山东大学 计算机 学院

计算机网络 课程实验报告

学号：202400130240	姓名： 贾宗翰	班级： 24.6

实验题目：

Wireshark Lab:HTTP v8.1

实验学时：2h	实验日期： 2025.9.9

实验目的： 了解 http 协议

硬件环境：

联想拯救者

软件环境：

Wireshark ， edge 浏览器

实验步骤与内容：

1. 基本的 HTTP GET/响应交互

http

No.	Time	Source	Destination	Protoco	Lengt	Info
118	3.065908	117.185.117.25	101.76.250.107	HTTP	447	HTTP/1.1 200 OK
265	8.692836	101.76.243.171	43.141.131.186	HTTP	457	GET /C200003mAan70zUy5O.m4a?vkey=375C416ADA454BEF5EA1A2A0A
268	8.740902	43.141.131.186	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)
288	9.094059	2001:250:5800:1000:…	2600:1417:4400:3::1…	HTTP	186	GET /connecttest.txt HTTP/1.1
292	9.094708	101.76.243.171	23.200.230.70	HTTP	165	GET /connecttest.txt HTTP/1.1
294	9.094826	2001:250:5800:1000:…	2600:1417:4400:3::1…	HTTP	186	GET /connecttest.txt HTTP/1.1
297	9.098719	101.76.243.171	23.200.230.70	HTTP	165	GET /connecttest.txt HTTP/1.1
300	9.114745	101.76.243.171	120.222.231.162	HTTP	478	GET /amobile.music.tc.qq.com/C200003mAan70zUy5O.m4a?vkey=37
303	9.121424	120.222.231.162	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)
306	9.143778	2600:1417:4400:3::1…	2001:250:5800:1000:…	HTTP	261	HTTP/1.1 200 OK (text/plain)
312	9.145309	2600:1417:4400:3::1…	2001:250:5800:1000:…	HTTP	261	HTTP/1.1 200 OK (text/plain)
316	9.145438	23.200.230.70	101.76.243.171	HTTP	241	HTTP/1.1 200 OK (text/plain)
325	9.153516	23.200.230.70	101.76.243.171	HTTP	241	HTTP/1.1 200 OK (text/plain)
345	9.551082	101.76.243.171	120.222.231.188	HTTP	478	GET /amobile.music.tc.qq.com/C200003mAan70zUy5O.m4a?vkey=37
348	9.557942	120.222.231.188	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)
360	9.985659	101.76.243.171	120.220.222.249	HTTP	478	GET /amobile.music.tc.qq.com/C200003mAan70zUy5O.m4a?vkey=37
385	10.418864	101.76.243.171	36.151.205.60	HTTP	464	GET /C200003mAan70zUy5O.m4a?vkey=375C416ADA454BEF5EA1A2A0A
389	10.436935	36.151.205.60	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)
400	10.855021	101.76.243.171	36.151.205.60	HTTP	463	GET /C200003mAan70zUy5O.m4a?vkey=375C416ADA454BEF5EA1A2A0A
405	10.876962	36.151.205.60	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)
418	11.303764	101.76.243.171	120.201.118.234	HTTP	457	GET /C200003mAan70zUy5O.m4a?vkey=375C416ADA454BEF5EA1A2A0A
423	11.339732	120.201.118.234	101.76.243.171	HTTP	60	HTTP/1.1 200 OK (audio/mp4)

2. HTTP 条件 GET/响应交互

在执行：

在浏览器中输入以下 URL

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html 您的浏览器应该显示一个非常简单的五行 HTML 文件。请快速再次在浏览器中输入相同的 URL（或只需选择浏览器上的刷新按钮）

之后，出现：

http

No.	Time	Source	Destination	Protoco	Lengt	Info
1473	21.460906	101.76.243.171	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1488	21.709881	128.119.245.12	101.76.243.171	HTTP	784	HTTP/1.1 200 OK (text/html)
1805	35.628853	101.76.243.171	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1807	35.878247	128.119.245.12	101.76.243.171	HTTP	294	HTTP/1.1 304 Not Modified
3306	62.630389	101.76.243.171	128.119.245.12	HTTP	685	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3313	62.879261	128.119.245.12	101.76.243.171	HTTP	294	HTTP/1.1 304 Not Modified

浏 览 器 对 应 ：

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE field in your browser's HTTP GET request to the server.

3.获取长文档

清除缓存之后，输入 http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html：

http

No.	Time	Source	Destination	Protoco	Lengt	Info
1044	8.330016	101.76.243.171	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file3.html HTT
1059	8.590156	128.119.245.12	101.76.243.171	HTTP	535	HTTP/1.1 200 OK (text/html)

4. 含嵌入对象的 Html

清除浏览数据之后，打开相应的链接：

http

No.	Time	Source	Destination	Protoco	Lengt	Info
1124	8.634872	101.76.243.171	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file4.html HT
1129	8.883633	128.119.245.12	101.76.243.171	HTTP	1355	HTTP/1.1 200 OK (text/html)
1132	8.926126	101.76.243.171	128.119.245.12	HTTP	519	GET /pearson.png HTTP/1.1
1188	9.174615	128.119.245.12	101.76.243.171	HTTP	745	HTTP/1.1 200 OK (PNG)
1206	9.467538	101.76.243.171	178.79.137.164	HTTP	486	GET /8E_cover_small.jpg HTTP/1.1
1217	9.702851	178.79.137.164	101.76.243.171	HTTP	225	HTTP/1.1 301 Moved Permanently

不安全 | gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

Pearson

This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The stored at, and served from, a WWW server kurose.cslash.net in France:

And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

5. http 认证：

访问目标网站：

http

No.	Time	Source	Destination	Protoco	Lengt	Info
3110	8.247111	101.76.243.171	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
3207	8.496627	128.119.245.12	101.76.243.171	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
7118	24.879526	101.76.243.171	128.119.245.12	HTTP	674	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
7170	25.129149	128.119.245.12	101.76.243.171	HTTP	544	HTTP/1.1 200 OK (text/html)

This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

结论分析与体会：

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

```
Hypertext Transfer Protocol
  GET /connecttest.txt HTTP/1.1\r\n
      Request Method: GET
      Request URI: /connecttest.txt
      Request Version: HTTP/1.1
    Connection: Close\r\n
    User-Agent: Microsoft NCSI\r\n
    Host: ipv6.msftconnecttest.com\r\n
    \r\n
```

可见都是 1.1 版本。

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

答案：见截图显示

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
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: "80-63e43e25c52c3"\r\n
If-Modified-Since: Mon, 08 Sep 2025 05:59:01 GMT\r\n
```

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

```
  88 3.109540    2001:250:5800:1000:… 2402:4e00:1620:1611… HTTP     836 POST /mmtls/00007833 HTTP/1.1
  91 3.177053    2402:4e00:1620:1611… 2001:250:5800:1000:… HTTP     433 HTTP/1.1 200 OK
 136 3.521952    101.76.243.171       128.119.245.12       HTTP     684 GET /wireshark-labs/HTTP-wireshark-file1.html
 143 3.770715    128.119.245.12       101.76.243.171       HTTP     293 HTTP/1.1 304 Not Modified
 187 6.117968    101.76.243.171       128.119.245.12       HTTP     684 GET /wireshark-labs/HTTP-wireshark-file1.html
 191 6.366832    128.119.245.12       101.76.243.171       HTTP     292 HTTP/1.1 304 Not Modified
```

分析得知我的 ip 是 101.76.243.171，对方的是 128.119.245.12

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

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
```

状态码是 200 OK，成功找到并返回。

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

```
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 09 Sep 2025 03:43:54 GMT\r\n
```

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

```
Date: Tue, 09 Sep 2025 03:43:54 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.
Last-Modified: Mon, 08 Sep 2025 05:59:01 GMT\r\n
ETag: "80-63e43e25c52c3"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
```

一共 128 字节。

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.

发送：

```
Hypertext Transfer Protocol
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
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
[Response in frame: 6054]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

回应：

```
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
Date: Tue, 09 Sep 2025 03:43:54 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Mon, 08 Sep 2025 05:59:01 GMT\r\n
ETag: "80-63e43e25c52c3"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
    [Content length: 128]
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[Request in frame: 5369]
[Time since request: 0.248805000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file1.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
```

没有找到。

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?

没有看到：

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    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/140.0.0.0 S
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
    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: "173-63e43e25c4af3"\r\n
    If-Modified-Since: Mon, 08 Sep 2025 05:59:01 GMT\r\n
    \r\n
    [Response in frame: 2264]
```

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   是，因为状态码是 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 GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?
    是，信息：

```
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    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/140.0.0.0 Sa
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicat
    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: "173-63e43e25c4af3"\r\n
    If-Modified-Since: Mon, 08 Sep 2025 05:59:01 GMT\r\n
    \r\n
```

    是最后一次修改的时间

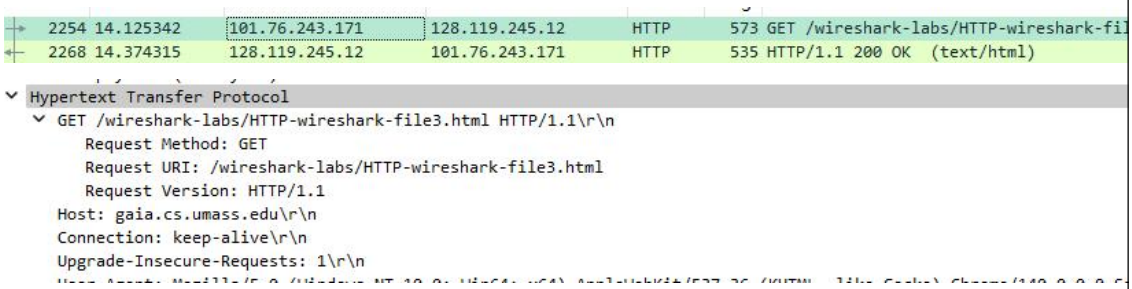
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
    HTTP 状态代码和短语：

```
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
    Date: Tue, 09 Sep 2025 03:49:05 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=98\r\n
```

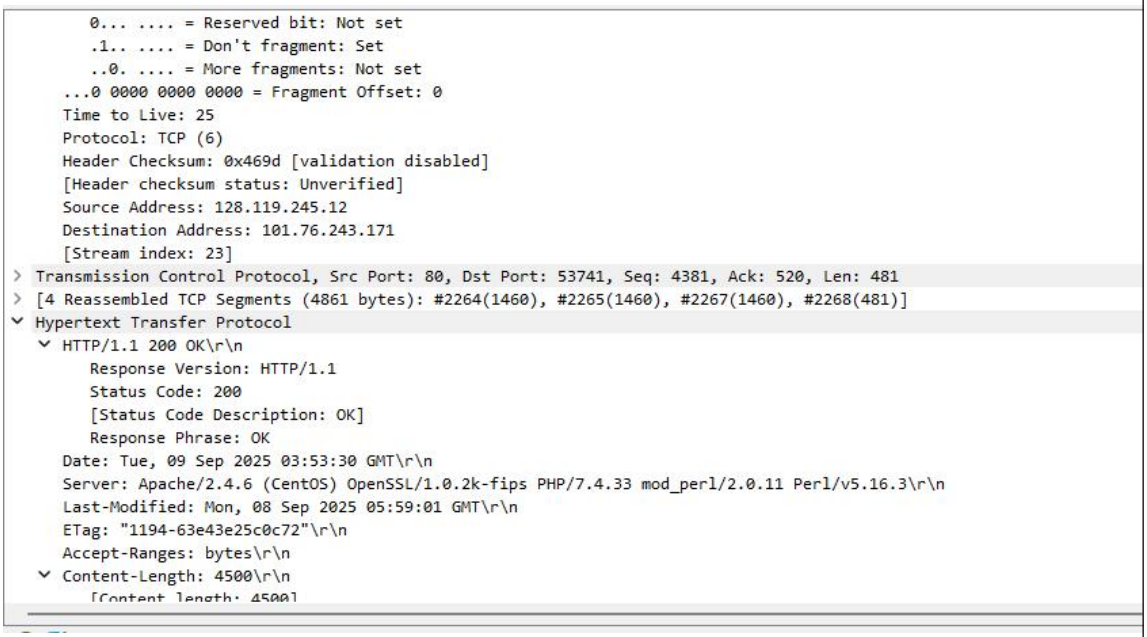
    没有明确的反汇文件内容，因为该网页内容在上次访问之后未被修改，且本地有上次访问的缓存。

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?

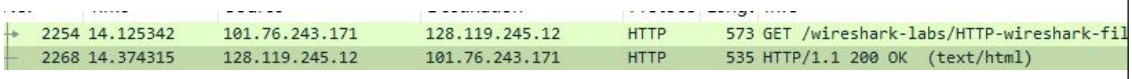
一个请求，在第一个包：



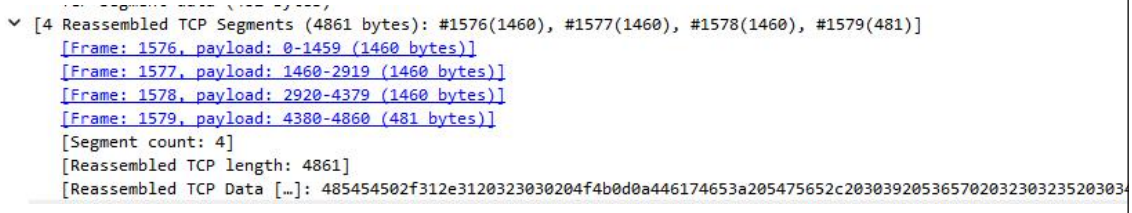
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
第一个数据包：



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?
一共有四个：



16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
发送了三条 http 的请求信息。这些 get 发送给了 128.119.245.12 和 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.
两张图片是先后发出请求的，看时间戳：

1331	5.714187	101.76.243.171	128.119.245.12	HTTP	573	GET /wireshark-labs/HTTP-wireshark-file4.
1348	5.962839	128.119.245.12	101.76.243.171	HTTP	1355	HTTP/1.1 200 OK (text/html)
1358	6.003155	101.76.243.171	128.119.245.12	HTTP	519	GET /pearson.png HTTP/1.1
1406	6.251522	128.119.245.12	101.76.243.171	HTTP	745	HTTP/1.1 200 OK (PNG)
1417	6.531974	101.76.243.171	178.79.137.164	HTTP	486	GET /8E_cover_small.jpg HTTP/1.1
1420	6.757110	178.79.137.164	101.76.243.171	HTTP	225	HTTP/1.1 301 Moved Permanently
1890	8.922375	101.76.243.171	128.119.245.12	HTTP	519	GET /favicon.ico HTTP/1.1
1891	9.170886	128.119.245.12	101.76.243.171	HTTP	538	HTTP/1.1 404 Not Found (text/html)

第一张图片返回 ok 之后才发送的第二个请求。

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

http

No.	Time	Source	Destination	Protoco	Lengt	Info
3110	8.247111	101.76.243.171	128.119.245.12	HTTP	589	GET /wireshark-labs/protected_pages/HTTP-wireshark-f
3207	8.496627	128.119.245.12	101.76.243.171	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
7118	24.879526	101.76.243.171	128.119.245.12	HTTP	674	GET /wireshark-labs/protected_pages/HTTP-wireshark-f
7170	25.129149	128.119.245.12	101.76.243.171	HTTP	544	HTTP/1.1 200 OK (text/html)

可见没有输入账号密码之前是 401 Unauthorized，输入正确之后是 200 OK。

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
对比：（回答问题的时候是第二次进去的，没让我输入用户名和密码，所以这里第一次的 401 那个用了别人的）

```
Hypertext Transfer Protocol
  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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
  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
  dnt: 1\r\n
  sec-gpc: 1\r\n
  \r\n
  [Response in frame: 570]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharl
```

```
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Request Method: GET
    Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
  Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Credentials: wireshark-students:network
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 S
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applic
  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
```

对比发现多了 Authorization.