Student Number: z5148637

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 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?

- The HTML file was last modified on Tue, 23 Sep 2003 05:29:00 GMT.
- The response does contain a date header: Date: Tue, 23 Sep 2003 05:29:50 GMT
- DATE header indicates the time when the HTTP response message was actually generated by the server. Last-modified is the last modified time for the requested object.

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

- The connection established between the browser and the server is persistent.
- In both the HTTP request and response headers, we can see that the connection field is “Keep-Alive”, which means using a single TCP connection to send and receive multiple HTTP requests / responses. This is by default on HTTP 1.1.

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

- 73 bytes of content are being returned to the browser.

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

- The file returned to the browser is an HTML file with the following content:

```
<html>
Congratulations.  You've downloaded the file lab2-1.html!
</html>
```

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, there is no "IF-MODIFIED-SINCE" line in the first HTTP GET request. This maybe because this is the first time that the browser is requesting this.

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

- The response indicates that: 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?

- In second HTTP GET request, there is "If-Modified-Since" and "IF-None-Match" lines.
- The contents are:

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

- The status code is 304 and phrase is Not Modified.
- The server did not return the body contents of the file. This is due to the fact that the GET request is only conditional. The server will only send back the request resource if only it has been last modified after a given date. If the request has not been modified since, the response will be 304 status without any body. So, the server does not respond back with the requested file. And the browser can simply display the caching version of this 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 1st response message was received?

- The entity tag (Tag) value is "1bfef-173-8f4ae900".
- It is used with "If-None-Match" header field and used by HTTP for cache validation.
- The Etag value has not changed since the 1st response message was received. This shows that the content has not been modified and the locally cached version of this file can be used.