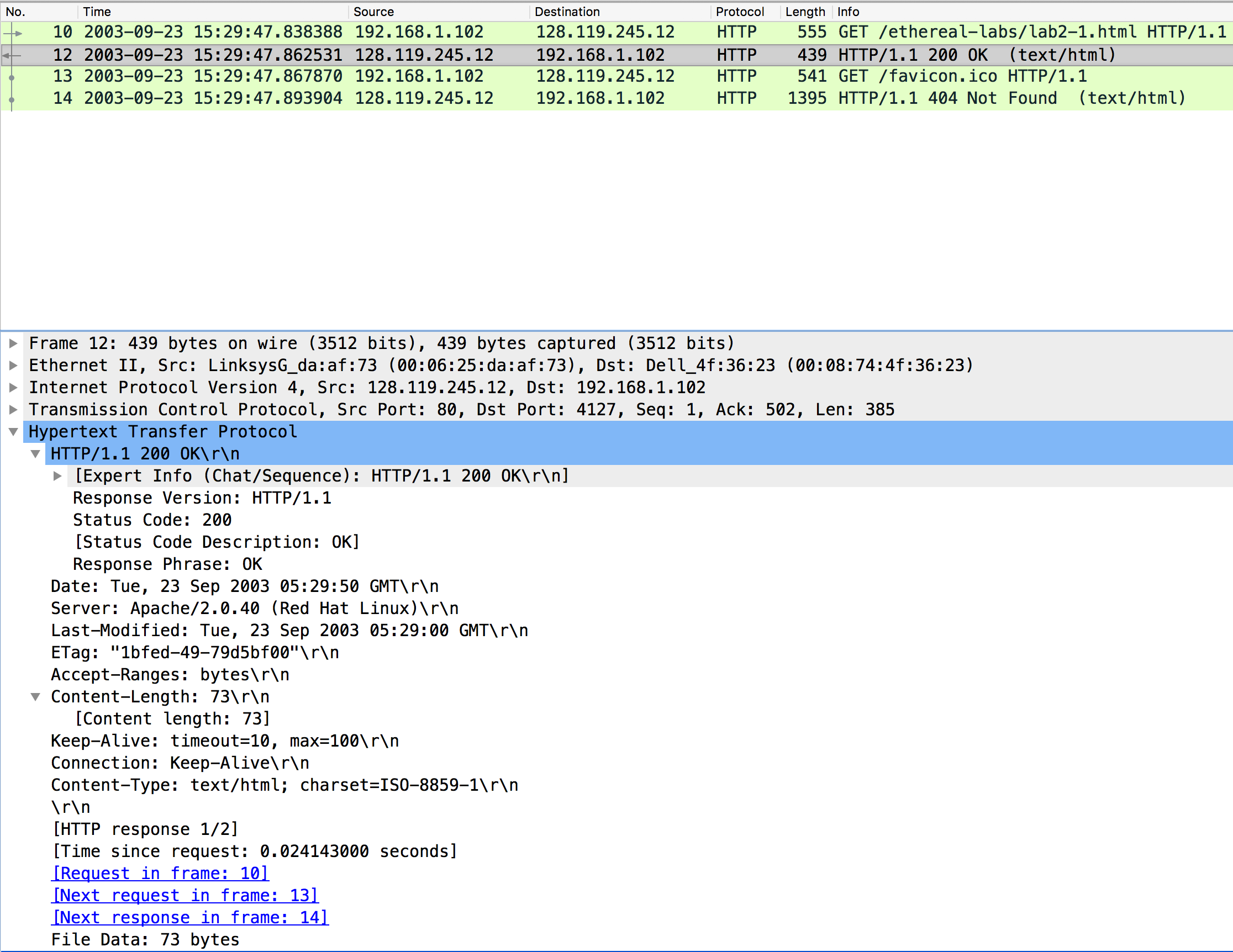
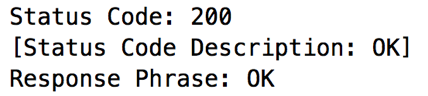
Exercise 3: Using Wireshark to understand basic HTTP request/response messages



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

The status code and phrase are 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?

The last modified time is : 

The response contains a DATE header, which indicates the time when the HTTP response message was actually generated by the server. Since these two fields are showing the same time in the current response, it is likely that the server is simply setting the file’s last-modified time to the time when the HTTP response message is created.

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



Both the client and server are using persistent HTTP connections.

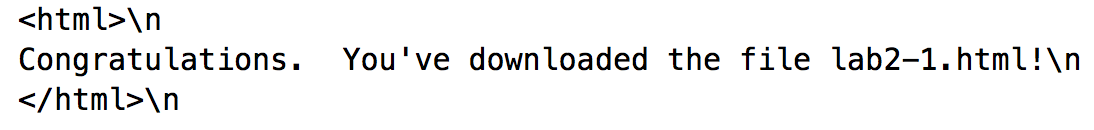
we can infer this by looking its connection, header in both the request and response.

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

73bytes

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

The file being returned the browser is an HTML file



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

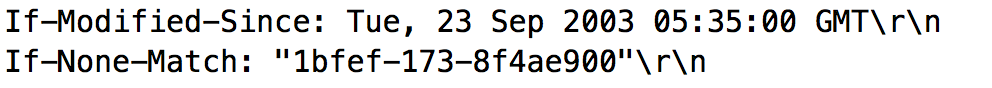
Question 1: Inspect the contents of the first HTTP GET request from the browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Answer: No

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

Yes,it is and the time is:

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. The information following is: 

which is the date of the last modification of the file from the previous get request.

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 status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn’t return the contents of the file since the browser loaded it from its cache.

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 :



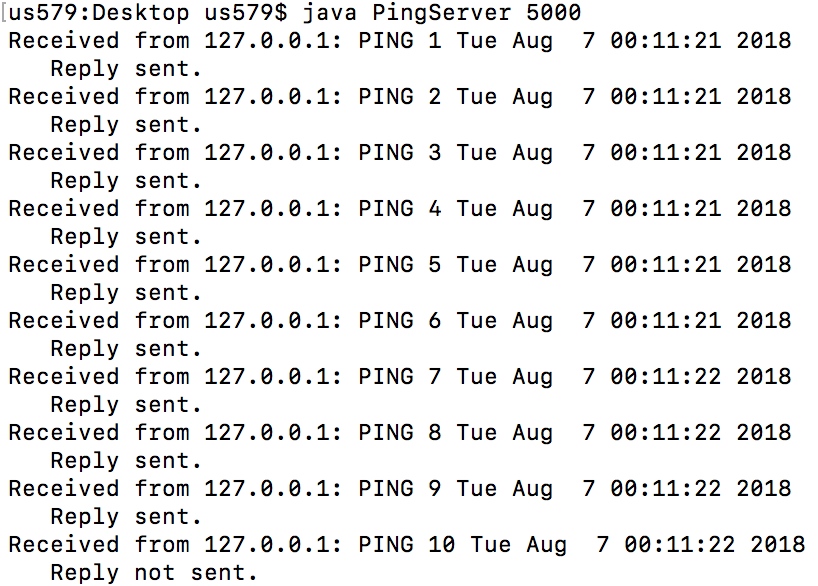
It is used to match the value of previous etag value, if the ETag values do not match, meaning the resource has likely changed, then a full response including the resource's content is returned,and if it match,then the server may send back a very short response with a [HTTP 304 Not Modified](https://en.wikipedia.org/wiki/HTTP_304) status. The 304 status tells the client that its cached version is still good and that it should use that.

The value didn’t change.

(\*) Exercise 5: Ping Client

Server

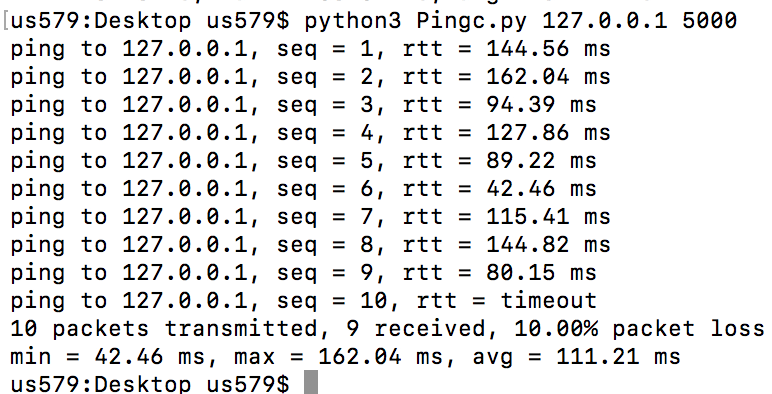
Port = 5000



Client

Host = local host 127.0.0.1

Port = 5000



For the client, I use python and the code is below.

