Computer Network 1

LAB 2

Wireshark LAB HTTP

Student Name: Alexandre Rousseau

Student ID: 1952001

I. The Basic HTTP GET/response interaction

1) Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

```
Request URI: /Wireshark_TCP.pdf
Request Version: HTTP/1.1
```

The Brower is running HTTP 1.1 and the server is running

2) What languages (if any) does your browser indicate that it can accept to the server?

```
Accept-Language: fr,en-US;q=0.9,en;q=0.8,vi;q=0.7\r\n
\r\n
```

It indicates that it can accept an en-US (English) language and FR language (French)

3) What is the IP address of your computer? Of the gaia.cs.umass.edu server?

```
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 202.9.85.68
```

The IP of my computer is 192.168.1.111 and the server IP is 202.9.85.68

4) What is the status code returned from the server to your browser?

200 OK is the status code returned to the browser.

5) When was the HTML file that you are retrieving last modified at the server?

```
If-Modified-Since: Fri, 15 Oct 2021 05:59:01 GMT\r\n
\r\n
```

It was last modified on October 15, 2021, at 05:59:01

6) How many bytes of content are being returned to your browser?

128 bytes is being returned to the browser.

7) By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, I don't see any in the HTTP Message below.

II. The HTTP conditional GET/response interaction

8) Inspect the contents of the first HTTP GET request from your 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.

9) Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes, the server did return the contents of the file as there is a "Line-based text data" Line and under it is the text.

10) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?

```
If-None-Match: "80-5ce5de452c151"\r\n
If-Modified-Since: Fri, 15 Oct 2021 05:59:01 GMT\r\n
\r\n
```

Yes, there is an "IF-MODIFIED-SINCE" line in the second GET request and it follows with a date of Friday October 15, 2021, 05:59:01

11) 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 Not Modified and this time it did not return the contents of the file. The reason is that since the was not modified there is no new content that needs to be passed and so there is no need to download the file again.

III. Retrieving Long Documents

12) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

Just one request message was sent by the browser. The packets number in the trace contains the GET message for the Bill or Rights is 8.

13) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

The packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request is 10.

14) What is the status code and phrase in the response?

The status code is 200 OK.

15) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Three packets (10, 11, 13 in the trace).

IV. HTML Documents with Embedded Objects

16) How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

There were three HTTP GET messages sent: packet 10 in the trace (to get the base file), packet 17 (to get the Pearson logo) and packet 20 (to get the textbook cover).

17) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain

The downloads occurred in parallel. Note that the two GET messages for the images are in packets 17 and 20. The 200OK reply containing the images sew up as packets 25, and 54. Thus the request for the second image file (packet 20) was made BEFORE packet 25, the first image file was received.

V. HTTP Authentication

18) What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Packet 6 in the trace contains the first GET and packet 9 contains the REPLY. The servers in packet 9 is: 401 Authorization Required.

19) When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The HTTP GET includes the Authorization: Basic: field.