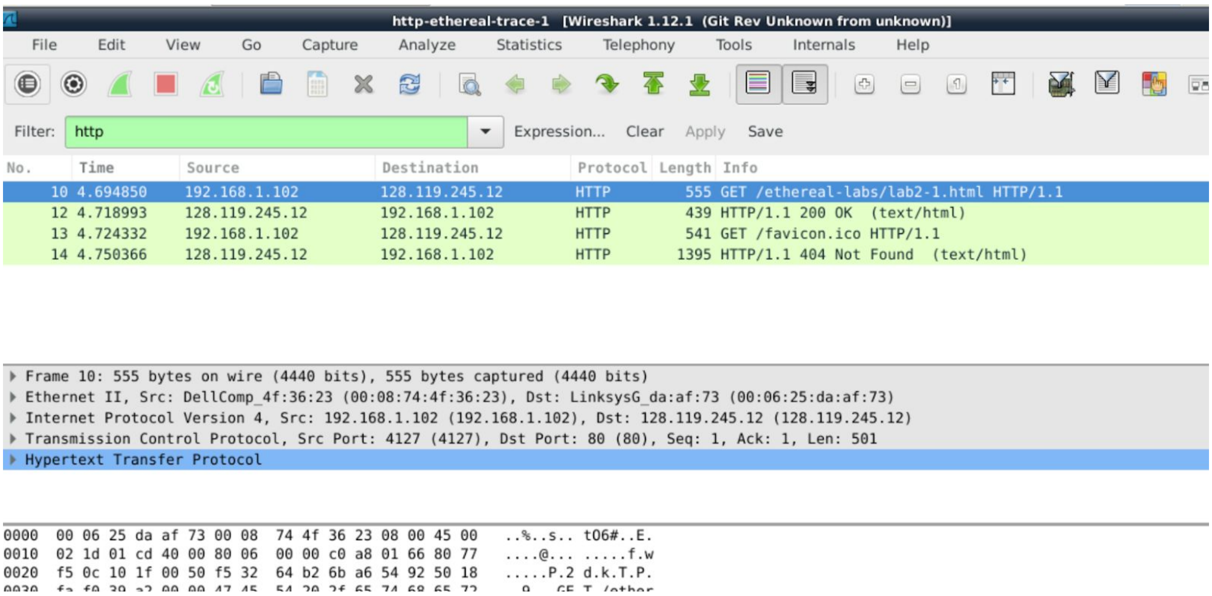
Exercise 3

By looking at the information in the HTTP GET and response messages (the first two messages), answer the following questions:

Question 1: What is the status code and phrase returned from the server to the client browser?
Status code and phrase returned from server to browser in response message: 200 OK



Filter: http

```
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)
```

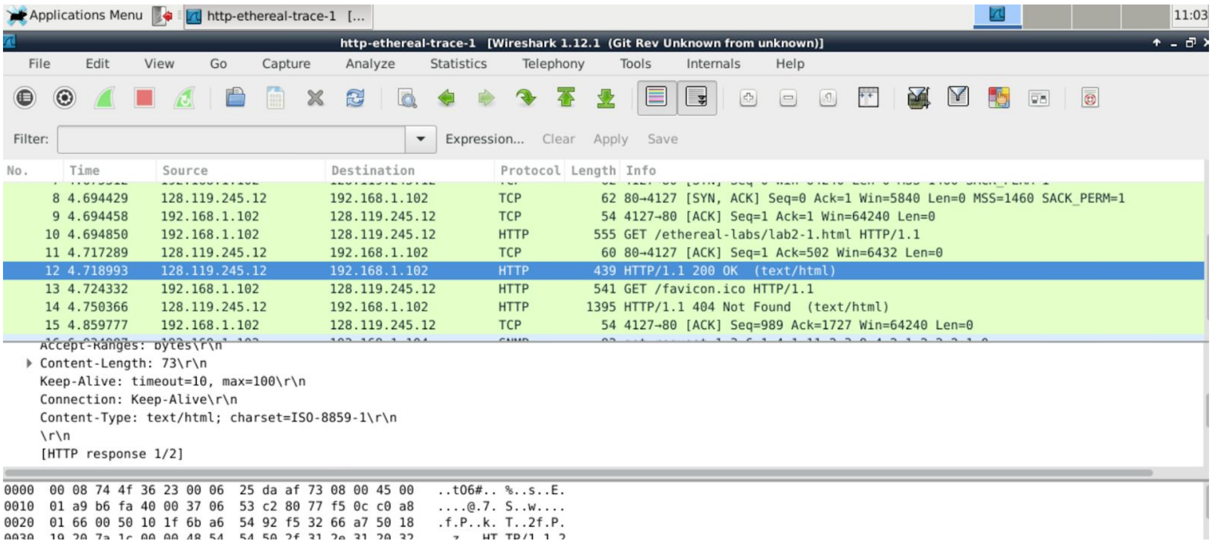
```
▸ Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
▸ Ethernet II, Src: DellComp_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
▸ Internet Protocol Version 4, Src: 192.168.1.102 (192.168.1.102), Dst: 128.119.245.12 (128.119.245.12)
▸ Transmission Control Protocol, Src Port: 4127 (4127), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 501
▸ Hypertext Transfer Protocol
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ..%..s.. tO6#..E.
0010  02 1d 01 cd 40 00 80 06  00 00 c0 a8 01 66 80 77   ....@... .....f.w
0020  f5 0c 10 1f 00 50 f5 32  64 b2 6b a6 54 92 50 18   .....P.2 d.k.T.P.
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ..9...GE T /ether
```

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?

Last modified Tuesday 23 Sep 2003, 05:29:00 GMT. The response also contains a DATE header which is 23 Sep 2003, 05:29:50 GMT. These two fields refer to different things - the last modified field refers to the date and time which the object being sent from the server to the browser was last modified, whereas the date refers to the date the message was sent. In this case the object was sent from the server to the browser 50 seconds after it was updated.

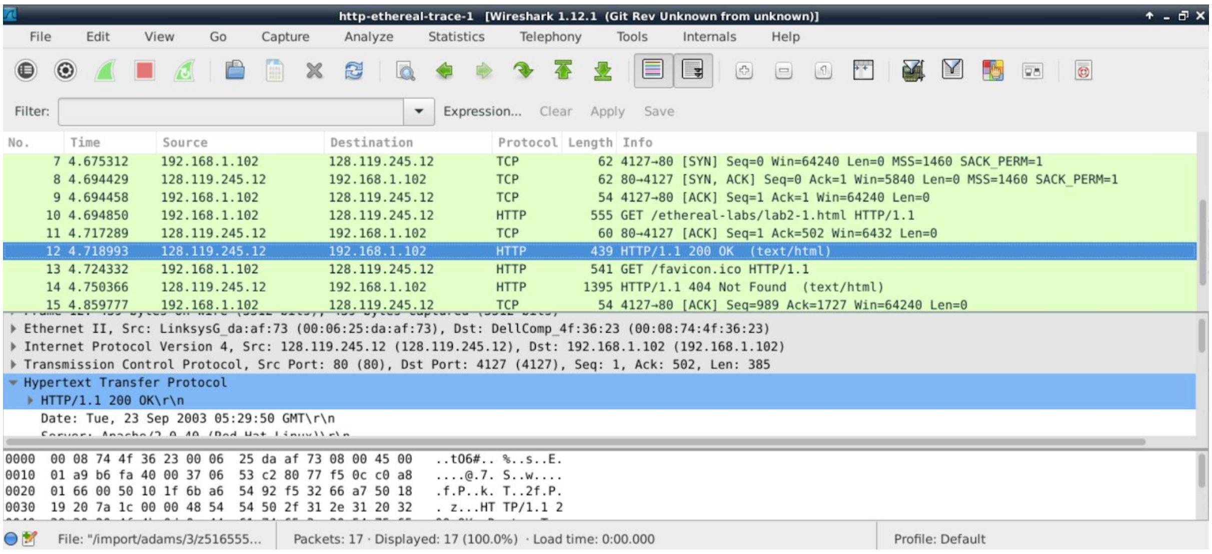
Question 3: Is the connection established between the browser and the server persistent or nonpersistent? How can you infer this?



```
No.   Time        Source           Destination      Protocol Length Info
    8 4.694429    128.119.245.12   192.168.1.102    TCP        62 80→4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    9 4.694458    192.168.1.102    128.119.245.12   TCP        54 4127→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10 4.694850    192.168.1.102    128.119.245.12   HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
   11 4.717289    128.119.245.12   192.168.1.102    TCP        60 80→4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
   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)
   15 4.859777    192.168.1.102    128.119.245.12   TCP        54 4127→80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
```

```
    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]
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ....@.7. S..w....
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   .f.P..k. T..2f.P.
```



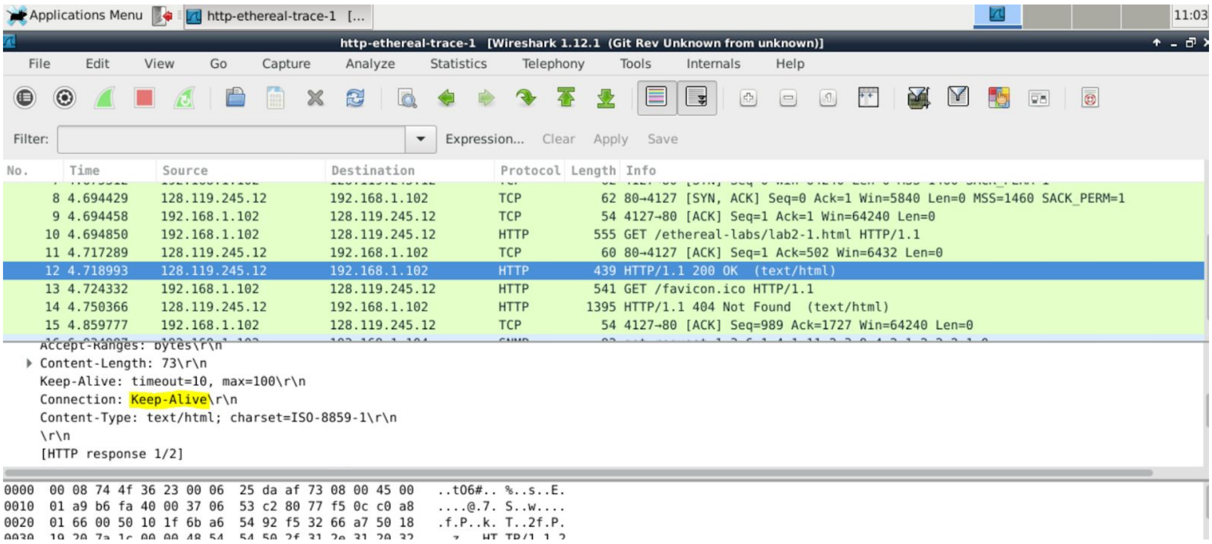
```
No.   Time        Source           Destination      Protocol Length Info
    7 4.675312    192.168.1.102    128.119.245.12   TCP        62 4127→80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
    8 4.694429    128.119.245.12   192.168.1.102    TCP        62 80→4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
    9 4.694458    192.168.1.102    128.119.245.12   TCP        54 4127→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10 4.694850    192.168.1.102    128.119.245.12   HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
   11 4.717289    128.119.245.12   192.168.1.102    TCP        60 80→4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
   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)
   15 4.859777    192.168.1.102    128.119.245.12   TCP        54 4127→80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
```

```
▸ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: DellComp_4f:36:23 (00:08:74:4f:36:23)
▸ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
▸ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 4127 (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
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ....@.7. S..w....
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   .f.P..k. T..2f.P.
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   . z...HT TP/1.1 2
```

File: "/import/adams/3/z516555... Packets: 17 · Displayed: 17 (100.0%) · Load time: 0:00.000 Profile: Default

The connection is persistent (i.e. only one TCP connection is required for multiple HTTP messages to be sent between a client/server pair). This can be inferred as the “Connection” type is specified as“Keep-Alive” in the GET/POST requests, which keeps the TCP connection open.



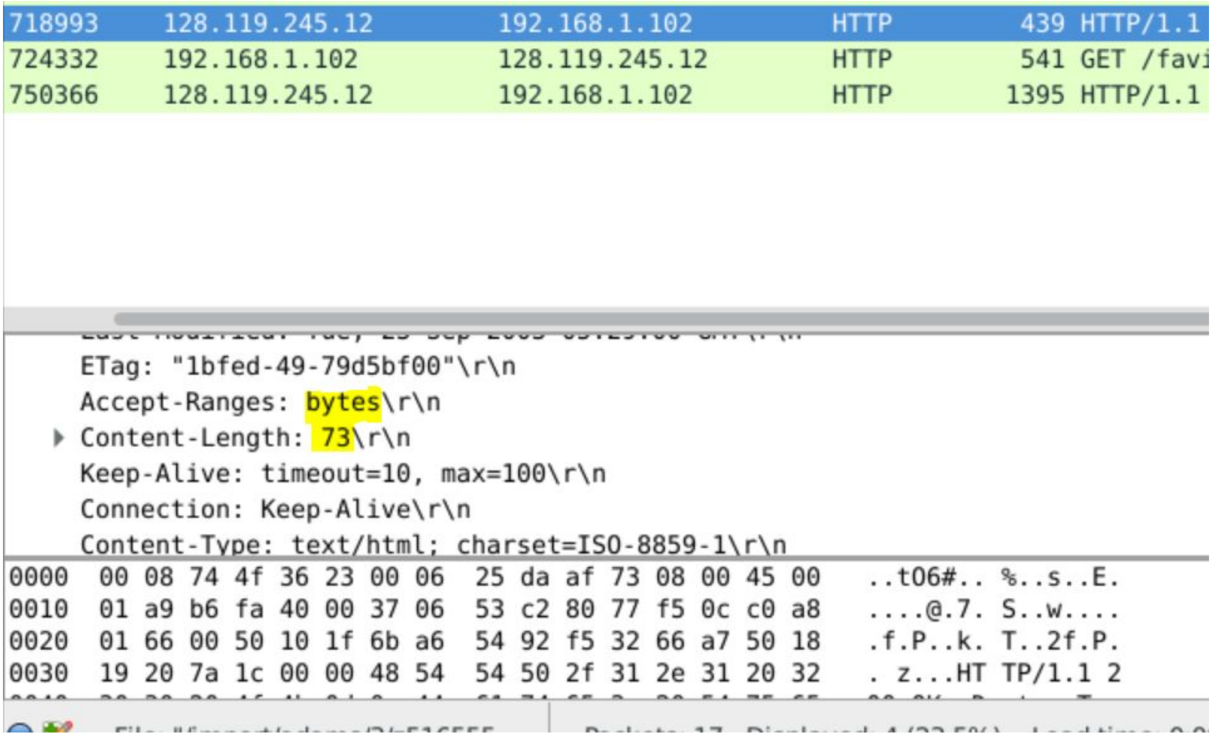
```
No.  Time      Source          Destination     Protocol Length Info
   8 4.694429  128.119.245.12  192.168.1.102   TCP        62 80→4127 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
   9 4.694458  192.168.1.102   128.119.245.12  TCP        54 4127→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  10 4.694850  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
  11 4.717289  128.119.245.12  192.168.1.102   TCP        60 80→4127 [ACK] Seq=1 Ack=502 Win=6432 Len=0
  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)
  15 4.859777  192.168.1.102   128.119.245.12  TCP        54 4127→80 [ACK] Seq=989 Ack=1727 Win=64240 Len=0
```

```
    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]
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ....@.7. S..w....
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   .f.P..k. T..2f.P.
```

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

73 bytes of content are being returned to the browser in the first HTTP response packet (size of lab2-1.html along with the text belong in Q5).



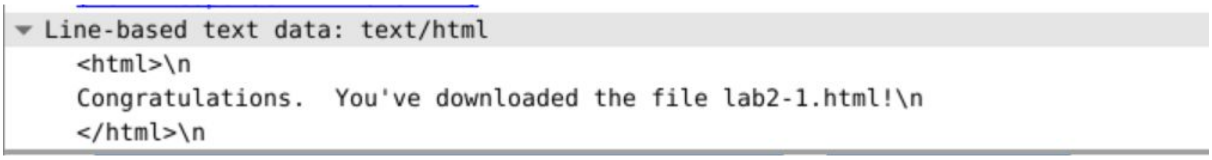
```
718993   128.119.245.12   192.168.1.102    HTTP    439 HTTP/1.1
724332   192.168.1.102    128.119.245.12   HTTP    541 GET /favi
750366   128.119.245.12   192.168.1.102    HTTP   1395 HTTP/1.1
```

```
    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
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  01 a9 b6 fa 40 00 37 06  53 c2 80 77 f5 0c c0 a8   ....@.7. S..w....
0020  01 66 00 50 10 1f 6b a6  54 92 f5 32 66 a7 50 18   .f.P..k. T..2f.P.
0030  19 20 7a 1c 00 00 48 54  54 50 2f 31 2e 31 20 32   . z...HT TP/1.1 2
```

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

The data contained inside the HTTP response packet is lab2-1.html along with the html text "Congratulations. You've downloaded the file lab2-1.html!"



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

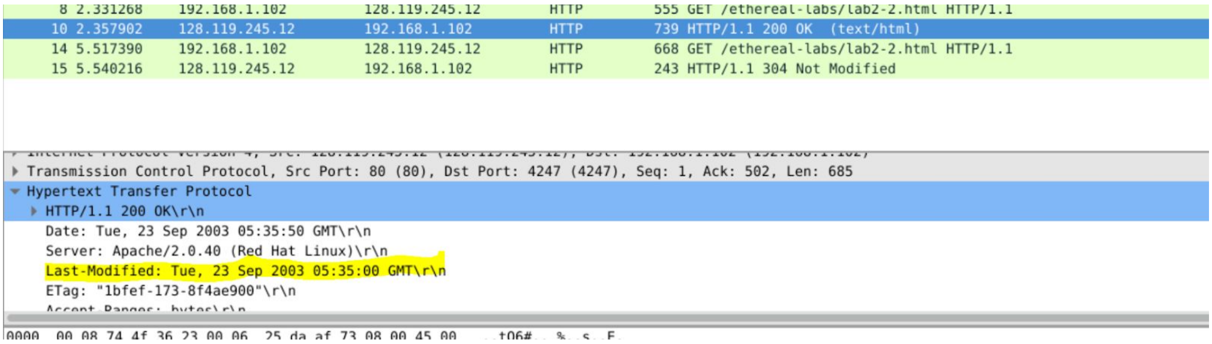
Exercise 4

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?

There is not an “IF-MODIFIED-SINCE” line in the first HTTP GET request but there is one in the second GET request from the browser.

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

Yes, the response indicates the requested file was last modified Tues 23 Sep 2003 05:35:00 GMT.



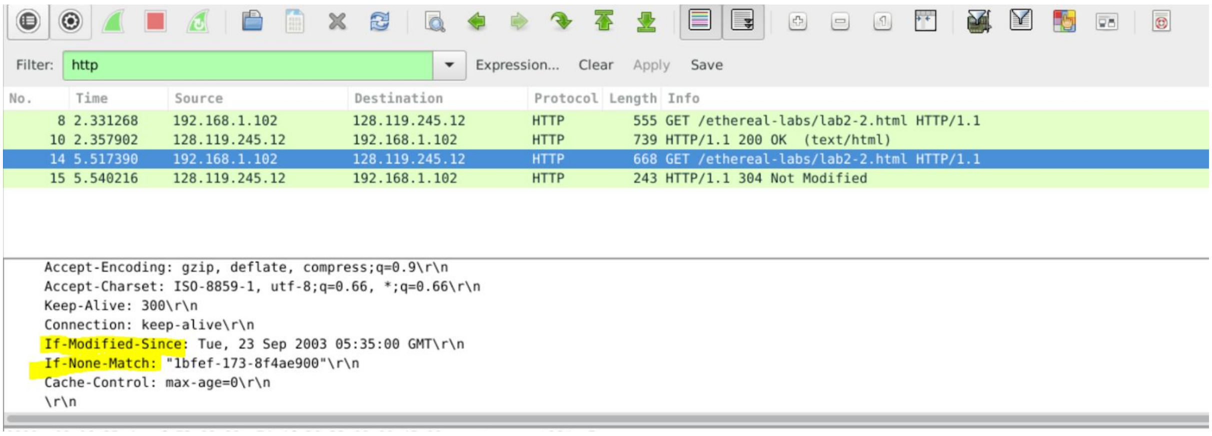
```
   8 2.331268    192.168.1.102     128.119.245.12    HTTP    555 GET /ethereal-labs/lab2-2.html HTTP/1.1
  10 2.357902    128.119.245.12    192.168.1.102     HTTP    739 HTTP/1.1 200 OK  (text/html)
  14 5.517390    192.168.1.102     128.119.245.12    HTTP    668 GET /ethereal-labs/lab2-2.html HTTP/1.1
  15 5.540216    128.119.245.12    192.168.1.102     HTTP    243 HTTP/1.1 304 Not Modified

▶ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.102 (192.168.1.102)
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 4247 (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

0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
```

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?

Yes, both lines are visible in the HTTP get. The field for the “If-Modified-Since” contains the date and time the requested file was last modified. The field for the “If-None-Match” line contains an entity tag supplied by the client to the server. The server compares the tag with tags it has for the requested file, returning the requested file to the client only if none of the tags match. This means that the file requested by the client has been modified since the client last requested the file.

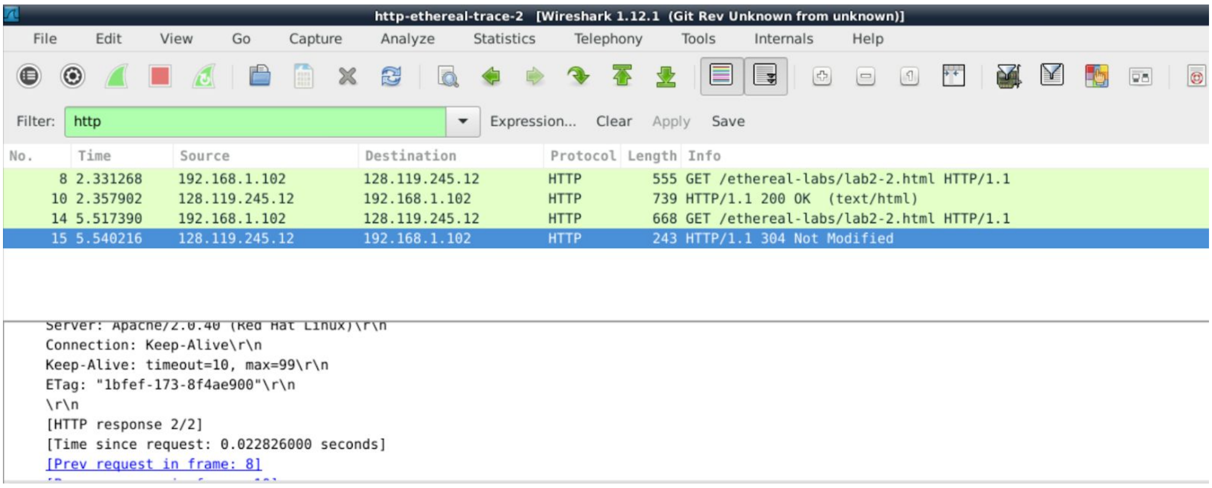


```
No.   Time        Source           Destination      Protocol Length Info
    8 2.331268    192.168.1.102    128.119.245.12   HTTP       555 GET /ethereal-labs/lab2-2.html HTTP/1.1
   10 2.357902    128.119.245.12   192.168.1.102    HTTP       739 HTTP/1.1 200 OK  (text/html)
   14 5.517390    192.168.1.102    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
```

```
    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
```

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.

The HTTP status code and phrase returned from the server in response is 304 Not Modified. This code is returned as the cached copy of the requested file is up-to-date with the server. The requested file is not explicitly returned by the server to the browser. The local copy on the cache is instead returned.

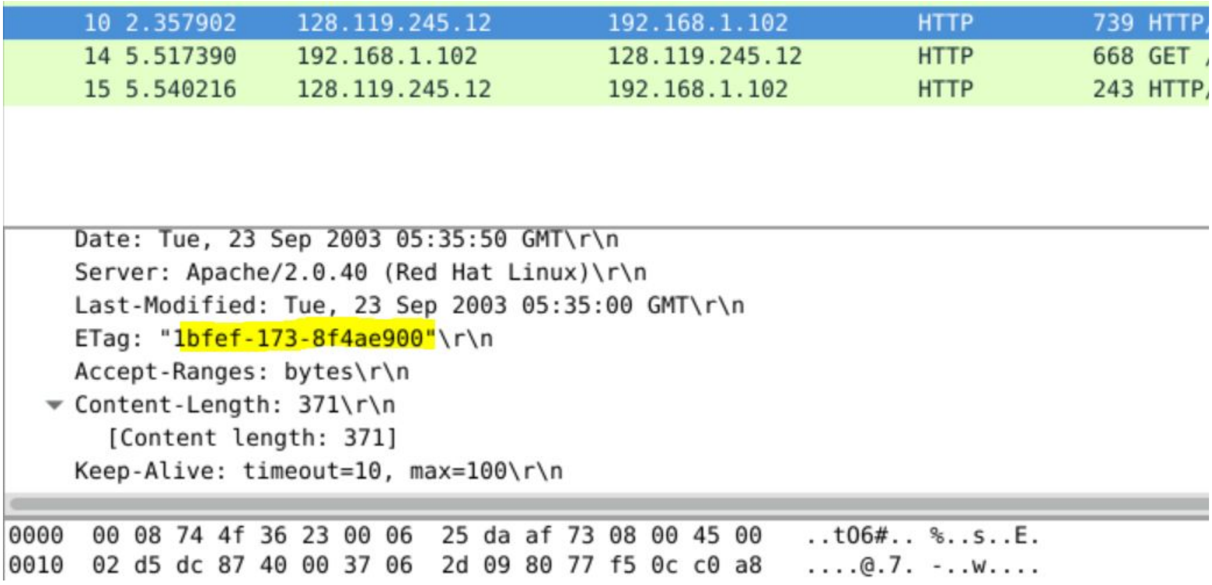

http-ethereal-trace-2 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Tools
Internals
Help
Filter: http
Expression... Clear Apply Save

```
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
```

```
    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]
```

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 1st response message was received?

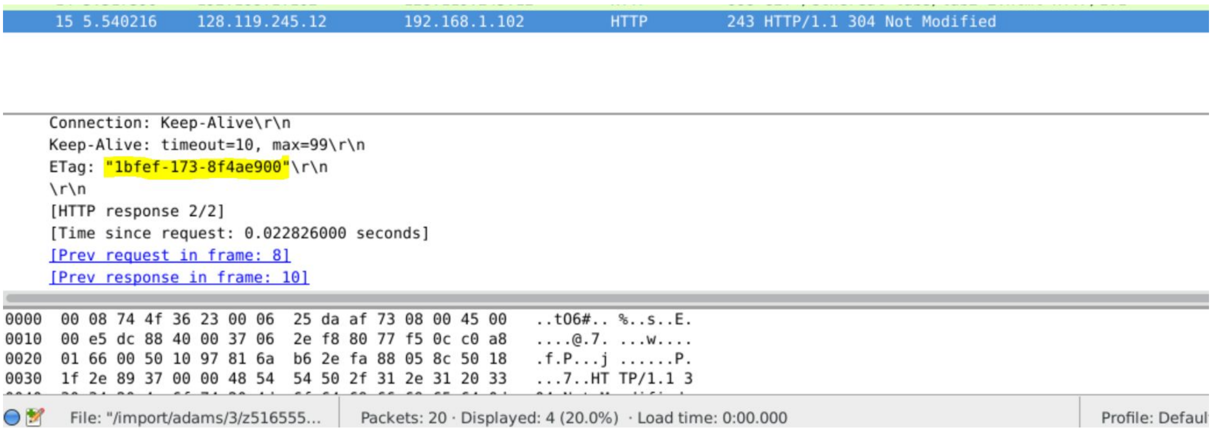
1st response message has Etag 1bfef-173-8f4ae900. This is identical to the value of the Etag field in the 2nd response message, so the value has not changed since the 1st response message was received. Etags are identifiers used to identify a specific version of a resource. If the resource changes, a new ETag is generated. In this way, the client is able to request resources only on the condition that they have been updated since the user's last visit to the site. As the Etag in the 1st response message and 2nd response message are the same, the server does not return the requested resource as there have been no new modifications to the file and instead, the client can obtain a copy from its local cache.



```
 10 2.357902   128.119.245.12    192.168.1.102    HTTP    739 HTTP/
 14 5.517390   192.168.1.102     128.119.245.12   HTTP    668 GET /
 15 5.540216   128.119.245.12    192.168.1.102    HTTP    243 HTTP/
```

```
   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
     [Content length: 371]
   Keep-Alive: timeout=10, max=100\r\n
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ..tO6#.. %..s..E.
0010  02 d5 dc 87 40 00 37 06  2d 09 80 77 f5 0c c0 a8   ....@.7. -..w....
```



```
 15 5.540216   128.119.245.12   192.168.1.102   HTTP   243 HTTP/1.1 304 Not Modified
```

```
   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]
```

```
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
```

File: "/import/adams/3/z516555... | Packets: 20 · Displayed: 4 (20.0%) · Load time: 0:00.000 | Profile: Defaul