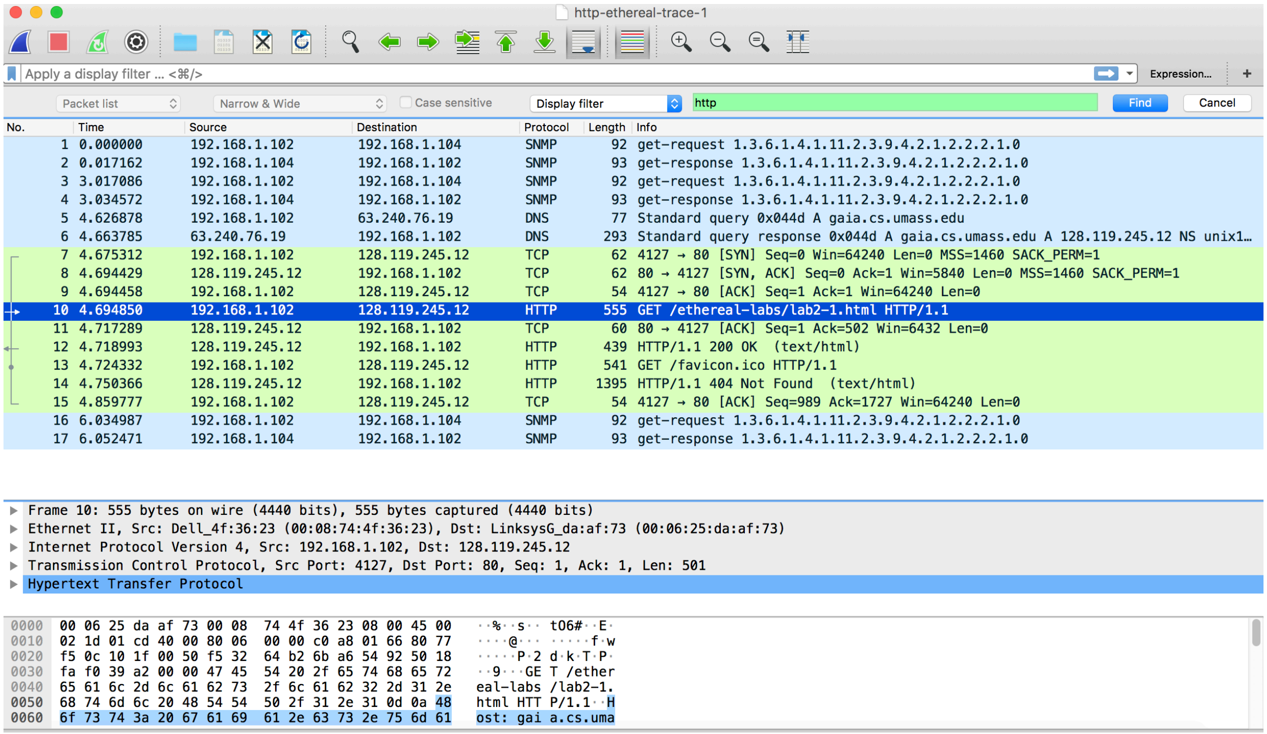
Exercise 3: Using Wireshark to understand basic HTTP request/response messages (marked, include in your report)



```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    2 0.017162  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    3 3.017086  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    4 3.034572  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    5 4.626878  192.168.1.102   63.240.76.19    DNS        77 Standard query 0x044d A gaia.cs.umass.edu
    6 4.663785  63.240.76.19    192.168.1.102   DNS       293 Standard query response 0x044d A gaia.cs.umass.edu A 128.119.245.12 NS unix1…
    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
   16 6.034987  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
   17 6.052471  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
```

```
▶ Frame 10: 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: 4127, Dst Port: 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
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 31 2e   eal-labs /lab2-1.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
```

Question 1:

Status Code: 200

Response Phrase: OK

Question 2:

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

It contains a Date header, another date is server’s time.

Question 3:

The connection is persistent, because the connection is keep-alive.

Connection: Keep-Alive\r\n

Keep-Alive: timeout=10, max=100\r\n

Question 4:

Content-Length: 73\r\n

73 bytes

Question 5:

The resources code is:

<html>\n

Congratulations. You’ve downloaded the file lab2.1.html\n

</html>\n

So it will response “ Congratulations. You’ve downloaded the file lab2.1.html” in HTTP response.

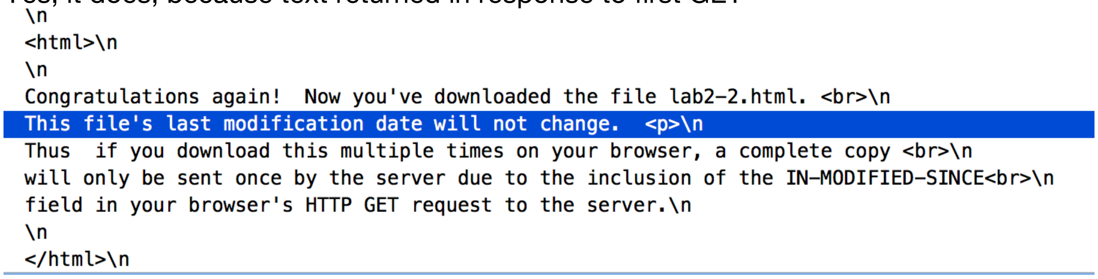
Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction (marked, include in your report)

Question 1:

No, both of them do not appear in first request.

Question 2:

Yes, it does, because text returned in response to first GET



```
\n
<html>\n
\n
Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change.  <p>\n
Thus  if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

Question 3:

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

If-None-Match: “1bfef-173-8f4ae900”\r\n

Question 4:

Status Code:304

Response Phrase: Not Modified

It doesn’t return the contents, because the statues code is 304 which represents the web is not modified last time and it returns empty.

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 stresponse message was received?

The value is: ETag: "1bfef-173-8f4ae900"\r\n

ETag can distinguish the resource representation at that URL ever changes, if changed a new and different ETag is assigned.

ETag allows a client to make conditional requests. This allows caches to be more efficient, and saves bandwidth, as a web server does not need to send a full response if the content has not changed.

It doesn’t change since the 1st response message received.