

计网 HTTP 抓包实验

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
1.1; 1.1
2. What languages (if any) does your browser indicate that it can accept to the server?
zh-Hans-CN;zh-Hans
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
10.132.1.247;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?
Wed, 06 Nov 2019 06:59:02 GMT
6. How many bytes of content are being returned to your browser?
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.
HTTP 请求报文中还有 Host 字段、connection 字段、Accept 字段、User-agent 字段、Accept-Encoding 字段等
HTTP 响应报文还有 server、connection、ETag、Date 等字段

```

Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Date: Wed, 13 Nov 2019 02:16:28 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.
    Last-Modified: Tue, 12 Nov 2019 06:59:04 GMT\r\n
    ETag: "80-59720c89fd24d"\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 1/1]
  [Time since request: 0.319938000 seconds]
  [Request in frame: 34]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  File Data: 128 bytes

Line-based text data: text/html (4 lines)
  <html>\n
  Congratulations. You've downloaded the file \n
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
  </html>\n

```

No.	Time	Source	Destination	Protocol	Length	Info
34	4.504350	10.132.12.102	128.119.245.12	HTTP	377	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
44	4.824288	128.119.245.12	10.132.12.102	HTTP	540	HTTP/1.1 200 OK (text/html)
57	5.240106	10.132.12.102	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
63	5.864112	128.119.245.12	10.132.12.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

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?

没有这个字段，因为浏览器首次获取该页面。

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

明确返回了，从 Line-based text data 可看出

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?

有那个字段了。信息是：Wed, 06 Nov 2019 06:59:02 GMT，是上次访问网站的最新修改时间。

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，表示未修改，没有返回页面的内容，因为没有修改，浏览器已缓存。

▼ Hypertext Transfer Protocol

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\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: 43]
```

▼ Hypertext Transfer Protocol

```
> HTTP/1.1 200 OK\r\n
Date: Wed, 13 Nov 2019 02:18:59 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: Tue, 12 Nov 2019 06:59:04 GMT\r\n
ETag: "173-59720c89f266c"\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: 0.416043000 seconds]
[Request in frame: 35]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
```

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

```
\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 IF-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\n
</html>\n
```

```

v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Tue, 12 Nov 2019 06:59:04 GMT\r\n
    If-None-Match: "173-59720c89f266c"\r\n
    Connection: Keep-Alive\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: 68]

v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Wed, 13 Nov 2019 02:29:13 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: "173-59720c89f266c"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.328523000 seconds]
    [Request in frame: 65]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.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 of Rights?
1; #52(1394)
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
#52(1394)
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?
4 个数据段

no.	time	source	destination	protocol	length	info
49	3.191497	10.132.12.102	128.119.245.12	HTTP	377	GET /wireshark-labs/HTTP-wireshark-file
55	3.494441	128.119.245.12	10.132.12.102	HTTP	733	HTTP/1.1 200 OK (text/html)
78	3.895505	10.132.12.102	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
95	4.209614	128.119.245.12	10.132.12.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

```

TCP segment data (679 bytes)
  [4 Reassembled TCP Segments (4861 bytes): #52(1394), #53(1394), #54(1394), #55(679)]
    [Frame: 52, payload: 0-1393 (1394 bytes)]
    [Frame: 53, payload: 1394-2787 (1394 bytes)]
    [Frame: 54, payload: 2788-4181 (1394 bytes)]
    [Frame: 55, payload: 4182-4860 (679 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057...]
  > Hypertext Transfer Protocol
  > Line-based text data: text/html (98 lines)
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 57 65 64 2c 20 31 33 20 4e ·Date: W ed, 13 N
0020  6f 76 20 32 30 31 39 20 30 32 3a 32 30 3a 32 34 ov 2019 02:20:24
0030  20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT·Se rver: Ap
0040  61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e 2k-fips PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_p erl/2.0.
0080  31 30 20 50 65 72 6c 2f 67 35 2e 31 36 2e 33 0d 10 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3a 20 ·Last-Mo dified:
00a0  54 75 65 2c 20 31 32 20 4e 6f 76 20 32 30 31 39 Tue, 12 Nov 2019
00b0  20 30 36 3a 35 39 3a 30 33 20 47 4d 54 0d 0a 45 06:59:0 3 GMT·E
00c0  54 61 67 3a 20 22 31 31 39 34 2d 35 39 37 32 30 Tag: "11 94-59720
00d0  63 38 39 61 37 65 66 63 22 0d 0a 41 63 63 65 70 c89a7efc "...Accep
00e0  74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Content -Length:
0100  20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c 69 76 4500·K eep-Aliv
0110  65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 e: timeo ut=5, ma
0120  78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f x=100·C onnectio
0130  6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 n: Keep- Alive·C
0140  6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 ontent-T ype: tex
0150  74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d t/html; charset=
0160  55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c UTF-8·... ·<html><

```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
3(出现 4 个有一个是获取.ico 文件); 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.
不是并发下载的，因为请求是先后到达的，所获取的对象也是先后到达的

No.	Time	Source	Destination	Protocol	Length	Info
300	2.722340	10.132.12.102	128.119.245.12	HTTP	377	GET /wireshark-labs/HTTP-wireshark-file4
302	3.332649	128.119.245.12	10.132.12.102	HTTP	1127	HTTP/1.1 200 OK (text/html)
355	3.367885	10.132.12.102	128.119.245.12	HTTP	437	GET /pearson.png HTTP/1.1
408	3.793358	128.119.245.12	10.132.12.102	HTTP	877	HTTP/1.1 200 OK (PNG)
420	3.794700	10.132.12.102	128.119.245.12	HTTP	451	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
1107	5.491626	128.119.245.12	10.132.12.102	HTTP	1004	HTTP/1.1 200 OK (JPEG JFIF image)
1127	5.853244	10.132.12.102	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
1262	6.441082	128.119.245.12	10.132.12.102	HTTP	539	HTTP/1.1 404 Not Found (text/html)

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
401, 未授权，授权访问
19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
新出现了一个字段，Authorization

✓ Hypertext Transfer Protocol

- > HTTP/1.1 401 Unauthorized\r\n

Date: Wed, 13 Nov 2019 08:44:03 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.0.1\r\nWWW-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]

Wireshark · 分组 369 · WLAN

> Transmission Control Protocol, Src Port: 62105, Dst Port: 80, Seq: 1, Ack: 1, Len: 398 ^

✓ Hypertext Transfer Protocol

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

Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Accept-Encoding: gzip, deflate\r\n
Host: gaia.cs.umass.edu\r\n
Connection: Keep-Alive\r\n
> Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]