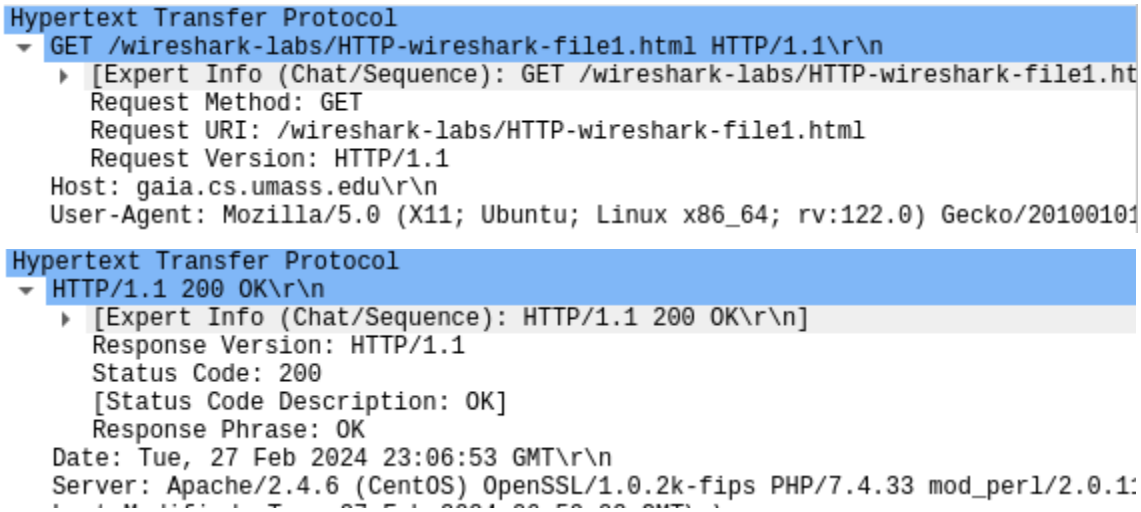
Austin Melendez
2/6/2024

CSC 138 Lab 2

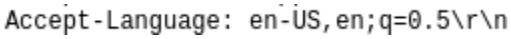
Task 1

---

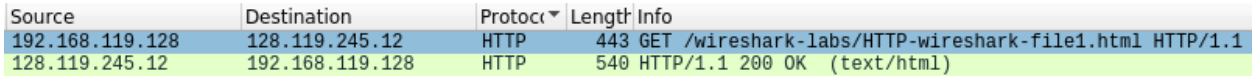
1) My browser is running HTTP 1.1 and the server is running HTTP 1.1



2) The languages by browser lists that it can accept to the server are en-US and en



3) The IP address of my computer is 192.168.119.128 and the IP address of the server is 128.119.245.12



Source	Destination	Protoc	Length	Info
192.168.119.128	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
128.119.245.12	192.168.119.128	HTTP	540	HTTP/1.1 200 OK (text/html)

4) The status code returned from the server to my browser is 200.

5) The file I'm retrieving from the server was last modified Tuesday, February 27 2024 at 06:59:02 GMT

6) There are 128 bytes of content being returned to my browser

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
```

Task 2

---

7) There is no “IF-MODIFIED-SINCE” line in the first HTTP GET

```
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.ht
        [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
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:122.0) Gecko/2010010
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-f
  [HTTP request 1/3]
  [Response in frame: 16]
  [Next request in frame: 24]
```

8) Yes, the server specifically returned the contents of the file. I can tell because it lists the content length, issues a connection, and gives the 200 status code response.

```
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
Date: Tue, 27 Feb 2024 23:29:59 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11
Last-Modified: Tue, 27 Feb 2024 06:59:02 GMT\r\n
ETag: "173-612578fadc6ea"\r\n
Accept-Ranges: bytes\r\n
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
```

9) In the second HTTP GET request there is an “IF-MODIFIED-SINCE” line that is followed by a date and time.

```
If-Modified-Since: Tue, 27 Feb 2024 06:59:02 GMT\r\n
```

10) The HTTP status code and phrase returned from the server during the second HTTP GET was “304 Not Modified”.

```
Status Code: 304
[Status Code Description: Not Modified]
```

Task 3

---

11) My browser only sent one HTTP GET request message, which is packet number 11.

No.	Time	Source	Destination	Protocol	Length	Info
11	18:47:24.483055276	192.168.119.128	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

12) The response to the GET request is packet number 21, which has a status code of “200 OK”.

21	18:47:24.578809065	128.119.245.12	192.168.119.128	HTTP	535	HTTP/1.1 200 OK (text/html)

13) The response contains the status code 200.

```
Status Code: 200
[Status Code Description: OK]
```

14) There are three TCP segments sent from the server containing the data of the Bill of RIghts and one TCP segment with the OK response. The other three TCP segments between the HTTP GET and OK response are the acknowledging responses between my browser and the server and contain no data.

9	19:01:44.208895062	192.168.119.128	128.119.245.12	HTTP	443	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/
10	19:01:44.209222096	128.119.245.12	192.168.119.128	TCP	60	80 → 56258 [ACK] Seq=1 Ack=390 Win=64240 Len=0
11	19:01:44.240950648				54	<Ignored>
12	19:01:44.308265517	128.119.245.12	192.168.119.128	TCP	1514	80 → 56258 [ACK] Seq=1 Ack=390 Win=64240 Len=1460 [
13	19:01:44.308280328	192.168.119.128	128.119.245.12	TCP	54	56258 → 80 [ACK] Seq=390 Ack=1461 Win=62780 Len=0
14	19:01:44.308314351	128.119.245.12	192.168.119.128	TCP	1514	80 → 56258 [ACK] Seq=1461 Ack=390 Win=64240 Len=146
15	19:01:44.308321135	192.168.119.128	128.119.245.12	TCP	54	56258 → 80 [ACK] Seq=390 Ack=2921 Win=62780 Len=0
16	19:01:44.308336705	128.119.245.12	192.168.119.128	TCP	1514	80 → 56258 [ACK] Seq=2921 Ack=390 Win=64240 Len=146
17	19:01:44.308340486	192.168.119.128	128.119.245.12	TCP	54	56258 → 80 [ACK] Seq=390 Ack=4381 Win=61320 Len=0
18	19:01:44.308355515	128.119.245.12	192.168.119.128	HTTP	535	HTTP/1.1 200 OK (text/html)

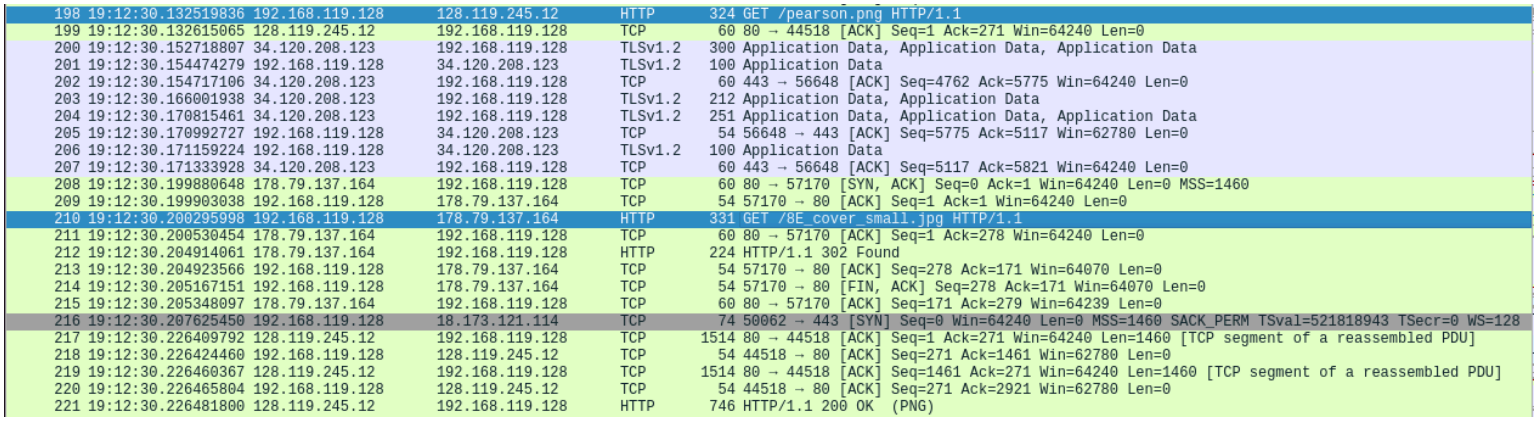
Task 4

---

15) My browser sent two HTTP GET request messages to the IP addresses 128.119.245.12 and 178.79.137.164

No.	Time	Source	Destination	Protocol	Length	Info
198	19:12:30.132519836	192.168.119.128	128.119.245.12	HTTP	324	GET /pearson.png HTTP/1.1
210	19:12:30.200295998	192.168.119.128	178.79.137.164	HTTP	331	GET /8E_cover_small.jpg HTTP/1.1

16) As far as I can tell, my browser downloaded the two images serially. I came to this conclusion because I see a TCP connection sending the data from the first image GET request before the next GET request and TCP responses are handled.



Task 5

---

17) The initial server response to the GET request is “401 Unauthorized”

```
Status Code: 401
[Status Code Description: Unauthorized]
Response Phrase: Unauthorized
```

18) The second HTTP GET request includes the new field “Authorization:” Which includes the login information (username/password) that we entered to get into the site.

```
▾ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
```