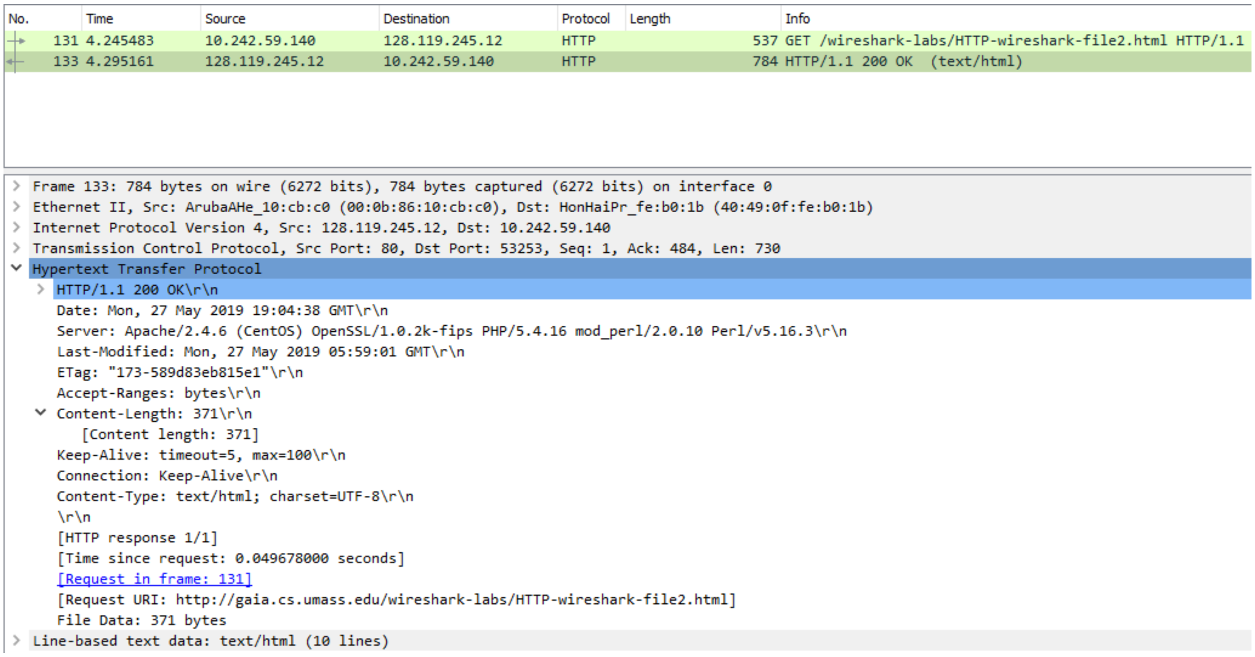
Wireshark Assignment # 1 (Application layer Packet Sniffer) HTTP

Denis Nadarevic
COMP3670
104445626
May 31st, 2019



No.	Time	Source	Destination	Protocol	Length	Info
131	4.245483	10.242.59.140	128.119.245.12	HTTP	537	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
133	4.295161	128.119.245.12	10.242.59.140	HTTP	784	HTTP/1.1 200 OK (text/html)

```
> Frame 133: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface 0
> Ethernet II, Src: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0), Dst: HonHaiPr_fe:b0:1b (40:49:0f:fe:b0:1b)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.242.59.140
> Transmission Control Protocol, Src Port: 80, Dst Port: 53253, Seq: 1, Ack: 484, Len: 730
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, 27 May 2019 19:04:38 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Mon, 27 May 2019 05:59:01 GMT\r\n
    ETag: "173-589d83eb815e1"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 371\r\n
      [Content length: 371]
    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: 0.049678000 seconds]
    [Request in frame: 131]
    [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)
```

***Figure 1.1** – This screenshot of the HTTP response message will be used to answer the following questions.*

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
   a. *My browser and the server is running on HTTP version 1.1. This information is provided on the top where the HTTP messages where captured. The message includes "HTTP/1.1" for both messages.*

2. What languages (if any) does your browser indicate that it can accept to the server?
   a. *My browser accepts* ***en-CA (Canadian English)****,* ***en-GB (British English)****,* ***en-US (American English)****, and* ***en (in general, I would assume)****.*

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

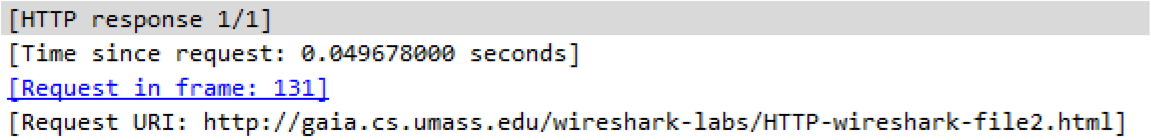
   a. *My IP address is the university's IP address, which is* ***10.242.59.140****. The IP address of the gaia.cs.umass.edu server is* ***128.119.245.12****.*

4. What is the status code returned from the server to your browser?
   a. *The status code is 200, which just means OK (it has successfully completed the request)*

5. When was the HTML file that you are retrieving last modified at the server?
   a. It was last modified on Monday, May 27th, 2019 at 05:59:01 GMT

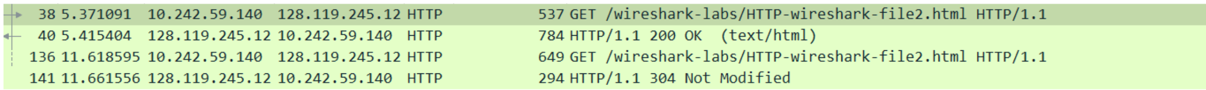
6. How many bytes of content are being returned to your browser?
   a. *The file data's number of bytes is 371 bytes.*

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.
   a. *The only information that doesn't highlight anything in the packet-listing window is shown in the screenshot below, other than that, everything shows up in the packet-listing:*

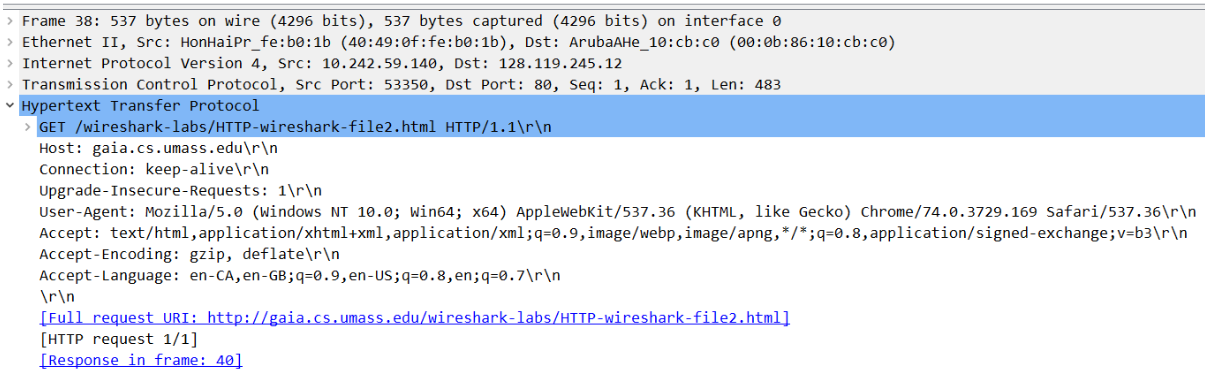


```
[HTTP response 1/1]
[Time since request: 0.049678000 seconds]
[Request in frame: 131]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

The HTTP CONDITIONAL GET/response interaction



```
 38 5.371091  10.242.59.140  128.119.245.12 HTTP           537 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 40 5.415404  128.119.245.12 10.242.59.140  HTTP           784 HTTP/1.1 200 OK  (text/html)
136 11.618595 10.242.59.140  128.119.245.12 HTTP           649 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141 11.661556 128.119.245.12 10.242.59.140  HTTP           294 HTTP/1.1 304 Not Modified
```



```
> Frame 38: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on interface 0
> Ethernet II, Src: HonHaiPr_fe:b0:1b (40:49:0f:fe:b0:1b), Dst: ArubaAHe_10:cb:c0 (00:0b:86:10:cb:c0)
> Internet Protocol Version 4, Src: 10.242.59.140, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53350, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-CA,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 40]
```

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?
   a. *No there is no such statement in the GET request message.*

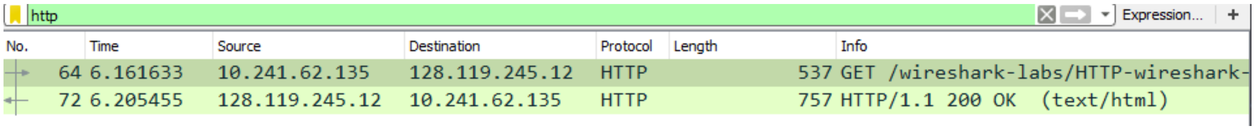
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   a. *Yes it returned the contents of the file, the status code is 200 which means the information was sent and my browser downloaded the file*

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?
    a. *I see an "IF-MODIFIED-SINCE" in the second HTTP GET request. The full line says "If-Modified-Since: Mon, 27 May 2019 05:59:01 gmt\r\n". Under this line contains the full request URI. The server will only send back the resource that was request ONLY IF the file was modified after the date given in the conditional.*

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.
    a. *The HTTP status code is 304 Not Modified. This means that the server did not download the file since my browser already has the latest modified version of that file. The file is stored in cache.*

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?
    a. *My browser sent only one HTTP GET request message. Packet #64 contains the GET message. *NOTE* I changed locations in campus, my IP address changed.*

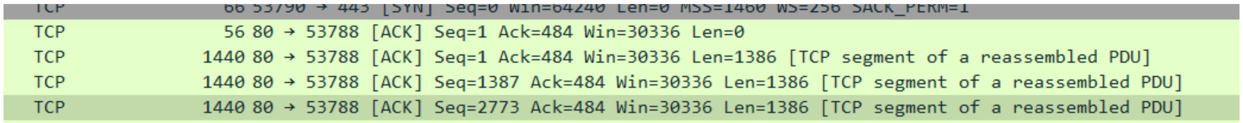


```
No.   Time       Source          Destination     Protocol  Length  Info
   64 6.161633   10.241.62.135   128.119.245.12  HTTP         537  GET /wireshark-labs/HTTP-wireshark-
   72 6.205455   128.119.245.12  10.241.62.135   HTTP         757  HTTP/1.1 200 OK  (text/html)
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
    a. *According to the screenshot above, packet #72 contains the status code and phrase.*

14. What is the status code and phrase in the response?
    a. *According to the screenshot above, the Status code is 200 and the response is OK.*

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

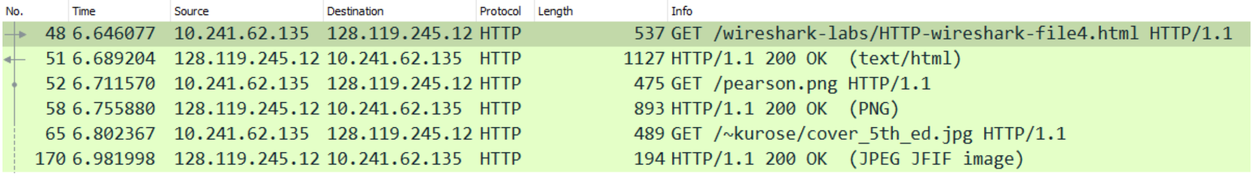


```
TCP          66 53790 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
TCP          56 80 → 53788 [ACK] Seq=1 Ack=484 Win=30336 Len=0
TCP        1440 80 → 53788 [ACK] Seq=1 Ack=484 Win=30336 Len=1386 [TCP segment of a reassembled PDU]
TCP        1440 80 → 53788 [ACK] Seq=1387 Ack=484 Win=30336 Len=1386 [TCP segment of a reassembled PDU]
TCP        1440 80 → 53788 [ACK] Seq=2773 Ack=484 Win=30336 Len=1386 [TCP segment of a reassembled PDU]
```

    a. *According to the screenshot above, a total of 3 data-containing TCP segments were needed to carry the HTTP response and the text.*

This assignment is for educational purposes only. Do not share this document with others without permission from Denis Nadarevic

HTML Documents with Embedded Objects

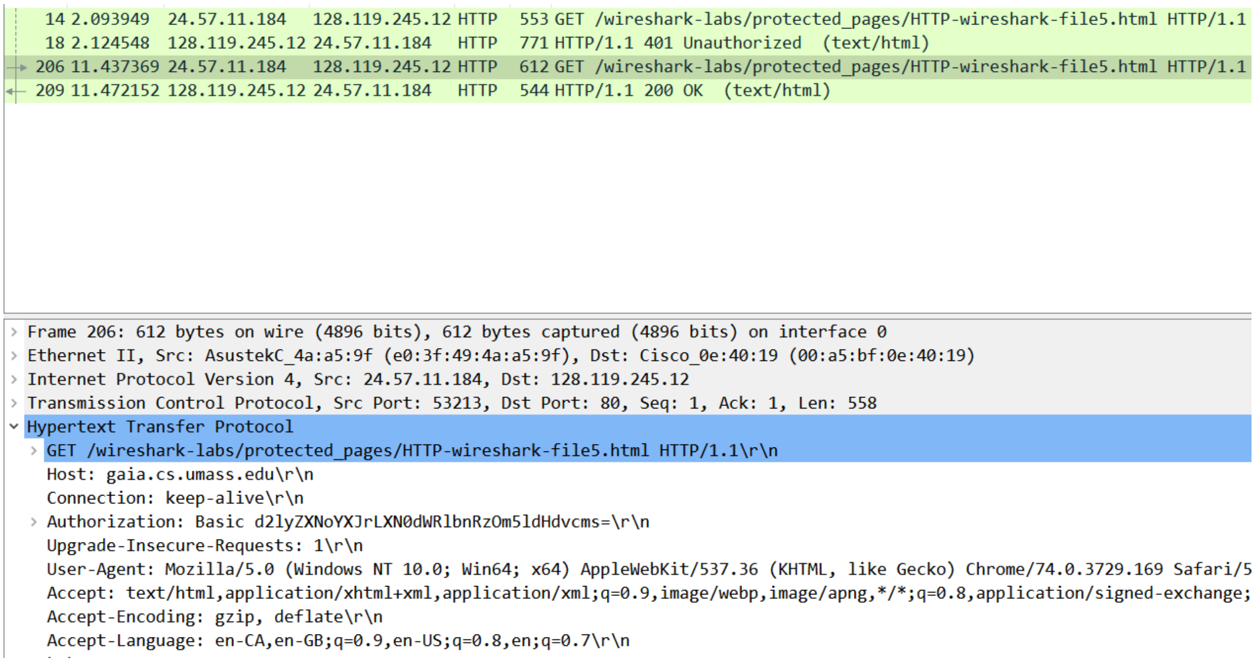


```
No.  Time      Source          Destination     Protocol Length Info
 48 6.646077  10.241.62.135   128.119.245.12  HTTP      537 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
 51 6.689204  128.119.245.12  10.241.62.135   HTTP     1127 HTTP/1.1 200 OK  (text/html)
 52 6.711570  10.241.62.135   128.119.245.12  HTTP      475 GET /pearson.png HTTP/1.1
 58 6.755880  128.119.245.12  10.241.62.135   HTTP      893 HTTP/1.1 200 OK  (PNG)
 65 6.802367  10.241.62.135   128.119.245.12  HTTP      489 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
170 6.981998  128.119.245.12  10.241.62.135   HTTP      194 HTTP/1.1 200 OK  (JPEG JFIF image)
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    a. *3 HTTP GET request messages were sent from my browser. All three requests were sent to* ***128.119.245.12.***

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.
    a. *I would like to assume that they were sent serially because each GET request message was sent right after an OK response message was received.*

HTTP Authentication



```
 14 2.093949  24.57.11.184    128.119.245.12 HTTP  553 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 18 2.124548  128.119.245.12 24.57.11.184    HTTP  771 HTTP/1.1 401 Unauthorized  (text/html)
206 11.437369 24.57.11.184    128.119.245.12 HTTP  612 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
209 11.472152 128.119.245.12 24.57.11.184    HTTP  544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 206: 612 bytes on wire (4896 bits), 612 bytes captured (4896 bits) on interface 0
> Ethernet II, Src: AsustekC_4a:a5:9f (e0:3f:49:4a:a5:9f), Dst: Cisco_0e:40:19 (00:a5:bf:0e:40:19)
> Internet Protocol Version 4, Src: 24.57.11.184, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53213, Dst Port: 80, Seq: 1, Ack: 1, Len: 558
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/5
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-CA,en-GB;q=0.9,en-US;q=0.8,en;q=0.7\r\n
```

This screenshot will be used to answer questions 18 and 19. Note: The IP changes are due to location changes. The new IP is from my home.

18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?
    a. *The server’s response was a status code 401 and phrase Unauthorized in response to the initial HTTP GET message. This means it lacks valid authentication credentials for the 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?
    a. According to the screenshot above, the “authorization” field is included in the second GET message.