

Benjamin Fondell

Introduction to Networks

October 20, 2017

## Lab 02

|     |                 |                |                |      |     |                                       |
|-----|-----------------|----------------|----------------|------|-----|---------------------------------------|
| 218 | 13:04:33.752478 | 10.0.1.20      | 128.119.245.12 | HTTP | 483 | GET /wireshark-labs/HTTP-wireshark-fi |
| 219 | 13:04:33.757006 | 128.119.245.12 | 10.0.1.20      | HTTP | 532 | HTTP/1.1 200 OK (text/html)           |
| 225 | 13:04:33.934266 | 10.0.1.20      | 128.119.245.12 | HTTP | 429 | GET /favicon.ico HTTP/1.1             |
| 227 | 13:04:33.938032 | 128.119.245.12 | 10.0.1.20      | HTTP | 551 | HTTP/1.1 404 Not Found (text/html)    |

1. Version 1.1



2. English(u.s.)

```
▼ Hypertext Transfer Protocol
  ► GET /wireshark-labs/HTTP-wireshark-fi
    Host: gaia.cs.umass.edu\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml
    User-Agent: Mozilla/5.0 (Macintosh; I
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
```



3.

My Computer IP: 10.0.1.20

Umass IP: 128.119.245.12



|     |                 |           |                |      |     |                                       |
|-----|-----------------|-----------|----------------|------|-----|---------------------------------------|
| 218 | 13:04:33.752278 | 10.0.1.20 | 128.119.245.12 | HTTP | 483 | GET /wireshark-labs/HTTP-wireshark-fi |
|-----|-----------------|-----------|----------------|------|-----|---------------------------------------|

| No. | Time            | Source         | Destination    | Protocol | Length | Info                                      |
|-----|-----------------|----------------|----------------|----------|--------|---|
| 218 | 13:04:31.752278 | 10.0.1.20      | 128.119.245.12 | HTTP     | 463    | GET /wireshark-labs/HTTP-wireshark-fil... |
| 220 | 13:04:31.837664 | 128.119.245.12 | 10.0.1.20      | HTTP     | 552    | HTTP/1.1 200 OK (text/html)               |

4. Status Code: 200 OK

```
HTTP/1.1 200 OK\r\n
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  Request Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
Date: Fri, 20 Oct 2017 20:04:31 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: Fri, 20 Oct 2017 05:59:01 GMT\r\n
—
```

5. Last-Modified: Fri, 20 Oct 2017 05:59:01 GMT

```
> 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: 0.086386000 seconds]
[Request in frame: 218]
File Data: 128 bytes
```

6. 128 bytes

7. No, all data appears to be displayed in the packet-listing window.

```

▼ 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]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1

```

8. No.

```

HTTP/1.1 200 OK\r\n
▶ [Expert Info [Chat/Sequence]: HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Content-Type: text/html

```

```

< Downloaded text data: text/html
<
<
<
<
< Congratulations again! Now you've downloaded the file lab2-2.html, done!
< This file's last modification date will not change. Again.
< Now, all you should see multiple times on your browser, a complete copy of the
< file only be sent out to the browser due to the inclusion of the Content-Type: text/html
< field in your browser's HTTP GET request to the server.
<
<

```

9. Yes. Because there is html in the response packet and the response status code is 200 OK.

```

▶ Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: 192.168.1.100:8080\r\n
  Connection: keep-alive\r\n
  Cache-Control: max-age=0\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 12_12_6; AppleWebKit/537.36; Chrome/102.0.5009.160) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5009.160 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "123-567890-123456789"\r\n
  If-Modified-Since: Fri, 20 Oct 2017 05:59:01 GMT\r\n

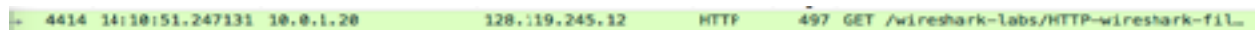
```

10. Yes. If-Modified-Since: Fri, 20 Oct 2017 05:59:01 GMT




35 13:43:33.485588 128.119.245.12 10.0.1.20 HTTP 305 HTTP/1.1 304 Not Modified

11. Status code: HTTP/1.1 304 Not Modified. The server did not respond with contents of the file because it will instead have been added and populated from the browser cache. This is for more rapid population of files during web browsing and limited network strain by duplicate responses. If the file is modified then a new version will be sent in response to a request and subsequently loaded into the browser cache.



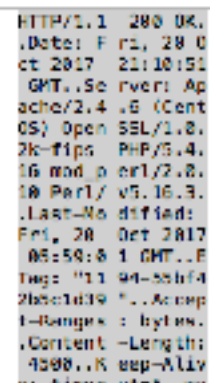
4414 14:10:51.247131 10.0.1.20 128.119.245.12 HTTP 497 GET /wireshark-labs/HTTP-wireshark-fil...

12. Browser sent one get request. 4414 contains the get request.



[Frame: 4502, payload: 0-1307 (1308 bytes)]

13. 4502 contains the status code and phrase.



```

HTTP/1.1 200 OK
Date: Fri, 20 Oct 2017 21:10:51 GMT
Server: Apache/2.4.18 (CentOS)
OpenSSL/1.0.2k-fips
PHP/5.4.16 mod_perl/2.2.3
Perl/v5.16.3
Last-Modified: Fri, 20 Oct 2017 05:59:01 GMT
Etag: "119d-551f42bdc1d39"
Accept-Ranges: bytes
Content-Length: 4500
Keep-Alive: timeout=5, max=1000

```

|      |                 |                |           |      |     |                             |
|------|-----------------|----------------|-----------|------|-----|-----------------------------|
| 4586 | 14:18:51.354000 | 128.119.245.12 | 10.0.1.28 | HTTP | 763 | HTTP/1.1 200 OK (text/html) |
|------|-----------------|----------------|-----------|------|-----|-----------------------------|

14. Status code and phrase is 200 OK.

[4 Reassembled TCP Segments (4061 bytes): #4582(1380), #4584(1380),  
 [Frame: 4582, payload: 0-1397 (1380 bytes)]  
 [Frame: 4584, payload: 1398-2775 (1380 bytes)]  
 [Frame: 4585, payload: 2776-4163 (1388 bytes)]  
 [Frame: 4586, payload: 4164-4860 (697 bytes)]  
 [Segment count: 4]

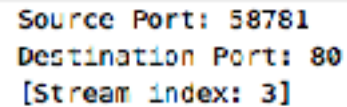
15. 4 TCP segments were needed for the entire Bill of Rights.

|     |                 |                |                |      |      |   |
|-----|-----------------|----------------|----------------|------|------|---|
| 18  | 14:23:08.481520 | 10.0.1.28      | 128.119.245.12 | HTTP | 497  | GET /wineshark-labs/HTTP-wineshark-fil... |
| 20  | 14:23:08.555010 | 128.119.245.12 | 10.0.1.28      | HTTP | 1139 | HTTP/1.1 200 OK (text/html)               |
| 22  | 14:23:08.570660 | 10.0.1.28      | 128.119.245.12 | HTTP | 468  | GET /pearson.png HTTP/1.1                 |
| 27  | 14:23:08.660197 | 128.119.245.12 | 10.0.1.28      | HTTP | 981  | HTTP/1.1 200 OK (PNG)                     |
| 33  | 14:23:08.788239 | 10.0.1.28      | 128.119.248.90 | HTTP | 482  | GET /~kurose/cover_5th_ed.jpg HTTP/1.1    |
| 35  | 14:23:08.874031 | 128.119.248.90 | 10.0.1.28      | HTTP | 522  | HTTP/1.1 302 Found (text/html)            |
| 46  | 14:23:08.985517 | 10.0.1.28      | 128.119.248.90 | HTTP | 402  | GET /~kurose/cover_5th_ed.jpg HTTP/1.1    |
| 174 | 14:23:09.589523 | 128.119.248.90 | 10.0.1.28      | HTTP | 1362 | HTTP/1.1 200 OK (JPEG image)              |

16. 4 total GET requests.

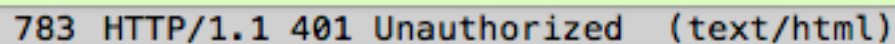
Addresses: 128.119.245.12 and 128.119.240.90

17. In this case the images were downloaded serially. The GET requests made to each address were made at relatively separate times and the second image request didn't begin until prior requests already received responses. I am not sure whether this would be an indicator of serial downloads but it may be an index of the download stream on the port and this would indicate serial separation of downloads.



```
Source Port: 58781
Destination Port: 80
[Stream index: 3]
```

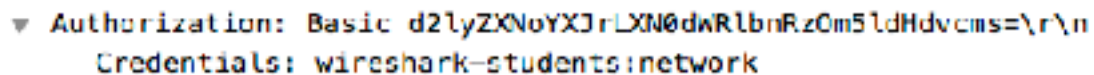
An arrow points from the text 'index of the download stream on the port' to the '[Stream index: 3]' field.



```
783 HTTP/1.1 401 Unauthorized (text/html)
```

An arrow points from the text 'Status code: 401 Unauthorized' to the '401 Unauthorized' part of the status line.

18. The response is: Status code: 401 Unauthorized



```
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm9s\r\n
Credentials: wireshark-students:network
```

An arrow points from the text 'Authorization with credentials' to the 'Credentials: wireshark-students:network' line.

19. Authorization with credentials.