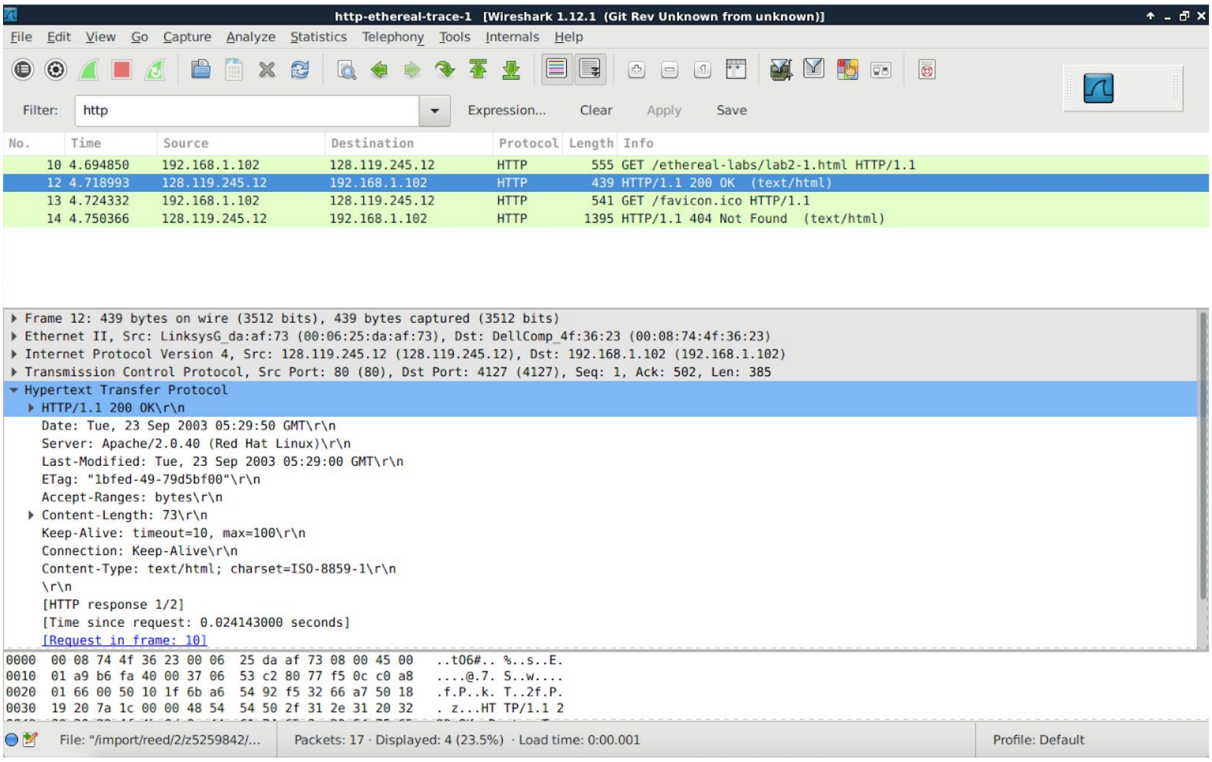
Exercise 3


http-ethereal-trace-1 [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
   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: 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
    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]
    [Time since request: 0.024143000 seconds]
    [Request in frame: 10]
```

```
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/reed/2/z5259842/... Packets: 17 · Displayed: 4 (23.5%) · Load time: 0:00.001 Profile: Default

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

The status code is 200 and the phrase returned from the server to the client browser is 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?

The HTML file that the browser is retrieving was last modified on Tuesday 23 September 2003 05:29:00 GMT.

The response contains a DATE header.

These two fields are different as date refers to the time the server responded to the request whereas last modified refers to the time when the HTML was last changed.

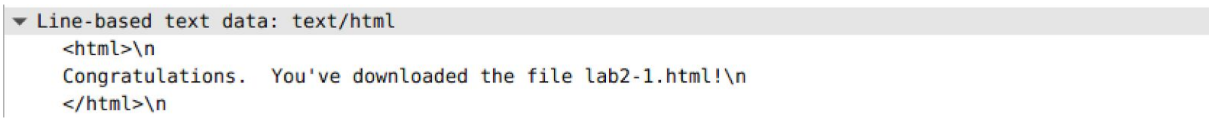
Question 3: Is the connection established between the browser and the server persistent or non-persistent? How can you infer this?

It is persistent. This can be observed by looking at the connection type - “Keep-Alive” which indicates that it is persistent.

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

73 bytes of content are being returned to the browser. This can be observed through “Content-length”.

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



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

The data contained inside the HTTP response packet is text/html. The data inside congratulates the successful download of the file lab2-1.html.

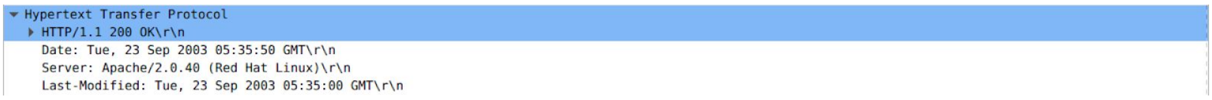
Exercise 4

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?

No

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

Yes, the requested file was last modified Tuesday 23 September 2003 05:35:50 GMT.



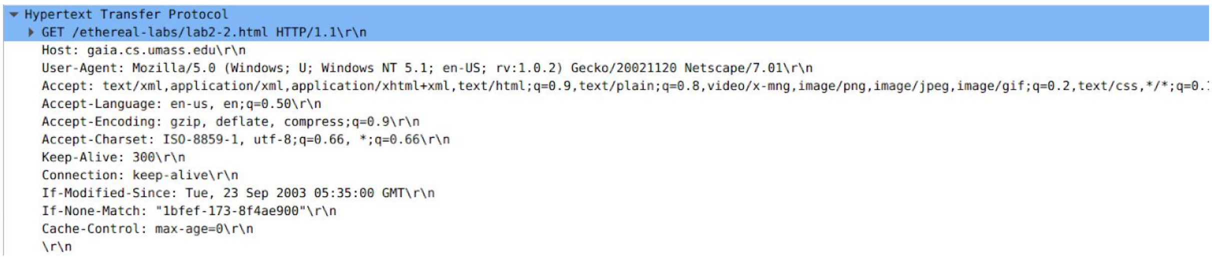
```
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
```

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.

If-Modified-Since: Tuesday 23 September 2003 05:35:00 GMT - if the requested resource has been modified after this specific date, the server will send back a 200 OK response

If-None-Match: “1bfef-173-8f4ae900” - if this etag does not match the others, the server will send back a 200 OK response



```
▾ 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
```

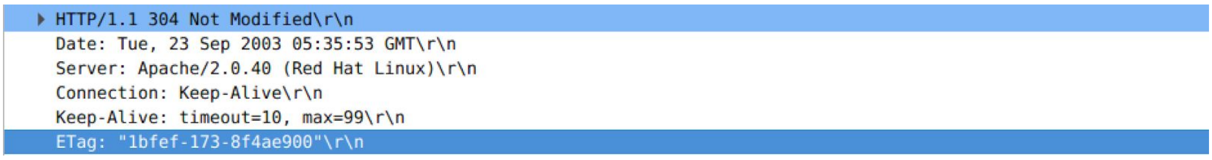
Question 4: What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP status code and phrase returned from the server was 304 Not Modified.

The server did not explicitly return the contents of the file. This is because the requested resource has not been modified since the previous request date. Therefore, it is unnecessary for it to return the contents of the file and it can be considered a waste of resources as nothing has changed, thus 304 Not Modified was returned from the server.

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?

The value of the Etag field in the 2nd response message is "1bfef-173-8f4ae900".



```
▸ 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
```

Etag is used as an identifier for a specific version of a resource. If the resource has been modified, a new Etag will be generated. This can further be used to compare 2 Etags to examine if the resource version is the same or not.

This value has not changed since the 1st response message was received which is an indication that the requested resource has not been modified.