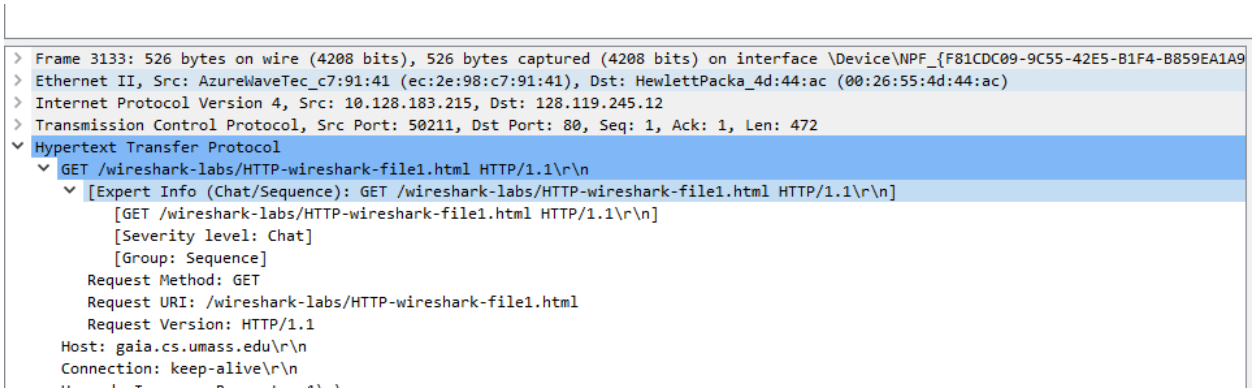
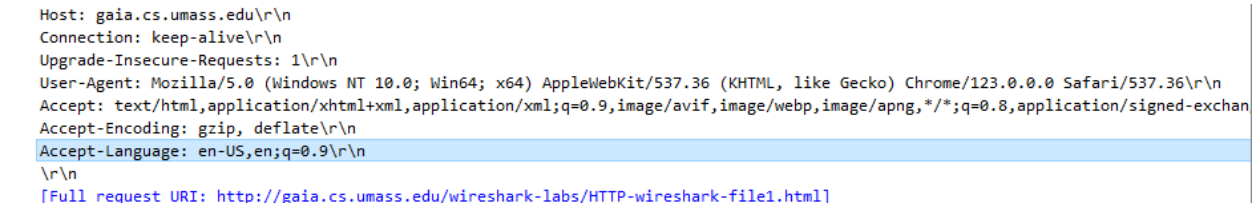
Lab1 Report

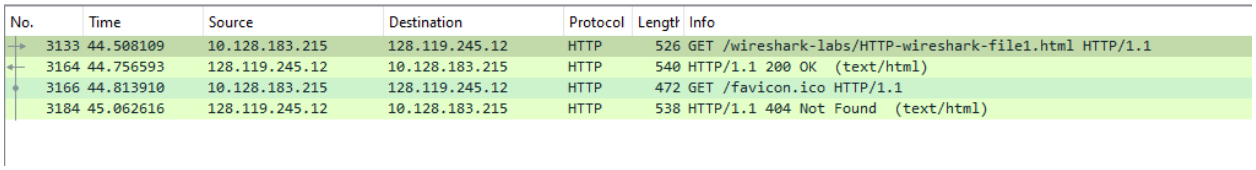
1. The Basic HTTP GET/response interaction
   a. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running ?
   Answer: My browser and the server running HTTP 1.1 version



   b. What language (if any) does your browser indicate that it can accept to the server?
   Answer:

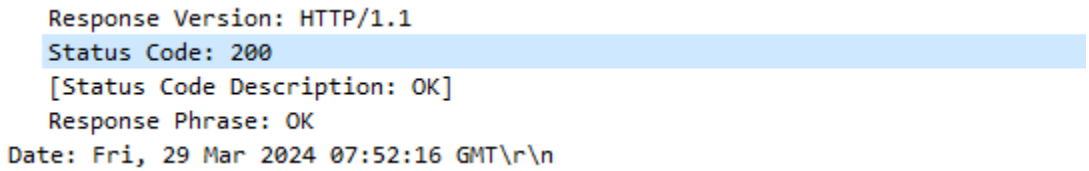


   c. What is the IP address of your computer? Of gaia.cs.umass.edu server ?
   Answer: My computer IP address is: 10.128.183.215

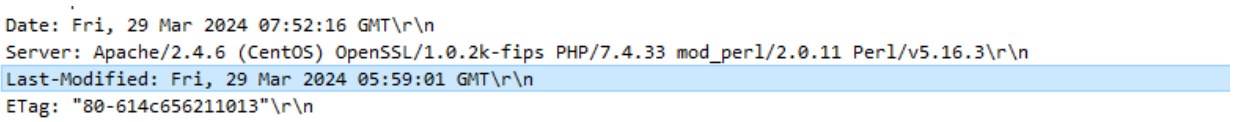


No.	Time	Source	Destination	Protocol	Length	Info
3133	44.508109	10.128.183.215	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
3164	44.756593	128.119.245.12	10.128.183.215	HTTP	540	HTTP/1.1 200 OK (text/html)
3166	44.813910	10.128.183.215	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
3184	45.062616	128.119.245.12	10.128.183.215	HTTP	538	HTTP/1.1 404 Not Found (text/html)

   d. What is the status code returned from server to your browser ?
   Answer:



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



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

Answer: 128 Bytes

```
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
```

g. 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.
Answer: I don't see any data that is mentioned:

```
Content-Length: 128\r\n
   [Content length: 128]
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 1/2]
[Time since request: 0.248484000 seconds]
[Request in frame: 3133]
[Next request in frame: 3166]
[Next response in frame: 3184]
```

2. The HTTP CONDITIONAL GET/ response interaction.
   a. 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?
   Answer: Yes

```
If-None-Match: "173-614c656210843"\r\n
If-Modified-Since: Fri, 29 Mar 2024 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]
```

   b. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   Answer: The server explicitly return the contents of the file due to the HTTP response 1/1

```
\r\n
[HTTP response 1/1]
[Time since request: 0.243881000 seconds]
[Request in frame: 807]
```

   c. 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
   Answer: Yes

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-614c656210843"\r\n
If-Modified-Since: Fri, 29 Mar 2024 05:59:01 GMT\r\n
\r\n
```

   d. 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.

Answer: The server explicitly return the contents of the file due to the HTTP response 1/1

```
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Fri, 29 Mar 2024 08:25:16 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-614c656210843"\r\n
\r\n
[HTTP response 1/1]
```

3. Retrieving Long Documents
   a. 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?
   Answer: 1. The packet is 38599

```
38599 199.852432    10.128.183.215    128.119.245.12    HTTP    639 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
38625 200.099664    128.119.245.12    10.128.183.215    HTTP    295 HTTP/1.1 304 Not Modified
```

   b. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
   Answer: 38599

```
38599 199.852432    10.128.183.215    128.119.245.12    HTTP    639 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
38625 200.099664    128.119.245.12    10.128.183.215    HTTP    295 HTTP/1.1 304 Not Modified
```

   c. What is the status code and phrase in the response?
   Answer:

```
        [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
    Response Phrase: Not Modified
Date: Fri, 29 Mar 2024 08:43:12 GMT\r\n
```

   d. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?
   Answer: 585

```
▾ [Conversation completeness: Complete, WITH_DATA (31)]
    ..0. .... = RST: Absent
    ...1 .... = FIN: Present
    .... 1... = Data: Present
    .... .1.. = ACK: Present
    .... ..1. = SYN-ACK: Present
    .... ...1 = SYN: Present
    [Completeness Flags: ·FDASS]
[TCP Segment Len: 585]
Sequence Number: 1    (relative sequence number)
```

4. HTML Documents with Embedded Objects
   a. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Answer: 4. The address is shown below

No.	Time	Source	Destination	Protocol	Length	Info
409	4.381820	10.128.183.215	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
467	5.165627	128.119.245.12	10.128.183.215	HTTP	1355	HTTP/1.1 200 OK (text/html)
479	5.226528	10.128.183.215	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
500	5.476420	128.119.245.12	10.128.183.215	HTTP	761	HTTP/1.1 200 OK (PNG)
505	5.497401	10.128.183.215	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
528	5.709128	178.79.137.164	10.128.183.215	HTTP	225	HTTP/1.1 301 Moved Permanently
590	6.335149	10.128.183.215	113.171.231.11	HTTP	333	GET /roots/dstrootcax3.p7c HTTP/1.1
596	6.372228	113.171.231.11	10.128.183.215	HTTP	1460	HTTP/1.1 200 OK

b. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain
Answer: The browser download serially, because when the response status of the first one is OK, the browser start download the 2nd .

500	5.476420	128.119.245.12	10.128.183.215	HTTP	761 HTTP/1.1 200 OK (PNG)
505	5.497401	10.128.183.215	178.79.137.164	HTTP	439 GET /8E_cover_small.jpg HTTP/1.1
528	5.709128	178.79.137.164	10.128.183.215	HTTP	225 HTTP/1.1 301 Moved Permanently

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

```
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Connection: close\r\n
```

   b. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
   Answer: It update the Authentication part

```
Authorization: Basic YXNkYXM6YXNkYXNkYWRz\r\n
   Credentials: asdas:asdasdads
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 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-exchan
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\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: 1468]
```