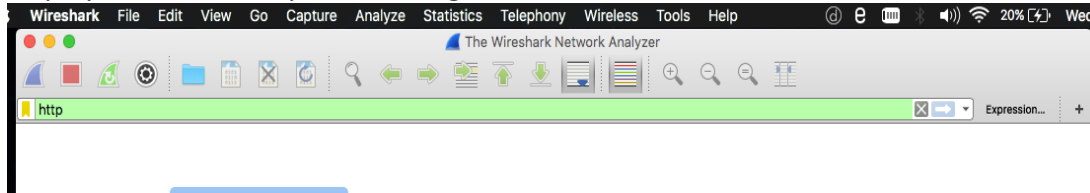
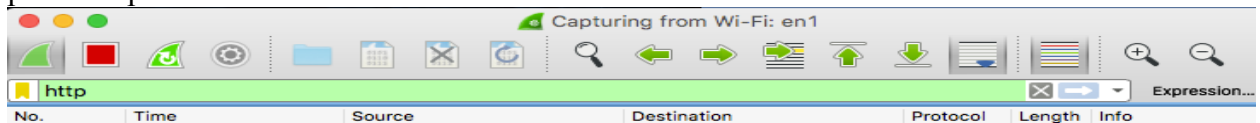


Lab 2 – Wireshark- HTTP

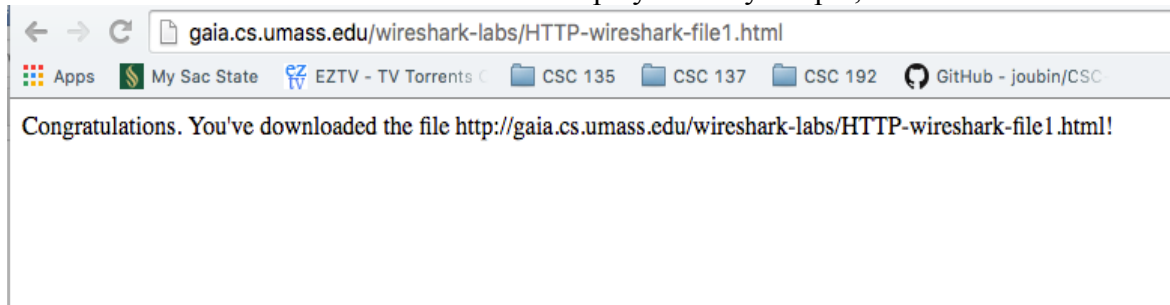
1. Start up your web browser – done.
2. Start up the Wireshark packet sniffer, as described in the introductory lab. Enter “http” in the display-filter-specification windows, so that only captured HTTP messages will be displayed later in the packet-listing window.



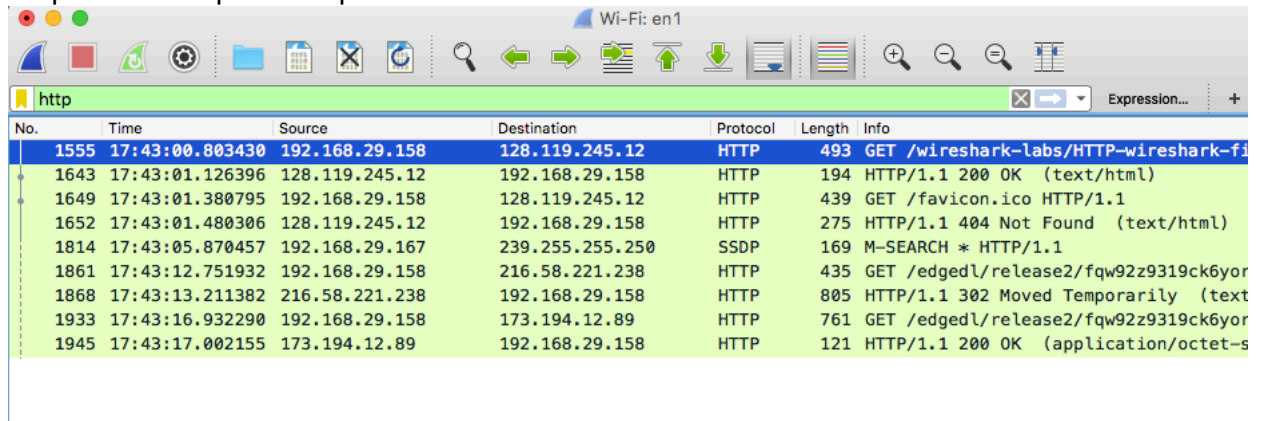
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.



4. Enter the following to your browser <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html> Your browser should display the very simple, one-line HTML file.



5. Stop Wireshark packet capture. - done



No.	Time	Source	Destination	Protocol	Length	Info
1555	17:43:00.803430	192.168.29.158	128.119.245.12	HTTP	493	GET /wireshark-labs/HTTP-wireshark-fi
1643	17:43:01.126396	128.119.245.12	192.168.29.158	HTTP	194	HTTP/1.1 200 OK (text/html)
1649	17:43:01.380795	192.168.29.158	128.119.245.12	HTTP	439	GET /favicon.ico HTTP/1.1
1652	17:43:01.480306	128.119.245.12	192.168.29.158	HTTP	275	HTTP/1.1 404 Not Found (text/html)
1814	17:43:05.870457	192.168.29.167	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
1861	17:43:12.751932	192.168.29.158	216.58.221.238	HTTP	435	GET /edgedl/release2/fqw92z9319ck6yor
1868	17:43:13.211382	216.58.221.238	192.168.29.158	HTTP	805	HTTP/1.1 302 Moved Temporarily (text
1933	17:43:16.932290	192.168.29.158	173.194.12.89	HTTP	761	GET /edgedl/release2/fqw92z9319ck6yor
1945	17:43:17.002155	173.194.12.89	192.168.29.158	HTTP	121	HTTP/1.1 200 OK (application/octet-s

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

- a. The browser is running HTTP version 1.1.

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
```

- b. The server is running HTTP version 1.1.

```
▼ Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Request Version: HTTP/1.1
    Status Code: 200
    Response Phrase: OK
```

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

- a. Accepted language is: en-US, en; q=0.8\r\n

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, l
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate, sdch\r\n
    Accept-Language: en-US,en;q=0.8\r\n
```

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

- a. IP address of computer is: 192.168.29.158
- b. IP address of gaia.cs.umass.edu server is: 128.119.245.12

► Header checksum: 0xe3f5 [validation disabled]

Source: 192.168.29.158

Destination: 128.119.245.12

[Source GeoIP: Unknown]

[Destination GeoIP: Unknown]

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

- a. The status code returned from the server to the browser is 200.

Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

► [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Request Version: HTTP/1.1

Status Code: 200

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

- a. The HTML file that is being retrieved was last modified at the server on

Date: Thu, 30 Jun 2016 00:43:01 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16

Last-Modified: Wed, 29 Jun 2016 05:59:01 GMT\r\n

ETag: "80-53664733ac6c5"\r\n

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

- a. 128 bytes are being returned to the browser.

Accept-Ranges: bytes\r\n

► Content-Length: 128\r\n

Content-Type: text/html; charset=UTF-8\r\n

12. 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.

- a. No, I do not see any headers within the data that are not displayed in the packet-listing windows.

13. 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?

- a. There is no IF-Modified-Since line in the first HTTP GET request.

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

- a. The server did explicitly return the contents of the file. The content is returned as Line-based text data.

```
▼ Line-based text data: text/html
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

15. 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

- a. An IF-MODIFIED-SINCE header appears in the second HTTP GET request. The information that follows the header is a date and time, Wed, 29 Jun 2016 05:59:01 GMT.

```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
If-None-Match: "173-53664733abb0d"\r\n
If-Modified-Since: Wed, 29 Jun 2016 05:59:01 GMT\r\n
\n
```

16. 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.

- a. Status code: 304 Not Modified. The file has not been modified, so the text of the file is not returned in the HTTP message.

```
Hypertext Transfer Protocol
▼ HTTP/1.1 304 Not Modified\r\n
  ▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    [HTTP/1.1 304 Not Modified\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 304
    Response Phrase: Not Modified
    Date: Thu, 30 Jun 2016 01:35:09 GMT\r\n
```

17. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

- a. Browser sends 1 GET request message.

- b. Packet number 8 in the trace contains the GET message for the bill of rights.

187	12:44:42.915091	10.117.145.119	128.119.245.12	HTTP	434 GET /wireshark-labs/HTTP-wires...
192	12:44:43.014875	128.119.245.12	10.117.145.119	HTTP	807 HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol					
Line-based text data: text/html					
<html><head> \n					
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n					
\n					
\n					
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n					
<p> \n					
</p>\n					
<p></p><center>THE BILL OF RIGHTS \n					
Amendments 1-10 of the Constitution\n					
</center>\n					
0170	3e 3c 68 65 61 64 3e 20	0a 3c 74 69 74 6c 65 3e	><head> .<title>		
0180	48 69 73 74 6f 72 69 63	61 6c 20 44 6f 63 75 6d	Historic al Docum		
0190	65 6e 74 73 3a 54 48 45	20 42 49 4c 4c 20 4f 46	ents:THE BILL OF		
01a0	20 52 49 47 48 54 53 3c	2f 74 69 74 6c 65 3e 3c	RIGHTS< /title><		
01b0	2f 68 65 61 64 3e 0a 0a	0a 3c 62 6f 64 79 20 62	/head>..<body b		

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

- a. Packet number 10 contains the status code and phrase associated with the response to the HTTP GET request.

0000	48 54 54 50 2f 31 2e 31	20 32 30 30 20 4f 4b 0d	HTTP/1.1 200 OK.
0010	0a 44 61 74 65 3a 20 54	68 75 2c 20 33 30 20 4a	.Date: T hu, 30 J

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

- a. Status code: 200
b. Phrase: OK

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

- a. Three packets needed to carry the single HTTP response and the text of the Bill of Rights, packets 10, 11, and 13.

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

- a. The browser sent 3 HTTP GET messages.
b. The addresses that the GET requests were sent to are: 128.119.245.12, 23.37.235.112, and 128.119.240.90

68	13:05:49.626715	10.117.145.119	128.119.245.12	HTTP	434 GET /wireshark-labs/HTTP-wireshark...
70	13:05:49.723126	128.119.245.12	10.117.145.119	HTTP	1168 HTTP/1.1 200 OK (text/html)
78	13:05:49.758100	10.117.145.119	23.37.235.112	HTTP	476 GET /assets/hip/us/hip_us_pearsonh...
80	13:05:49.766526	23.37.235.112	10.117.145.119	HTTP	305 HTTP/1.1 301 Moved Permanently
95	13:05:49.880789	10.117.145.119	128.119.240.90	HTTP	435 GET /~kurose/cover_5th_ed.jpg HTTP...
100	13:05:49.977027	128.119.240.90	10.117.145.119	HTTP	522 HTTP/1.1 302 Found (text/html)
111	13:05:50.077594	10.117.145.119	128.119.240.90	HTTP	435 GET /~kurose/cover_5th_ed.jpg HTTP...
252	13:05:50.657254	128.119.240.90	10.117.145.119	HTTP	976 HTTP/1.1 200 OK (JPEG JFIF image)

Frame 95: 435 bytes on wire (3480 bits): 435 bytes captured (3480 bits) on interface 0

22. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain
- Downloads occurred in parallel, the request for the second image file in packet 20 was made before the OK replay in packet 20 for the first image file was received.

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

- Servers response to the initial HTTP GET message is 401 Unauthorized.

81	13:21:41.513683	10.117.145.119	128.119.245.12	HTTP	449	GET /wireshark-labs/protected_pages/HTTP-wiresh...
83	13:21:41.613141	128.119.245.12	10.117.145.119	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
21	13:21:42.006799	10.117.145.119	128.119.245.12	HTTP	449	GET /wireshark-labs/protected_pages/HTTP-wiresh...
23	13:21:42.105862	128.119.245.12	10.117.145.119	HTTP	785	HTTP/1.1 401 Unauthorized (text/html)
25	13:21:42.125541	10.117.145.119	128.119.245.12	HTTP	449	GET /wireshark-labs/protected_pages/HTTP-wiresh...
26	13:21:42.221797	128.119.245.12	10.117.145.119	HTTP	784	HTTP/1.1 401 Unauthorized (text/html)
74	13:21:49.542130	10.117.145.119	128.119.245.12	HTTP	508	GET /wireshark-labs/protected_pages/HTTP-wiresh...
76	13:21:49.639449	128.119.245.12	10.117.145.119	HTTP	597	HTTP/1.1 404 Not Found (text/html)

24. 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 message should include the Authorization: Basic field and the credentials subfield in the second GET message.

```
GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n
Credentials: wireshark-students:network
```