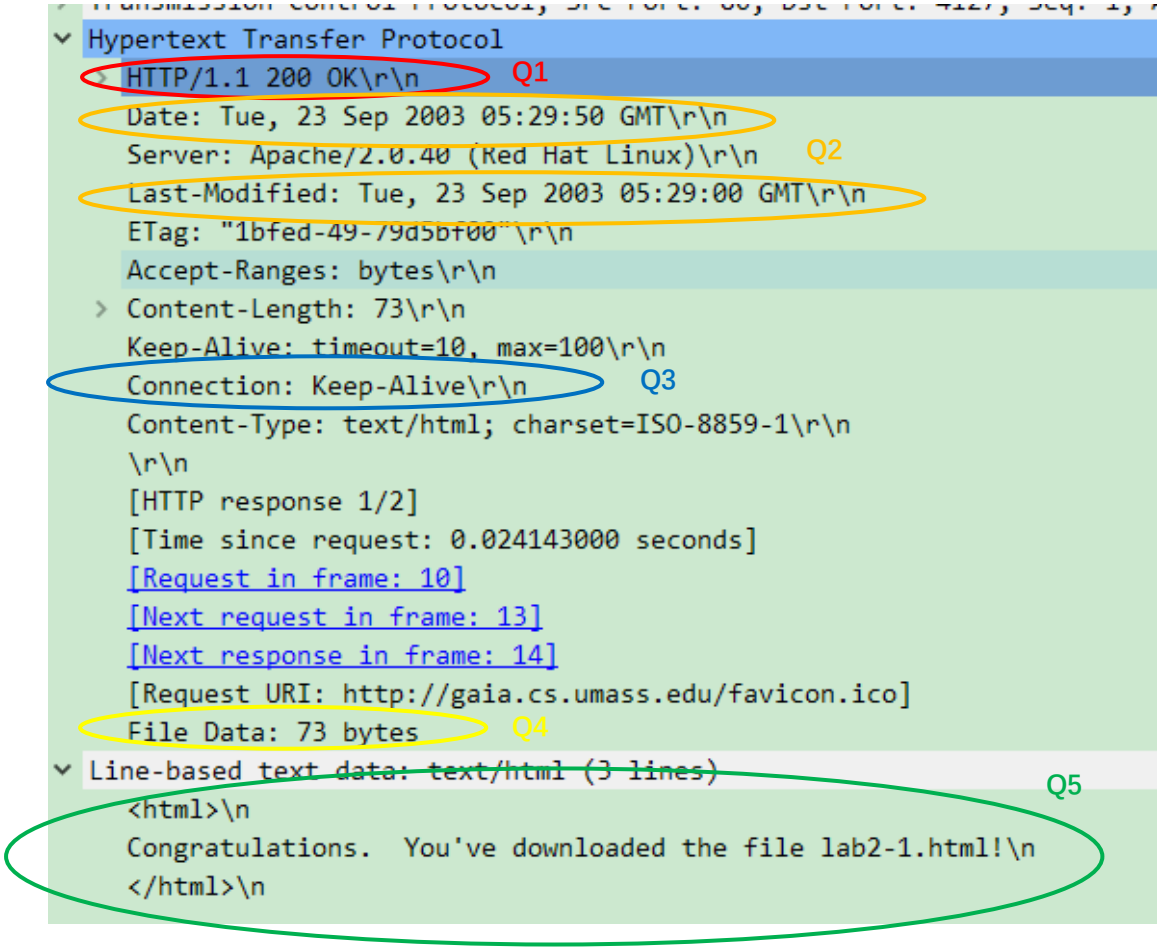
Exercise 3: Using Wireshark to understand basic HTTP request/response messages



Q1:

The status code is 200 and phrase is "OK".

Q2:

The last modification is made on (Tuesday, 23rd September 2003, 05:29:00 GMT). The response also has the Date header, which contains information about the time that this message was generated by the server. By comparing these two times, it seems that this file is modified just 50 sec before been sent.

Q3:

As the connection is "Keep-Alive", the client and server are configured to use persistent HTTP connections.

Q4:

As shown in the "File Data", 73 bytes have been returned to the client.

Q5:

The content of the return file is an 3-lined HTML file:

```
<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

```
Hypertext Transfer Protocol
  GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.
  Accept-Language: en-us, en;q=0.50\r\n
  Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
  Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
  Keep-Alive: 300\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
  [HTTP request 1/2]
  [Response in frame: 10]
  [Next request in frame: 14]
```

Q1:

No, in the request, there is no header named “IF-MODIFIED-SINCE”.

```
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
  ETag: "1bfef-173-8f4ae900"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
```

Q2

Q2:

From the content of response, this file was last modified on (Tuesday, 23rd September, 2003, 05:35 GMT).

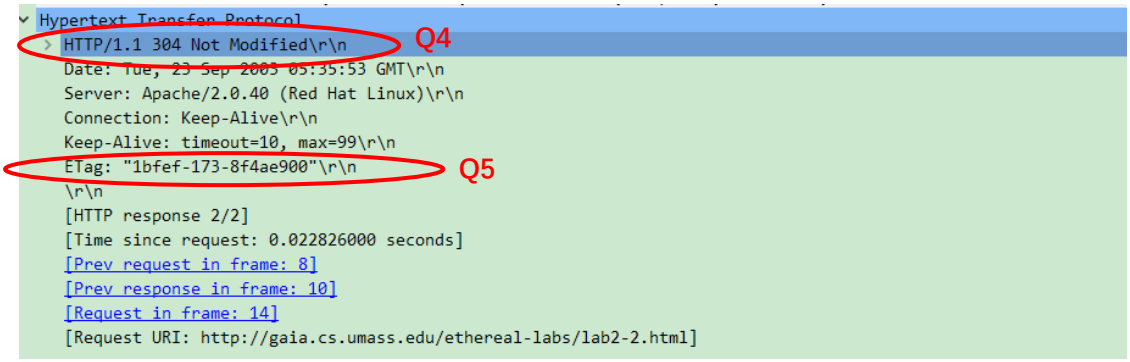
```
Hypertext Transfer Protocol
  GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
  Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.
  Accept-Language: en-us, en;q=0.50\r\n
  Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
  Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
  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
  Cache-Control: max-age=0\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
  [HTTP request 2/2]
  [Prev request in frame: 8]
  [Response in frame: 15]
```

Q3

Q3:

Yes, both “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” are contained in the second GET request.

The IF-MODIFIED-SINCE indicates the modified time of the local cached file, which is exactly the same time of “LAST-MODIFIED” time in the first response. The IF-NONE-MATCH is the previous ETag, it was sent for the server to check cache validation.



Q4:

The status code is 304 and phrase is “Not Modified”.

No, it didn’t. This message indicated that the server hasn’t make modification since IF-MODIFIED-SINCE time. So, the server has no need to respond. The local cached file still can be used.

Q5:

The ETag value of the second response is “1bfef-173-8f4ae900". Comparing to the content in first response, the ETag hasn’t be changed. This shows that local cached version of this file is still valid, as ETag is a mechanism for cache validation.