Paul Williams Diaz
CIS 151

Sept. 16, 2011
Prof. Brown

Wireshark Lab 2 :HTTP

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

   Answer: My browser is running HTTP version 1.1. The server is running HTTP version 1.1 as well.

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

   Answer: `Accept-Language: en-us,en; q=0.5\r\n.` Therefore the language is English-US.

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

   Answer: My IP address is 192.168.1.101 and gaia.cs.umass.edu server is 208.122.62.226.

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

   Answer: My status code in my browser from the server is `HTTP/1.1 200 OK\r\n`

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

   Answer: `Last-Modified: Wed, 14 Sept 2011 01:04:03 GMT\r\n`

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

   Answer: `Content-Length :133\r\n`
   `\r\n`
   `Content-encoded entity body (gzip): 133 bytes`
   Therefore there are 133 bytes returned in my browser.

7. By inspecting 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.

   Answer: None. In packet-content window, it only displays the contents of the captured frame in ASCII and hexadecimal format.

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?

   Answer: No, not in the first line but in second HTTP GET there is a line “IF-MODIFIED-SINCE”.

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

   Answer: Yes, the server provided the data which is a text/html from the `Content-Type`, and also provided the `Content Length` which is `371\r\n`. So, from these information, we will know that a file was sent.

10. Now inspects 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?

    Answer: Yes. `IF-MODIFIED-SINCE: Wed, 14 Sept 2011 02:12.01 GMT\r\n.` Followed by the date and time of the modified previous file requested. Below is `IF-NONE-MATCH: “d6c96-173-7b20880”\r\n.`

11. What is the HTTP status code and the phrase returned from the server in the response to this HTTP GET? Did the server explicitly return the contents of the file? Explain.

    Answer: The HTTP status code and phrase in response to the second GET is...

    ```
    Request Version:HTTP/1.1
    Status Code: 404
    Response Phrase: Not Found
    ```

    My browser’s cache was stored in my computer temporarily, since I clicked the “refresh button”, the server is not going to return the contents of the file anymore as it is available in my computer temporarily (and that is what web caches are for).

12. How many HTTP GET request messages were sent by your browser?

    Answer: There is only one HTTP GET message that my browser sent which is the `GET /wireshark-labs/HTTP-wireshark-file3.html HTTP 1.1`

13. How many data containing TCP segments were needed to carry the single HTTP response?

    Answer: There are 4 segments of TCP that were needed to carry the HTTP response. They are `#143(1452), #144(1452), #147(1452) and #148(447)`

14. What is the status code and phrase associated with the response to the HTTP GET request?

Answer: The status code and phrase associated with the response to the HTTP GET request is `Status Code : 200`
`Response Phrase: OK`

15. Are there any HTTP status lines in the transmitted data associated with a TCP-induced "Continuation"?

Answer: Yes. According to the listing of packets captured there are 4 `55 continuation or non-HTTP traffic[Malformed Packet]` appeared.

16. How many HTTP GET request messages were sent by your browser? To which Internet address were these GET request sent?

Answer: There are 3 HTTP GET request messages were sent by my browser. It was sent to the following Internet addresses 1. 128.119.240.90
2. 165.193.140.14
3. 128.119.245.12

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.

Answer: In parallel download, multiple segments are being downloaded. In serial, bits by bits are downloaded one at a time. All of the 3 HTTP GET were OKed with the SAME TIME which is...
`Date: Fri, 16, Sept 2011 18:42:11 GMT\r\n.`
Therefore, images are downloaded parallel.

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

Answer: The server response is `Status Code: 401`
`Response Phrase: Authentication Required`

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

Answer: The new field included in the HTTP GET message is

```
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRZOm51dHdvcms=\r\n
```