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?

Answer:

The status code is 200 and the phrase is 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?

Answer:

Last modified on Tuesday, 23 September 2003 at 05:29:00 GMT.

It contains a DATE header. DATE is the time when the HTTP response is created, the Last modified time is almost same as the DATE, which is very likely that the server set the time as the last modify time when the response message is generated.

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

Answer:

Persistent. Because the connection status is keep-alive.

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

Answer:

73 bytes of content are being returned to the browser.

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

Answer:

The data contained inside the HTTP with the following content:

```
<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?

Answer:

No. It does not have an "IF-MODIFIED-SINCE" line in the HTTP GET.

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

Answer:

Yes, the last modified on Tuesday, 23 September 2003 at 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?

Answer:

I see an "IF-MODIFIED-SINCE:" and "IF-NONE-MATCH" lines in the HTTP GET.

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

Answer:

Status code: 304

Phrase: Not Modified

The server doesn't return the contents of file. This code returned to the client when the cached copy of a particular file is up to date with the server. And the server This means that the page hasn't been modified by the server and the client can use the cached version.

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 1st response message was received?

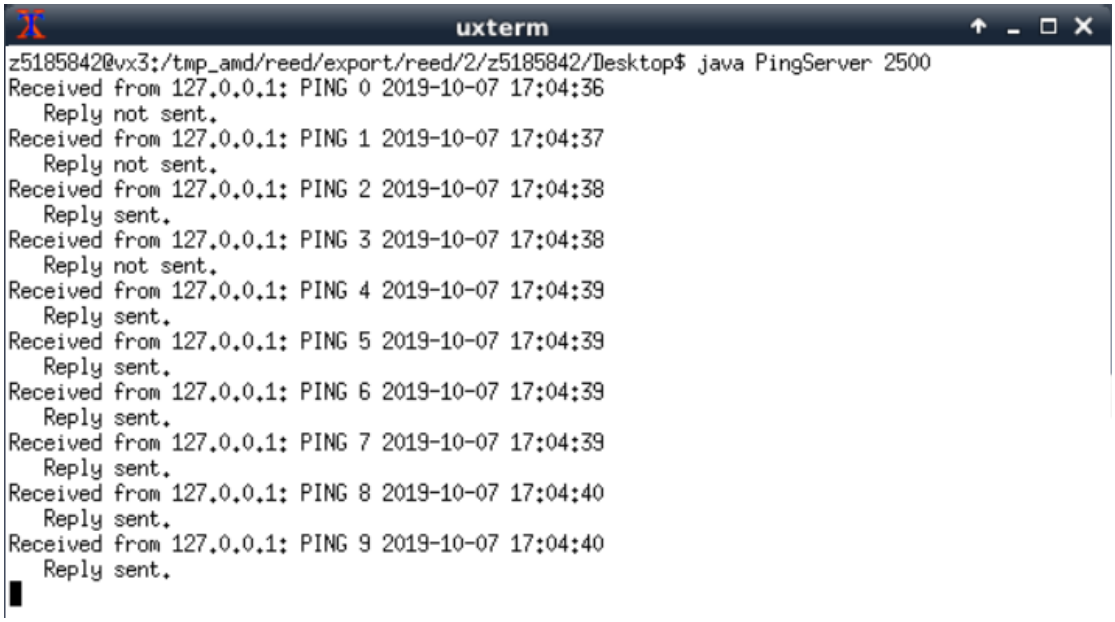
Answer:

ETag: "1bfef-173-8f4ae900"

No. The Etag won't change if the file has not been modified, it can quickly determine whether two representations of a resource are the same(is modified). If the content is not modified, it will retrieve the locally cached resource. Otherwise, the client will contact the server and send its previously-saved copy of the ETag along with the request in an "If-None-Match" field.

Exercise 5: Ping Client

Server:



Client: