

Lab2-Wireshark

Roll: 13 - 47

1.

No.	Time	Source	Destination	Protocol	Length	Info
93	0.000475	10.0.0.44	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	0.001546	128.119.245.12	10.0.0.44	HTTP	552	HTTP/1.1 200 OK (text/html)


```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Sat, 30 Jan 2021 21:43:30 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 30 Jan 2021 06:59:02 GMT
ETag: "80-5ba18a7e1c636"
Accept-Ranges: bytes
Content-Length: 128
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
Congratulations. You've downloaded the file
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!
</html>
```

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

Ans: 1.1, 1.1

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

Ans: en-GB, en-US, en, bn

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

Ans: PC: 10.0.0.44

Server: 128.119.245.12

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

Ans: 200 OK

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

Ans: Sat, 30 Jan 2021 21:43:30 GMT

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

Ans: 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.

Ans: Upgrade-Insecure-Requests: 1 (Here 1 means the browser prefers an upgrade, we need to replace them in HTTPS version)

2:

```
Date: Sat, 30 Jan 2021 18:19:53 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 30 Jan 2021 06:59:02 GMT
ETag: "173-5ba18a7e1ba7e"
Accept-Ranges: bytes
Content-Length: 371
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>

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

</html>
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
If-None-Match: "173-5ba18a7e1ba7e"
If-Modified-Since: Sat, 30 Jan 2021 06:59:02 GMT

HTTP/1.1 304 Not Modified
Date: Sat, 30 Jan 2021 18:19:56 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Connection: Keep-Alive
Keep-Alive: timeout=5, max=99
ETag: "173-5ba18a7e1ba7e"
```

No.	Time	Source	Destination	Protocol	Length	Info
56	0.000863	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
58	0.000391	128.119.245.12	10.0.0.44	HTTP	796	HTTP/1.1 200 OK (text/html)
555	0.424913	10.0.0.44	128.119.245.12	HTTP	659	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
556	0.022630	128.119.245.12	10.0.0.44	HTTP	305	HTTP/1.1 304 Not Modified

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?

Ans: NO, the browser does not when it was last modified

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

Ans : Yes, we are seeing the HTML content giving 200 OK

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 GET6? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans: Yes, **If-Modified-Since: Sat, 30 Jan 2021 06:59:02 GMT**

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

Ans: **HTTP/1.1 304 Not Modified**, browser did not return file contents because browser used it cache version to speed up and save browsing

3:

http					
No.	Time	Source	Destination	Protocol	Length Info
26	0.000540	10.0.0.44	128.119.245.12	HTTP	547 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
32	0.000004	128.119.245.12	10.0.0.44	HTTP	583 HTTP/1.1 200 OK (text/html)

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?

Ans: 1, 26

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

Ans: 32

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

Ans: **Status Code 200, Phase : OK**

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

tcp.len > 0						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.028843	10.0.0.44	157.240.220.16	TLSv1.2	114	Application Data
4	0.060423	10.0.0.44	157.240.220.16	TLSv1.2	98	Application Data
5	0.003072	157.240.220.16	10.0.0.44	TLSv1.2	96	Application Data
7	0.060070	157.240.220.16	10.0.0.44	TLSv1.2	96	Application Data
26	0.000540	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTT
28	0.000560	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=1
29	0.000004	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=14
31	0.000144	128.119.245.12	10.0.0.44	TCP	1514	80 → 54985 [ACK] Seq=28
32	0.000004	128.119.245.12	10.0.0.44	HTTP	583	HTTP/1.1 200 OK (text/
36	0.189662	10.0.0.44	157.240.220.16	TLSv1.2	120	Application Data
39	0.068846	157.240.220.16	10.0.0.44	TLSv1.2	96	Application Data
43	0.001652	10.0.0.44	18.224.239.181	TLSv1.2	979	Application Data
45	0.025256	18.224.239.181	10.0.0.44	TLSv1.2	407	Application Data
50	0.600228	10.0.0.44	157.240.220.16	TLSv1.2	116	Application Data
51	0.064836	157.240.220.16	10.0.0.44	TLSv1.2	96	Application Data
58	0.070255	10.0.0.44	157.240.220.16	TLSv1.2	98	Application Data
59	0.062995	157.240.220.16	10.0.0.44	TLSv1.2	96	Application Data

Ans: Three TCP segments

4:

http						
No.	Time	Source	Destination	Protocol	Length	Info
95	0.000311	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
97	0.000006	128.119.245.12	10.0.0.44	HTTP	1367	HTTP/1.1 200 OK (text/html)
99	0.023634	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
104	0.000004	128.119.245.12	10.0.0.44	HTTP	781	HTTP/1.1 200 OK (PNG)
118	0.000323	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
120	0.000323	178.79.137.164	10.0.0.44	HTTP	237	HTTP/1.1 301 Moved Permanently
144	0.000635	10.0.0.44	104.98.115.146	HTTP	361	GET /MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMXt1hWy65QCUDmH6%2BdixTCxgISBH7WwlyAN
155	0.006884	104.98.115.146	10.0.0.44	OCSP	955	Response

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

Length	Info
547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
493	GET /pearson.png HTTP/1.1
500	GET /8E_cover_small.jpg HTTP/1.1
361	GET /MFgwVqADAgEAME8wTTBLMAkGBSsOAwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%2BbPEBBQULrMXt1hWy65QCUDmH6%2BdixTCxgISBH7WwlyAN

Ans : 4,

128.119.245.1	gaia.cs.umass.edu
128.119.245.1	gaia.cs.umass.edu
178.79.137.16	kurose.cslash.net

104.98.115.14	r3.o.lencr.org
---------------	----------------

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.

No.	Time	Source	Destination	Protocol	Length	Info
95	0.000311	10.0.0.44	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
97	0.000006	128.119.245.12	10.0.0.44	HTTP	1367	HTTP/1.1 200 OK (text/html)
99	0.023634	10.0.0.44	128.119.245.12	HTTP	493	GET /pearson.png HTTP/1.1
104	0.000004	128.119.245.12	10.0.0.44	HTTP	781	HTTP/1.1 200 OK (PNG)
118	0.000323	10.0.0.44	178.79.137.164	HTTP	500	GET /8E_cover_small.jpg HTTP/1.1
120	0.000323	178.79.137.164	10.0.0.44	HTTP	237	HTTP/1.1 301 Moved Permanently
144	0.000635	10.0.0.44	104.98.115.146	HTTP	361	GET /MFgwVqADAgEAME8wTTBLMAkGBSs0AwIaBQAEFEjayaD7K9MtT%2FDeaNL1Z7c1%28bPEBBQULr
155	0.006884	104.98.115.146	10.0.0.44	OCSP	955	Response

Ans: The GET requests for `/pearson.png` (to 128.119.245.12) and `/8E_cover_small.jpg` (to 178.79.137.164) are sent within milliseconds of each other, close timing means there was no wait for one image to finish downloading before starting the next.

5:

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

No.	Time	Source	Destination	Protocol	Length	Info
92	0.000331	10.0.0.44	128.119.245.12	HTTP	563	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
94	0.003968	128.119.245.12	10.0.0.44	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
478	0.001309	10.0.0.44	128.119.245.12	HTTP	648	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
482	0.000001	128.119.245.12	10.0.0.44	HTTP	556	HTTP/1.1 200 OK (text/html)

```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML,
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 401 Unauthorized
Date: Sat, 30 Jan 2021 22:04:57 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16
WWW-Authenticate: Basic realm="wireshark-students only"
Content-Length: 381
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
```

Ans: 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?

```

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4398.95 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 401 Unauthorized
Date: Sat, 30 Jan 2021 22:04:57 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
WWW-Authenticate: Basic realm="wireshark-students only"
Content-Length: 381
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>

```

```

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmst
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4398.95 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

HTTP/1.1 200 OK
Date: Sat, 30 Jan 2021 22:05:12 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3
Last-Modified: Sat, 30 Jan 2021 06:59:02 GMT
ETag: "84-5ba18a7e1d5d6"
Accept-Ranges: bytes
Content-Length: 132
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<html>
<body>
<p>This page is password protected! If you're seeing this, you've downloaded the page correctly <br>
Congratulations!</p>
</body>
</html>

```

Input

d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmst

Output

wireshark-students:network

Ans: **Authorization** header appears in the second GET request allowing the browser to access the password-protected page.

