Alexandru Seremet
WireShark Lab2
3/17/2019

Wireshark Report Lab 2

1. The Basic HTTP GET/response interaction

GET Report

```
      /home/aser1206/CSCClasses/CSC138/WireShark/getRepLab2.pcapng 34 total packets, 4
shown
No.    Time                              Source          Destination       Protocol Length Info
14  2019-03-17 12:05:37.159987097 192.168.0.24  128.119.245.12   HTTP     423     GET
/wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 14: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface 0
Ethernet II, Src: LiteonTe_c6:fb:39 (98:22:ef:c6:fb:39), Dst: ArrisGro_92:4e:ca
(d4:0a:a9:92:4e:ca)
Internet Protocol Version 4, Src: 192.168.0.24, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 48426, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
Hypertext Transfer Protocol
      GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Language: en-US,en;q=0.5\r\n
      Accept-Encoding: gzip, deflate\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
      [HTTP request 1/2]
      [Response in frame: 16]
      [Next request in frame: 18]
```

OK Report

```
      /home/aser1206/CSCClasses/CSC138/WireShark/getRepLab2.pcapng 34 total packets, 4
shown
No.   Time                              Source             Destination     Protocol Length Info
16   2019-03-17 12:05:37.249655549 128.119.245.12    192.168.0.24   HTTP   552       HTTP/1.1
200 OK
Frame 16: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface 0
Ethernet II, Src: ArrisGro_92:4e:ca (d4:0a:a9:92:4e:ca), Dst: LiteonTe_c6:fb:39
(98:22:ef:c6:fb:39)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.24
Transmission Control Protocol, Src Port: 80, Dst Port: 48426, Seq: 1, Ack: 358, Len: 486
Hypertext Transfer Protocol
      HTTP/1.1 200 OK\r\n
      Date: Sun, 17 Mar 2019 19:05:37 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10
      Perl/v5.16.3\r\n
      Last-Modified: Sun, 17 Mar 2019 05:59:02 GMT\r\n
      ETag: "80-58443f80117c8"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 128\r\n
      Keep-Alive: timeout=5, max=100\r\n
```

```
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.089668452 seconds]
    [Request in frame: 14]
    [Next request in frame: 18]
    [Next response in frame: 20]
    File Data: 128 bytes
    Line-based text data: text/html (4 lines)
```

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

Browser Runs HTTP 1.1 (GET Report)

Server is running HTTP 1.1 (OK Report)

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

Accept-Language: en-US,en;q=0.5\r\n

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

My computer IP 192.168.0.24 Server IP 128.119.245.12

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

200 OK

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

Last-Modified: Sun, 17Mar 2019 19:05:37 GMT

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

Content-Length: 128

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, all headers are displayed.

2. The HTTP CONDITIONAL GET/response interaction

```
No.     Time                           Source               Destination          Protocol Length Info
     14 2019-03-17 14:08:22.571084958 192.168.0.24          128.119.245.12        HTTP      423    GET
/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 14: 423 bytes on wire (3384 bits), 423 bytes captured (3384 bits) on interface 0
Ethernet II, Src: LiteonTe_c6:fb:39 (98:22:ef:c6:fb:39), Dst: ArrisGro_92:4e:ca
(d4:0a:a9:92:4e:ca)
Internet Protocol Version 4, Src: 192.168.0.24, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 48770, Dst Port: 80, Seq: 1, Ack: 1, Len: 357
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
    [HTTP request 1/1]
    [Response in frame: 16]

No.     Time                           Source                Destination           Protocol Length Info
     16 2019-03-17 14:08:22.664191294 128.119.245.12        192.168.0.24          HTTP     796
HTTP/1.1 200 OK  (text/html)

Frame 16: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface 0
Ethernet II, Src: ArrisGro_92:4e:ca (d4:0a:a9:92:4e:ca), Dst: LiteonTe_c6:fb:39
(98:22:ef:c6:fb:39)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.24
Transmission Control Protocol, Src Port: 80, Dst Port: 48770, Seq: 1, Ack: 358, Len: 730
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 17 Mar 2019 21:08:22 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10
Perl/v5.16.3\r\n
    Last-Modified: Sun, 17 Mar 2019 05:59:02 GMT\r\n
    ETag: "173-58443f8010c10"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.093106336 seconds]
    [Request in frame: 14]
    File Data: 371 bytes
Line-based text data: text/html (10 lines)

No.     Time                           Source                Destination           Protocol Length Info
     30 2019-03-17 14:08:39.639700824 192.168.0.24          128.119.245.12        HTTP     535    GET
/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Frame 30: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
Ethernet II, Src: LiteonTe_c6:fb:39 (98:22:ef:c6:fb:39), Dst: ArrisGro_92:4e:ca
(d4:0a:a9:92:4e:ca)
Internet Protocol Version 4, Src: 192.168.0.24, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 48772, Dst Port: 80, Seq: 1, Ack: 1, Len: 469
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Sun, 17 Mar 2019 05:59:02 GMT\r\n
    If-None-Match: "173-58443f8010c10"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 33]

No.     Time                           Source                Destination           Protocol Length Info
     33 2019-03-17 14:08:39.728867229 128.119.245.12        192.168.0.24          HTTP     306
HTTP/1.1 304 Not Modified

Frame 33: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface 0
Ethernet II, Src: ArrisGro_92:4e:ca (d4:0a:a9:92:4e:ca), Dst: LiteonTe_c6:fb:39
(98:22:ef:c6:fb:39)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.24
Transmission Control Protocol, Src Port: 80, Dst Port: 48772, Seq: 1, Ack: 470, Len: 240
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 17 Mar 2019 21:08:39 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10
Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-58443f8010c10"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.089166405 seconds]
    [Request in frame: 30]
```

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. *Line-based text data: text/html (10 lines)*

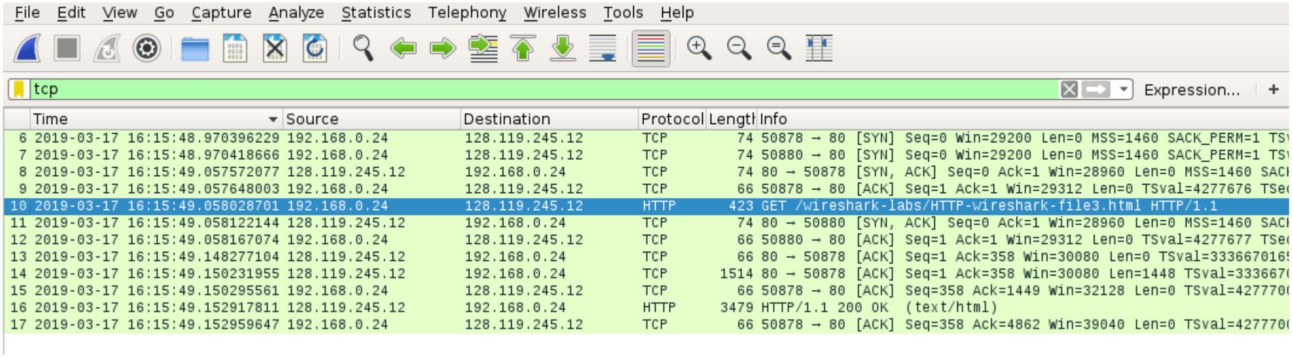
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Yes. *Sun, 17 Mar 2019 05:59:02 GMT\r\n* which is the date of last modification.

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.

HTTP/1.1 304 Not Modified. Nothing returned from the since there are no modifications, so browser loaded the information from its cache

3. Retrieving Long Documents


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

tcp

	Time	Source	Destination	Protocol	Lengtl	Info
6	2019-03-17 16:15:48.970396229	192.168.0.24	128.119.245.12	TCP	74	50878 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
7	2019-03-17 16:15:48.970418666	192.168.0.24	128.119.245.12	TCP	74	50880 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
8	2019-03-17 16:15:49.057572077	128.119.245.12	192.168.0.24	TCP	74	80 → 50878 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SAC
9	2019-03-17 16:15:49.057648003	192.168.0.24	128.119.245.12	TCP	66	50878 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4277676 TSe
10	2019-03-17 16:15:49.058028701	192.168.0.24	128.119.245.12	HTTP	423	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
11	2019-03-17 16:15:49.058122144	128.119.245.12	192.168.0.24	TCP	74	80 → 50880 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SAC
12	2019-03-17 16:15:49.058167074	192.168.0.24	128.119.245.12	TCP	66	50880 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=4277677 TSe
13	2019-03-17 16:15:49.148277104	128.119.245.12	192.168.0.24	TCP	66	80 → 50878 [ACK] Seq=1 Ack=358 Win=30080 Len=0 TSval=33367016
14	2019-03-17 16:15:49.150231955	128.119.245.12	192.168.0.24	TCP	1514	80 → 50878 [ACK] Seq=1 Ack=358 Win=30080 Len=1448 TSval=333667
15	2019-03-17 16:15:49.150295561	192.168.0.24	128.119.245.12	TCP	66	50878 → 80 [ACK] Seq=358 Ack=1449 Win=32128 Len=0 TSval=427770
16	2019-03-17 16:15:49.152917811	128.119.245.12	192.168.0.24	HTTP	3479	HTTP/1.1 200 OK (text/html)
17	2019-03-17 16:15:49.152959647	192.168.0.24	128.119.245.12	TCP	66	50878 → 80 [ACK] Seq=358 Ack=4862 Win=39040 Len=0 TSval=427770

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?

Browser requested only one GET. The Get message is in packet 10

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

Packet 16

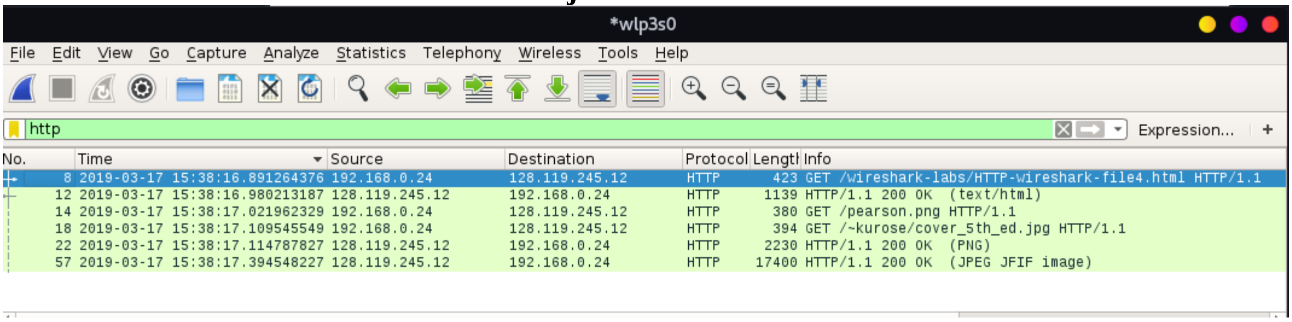
14. What is the status code and phrase in the response?

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?

only 3 packets were needed

4. HTML Documents with Embedded Objects


*wlp3s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
8	2019-03-17 15:38:16.891264376	192.168.0.24	128.119.245.12	HTTP	423	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
12	2019-03-17 15:38:16.980213187	128.119.245.12	192.168.0.24	HTTP	1139	HTTP/1.1 200 OK (text/html)
14	2019-03-17 15:38:17.021962329	192.168.0.24	128.119.245.12	HTTP	380	GET /pearson.png HTTP/1.1
18	2019-03-17 15:38:17.109545549	192.168.0.24	128.119.245.12	HTTP	394	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
22	2019-03-17 15:38:17.114787827	128.119.245.12	192.168.0.24	HTTP	2230	HTTP/1.1 200 OK (PNG)
57	2019-03-17 15:38:17.394548227	128.119.245.12	192.168.0.24	HTTP	17400	HTTP/1.1 200 OK (JPEG JFIF image)

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

3 Gets from

a.http://gaia.cs.umass.edu/pearson.png

b.http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

c.http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg

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.

Based on the GET and OK time stamps looks like the messages were downloaded in parallel. The browser did not wait for the first site to respond but initiated another request to the second website.

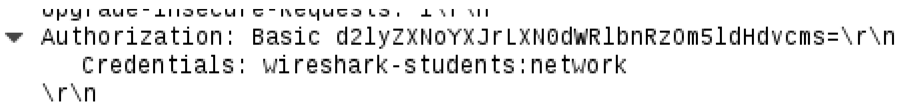
5 HTTP Authentication

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?

Authorization :



```
  Upgrade-Insecure-Requests: 1\r\n
▼ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
      Credentials: wireshark-students:network
  \r\n
```