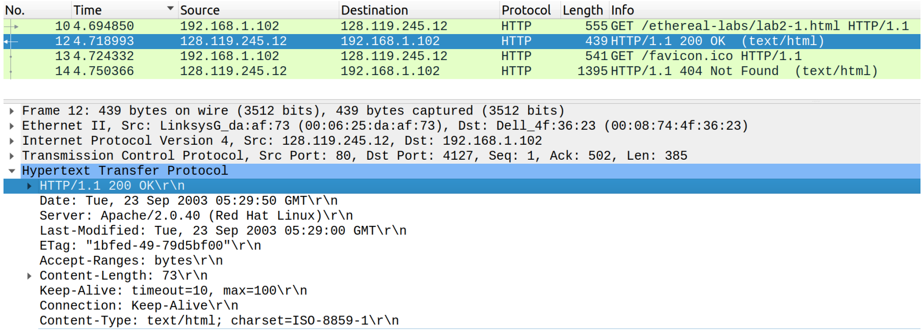
Lab 02 - Ryan McClue (z5346008)

1. Wireshark HTTP GET Request/Response



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)

```
▸ Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)
▸ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385
▾ 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
```

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

Status Code: 200

Status Phrase: OK

2.1 *When was the HTML file that the browser is retrieving last modified at the server?*

Tue, 23 Sep 2003, 5:29:00 GMT

2.2 *Does the response also contain a DATE header?*

Yes. It's Tue, 23 Sep 2003, 5:29:50 GMT

2.3 *How are these two fields different?*

The `Date` header is the time when the server sent the response message. The `Last-Modified` header is the time when the server believes the resource requested was last changed.

3.1 *Is the connection established between the browser and the server persistent or non-persistent?*

Persistent.

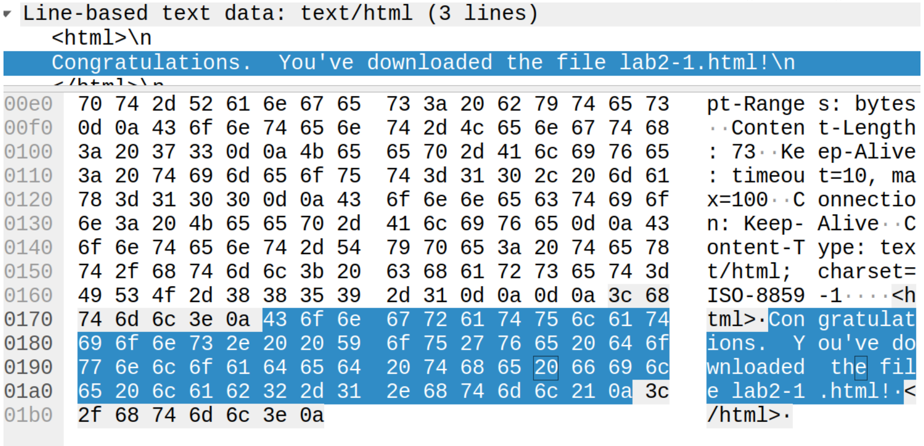
3.2 *How can you infer this?*

HTTP1.1 is being used, which introduced persistent connection capabilities. Furthermore, the presence of the header field `Connection: Keep-Alive` in the HTTP request/response indicates that a single TCP connection can be used for multiple requests/responses.

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

73

5.1 *What is the data contained inside the HTTP response packet?*



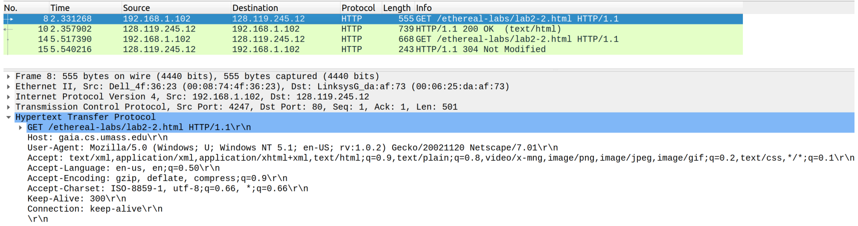
```
▾ Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations.  You've downloaded the file lab2-1.html!\n
    </html>\n
00e0  70 74 2d 52 61 6e 67 65  73 3a 20 62 79 74 65 73   pt-Range s: bytes
00f0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
0100  3a 20 37 33 0d 0a 4b 65  65 70 2d 41 6c 69 76 65   : 73··Ke ep-Alive
0110  3a 20 74 69 6d 65 6f 75  74 3d 31 30 2c 20 6d 61   : timeou t=10, ma
0120  78 3d 31 30 30 0d 0a 43  6f 6e 6e 65 63 74 69 6f   x=100··C onnectio
0130  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
0140  6f 6e 74 65 6e 74 2d 54  79 70 65 3a 20 74 65 78   ontent-T ype: tex
0150  74 2f 68 74 6d 6c 3b 20  63 68 61 72 73 65 74 3d   t/html;  charset=
0160  49 53 4f 2d 38 38 35 39  2d 31 0d 0a 0d 0a 3c 68   ISO-8859 -1····<h
0170  74 6d 6c 3e 0a 43 6f 6e  67 72 61 74 75 6c 61 74   tml>·Con gratulat
0180  69 6f 6e 73 2e 20 20 59  6f 75 27 76 65 20 64 6f   ions.  Y ou've do
0190  77 6e 6c 6f 61 64 65 64  20 74 68 65 20 66 69 6c   wnloaded  the fil
01a0  65 20 6c 61 62 32 2d 31  2e 68 74 6d 6c 21 0a 3c   e lab2-1 .html!·<
01b0  2f 68 74 6d 6c 3e 0a                               /html>·
```

A html file containing:

```
<html>
Congratulations.  You've downloaded the file lab2-1.html!
</html>
```

2. Wireshark HTTP Conditional GET Request/Response

1. *Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?*

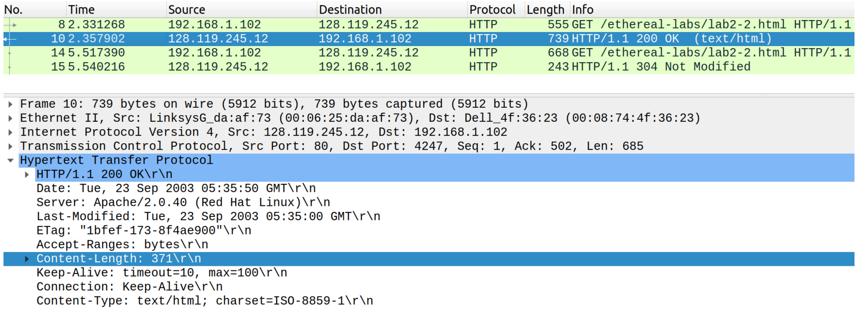


```
No.  Time      Source          Destination     Protocol Length Info
   8 2.331268  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-2.html HTTP/1.1
  10 2.357902  128.119.245.12  192.168.1.102   HTTP      739 HTTP/1.1 200 OK  (text/html)
  14 5.517390  192.168.1.102   128.119.245.12  HTTP      668 GET /ethereal-labs/lab2-2.html HTTP/1.1
  15 5.540216  128.119.245.12  192.168.1.102   HTTP      243 HTTP/1.1 304 Not Modified

▸ Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
▸ Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▸ Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
▾ 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=0.1\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
    \r\n
```

No

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

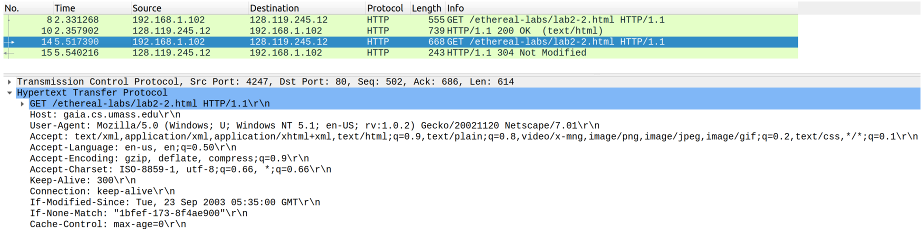


```
No.  Time      Source          Destination     Protocol Length Info
   8 2.331268  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-2.html HTTP/1.1
  10 2.357902  128.119.245.12  192.168.1.102   HTTP      739 HTTP/1.1 200 OK  (text/html)
  14 5.517390  192.168.1.102   128.119.245.12  HTTP      668 GET /ethereal-labs/lab2-2.html HTTP/1.1
  15 5.540216  128.119.245.12  192.168.1.102   HTTP      243 HTTP/1.1 304 Not Modified

▸ Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
▸ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685
▾ 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
```

Yes.

3.1 *Do you see an “IF-MODIFIED-SINCE:” and “IF-NONE-MATCH” lines in the HTTP GET?*



```
No.     Time        Source          Destination     Protocol Length Info
      8 2.331268    192.168.1.102   128.119.245.12  HTTP        555 GET /ethereal-labs/lab2-2.html HTTP/1.1
     10 2.357902    128.119.245.12  192.168.1.102   HTTP        739 HTTP/1.1 200 OK  (text/html)
     14 5.517390    192.168.1.102   128.119.245.12  HTTP        668 GET /ethereal-labs/lab2-2.html HTTP/1.1
     15 5.540216    128.119.245.12  192.168.1.102   HTTP        243 HTTP/1.1 304 Not Modified

▸ Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 614
▾ 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=0.1\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
    Cache-Control: max-age=0\r\n
```

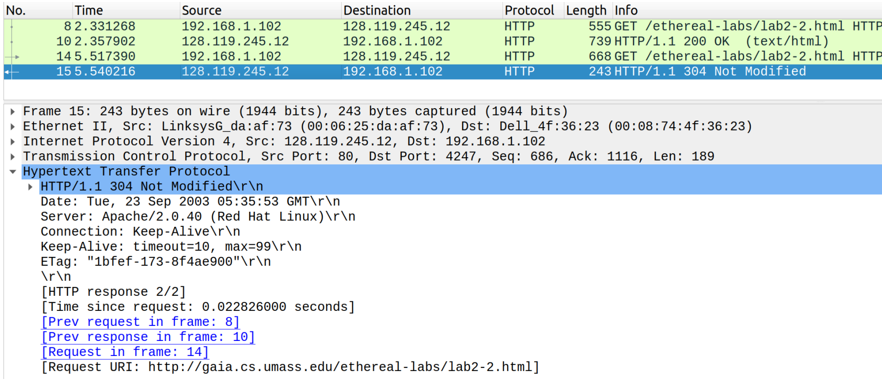
Yes

3.2 *If so, what information is contained in these header lines?*

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

If-None-Match: “1bfef-173-8f4ae900”

4.1 *What is the HTTP status code and phrase returned from the server in response to this second HTTP GET?*



```
No.     Time        Source          Destination     Protocol Length Info
      8 2.331268    192.168.1.102   128.119.245.12  HTTP        555 GET /ethereal-labs/lab2-2.html HTTP
     10 2.357902    128.119.245.12  192.168.1.102   HTTP        739 HTTP/1.1 200 OK  (text/html)
     14 5.517390    192.168.1.102   128.119.245.12  HTTP        668 GET /ethereal-labs/lab2-2.html HTTP
     15 5.540216    128.119.245.12  192.168.1.102   HTTP        243 HTTP/1.1 304 Not Modified

▸ Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
▸ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len: 189
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=10, max=99\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.022826000 seconds]
    [Prev request in frame: 8]
    [Prev response in frame: 10]
    [Request in frame: 14]
    [Request URI: http://gaia.cs.umass.edu/ethereal-labs/lab2-2.html]
```

Status Code: 304

Status Phrase: Not Modified

4.2 *Did the server explicitly return the contents of the file? Explain.*

No. The webserver determined that the file requested was already present in the client’s browser cache and therefore did not need to return the file contents.

5.1 *What is the value of the Etag field in the 2nd response message and how it is used?*

`ETag: "1bfef-173-8f4ae900"`. It’s used to determine if the content of a requested resource has changed on the server side and needs to be sent back to the client. Furthermore, it’s used in conjunction with the timestamp given by `If-Modified-Since` to implement conditional GET requests.

5.2 *Has this value changed since the 1st response message was received?*

No