

# 计算机网络 HTTP 实验

PB20000180 刘良宇

## 1. 基本的 HTTP GET 响应

```
No.      Time                Source                Destination            Protocol Length Info
128 16:20:54.561422481 114.214.255.65        128.119.245.12        HTTP      553    GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1
Frame 128: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 114.214.255.65, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 48690, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file1.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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh,en;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
[HTTP request 1/1]
[Response in frame: 139]
No.      Time                Source                Destination            Protocol Length Info
139 16:20:54.942389775 128.119.245.12        114.214.255.65        HTTP      554    HTTP/1.1 200 OK (text/html)
Frame 139: 554 bytes on wire (4432 bits), 554 bytes captured (4432 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.255.65
Transmission Control Protocol, Src Port: 80, Dst Port: 48690, Seq: 1, Ack: 486, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Mon, 19 Sep 2022 08:20:54 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Mon, 19 Sep 2022 05:59:01 GMT\r\n
ETag: "80-5e901688a434a"\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: 0.380967294 seconds]
[Request in frame: 128]
[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)
```

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

都是 HTTP 1.1

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

zh, en

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

本机: 114.214.255.65

服务器: 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?

Mon, 19 Sep 2022 05:59:01 GMT

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

Content-Length: 128

- 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.

例如 `Accept-Language`

## 2. 有条件的 HTTP GET 响应

- 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?

无

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

No.	Time	Source	Destination	Protocol	Length	Info
245	16:46:39.612272979	114.214.255.65	128.119.245.12	HTTP	527	GET /wireshark-labs
278	16:46:39.901487523	128.119.245.12	114.214.255.65	HTTP	798	HTTP/1.1 200 OK (text/html)
357	16:46:40.984464368	114.214.255.65	128.119.245.12	HTTP	639	GET /wireshark-labs
395	16:46:41.336943423	128.119.245.12	114.214.255.65	HTTP	307	HTTP/1.1 304 Not Modified

Frame 278: 798 bytes on wire (6384 bits), 798 bytes captured (6384 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.255.65

Transmission Control Protocol, Src Port: 80, Dst Port: 35276, Seq: 1, Ack: 460, Len: 730

Hypertext Transfer Protocol

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

存在 `content` (从头条里的 `content-length` 也可以看出)

- 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?

No.	Time	Source	Destination	Protocol	Length	Info
245	16:46:39.612272979	114.214.255.65	128.119.245.12	HTTP	527	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
278	16:46:39.901487523	128.119.245.12	114.214.255.65	HTTP	798	HTTP/1.1 200 OK (text/html)
357	16:46:40.984464368	114.214.255.65	128.119.245.12	HTTP	639	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
395	16:46:41.336943423	128.119.245.12	114.214.255.65	HTTP	307	HTTP/1.1 304 Not Modified

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 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36\r\n

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\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: zh,en;q=0.9\r\n

If-None-Match: "173-5e901688a3792"\r\n

If-Modified-Since: Mon, 19 Sep 2022 05:59:01 GMT\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

存在，和上一条 GET 服务器返回内容的 **Last-Modified** 值 **Mon, 19 Sep 2022 05:59:01 GMT** 相同

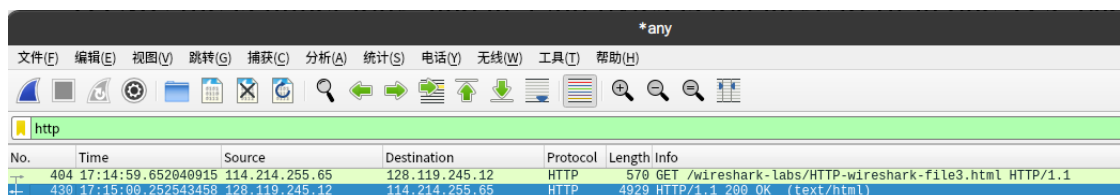
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

**304 Not Modified**

没有返回文件内容（没有 **content**，头里也没有 **content-length**）

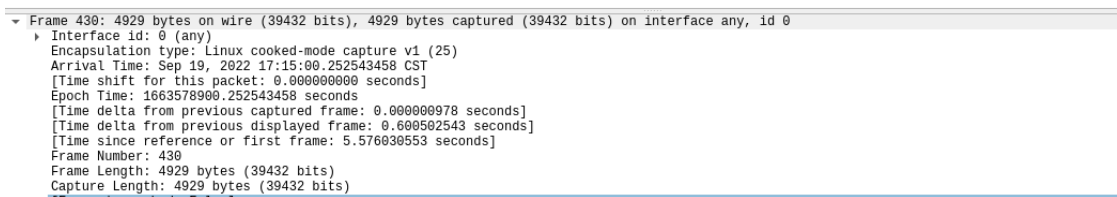
### 3. 检索长文档

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?



The image shows a Wireshark packet capture of an HTTP GET request. The packet list pane shows two packets. Packet 404 is a GET request for /wireshark-labs/HTTP-wireshark-file3.html. Packet 430 is the response, which is a 200 OK status with content type text/html.

No.	Time	Source	Destination	Protocol	Length	Info
404	17:14:59.652040915	114.214.255.65	128.119.245.12	HTTP	570	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
430	17:15:00.252543458	128.119.245.12	114.214.255.65	HTTP	4929	HTTP/1.1 200 OK (text/html)



The image shows the packet details pane for packet 430. It displays the frame structure, including the interface, encapsulation type, arrival time, and frame length. The frame length is 4929 bytes (39432 bits).

```
Frame 430: 4929 bytes on wire (39432 bits), 4929 bytes captured (39432 bits) on interface any, id 0
  Interface id: 0 (any)
    Encapsulation type: Linux cooked-mode capture v1 (25)
    Arrival Time: Sep 19, 2022 17:15:00.252543458 CST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1663570900.252543458 seconds
    [Time delta from previous captured frame: 0.000000978 seconds]
    [Time delta from previous displayed frame: 0.600502543 seconds]
    [Time since reference or first frame: 5.576030553 seconds]
    Frame Number: 430
    Frame Length: 4929 bytes (39432 bits)
    Capture Length: 4929 bytes (39432 bits)
```

- 发送了 1 个 GET 请求
- 430 收到了结果

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

- 也为 430

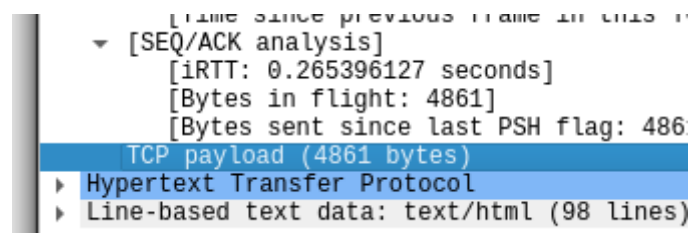
14. What is the status code and phrase in the response?

- **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?

- 1 个

注：以上经过反复实验，均只有一个 packet



The image shows the packet details pane for packet 430, highlighting the TCP payload. The payload is 4861 bytes and contains Hypertext Transfer Protocol data, which is line-based text data (text/html) consisting of 98 lines.

```
Time since previous frame in this trace: 0.600502543 seconds
[SEQ/ACK analysis]
  [iRTT: 0.265396127 seconds]
  [Bytes in flight: 4861]
  [Bytes sent since last PSH flag: 4861]
  TCP payload (4861 bytes)
    Hypertext Transfer Protocol
    Line-based text data: text/html (98 lines)
```

作为对比，这里抓取另外一个网页的 GET 包：

```

[Bytes in flight: 2/81]
[Bytes sent since last PSH flag: 2528]
TCP payload (2528 bytes)
TCP segment data (2528 bytes)
[2 Reassembled TCP Segments (2781 bytes): #590(253), #591(2528)]
[Frame: 590, payload: 0-252 (253 bytes)]
[Frame: 591, payload: 253-2780 (2528 bytes)]
[Segment count: 2]
[Reassembled TCP length: 2781]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d61]

```

对于这个示例而言，GET 的结果存在了 590 和 591 中，用了两个 packet，返回的 HTTP 状态码信息在第一个包中

Frame (2616 bytes)    Reassembled TCP (2781 bytes)

TCP Segment (tcp.segment), 253 byte(s)

```

[Frame: 590, payload: 0-252 (253 bytes)]
[Frame: 591, payload: 253-2780 (2528 bytes)]
[Segment count: 2]
[Reassembled TCP length: 2781]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d61]
Hypertext Transfer Protocol
Line-based text data: text/html (57 lines)
<!DOCTYPE html>\r\n
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 4d 6f 6e 2c 20 31 39 20 53 .Date: Mon, 19 S
0020 65 70 20 32 30 32 32 20 30 39 3a 32 37 3a 33 33 ep 2022 09:27:33
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT·Server: Ap
0040 61 63 68 65 2f 32 2e 30 2e 35 32 20 28 52 65 64 ache/2.0 .52 (Red
0050 20 48 61 74 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 Hat)·L ast-Modi
0060 66 69 65 64 3a 20 54 75 65 2c 20 30 39 20 41 75 fied: Tue, 09 Au
0070 67 20 32 30 32 32 20 31 31 3a 30 32 3a 31 37 20 g 2022 1 1:02:17
0080 47 4d 54 0d 0a 45 54 61 67 3a 20 22 39 39 32 34 GMT·ETa g: "9924
0090 31 30 30 2d 39 65 30 2d 64 64 39 32 36 30 34 30 100-9e0- dd926040
00a0 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 "·Accep t-Ranges
00b0 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 : bytes·Content

```

## 4. 内嵌对象的 HTML 文档

No.	Time	Source	Destination	Protocol	Length	Info
129	17:34:46.897226276	114.214.255.65	128.119.245.12	HTTP	570	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
148	17:34:47.170217777	128.119.245.12	114.214.255.65	HTTP	1369	HTTP/1.1 200 OK (text/html)
153	17:34:47.206510586	114.214.255.65	128.119.245.12	HTTP	516	GET /pearson.png HTTP/1.1
174	17:34:47.499248587	128.119.245.12	114.214.255.65	HTTP	783	HTTP/1.1 200 OK (PNG)
208	17:34:47.852323023	114.214.255.65	178.79.137.164	HTTP	483	GET /8E_cover_small.jpg HTTP/1.1
226	17:34:48.177494136	178.79.137.164	114.214.255.65	HTTP	239	HTTP/1.1 301 Moved Permanently

```

Frame 129: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface any, id 0
  Interface id: 0 (any)
  Encapsulation type: Linux cooked-mode capture v1 (25)
  Arrival Time: Sep 19, 2022 17:34:46.897226276 CST
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1663580086.897226276 seconds
  [Time delta from previous captured frame: 0.005405529 seconds]

```

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

3 个

- HTML 文档和第一张图片: 128.119.245.12
- 第二张图片: 178.79.137.164

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.

从时间上无法辨别（可能是串行，可能是并行）

对另一个资源较多的网站进行抓包，可以看出另一个网站是并行的：

112	17:38:44.604295118	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	515	GET /~pro/css/katex.min.css HTTP/1.1
129	17:38:44.640699093	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	510	GET /~pro/css/main.css HTTP/1.1
130	17:38:44.641844241	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	517	GET /~pro/css/prism_light.css HTTP/1.1
131	17:38:44.641972543	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	515	GET /~pro/css/nprogress.css HTTP/1.1
145	17:38:44.673801655	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	498	GET /~pro/js/nprogress.js HTTP/1.1
146	17:38:44.673930795	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	501	GET /~pro/js/showdown.min.js HTTP/1.1
152	17:38:44.726075941	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	1780	HTTP/1.1 200 OK (text/css)
172	17:38:44.738926235	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	3817	HTTP/1.1 200 OK (text/css)
189	17:38:44.750387560	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	1175	HTTP/1.1 200 OK (text/css)
206	17:38:44.753757420	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	498	GET /~pro/js/katex.min.js HTTP/1.1
207	17:38:44.753862743	2001:da8:d800:186:f...	2001:da8:d800:186:f...	HTTP	510	GET /~pro/js/katex-auto-render.min.js HTTP/1.1

## 5. HTTP 鉴权

```
No.      Time                Source                Destination            Protocol Length Info
175 17:40:45.409976017 114.214.255.65        128.119.245.12        HTTP      586      GET /wireshark-labs/protected_pages/
HTTP-wireshark-file5.html HTTP/1.1
Frame 175: 586 bytes on wire (4688 bits), 586 bytes captured (4688 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 114.214.255.65, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60808, Dst Port: 80, Seq: 1, Ack: 1, Len: 518
Hypertext Transfer Protocol
No.      Time                Source                Destination            Protocol Length Info
220 17:40:45.704283677 128.119.245.12        114.214.255.65        HTTP      785      HTTP/1.1 401 Unauthorized (text/html)
Frame 220: 785 bytes on wire (6280 bits), 785 bytes captured (6280 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.255.65
Transmission Control Protocol, Src Port: 80, Dst Port: 60808, Seq: 1, Ack: 519, Len: 717
Hypertext Transfer Protocol
Line-based text data: text/html (12 lines)
No.      Time                Source                Destination            Protocol Length Info
1186 17:40:55.227248570 114.214.255.65        128.119.245.12        HTTP      645      GET /wireshark-labs/protected_pages/
HTTP-wireshark-file5.html HTTP/1.1
Frame 1186: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 114.214.255.65, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53354, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
Hypertext Transfer Protocol
No.      Time                Source                Destination            Protocol Length Info
1219 17:40:55.544139377 128.119.245.12        114.214.255.65        HTTP      558      HTTP/1.1 200 OK (text/html)
Frame 1219: 558 bytes on wire (4464 bits), 558 bytes captured (4464 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.255.65
Transmission Control Protocol, Src Port: 80, Dst Port: 53354, Seq: 1, Ack: 578, Len: 490
Hypertext Transfer Protocol
Line-based text data: text/html (6 lines)
```

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?

```
Connection: keep-alive\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcmcs=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
```