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

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

A: The status code is 200 and the phrase returned is OK.

	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)

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?

A: Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n. It contains a DATE Header which is Tue, 23 Sep 2003 05:29:50 GMT\r\n. The difference is that Last-Modified is the last changed time and the DATE is the time of creating this message.

```
> 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
v 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
```

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

A: The connection is Keep-Alive so it's persistent. It also told that Keep-Alive: timeout=10, max=100\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
```

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

A: 73 Bytes.

```
Content-Length: 73\r\n
    [Content length: 73]
```

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

A: “Congratulations. You've downloaded the file lab2-1.html!\n”

```
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 (marked, include in your report)

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?

A: No.

```
Hypertext Transfer Protocol
  GET /ethereal-labs/lab2-2.html HTTP/1.1\r\n
```

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

A: Yes.

```
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
```

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?

A: Yes. If-Modified-Since contains the information same as the DATE Header. If-None-Match contains the information about the Etag value.

```
> 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
  Accept: text/xml,application/xml,application/xhtml+xml,text/html
  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.

A: Status Code: 304. Response Phrase: Not Modified. The server didn’t explicitly return the contents of the file since the Etag value match the If-None-Match.

```
v Hypertext Transfer Protocol
  v 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
```

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?

A: The ETag: "1bfef-173-8f4ae900"\r\n didn’t been modified. It is used to compare whether the resource has changed. If the resource has not changed, the 304 HTTP status code will be returned instead of the specific resource.

Exercise 5: Ping Client (marked, submit source code as a separate file, include sample output in the report)