Lab 9
Haq Nawaz

<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
TASK 1 :

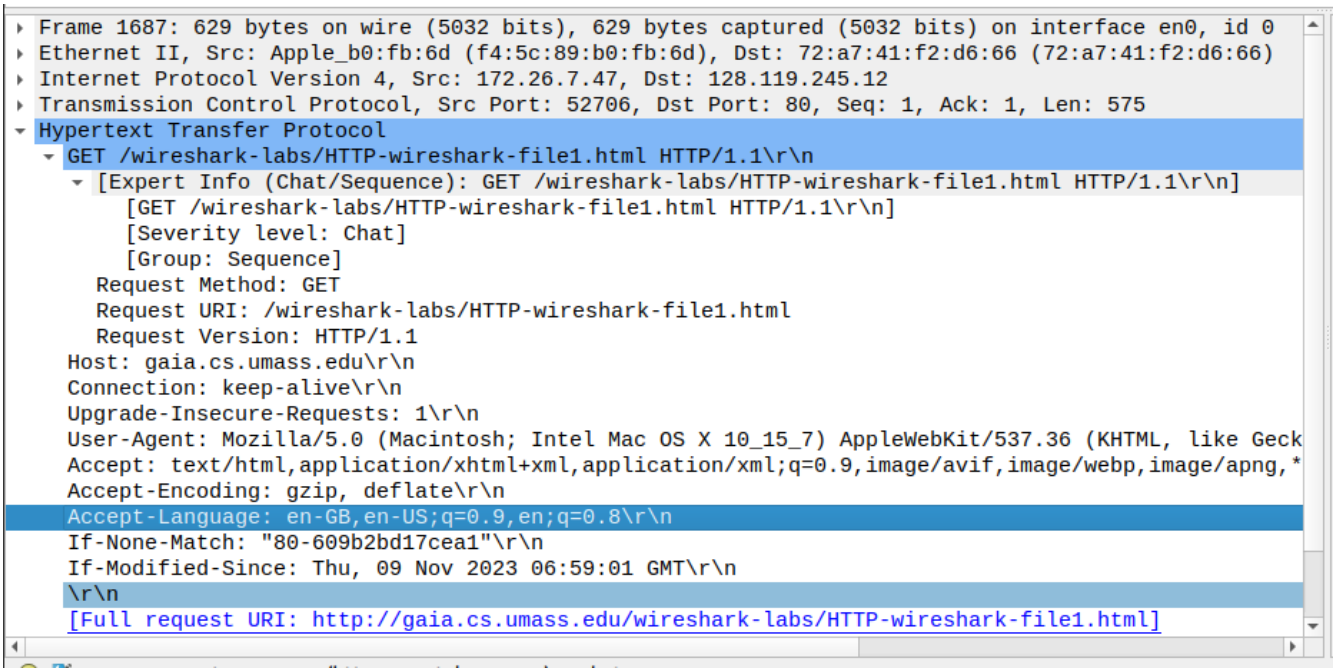
1 : Is your browser running HTTP version 1.0, 1.1, or 2?

```
> Frame 1687: 629 bytes on wire (5032 bits), 629 bytes captured (5032 bits) on interface en0, id 0
> Ethernet II, Src: Apple_b0:fb:6d (f4:5c:89:b0:fb:6d), Dst: 72:a7:41:f2:d6:66 (72:a7:41:f2:d6:66)
> Internet Protocol Version 4, Src: 172.26.7.47, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52706, Dst Port: 80, Seq: 1, Ack: 1, Len: 575
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Geck
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    If-None-Match: "80-609b2bd17cea1"\r\n
    If-Modified-Since: Thu, 09 Nov 2023 06:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

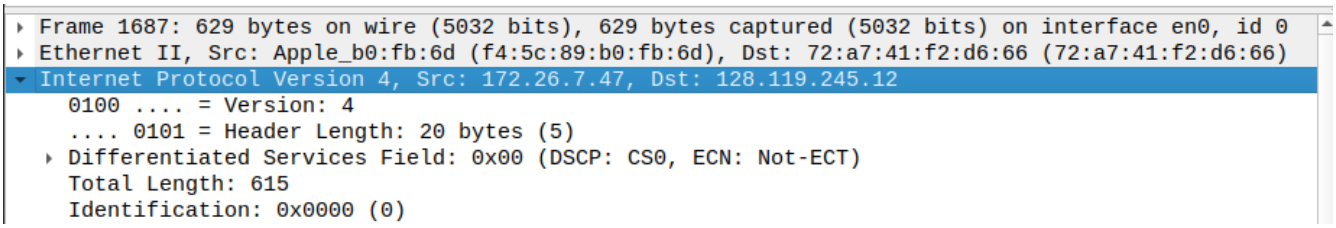
2 : What version of HTTP is the server running?

```
> Frame 1695: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id 0
> Ethernet II, Src: 72:a7:41:f2:d6:66 (72:a7:41:f2:d6:66), Dst: Apple_b0:fb:6d (f4:5c:89:b0:fb:6d)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.26.7.47
> Transmission Control Protocol, Src Port: 80, Dst Port: 52706, Seq: 1, Ack: 576, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Thu, 16 Nov 2023 04:08:28 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
    Last-Modified: Wed, 15 Nov 2023 06:59:01 GMT\r\n
    ETag: "80-60a2b70292f2b"\r\n
    Accept-Ranges: bytes\r\n
  > 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 1/2]
```

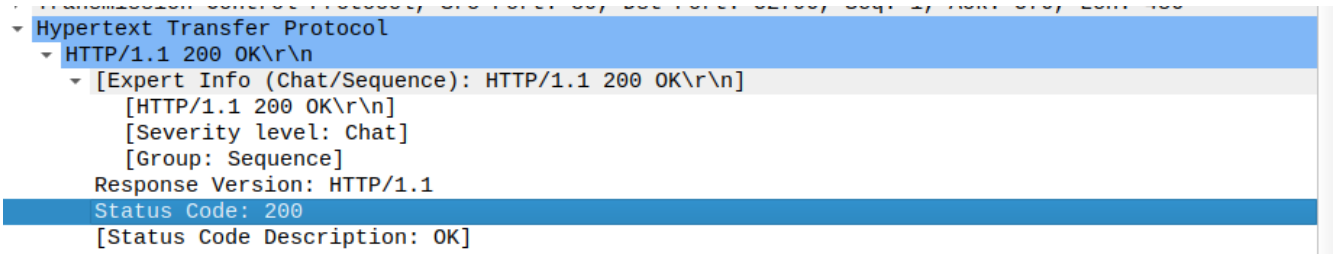
3 : What languages (if any) does your browser indicate that it can accept to the server?



4 : What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?



5 : What is the status code returned from the server to your browser?



6: When was the HTML file that you are retrieving last modified at the server?

```
Last-Modified: Wed, 15 Nov 2023 06:59:01 GMT\r\n
ETag: "80-60a2b70292f2b"\r\n
Accept-Ranges: bytes\r\n
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 1/2]
```

7 : How many bytes of content are being returned to your browser?

```
Accept-Ranges: bytes\r\n
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 1/2]
[Time since request: 0.232667000 seconds]
[Request in frame: 1687]
```

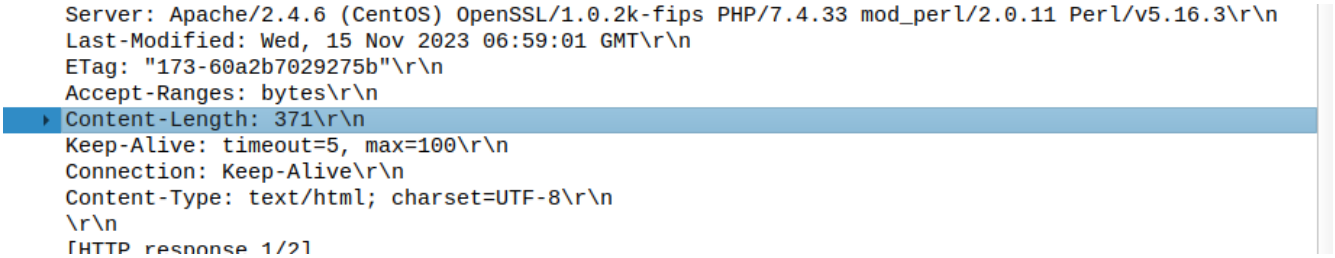
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>

TASK 2 :

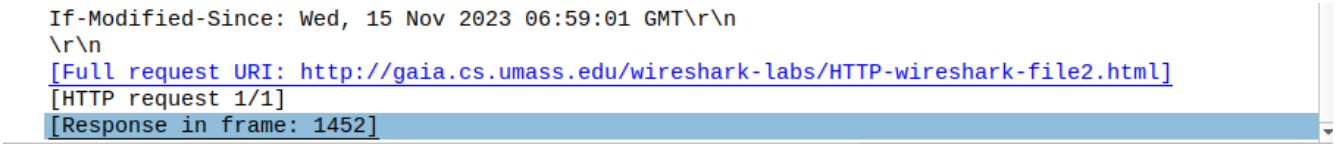
1. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Geck
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
If-None-Match: "173-609b2bd17c6d1"\r\n
If-Modified-Since: Thu, 09 Nov 2023 06:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

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



3. 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?

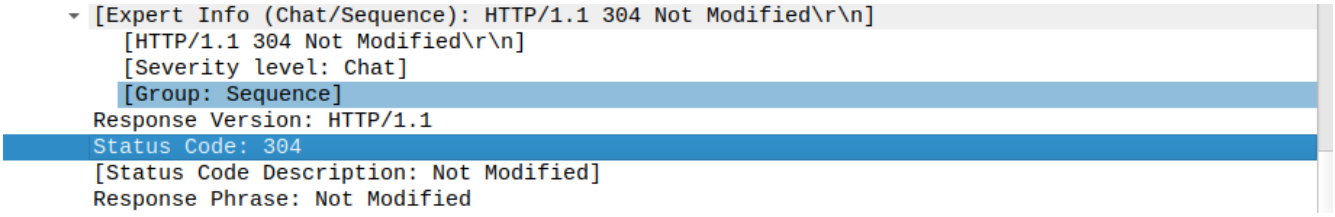


1/1 means this is the first request in persistent connection

1452 means return that much frames

URI means uniform resource identifier that was included in the first http request. This includes the scheme http, host name and path to the resource.

4. 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.



NOTE : An HTTP 304 not modified status code means that the website you're requesting hasn't been updated since the last time you accessed