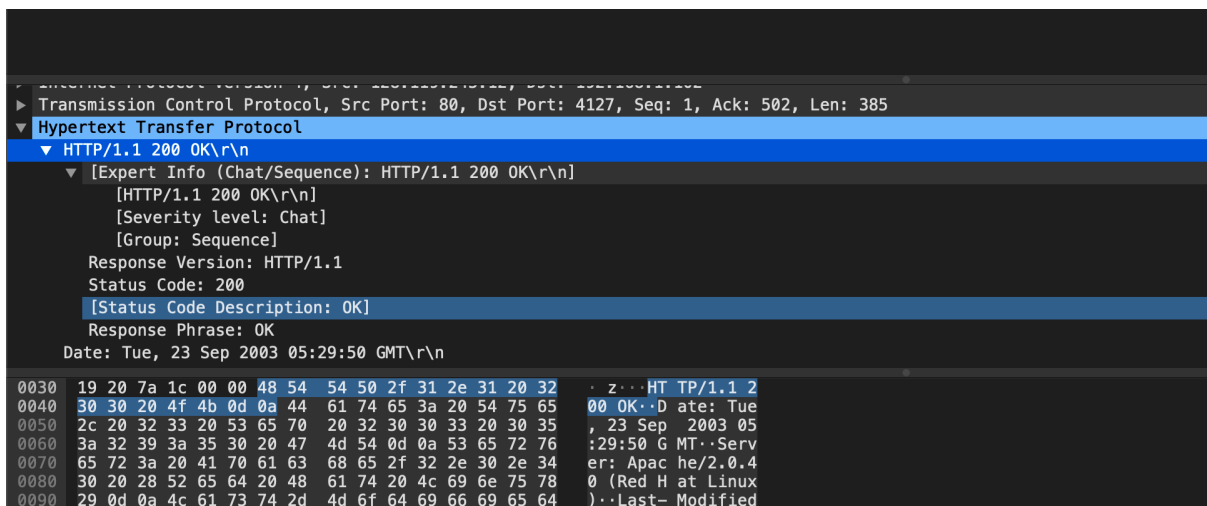


# Lab 2

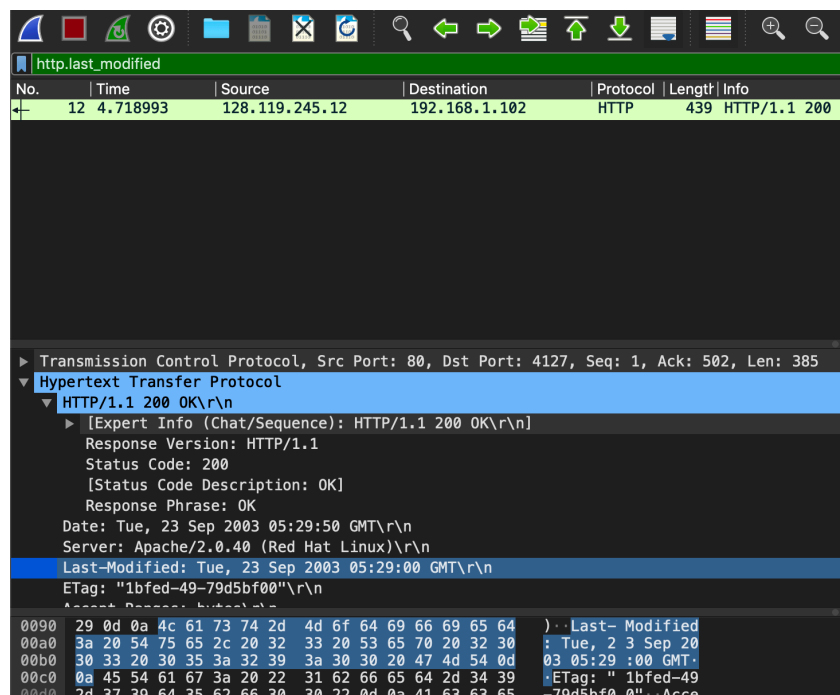
## Exercise 3: Using Wireshark to understand basic HTTP request/response messages

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



Here are the status code and the phrase. 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?



(1) Using the command `http.last_modified` to filter out the detail of last modification. Its last modification occurred in Tue, 23 Sep 2003 05:29:00

(2) It also contains a DATE header. In general, these two fields are almost the same. Except the seconds of time displayed, where the Date header (05:29:50) is slightly later than Last-Modified (05:29:00), other details are the same.

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

```
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1000000000
▼ 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
  00d0 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65 -79d5b
  00e0 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 nt-Ran
```

As the screen shot shows, the connection keeps alive, which is persistent. Actually, this is also a default option of HTTP/1.1.

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

```
▶ Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits) on interface 0
▶ 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
    \r\n
  [HTTP response 1/2]
  [Time since request: 0.024143000 seconds]
  [Request in frame: 10]
  [Next request in frame: 13]
  [Next response in frame: 14]
  [Request URI: http://gaia.cs.umass.edu/favicon.ico]
  File Data: 73 bytes
  Line-based text data: text/html (3 lines)
```

73 bytes are being returned

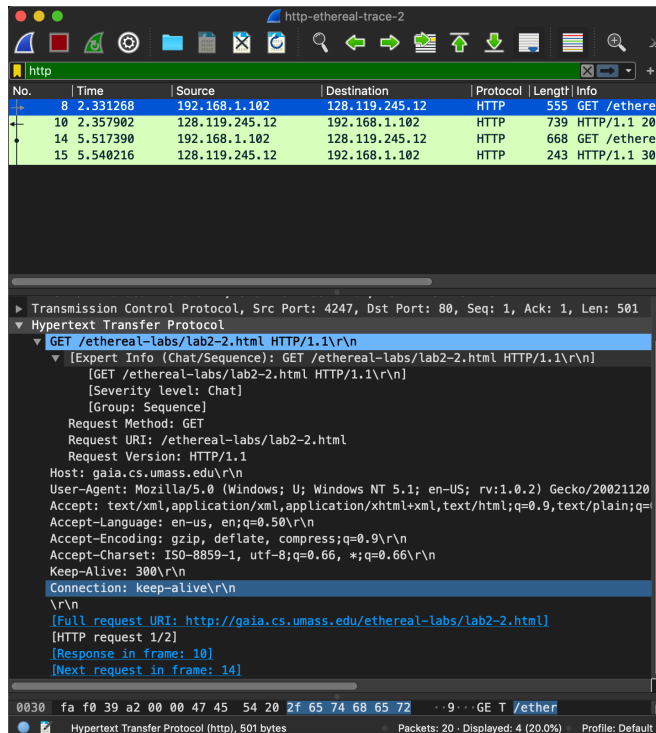
**Question 5: What is the data contained inside the HTTP response packet?**

text/html

```
▼ Line-based text data: text/html (3 lines)
  <html>\n
  Congratulations. You've downloaded the file lab2-1.html!\n
  </html>\n
```

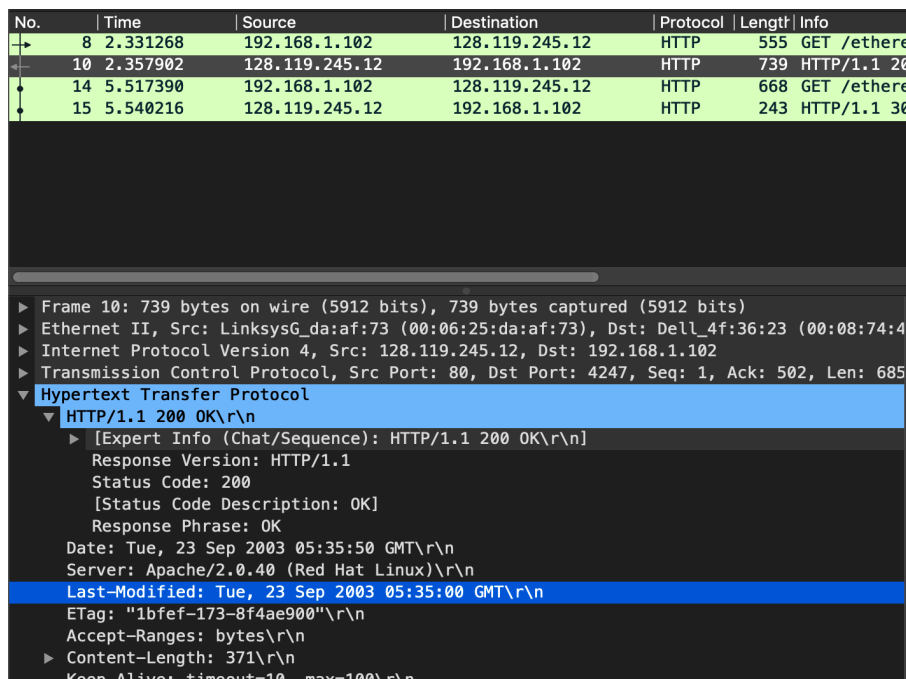
## Exercise 4: Using Wireshark to understand the HTTP CONDITIONAL GET/response interaction

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, it was modified on 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?

```

▶ Transmission Control Protocol, Src Port: 4247, Dst Port: 80, Seq: 502, Ack: 686, Len: 6
▼ 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]
      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
      Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=
      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

```

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

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

14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /etherea
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304

```

▶ 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: 18
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 304 Not Modified\r\n
    ▶ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      Response Version: HTTP/1.1
      Status Code: 304

```

(1) The status code and phrase: 304 Not Modified\r\n

(2) No, because the status code is Not modified, which is a response for the “**IF-MODIFIED-SINCE:**” line in second GET request. It means that the contents in the cache is up to date. Then the server would not return the whole file and the content would be displayed for clients directly from cachew

**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?**

(1) Here are the values of Etag field in 1st and 2nd responses. The value has not changed during two responses.

(2) It allows a client to make conditional request, which makes the 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.

1st:

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /et
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /et
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.

Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
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

2nd:

14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /et
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.

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 (00:01:02:4f: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: 11
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
Response Version: HTTP/1.1
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
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

## Exercise 5: Ping Client

sample output as follows:

client (PingClient.py):

```
ping to 127.0.0.1, seq = 0, rtt = 120.0 ms
ping to 127.0.0.1, seq = 1, rtt = 90.9 ms
ping to 127.0.0.1, seq = 2, rtt = time out
ping to 127.0.0.1, seq = 3, rtt = 48.9 ms
ping to 127.0.0.1, seq = 4, rtt = 67.2 ms
ping to 127.0.0.1, seq = 5, rtt = 40.9 ms
ping to 127.0.0.1, seq = 6, rtt = 19.9 ms
ping to 127.0.0.1, seq = 7, rtt = time out
ping to 127.0.0.1, seq = 8, rtt = 108.0 ms
ping to 127.0.0.1, seq = 9, rtt = time out
```

Process finished with exit code 0

Server (PingServer.java)

```
[(base) VigodeMacBook-Pro:lab2 huhawel$ java PingServer 1200
Received from 127.0.0.1: PING 1 2020-03-04 00:17:31.791920
  Reply sent.
Received from 127.0.0.1: PING 2 2020-03-04 00:17:31.912435
  Reply sent.
Received from 127.0.0.1: PING 3 2020-03-04 00:17:32.003737
  Reply not sent.
Received from 127.0.0.1: PING 4 2020-03-04 00:17:33.004682
  Reply sent.
Received from 127.0.0.1: PING 5 2020-03-04 00:17:33.053949
  Reply sent.
Received from 127.0.0.1: PING 6 2020-03-04 00:17:33.121489
  Reply sent.
Received from 127.0.0.1: PING 7 2020-03-04 00:17:33.162700
  Reply sent.
Received from 127.0.0.1: PING 8 2020-03-04 00:17:33.183089
  Reply not sent.
Received from 127.0.0.1: PING 9 2020-03-04 00:17:34.185563
  Reply sent.
Received from 127.0.0.1: PING 10 2020-03-04 00:17:34.293879
  Reply not sent.
```