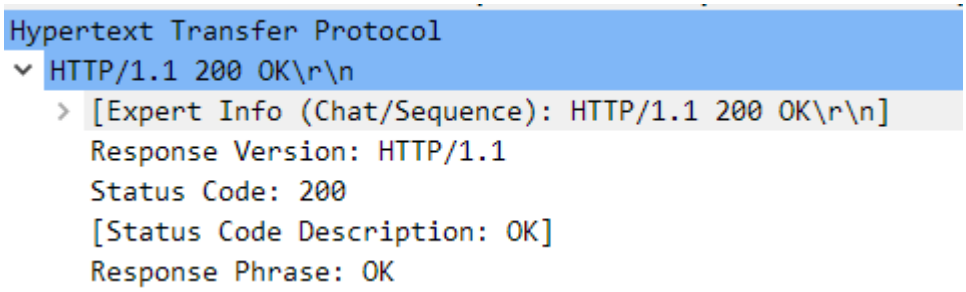
Exercise 3: Using Wireshark to understand basic HTTP request/response messages

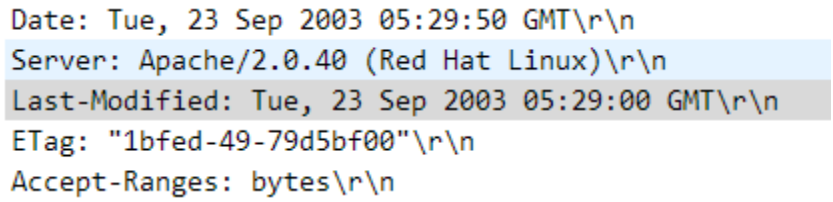
Q1

The status code is 200, Response Phase is OK.



Q2

The last modified date is Tue,23 Sep 2003 05:29:00. The response also contains a DATE Header. Date is the time point that the server makes a response. Last-Modified time is the last time that the file is modified.



Q3

The connection is persistent because the status of connection is Keep-Alive.

```
Keep-Alive: timeout=10, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=ISO-8859-1\r\n
```

Q4

The payload length is 73 and the total length of the response is 439.

```
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
Accept-Ranges: bytes\r\n
> Content-Length: 73\r\n
Keep-Alive: timeout=10, max=100\r\n
```

```
555 GET /ethereal-labs/lab2-1.html HTTP/1.1
439 HTTP/1.1 200 OK  (text/html)
```

Q5

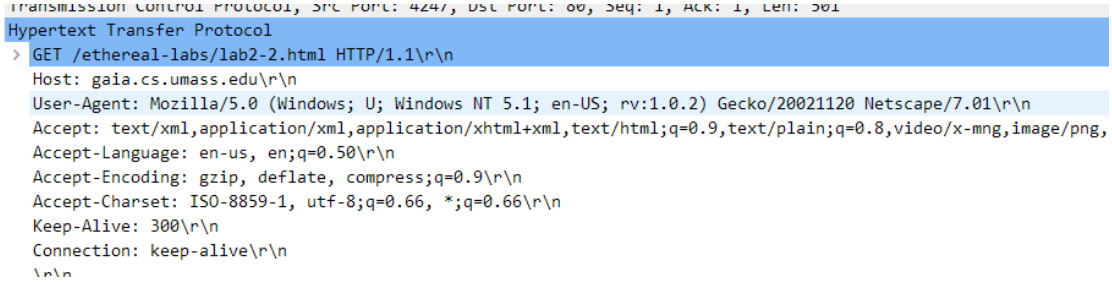
The data is a sentence.

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

Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

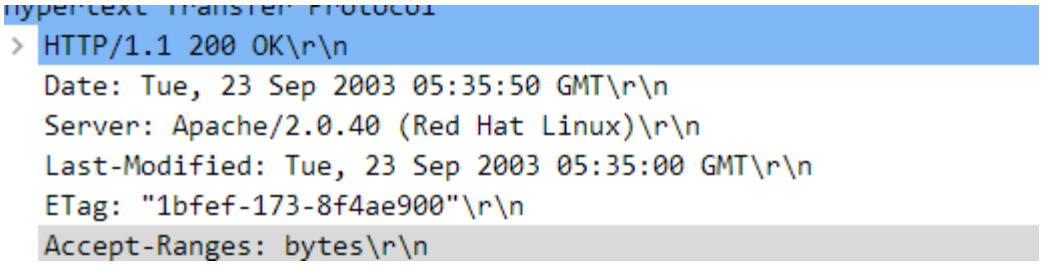
Q1

The first HTTP GET does not have 'IF-MODIFIED-SINCE' line.



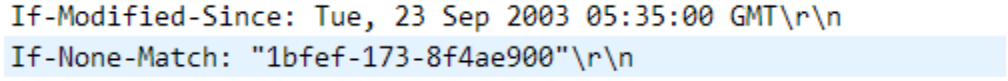
Q2

Yes, the response indicates the last modified time



Q3

The If-Modified-Since time is the copy of Last-Modified time.
If-None-Match is the copy of E-Tag from last response.



Q4

The status code is 304, the Phase is Not Modified. The server does not return the contents of the file because the server check the Last-Modified time and it is same, so the server decides not to return any contents of the file.

```
243 HTTP/1.1 304 Not Modified
```

Q5

The E-tag value shows below, and the value is not changed.

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

Exercise 5: Ping Client

Sample output: