Assignment 3

Part 1:-

1)
My browser is running HTTP/1.1
The server is running HTTP/1.1

2)
Accept-Language: en-US,en;q=0.5
Hence, the language is English(US).

3)
My computer ip is **10.196.8.81**
gaia.cs.umass.edu server's IP is **128.119.245.12**

4)
Status code: **200** is returned from the server to my computer.

5)
The HTML file which I retreived was last modified on Tue, 16 Jan 2024 06:59:02 GMT

6)
128 bytes of content are being returned to your browser

7)
The following are not in the packet listing window but are in the package content window

```
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.303323000 seconds]
[Request in frame: 386]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

Part 2:-

1)
No, I did not see "IF-MODIFIED-SINCE" line in the HTTP GET.

2)
Yes, initially the server did explicitly return the contents of the file as follows:

```
∨ Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

3)
Yes, I see an "IF-MODIFIED-SINCE:" line in the HTTP GET.
Tue, 16 Jan 2024 06:59:02 GMT\r\n follows the respective header.

4)
Status code **304** status code is returned from the server in response to this second HTTP GET.
No, the server did not explicitly return the contents of the file since the IF-MODIFIED-SINCE time is same as the time for last modified in the previous request. Since, nothing was modified in the previous sent file, no new content was received.

Part 3:-


```
53 11:48:45.460373 10.240.23.79      128.119.245.12   HTTP   356 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.0
54 11:48:45.742399 128.119.245.12    10.240.23.79     TCP    54 80 → 60997 [ACK] Seq=1 Ack=303 Win=30336 Len=0
55 11:48:45.742402 128.119.245.12    10.240.23.79     TCP    1304 80 → 60997 [ACK] Seq=1 Ack=303 Win=30336 Len=1250 [TCP segment of a reassembled
56 11:48:45.742403 128.119.245.12    10.240.23.79     TCP    1304 80 → 60997 [ACK] Seq=1251 Ack=303 Win=30336 Len=1250 [TCP segment of a reassembl
57 11:48:45.742405 128.119.245.12    10.240.23.79     TCP    1304 80 → 60997 [ACK] Seq=2501 Ack=303 Win=30336 Len=1250 [TCP segment of a reassembl
58 11:48:45.742407 128.119.245.12    10.240.23.79     HTTP   1128 HTTP/1.1 200 OK  (text/html)
```

1)
The browser sent 1 HTTP GET request message. The associated packet number is **53**.

2)
Packet number **58** contains the status code and phrase associated with the response to the request.

3)
Status code: **200**
Response Phrase: **OK**

4)


```
[4 Reassembled TCP Segments (4824 bytes): #55(1250), #56(1250), #57(1250), #58(1074)]
    [Frame: 55, payload: 0-1249 (1250 bytes)]
    [Frame: 56, payload: 1250-2499 (1250 bytes)]
    [Frame: 57, payload: 2500-3749 (1250 bytes)]
    [Frame: 58, payload: 3750-4823 (1074 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4824]
    [Reassembled TCP Data [truncated]: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c203231204a616e2032303232030363a31383a343620474d540d0a5365727665723a204170616368652f...
```

4 TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights with the data distribution as follows: **1250 bytes** in the first three and **1074 bytes** in the last one sending a total of **4824 bytes**.

Part 4:-

1)
The browser sent 3 HTTP GET response to the source.

The first one was sent to **128.119.245.12**
The second one was sent to **128.119.245.12**
The third one was sent to **178.79.137.164**

2)
The images were downloaded serially. We can tell this by looking at the time log of each of the packets as shown in the below screenshot.

```
363 11:39:14.926894 10.240.23.79      128.119.245.12  HTTP      350 GET /pearson.png HTTP/1.1
374 11:39:15.184440 128.119.245.12    10.240.23.79    HTTP     1166 HTTP/1.1 200 OK  (PNG)
392 11:39:16.046603 10.240.23.79      178.79.137.164  HTTP      369 GET /8E_cover_small.jpg HTTP/1.1
396 11:39:16.206296 178.79.137.164    10.240.23.79    HTTP      237 HTTP/1.1 301 Moved Permanently
```

There was a time difference of nearly 1.02 seconds between the downloading of these two images.

Part 5:-

 1)
The server's response for the first HTTP GET request sent was
status code: **401** message: **Unauthorized** message

```
123 11:46:13.320487 10.240.23.79      128.119.245.12  HTTP      372 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.0
126 11:46:13.578126 128.119.245.12    10.240.23.79    HTTP      734 HTTP/1.1 401 Unauthorized  (text/html)
```

2)
When the browser sends the GET request for the second time, there is an extra field of Authorization: Basic header which took in our login credentials such as username and password.

```
✓ Hypertext Transfer Protocol
  ✓ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.0\r\n
      > [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.0\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
        Request Version: HTTP/1.0
    Host: gaia.cs.umass.edu\r\n
    Accept: text/html, text/plain, text/sgml, text/css, application/xhtml+xml, */*;q=0.01\r\n
    Accept-Encoding: gzip, compress, bzip2\r\n
    Accept-Language: en\r\n
    User-Agent: Lynx/2.8.9rel.1 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/3.2.0\r\n
  > Authorization: Basic d2lyZXNoYXJrOnddWRlbnRzOm5ldHdvcms=\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: 310]
```