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?
Status code: 200
Phrase: 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?
Date: Tue, 23 Sep 2003 05:29:50 GMT
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT
The Date field is a general-type header used to pass additional information with HTTP response or HTTP request. While the Last-Modified field is sent by the server specifying the date of the last modification of the requested source.

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

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

Question 5: What is the data contained inside the HTTP response packet?
<html>\n
Congratulations. You've downloaded the file http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file1.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. Last-Modified: 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?

Yes.

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

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

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.

Status code: 304

phrase: Not Modified

The Server did not explicitly return the contents of the file.

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?

ETag: "1bfef-173-8f4ae900"

Etag is a response-type header used as an identifier for a specific version of a resource.

This value has not changed since the 1st response.

Exercise 5:

See java code attached.