

lab2 Wireshark_HTTP

- 学号:1813075
- 姓名:刘茵

1.The Basic HTTP GET/response interaction

打印

```
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/86.0.4240.183 Safari/537.36 Edg/86.0.622.63\r\n
Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,;q=
0.8,application/signedexchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 5098]
```

```
HTTP/1.1 200 OK\r\n
Date: Wed, 11 Nov 2020 11:50:16 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11
Perl/v5.16.3\r\n
Last-Modified: Wed, 11 Nov 2020 06:59:02 GMT\r\n
ETag: "51-5b3cf549c4601"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 81\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: 0.275670000 seconds]
[Request in frame: 5053]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
File Data: 81 bytes
```

问题:

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

答: 都为HTTP 1.1

(HTTP/1.1 200 OK\r\n | GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n)

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

答: zh-CN | zh | en | en-GB | en-US

(Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n)

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

答: the Internet address of my computer 10.22.80.131

the Internet address of the gaia.cs.umass.edu 128.119.245.12

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

答: 200OK

(HTTP/1.1 200 OK\r\n)

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

答: Last-Modified: Wed, 11 Nov 2020 06:59:02 GMT

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

答: File Data: 81 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.

答: 没有

2.The HTTP CONDITIONAL GET/response interaction

```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.183 Safari/537.36 Edg/86.0.622.63\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
If-None-Match: "173-5b3cf549ef19d"\r\n
If-Modified-Since: Wed, 11 Nov 2020 06:59:02 GMT\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: 2016]
```

问题:

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?

答: 没看到

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

答: 显示返回了内容, 可以在实体部分 Line-based text data看到

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?

答: 看到了, 包含了本地保存的文件在服务器上的最后修改日期。

If-Modified-Since: Wed, 11 Nov 2020 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.

答: 304 Not Modified

没有明确返回文件内容, 因为文件在服务器没有被修改

3.Retrieving Long Documents

问题:

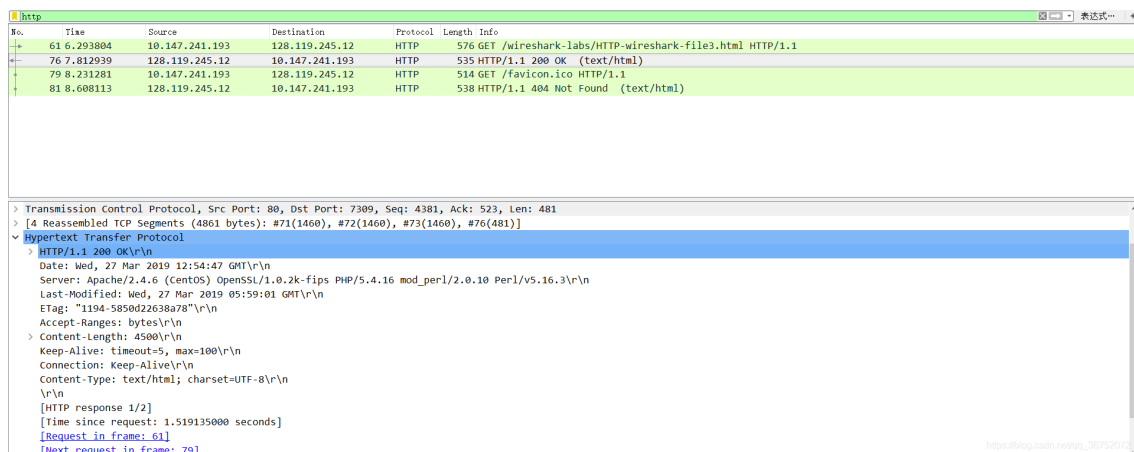
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

答:

I have sent 2 HTTP/GET request messages. One of them(61) is request of the HTML, while another(79) is request for the icon next to the title. Packet 61 contains the GET message for Bill or Rights.

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

答: TCP packet [76]



The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets. Packet 61 is a GET request for /wireshark-labs/HTTP-wireshark-file3.html. Packet 76 is a TCP segment with status code 200 OK. Packet 79 is a GET request for /favicon.ico. Packet 81 is a 404 Not Found response for the favicon.

No.	Time	Source	Destination	Protocol	Length	Info
61	6.293804	10.147.241.193	128.119.245.12	HTTP	576	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
76	7.812939	128.119.245.12	10.147.241.193	HTTP	535	HTTP/1.1 200 OK (text/html)
79	8.231281	10.147.241.193	128.119.245.12	HTTP	514	GET /favicon.ico HTTP/1.1
81	8.608113	128.119.245.12	10.147.241.193	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The bottom pane shows the details of packet 76, which is a TCP segment. It includes the status code 200 OK and the phrase OK. The details pane also shows the HTTP response structure, including the status line, headers, and body.

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

答: 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?

答: 需要4个TCP数据包

4. HTML Documents with Embedded Objects

问题:

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

答: 浏览器发送了3个HTTP GET请求消息。都发送到了 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.

答: 串行, 因为有Connection: Keep-Alive 实行长连接传输。

5. HTTP Authentication

HTTP/1.1 401 Unauthorized\r\n

Date: Wed, 11 Nov 2020 13:46:54 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n

WWW-Authenticate: Basic realm="wireshark-students only"\r\n

Content-Length: 381\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=iso-8859-1\r\n

\r\n

[HTTP response 1/1]

[Time since request: 2.681741000 seconds]

[Request in frame: 1838]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]

File Data: 381 bytes

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network

New

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appli

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.ht

[HTTP request 1/1]

[Response in frame: 3412]

问题:

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

答: 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?

答:

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n

Credentials: wireshark-students:network