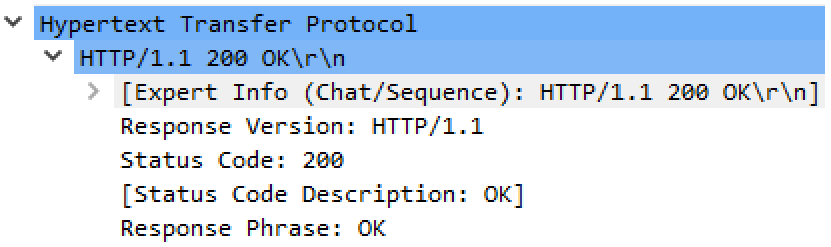
# Lab Exercise 3

## Exercise 3: Using Wireshark to understand basic HTTP request/response messages (marked, include in your report)

**Question 1: What is the status code and phrase returned from the server to the client browser?**

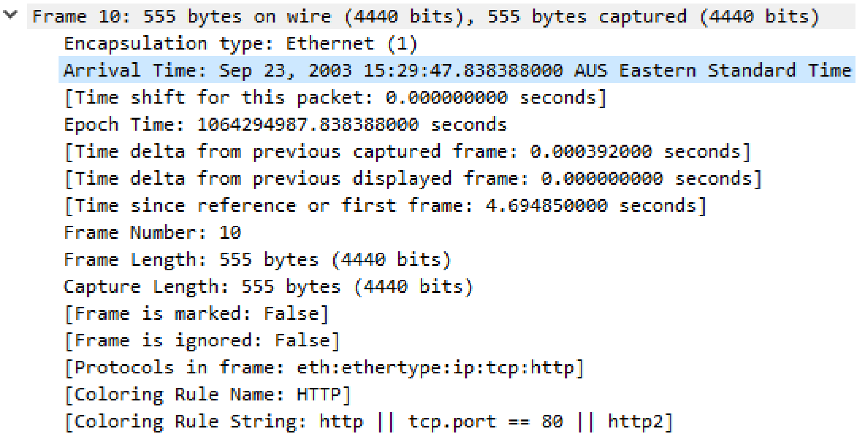


```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

*Figure 1. Screenshot of trace 1*

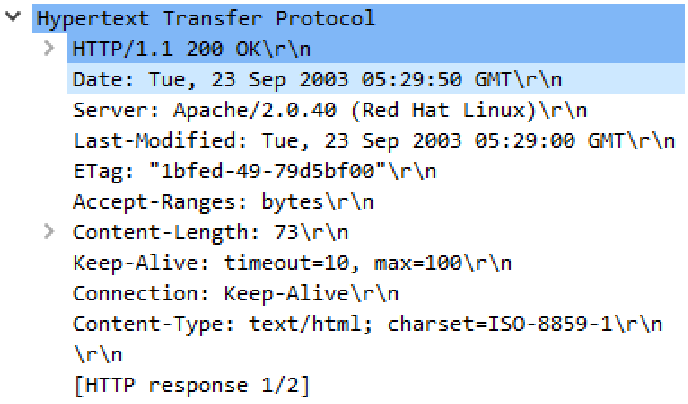
The status code and phrase used in this request is “200 OK”.

**Question 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?**



```
Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 23, 2003 15:29:47.838388000 AUS Eastern Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1064294987.838388000 seconds
  [Time delta from previous captured frame: 0.000392000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 4.694850000 seconds]
  Frame Number: 10
  Frame Length: 555 bytes (4440 bits)
  Capture Length: 555 bytes (4440 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

*Figure 2. HTTP Request Time*

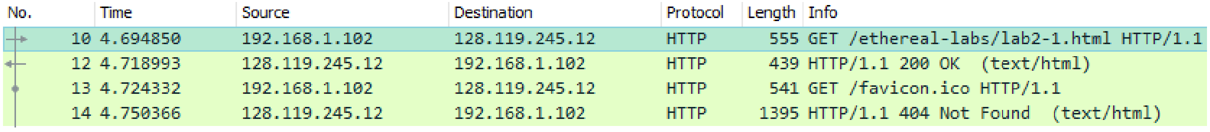


```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n
  Server: Apache/2.0.40 (Red Hat Linux)\r\n
  Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
  ETag: "1bfed-49-79d5bf00"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 73\r\n
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
  \r\n
  [HTTP response 1/2]
```

*Figure 3. HTTP Response Time*

The HTML file that the browser is retrieving was last modified at the server on the 23 Sept 2003 at 15:29:47. The Response also contains a Date header in figure 3. The two fields are different as the request is in Eastern Standard Time and the response is Greenwich Mean Time.

**Question 3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?**

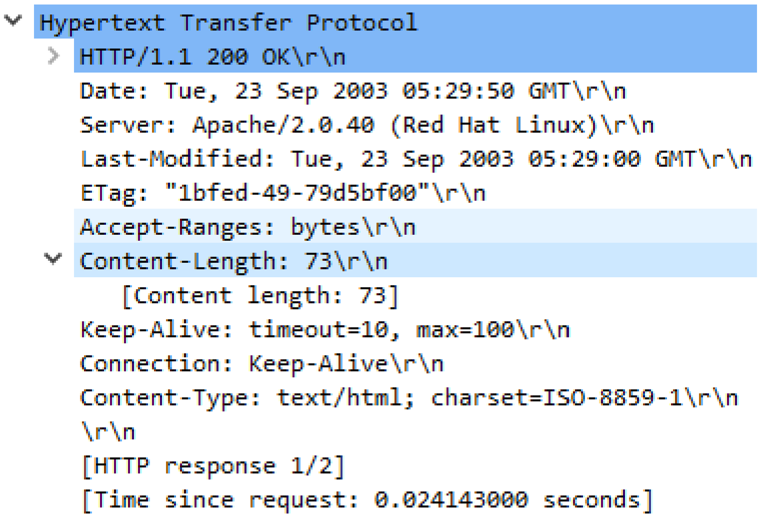


| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 10 | 4.694850 | 192.168.1.102 | 128.119.245.12 | HTTP | 555 | GET /ethereal-labs/lab2-1.html HTTP/1.1 |
| 12 | 4.718993 | 128.119.245.12 | 192.168.1.102 | HTTP | 439 | HTTP/1.1 200 OK  (text/html) |
| 13 | 4.724332 | 192.168.1.102 | 128.119.245.12 | HTTP | 541 | GET /favicon.ico HTTP/1.1 |
| 14 | 4.750366 | 128.119.245.12 | 192.168.1.102 | HTTP | 1395 | HTTP/1.1 404 Not Found  (text/html) |

*Figure 4. Wireshark Screenshot*

The connection established between the browser and the server is persistent. You can tell this because it has the connection type “1.1” in the first row of figure 4.

**Question 4: How many bytes of content are being returned to the browser?**



```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  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
  Accept-Ranges: bytes\r\n
  Content-Length: 73\r\n
     [Content length: 73]
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.024143000 seconds]
```

*Figure 5. Bytes of content being returned*

There are 73 bytes of content being returned to the browser as per the “Content-Length” field.

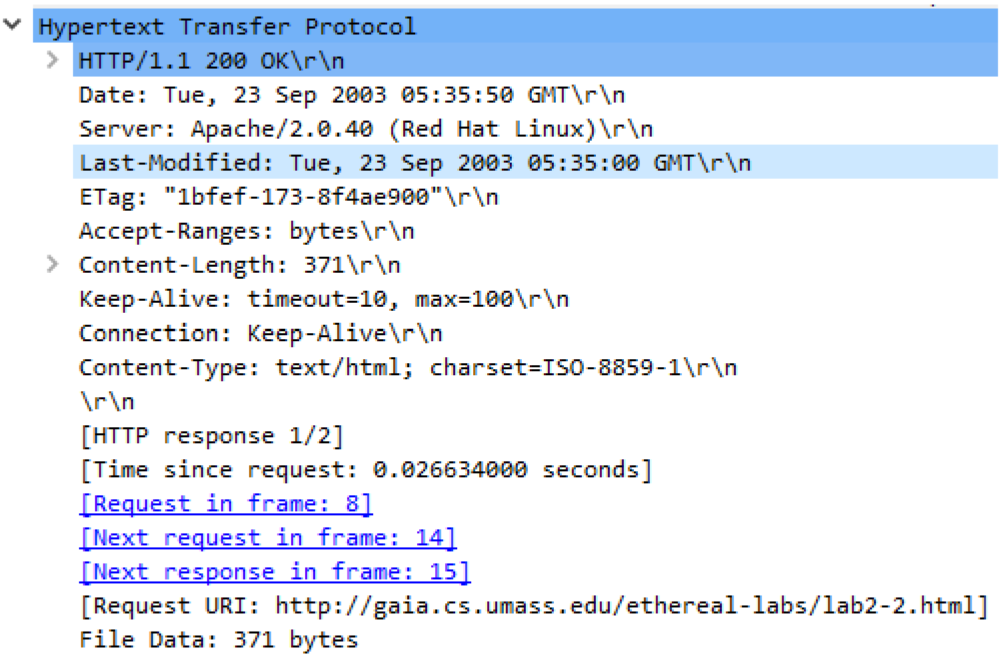
**Question 5: What is the data contained inside the HTTP response packet?**

## Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction (marked, include in your report)

**Question 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?**

No

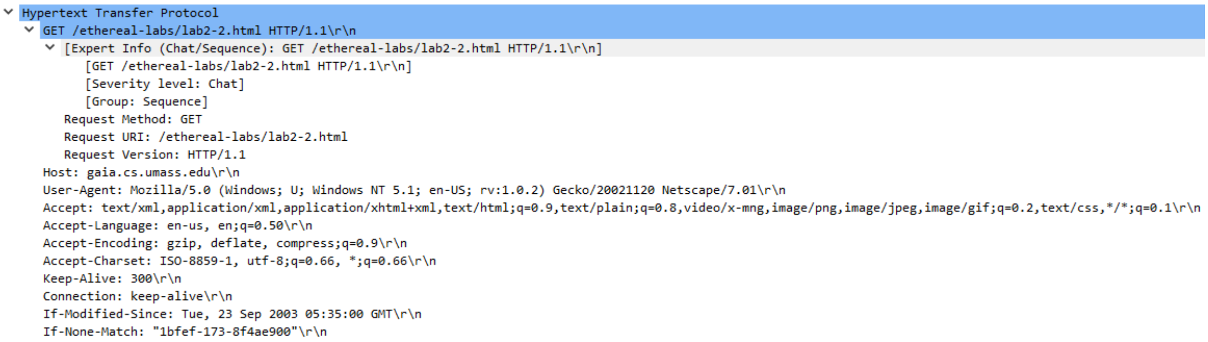
**Question 2: Does the response indicate the last time that the requested file was modified?**



```
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
  ETag: "1bfef-173-8f4ae900"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
  Keep-Alive: timeout=10, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=ISO-8859-1\r\n
  \r\n
  [HTTP response 1/2]
  [Time since request: 0.026634000 seconds]
  [Request in frame: 8]
  [Next request in frame: 14]
  [Next response in frame: 15]
  [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
  File Data: 371 bytes
```

Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT

**Question 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?**

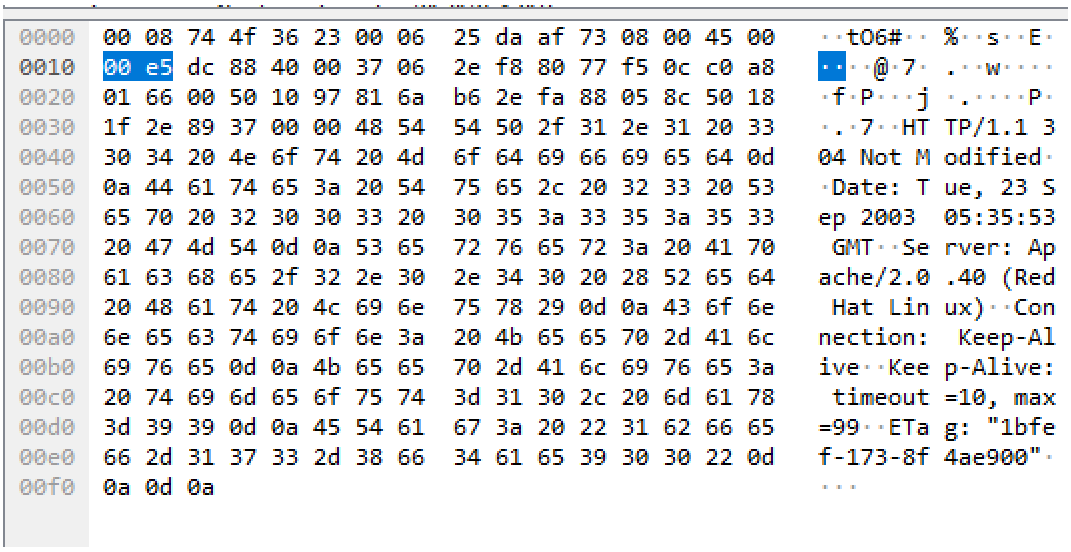


```
Hypertext Transfer Protocol
  GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
    Request Method: GET
    Request URI: /ethereal-labs/lab2-2.html
    Request Version: HTTP/1.1
  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=0.1\r\n
  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
```

If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT

If-None-Match: "1bfef-173-8f4ae900"

**Question 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.**



```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  00 e5 dc 88 40 00 37 06  2e f8 80 77 f5 0c c0 a8   ····@·7· .··w····
0020  01 66 00 50 10 97 81 6a  b6 2e fa 88 05 8c 50 18   ·f·P···j ·.····P·
0030  1f 2e 89 37 00 00 48 54  54 50 2f 31 2e 31 20 33   ·.·7··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 54  75 65 2c 20 32 33 20 53   ·Date: T ue, 23 S
0060  65 70 20 32 30 30 33 20  30 35 3a 33 35 3a 35 33   ep 2003  05:35:53
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 30  2e 34 30 20 28 52 65 64   ache/2.0 .40 (Red
0090  20 48 61 74 20 4c 69 6e  75 78 29 0d 0a 43 6f 6e    Hat Lin ux)··Con
00a0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00b0  69 76 65 0d 0a 4b 65 65  70 2d 41 6c 69 76 65 3a   ive··Kee p-Alive:
00c0  20 74 69 6d 65 6f 75 74  3d 31 30 2c 20 6d 61 78    timeout =10, max
00d0  3d 39 39 0d 0a 45 54 61  67 3a 20 22 31 62 66 65   =99··ETa g: "1bfe
00e0  66 2d 31 37 33 2d 38 66  34 61 65 39 30 30 22 0d   f-173-8f 4ae900"·
00f0  0a 0d 0a                                           ···
```

The HTTP status code and phrase returned is “304 Not Modified Response”. The server did not explicitly return the contents of the file as the return packet is much smaller.

**Question 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 1 st response message was received?**

ETag: "1bfef-173-8f4ae900", the idea of ETags is to let caches be more efficient and thus save bandwidth. The Etag value has not changed since the 1st message was received.

## Exercise 5: Ping Client (marked, submit source code as a separate file, include sample output in the report)