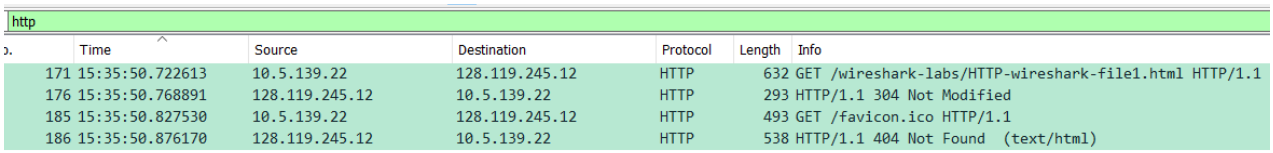
ENGR 3321 - Lab 2: Wireshark HTTP
September 29th 2022
Nathan Cauwet
873271826

1. The Basic HTTP GET/response interaction:



http

No.	Time	Source	Destination	Protocol	Length	Info
171	15:35:50.722613	10.5.139.22	128.119.245.12	HTTP	632	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
176	15:35:50.768891	128.119.245.12	10.5.139.22	HTTP	293	HTTP/1.1 304 Not Modified
185	15:35:50.827530	10.5.139.22	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
186	15:35:50.876170	128.119.245.12	10.5.139.22	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Prefer: safe
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/105.0.0.0 Safari/537.36 Edg/105.0.1343.42
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "80-5e951dfebb45b"
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT
```

1.1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

HTTP version 1.1 is running on both

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

HTML

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

My IP: 10.5.139.22

Gaia.cs.umass.edu IP: 128.199.245.12

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

The server replies to the 1st GET with “304 Not Modified”. For the 2nd GET it returns “404 Not Found”

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

Fri, 23 Sep 2022 05:59:01 GMT

```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Prefer: safe\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
Accept: text/html,application/xhtml+xml,application/xml
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "80-5e951dfebb45b"\r\n
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n
\r\n
```

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

From server: 293 + 538 = 831 bytes

Sent to server : 632 + 493 = 1125 bytes

1.7. 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.

I assume there is one but I can't find it. I thought I saw php in there, however I am now unable to find it.

2. The HTTP CONDITIONAL GET/response interaction:

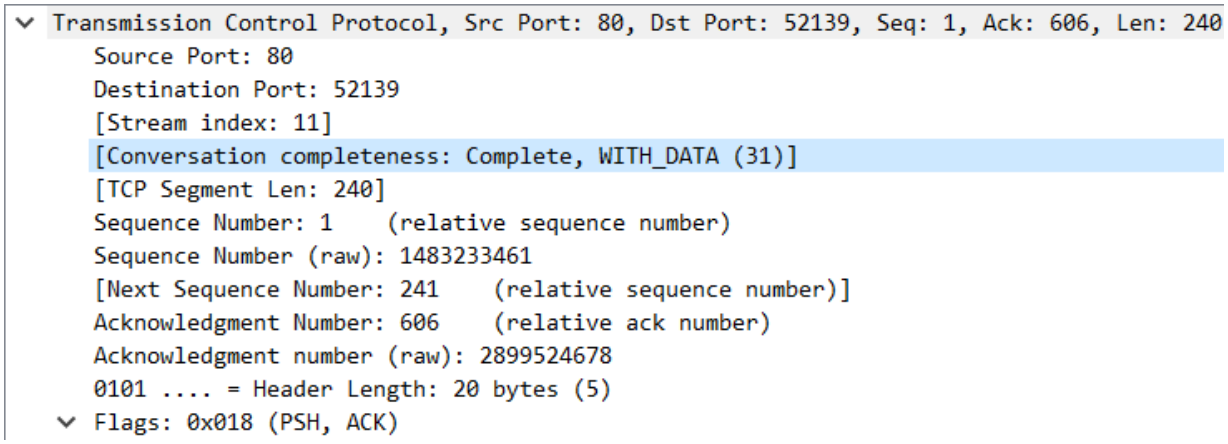
Q8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

Yes, highlighted in green here:

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Prefer: safe\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/105.0.0.0 Safari/537.36 Edg/105.0.1343.42\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;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5e951dfebac8b"\r\n
If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\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: 54]
```

Q9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, the TCP response analysis states that the conversation is complete. It is notable that it only shows as complete if the cache is empty in the browser before loading the page.



Q10) 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?

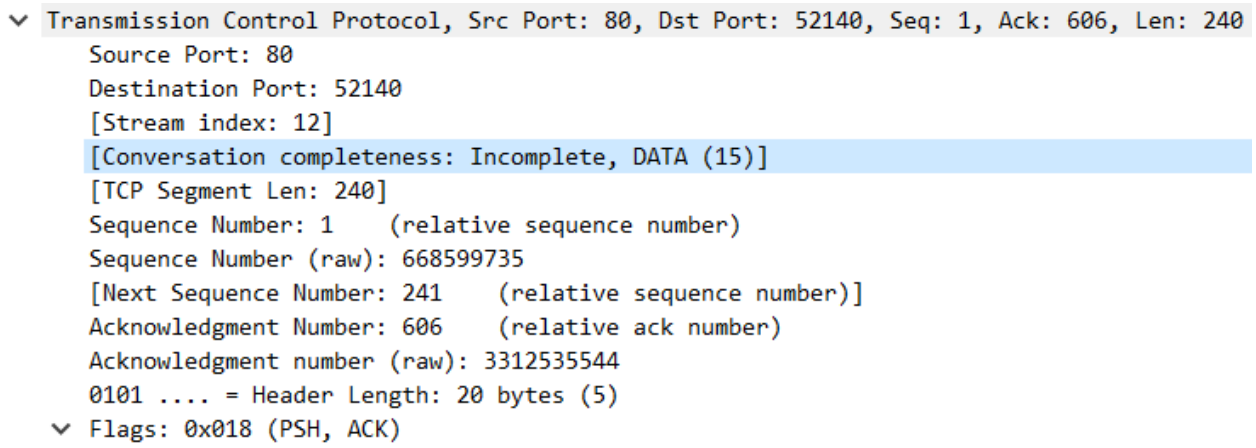
Yes. It shows the following:

If-Modified-Since: Fri, 23 Sep 2022 05:59:01 GMT\r\n

\r\n

Q11) 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.

The HTTP status code returned is "304 Not Modified". The server did not explicitly return the contents, it appears to have updated the contents (based on the cached data):



3. Retrieving Long Documents:

Q12) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

No.	Time	Source	Destination	Protocol	Length	Info
232	10:27:21.222086	10.5.139.22	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
245	10:27:21.282464	128.119.245.12	10.5.139.22	HTTP	757	HTTP/1.1 200 OK (text/html)
257	10:27:21.366654	10.5.139.22	128.119.245.12	HTTP	493	GET /favicon.ico HTTP/1.1
260	10:27:21.412463	128.119.245.12	10.5.139.22	HTTP	538	HTTP/1.1 404 Not Found (text/html)

My browser sent **2** HTTP GET request messages. The packet number of the trace containing the GET for the Bill of Rights was 232 (the first one).

Q13) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

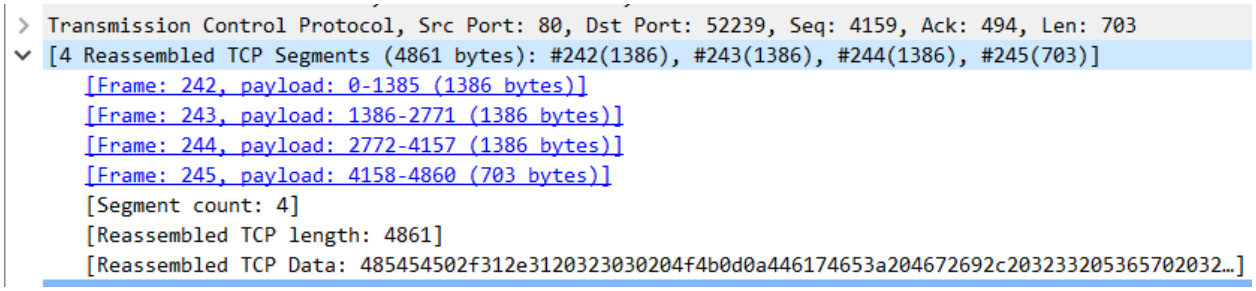
Packet number 245 contains the response and the status code.

Q14) What is the status code and phrase in the response?

The status code is 200 and the phrase is "OK".

Q15) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Four TCP segments were returned containing data for the HTTP response and the Bill of Rights text.



4. HTML Documents with Embedded Objects:

Q16) How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Three total HTTP GET requests were sent.

The first two went to gaia.cs.umass.edu (ip: 128.119.245.12) and the third went to kurose.cslash.net (ip: 178.79.137.164)

Q17) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Wireshark is able to make a flow diagram from your data (shown below). According to this flow diagram the first GETs were parallel, however, the first and second image were not downloaded in parallel because they are from two different hosts. The time is also slightly different.

5. HTTP Authentication:

No.	Time	Source	Destination	Protocol	Length	Info
59	10:45:17.644217	10.5.139.22	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
66	10:45:17.692151	128.119.245.12	10.5.139.22	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
10847	10:45:38.224262	10.5.139.22	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
10854	10:45:38.271155	128.119.245.12	10.5.139.22	HTTP	544	HTTP/1.1 200 OK (text/html)

Q18) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

The server's response to the initial GET message is status code 401 "Unauthorized".

```
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
    Response Version: HTTP/1.1
    Status Code: 401
    [Status Code Description: Unauthorized]
    Response Phrase: Unauthorized
  Date: Fri, 23 Sep 2022 16:45:17 GMT\r\n
```

Q19) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The second time two new fields are included: Cache-Control and Authorization.

```
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
  Cache-Control: max-age=0\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Prefer: safe\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/105.0.0.0 Safari/537.36 Edg/105.0.1343.50\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;q=0.9\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  \r\n
```

The username and password are encoded in Base64.

Using this online tool https://www.motobit.com/util/base64-decoder-encoder.asp one can see that d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms= in base64 is equal to wireshark-students:network in regular text.