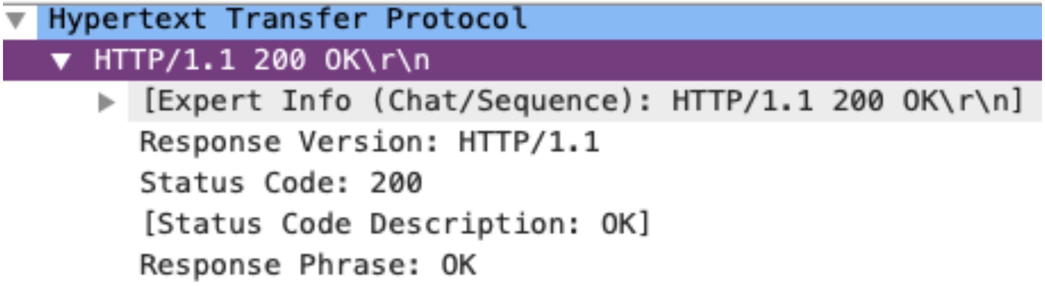
z5147986
Lab2

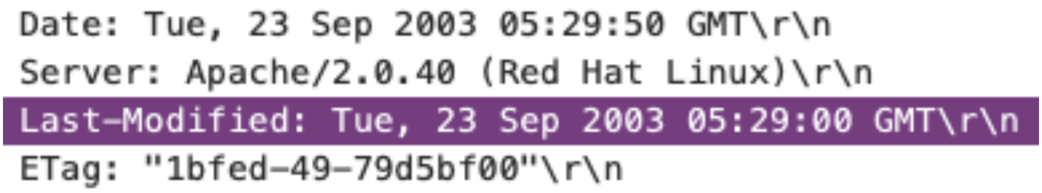
Exercise 3: Using Wireshark to understand basic HTTP request/ response messages

3.1
What is the status code and phrase returned from the server to the client browser?



```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

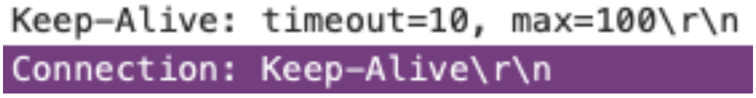
3.2
When was the HTML file that the browser is retrieving last modified at the server? Does the response also contain a DATE header? How are these two fields different?



```
Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
Server: Apache/2.0.40 (Red Hat Linux)\r\n
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
ETag: "1bfed-49-79d5bf00"\r\n
```

DATE header contains the day, date and time at which the message was created.
LAST-MODIFIED header validator is used to determine if resource received or stored is the same, and it contains a similar format as the DATE header.

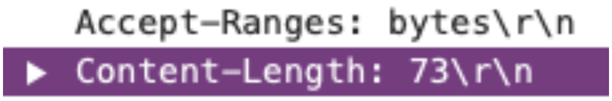
3.3
Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?



```
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
```

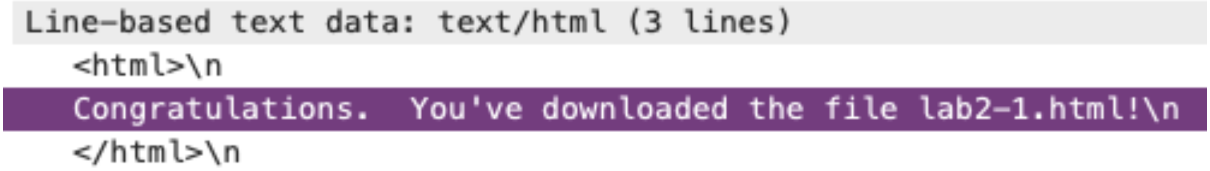
The connection established is persistent, since the connection is being keep-alive also it is the default on HTTP/1.1 requests to have a persistent connection which indicates that the client wants to keep the connection open.

3.4
How many bytes of content are being returned to the browser?



```
  Accept-Ranges: bytes\r\n
▶ Content-Length: 73\r\n
```

3.5
What is the data contained inside the HTTP response packet?



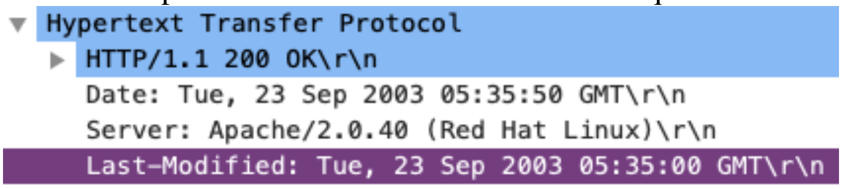
```
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations.  You've downloaded the file lab2-1.html!\n
    </html>\n
```

z5147986
Lab2

Exercise 4

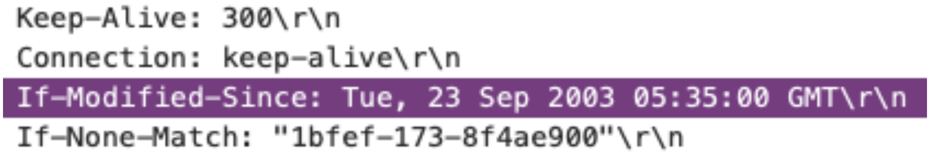
4.1
Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?
The first GET request does not contain an IF-MODIFIED-SINCE header.

4.2
Does the response indicate the last time that the requested file was modified?



```
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
```

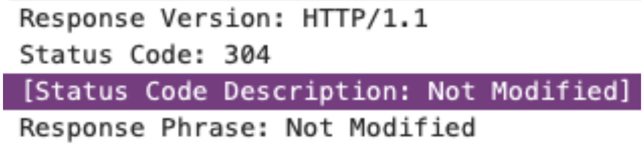
4.3
Now inspect the contents of the second HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in the HTTP GET? If so, what information is contained in these header lines?



```
Keep-Alive: 300\r\n
Connection: keep-alive\r\n
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
If-None-Match: "1bfef-173-8f4ae900"\r\n
```

IF-MODIFIED-SINCE contains day, date and time, contains similar syntax as the DATE and LAST-MODIFIED header
IF-NONE-MATCH contains Etag value(s)

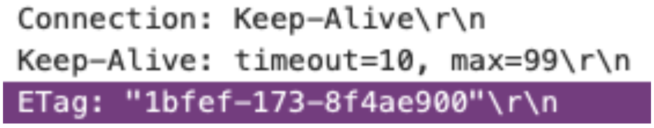
4.4
What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.



```
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
```

The server did not explicitly return the contents of the file. It means that when a cached copy is up to date with the server by checking the request Etag and the server’s Etag value for the requested file are both the same, thus server sends back a 304.

4.5
What is the value of the Etag field in the 2nd response message and how it is used? Has this value changed since the 1st response message was received?



```
Connection: Keep-Alive\r\n
Keep-Alive: timeout=10, max=99\r\n
ETag: "1bfef-173-8f4ae900"\r\n
```

The Etag value has not been changed. As mentioned in 4.4, it is used to check if there is any change in the server’s Etag value, if the Etag values are not the same, the browser and the server will the communicate efficiently on what is needed to be downloaded again and what can be still delivered from cache.