 80, Dst Port: 55220, Seq: 1, Ack: 592, Len: 490
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
```

/var/folders/r4/7lrsckd54gl064udlpx3djnh0000gn/T/wireshark_Wi-FiX3PMZ0.pcapng 1031 total packets, 4 shown

```
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Wed, 03 Mar 2021 05:39:12 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/
v5.16.3\r\n
    Last-Modified: Tue, 02 Mar 2021 06:59:01 GMT\r\n
    ETag: "84-5bc8844f09a66"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 132\r\n
        [Content length: 132]
    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 1/1]
    [Time since request: 0.089342000 seconds]
    [Request in frame: 970]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-
file5.html]
    File Data: 132 bytes
Line-based text data: text/html (6 lines)
    \n
    <html>\n
    \n
    This page is password protected!  If you're seeing this, you've downloaded the page
correctly <br>\n
    Congratulations!\n
    </html>
```

Questions:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Answers:

18. Packet NO.946 is the initial server's response to the initial HTTP GET message from my browser. The status code and phrase is **401 Unauthorized**.
19. The new field included in the second HTTP GET message is **Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=** , which is the password of the website.