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?

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT

Yes, the DATE header is:

Date: Tue, 23 Sep 2003 05:29:50 GMT

The DATE header shows when this message is created, while Last-Modified header indicates when the content is lately modified.

Question 3

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

It's persistent, because the connection headers is keep-alive:

Connection: keep-alive

If the connection type is keep-alive, the connection would not be closed after the request, this allows the connection to be persistent.

Question 4

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

73 Bytes

Question 5

What is the data contained inside the HTTP response packet?

The response is Line-based HTML text file:

<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

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, It's:

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, it contains both, they are:

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

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

IF-MODIFIED-SINCE indicates when is the resource lately modified and IF-NONE-MATCH is an identification hash key to determine whether it is modified.

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 didn't explicitly return the content, because the content is not modified since last get request, so the client can directly use the cached one. This can help to reduce the traffic load.

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 value of the Etag filed is:

ETag: "1bfef-173-8f4ae900". Etag is used to be compare with the value in IF-NONE-MATCH field to validate that the resource in the client cache is the latest version. Then client may choose to keep a copy of Etag for specific resource when caching it.

It is the same as the value in the 1st response message.

Exercise 5: Ping Client

```
z5183946@wagner:~/9331/lab2$ python3 PingClient.py 127.0.0.1 10086
ping to 127.0.0.1, seq = 1, rtt = 57 ms
ping to 127.0.0.1, seq = 2, time out
ping to 127.0.0.1, seq = 3, rtt = 12 ms
ping to 127.0.0.1, seq = 4, rtt = 27 ms
ping to 127.0.0.1, seq = 5, rtt = 165 ms
ping to 127.0.0.1, seq = 6, time out
ping to 127.0.0.1, seq = 7, rtt = 143 ms
ping to 127.0.0.1, seq = 8, rtt = 178 ms
ping to 127.0.0.1, seq = 9, rtt = 67 ms
ping to 127.0.0.1, seq = 10, rtt = 150 ms
ping to 127.0.0.1, seq = 11, rtt = 150 ms
ping to 127.0.0.1, seq = 12, rtt = 27 ms
ping to 127.0.0.1, seq = 13, time out
ping to 127.0.0.1, seq = 14, rtt = 9 ms
ping to 127.0.0.1, seq = 15, rtt = 19 ms
Packages: Sent=15, Received=12, Lost=3 (20% lost)
Minimum RTT is:9 ms
Maximum RTT is:178 ms
Average RTT is:83 ms
```

This is the output of PingClient function written in python, and the output from server side is attached below.

```
z5183946@wagner:~/9331/lab2$ java PingServer 10086
Received from 127.0.0.1: PING 3331
   Reply sent.
Received from 127.0.0.1: PING 3332
   Reply not sent.
Received from 127.0.0.1: PING 3333
   Reply sent.
Received from 127.0.0.1: PING 3334
   Reply sent.
Received from 127.0.0.1: PING 3335
   Reply sent.
Received from 127.0.0.1: PING 3336
   Reply not sent.
Received from 127.0.0.1: PING 3337
   Reply sent.
Received from 127.0.0.1: PING 3338
   Reply sent.
Received from 127.0.0.1: PING 3339
   Reply sent.
Received from 127.0.0.1: PING 3340
   Reply sent.
Received from 127.0.0.1: PING 3341
   Reply sent.
Received from 127.0.0.1: PING 3342
   Reply sent.
Received from 127.0.0.1: PING 3343
   Reply not sent.
Received from 127.0.0.1: PING 3344
   Reply sent.
Received from 127.0.0.1: PING 3345
   Reply sent.
```