Warren Quattrocchi
CSC 138

Lab 2- wireshark HTTP

Part 1)

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

They are both using HTTP 1.1

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

en-US

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

My computer: 192.168.0.15
gaia.cs.umass.edu: 128.119.245.12

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

200

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

Sat, 23 Feb 2019 06:59:01 GMT

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

128 bytes

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.

They are all displayed

```
No.    Time                  Source              Destination        Protocol    Length      Info
245 16:25:06.197145    192.168.0.15         128.119.245.12       HTTP     480    GET /wireshark-
labs/HTTP-wireshark-file1.html HTTP/1.1
248 16:25:06.321223    128.119.245.12        192.168.0.15        HTTP     540    HTTP/1.1 200 OK
(text/html)
```

Part 2)

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

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

Yes, the HTTP 200 OK response

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?

Yes, The time at which I last visited the website

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.

304 Not Modified, no it did not explicitly return the contents, as it was already cached from the first visit, and hadn't yet been updated.

Part 3)

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?

One
Packet 9

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

Packet 15

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

200 OK

15.How many data-containing TCP segments were needed tocarry the single HTTP response and the text of theBill of Rights?

4 TCP segments

```
No.    Time              Source            Destination       Protocol  Length          Info
4 17:11:04.603423    192.168.0.15        128.119.245.12       TCP      66     60887 → 80 [SYN] Seq=0
Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
6 17:11:04.727155    128.119.245.12       192.168.0.15        TCP      66     80 → 60887 [SYN, ACK]
Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
8 17:11:04.727258    192.168.0.15        128.119.245.12       TCP      54     60887 → 80 [ACK] Seq=1
Ack=1 Win=65536 Len=0
9 17:11:04.727358    192.168.0.15        128.119.245.12       HTTP     480    GET /wireshark-
labs/HTTP-wireshark-file3.html HTTP/1.1
11 17:11:04.860201    128.119.245.12       192.168.0.15        TCP      56     80 → 60887 [ACK] Seq=1
Ack=427 Win=30336 Len=0
12 17:11:04.864271    128.119.245.12       192.168.0.15        TCP      1514   80 → 60887 [ACK]
Seq=1 Ack=427 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
13 17:11:04.864272    128.119.245.12       192.168.0.15        TCP      1514   80 → 60887 [ACK]
Seq=1461 Ack=427 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
14 17:11:04.864275    128.119.245.12       192.168.0.15        TCP      1514   80 → 60887 [ACK]
Seq=2921 Ack=427 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
15 17:11:04.864276    128.119.245.12       192.168.0.15        HTTP     535    HTTP/1.1 200 OK
(text/html)     16 17:11:04.864309    192.168.0.15
```

Part 4)

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

Three
first two sent to: gaia.cs.umass.edu
third sent to: manic.cs.umass.edu

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.

Serially, the second GET request for the second image was sent until after the first image finished downloading

part 5)

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

401 Unauthorized

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 Authorization field, with the username and password entered encoded as a string of characters in Base64 format

```
No.    Time                 Source             Destination         Protocol  Length          Info
20 17:34:57.429094    192.168.0.15         128.119.245.12       HTTP     496    GET /wireshark-
labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
24 17:34:57.550696    128.119.245.12        192.168.0.15        HTTP     771    HTTP/1.1 401
Unauthorized  (text/html)
26 17:34:58.025416    192.168.0.15         128.119.245.12       HTTP     523    GET /wireshark-
labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
27 17:34:58.137927    128.119.245.12        192.168.0.15        HTTP     770    HTTP/1.1 401
Unauthorized  (text/html)
408 17:35:43.435322    192.168.0.15         128.119.245.12       HTTP     555    GET /wireshark-
labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
411 17:35:43.577951    128.119.245.12        192.168.0.15        HTTP     544    HTTP/1.1 200 OK
(text/html)
```