

实验报告

实验二 HTTP与DNS

Lab2 HTTP & DHS

PART 1 HTTP

罗晏宸

PB17000297

2019.9.23

实验目的

1. 研究学习HTTP协议

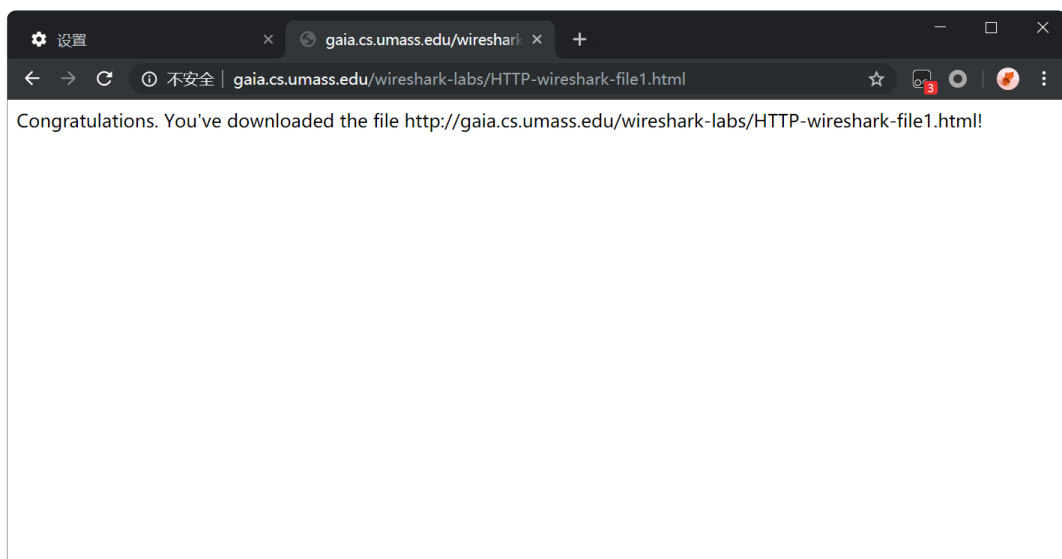
1. 认识学习基础请求响应的报文交互
2. 熟悉HTTP报文格式与内容
3. 利用HTTP协议取回大型HTML文件
4. 利用HTTP取回嵌有对象的HTML文件
5. HTTP授权与安全

实验内容

基础请求响应(GET/response)报文交互

1. 在Wireshark中对捕获的分组应用HTTP协议过滤
2. 浏览给定网址

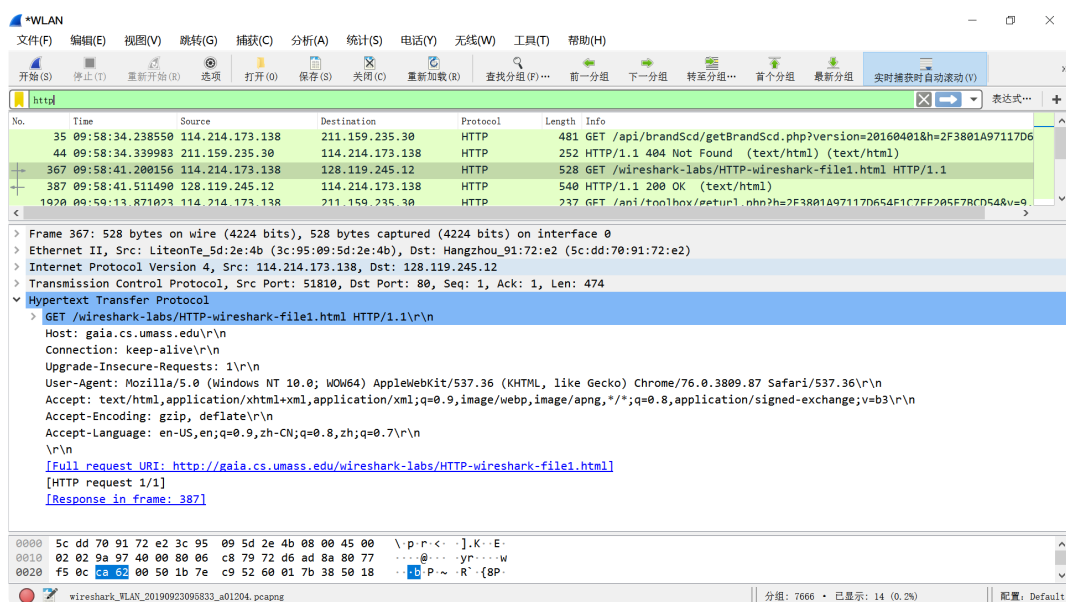
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>



3. 捕获如下分组

1. HTTP GET 报文

```
1 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Upgrade-Insecure-Requests: 1\r\n
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
  age/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
7 Accept-Encoding: gzip, deflate\r\n
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
9 \r\n
```



2. HTTP 响应报文

```
1 | HTTP/1.1 200 OK\r\n
2 | Date: Mon, 23 Sep 2019 01:58:39 GMT\r\n
3 | 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
4 | Last-Modified: Sun, 22 Sep 2019 05:59:01 GMT\r\n
5 | ETag: "80-5931dfff61479"\r\n
6 | Accept-Ranges: bytes\r\n
7 | Content-Length: 128\r\n
8 | Keep-Alive: timeout=5, max=100\r\n
9 | Connection: Keep-Alive\r\n
10 | Content-Type: text/html; charset=UTF-8\r\n
11 | \r\n
```

```
1 | <html>\n
2 | Congratulations. You've downloaded the file \n
3 | http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
  | file1.html!\n
4 | </html>\n
```

*WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T)

开始(S) 停止(T) 重新开始(R) 选项 打开(O) 保存(S) 关闭(C) 重新加载(R) 查找分组(F)...

http

Destination	Protocol	Length	Info
11.159.235.30	HTTP	481	GET /api/brandScd/getBrandScd.php?version=2016
14.214.173.138	HTTP	252	HTTP/1.1 404 Not Found (text/html) (text/html)
28.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file1.html
14.214.173.138	HTTP	540	HTTP/1.1 200 OK (text/html)
11.159.235.30	HTTP	237	GET /api/toolbox/geturl.php?h=2F3801A97117D654
14.214.173.138	HTTP	371	HTTP/1.1 200 OK (text/html) (text/html)

< >

> Frame 387: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface

> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: LiteonTe_5d:2e:4b (3c:95

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.173.138

> Transmission Control Protocol, Src Port: 80, Dst Port: 51810, Seq: 1, Ack: 475, Len: 4

▼ Hypertext Transfer Protocol

▼ HTTP/1.1 200 OK\r\n

▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity level: Chat]

[Group: Sequence]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Mon, 23 Sep 2019 01:58:39 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

Last-Modified: Sun, 22 Sep 2019 05:59:01 GMT\r\n

ETag: "80-5931dfff61479"\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

[HTTP response 1/1]

[Time since request: 0.311334000 seconds]

[\[Request in frame: 367\]](#)

[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)

< >

0000	3c 95 09 5d 2e 4b 5c dd	70 91 72 e2 08 00 45 04	<...].K\ p.r...E.
0010	02 0e 8a 3e 40 00 2a 06	2e c3 80 77 f5 0c 72 d6	...>@.*. .w.r.
0020	ad 8a 00 50 ca 62 60 01	7b 38 1b 7e cb 2c 50 18	...P.b` {8~.,P.
0030	00 ed e0 87 00 00 48 54	54 50 2f 31 2e 31 20 32HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 4d 6f 6e	00 OK..D ate: Mon
0050	2c 20 32 33 20 53 65 70	20 32 30 31 39 20 30 31	, 23 Sep 2019 01

Frame (frame), 540 字节 | 分组: 7666 • 已显示: 14 (0.2%) • 已丢弃: 0 (0.0%) | 配置: Default

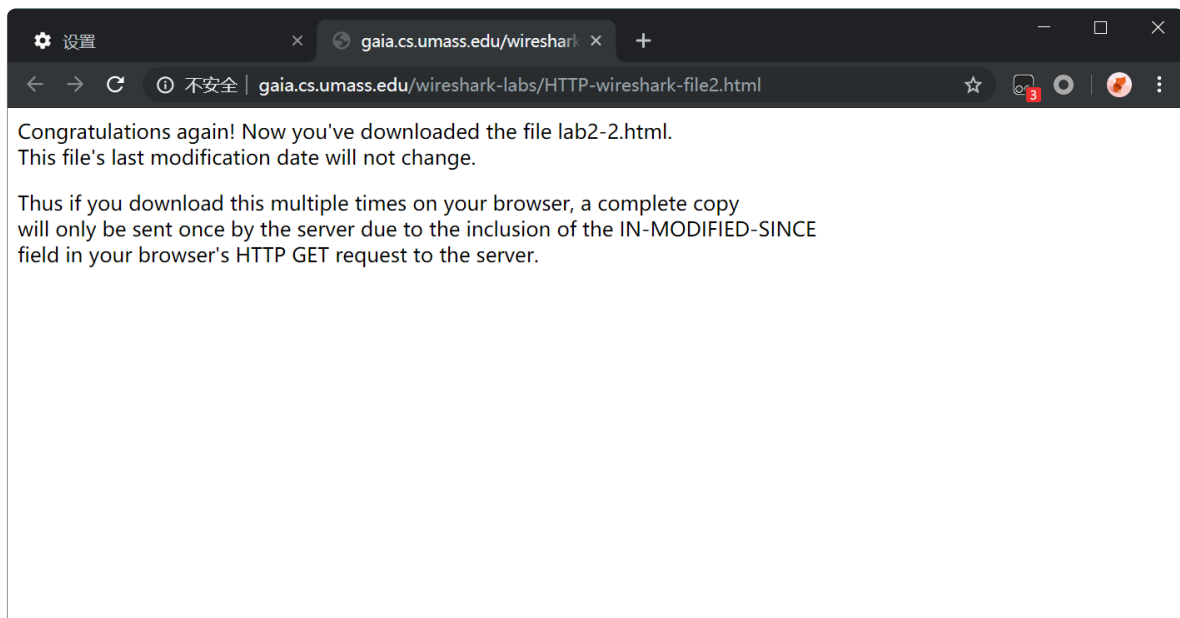
4. 阅读分组具体内容，对实验问题的回答如下

1. 本地浏览器运行的HTTP版本是1.1，服务器运行HTTP 1.1
2. 由内容 `Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n` 可知，浏览器显示可从服务器接收英文(en-US)和中文(zh-CN, zh)
3. 本机IP地址为 `114.214.173.138`，服务器IP地址为 `128.119.245.12`
4. 从服务器返回的状态码为 `200`
5. 由内容 `Last-Modified: Sun, 22 Sep 2019 05:59:01 GMT\r\n` 可知，取回的HTML文件最后修改时间为格林威治时间2019年9月22日5:59:01
6. 由内容 `File Data: 128 bytes` 可知，返回浏览器的内容大小为128字节
7. 有部分没有出现在列表中的条目标题，比如 `Connection:` 等

条件请求响应(GET/response)报文交互

1. 清除浏览器缓存
2. 设置Wireshark捕获
3. 浏览给定网址

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>



4. 刷新网页
5. 捕获如下分组

1. HTTP请求报文

```
1 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Upgrade-Insecure-Requests: 1\r\n
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
  age/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
7 Accept-Encoding: gzip, deflate\r\n
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
9 \r\n
```

2. HTTP响应报文

```
1 HTTP/1.1 200 OK\r\n
2 Date: Mon, 23 Sep 2019 04:03:15 GMT\r\n
3 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
4 Last-Modified: Sun, 22 Sep 2019 05:59:01 GMT\r\n
5 ETag: "173-5931dfff60ca9"\r\n
6 Accept-Ranges: bytes\r\n
7 Content-Length: 371\r\n
8 Keep-Alive: timeout=5, max=100\r\n
9 Connection: Keep-Alive\r\n
10 Content-Type: text/html; charset=UTF-8\r\n
11 \r\n
```

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

3. HTTP请求报文

```

1 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Cache-Control: max-age=0\r\n
5 Upgrade-Insecure-Requests: 1\r\n
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.87
  Safari/537.36\r\n
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
  mage/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
8 Accept-Encoding: gzip, deflate\r\n
9 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
10 If-None-Match: "173-5931dfff60ca9"\r\n
11 If-Modified-Since: Sun, 22 Sep 2019 05:59:01 GMT\r\n
12 \r\n

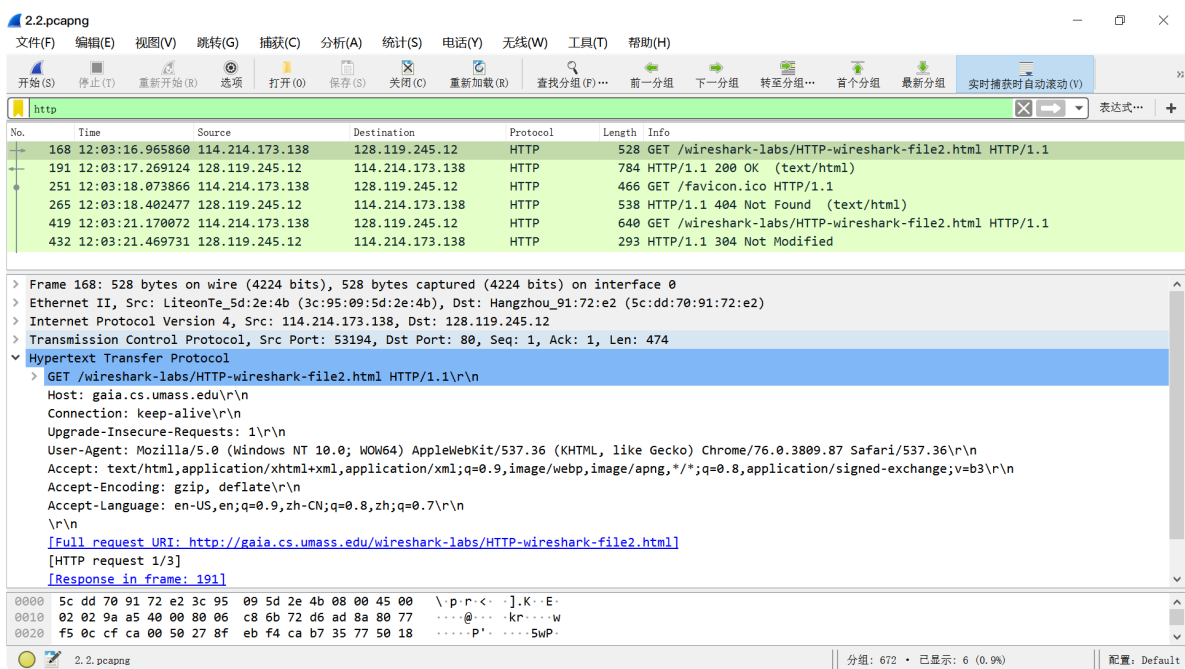
```

4. HTTP响应报文

```

1 HTTP/1.1 304 Not Modified\r\n
2 Date: Mon, 23 Sep 2019 04:03:19 GMT\r\n
3 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
4 Connection: Keep-Alive\r\n
5 Keep-Alive: timeout=5, max=98\r\n
6 ETag: "173-5931dfff60ca9"\r\n
7 \r\n

```



6. 阅读分组具体内容，对实验问题的回答如下

8. 在第一次请求报文中，相关内容没有出现

9. 在第一次的响应报文中，服务器显式地返回了html文件内容

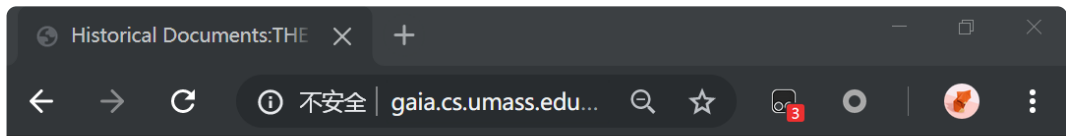
10. 内容 `If-Modified-Since: Sun, 22 Sep 2019 05:59:01 GMT\r\n` 出现于第二次请求报文

11. 第二次响应报文的状态码为 **304**，响应短语为 **Not Modified**，意为在上次请求响应之后，内容没有修改，因此这次响应报文不再显式地返回文件内

取回长文档

1. 清除浏览器缓存
2. 设置Wireshark捕获
3. 浏览给定网址

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>



THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Amendment VI

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

Amendment VII

In suits at common law, where the value in controversy shall exceed twenty dollars, the right of trial by jury shall be preserved, and no fact tried by a jury, shall be otherwise reexamined in any court of the United States, than according to the rules of the common law.

Amendment VIII

Excessive bail shall not be required, nor excessive fines imposed, nor cruel and unusual punishments inflicted.

Amendment IX

The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Amendment X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.

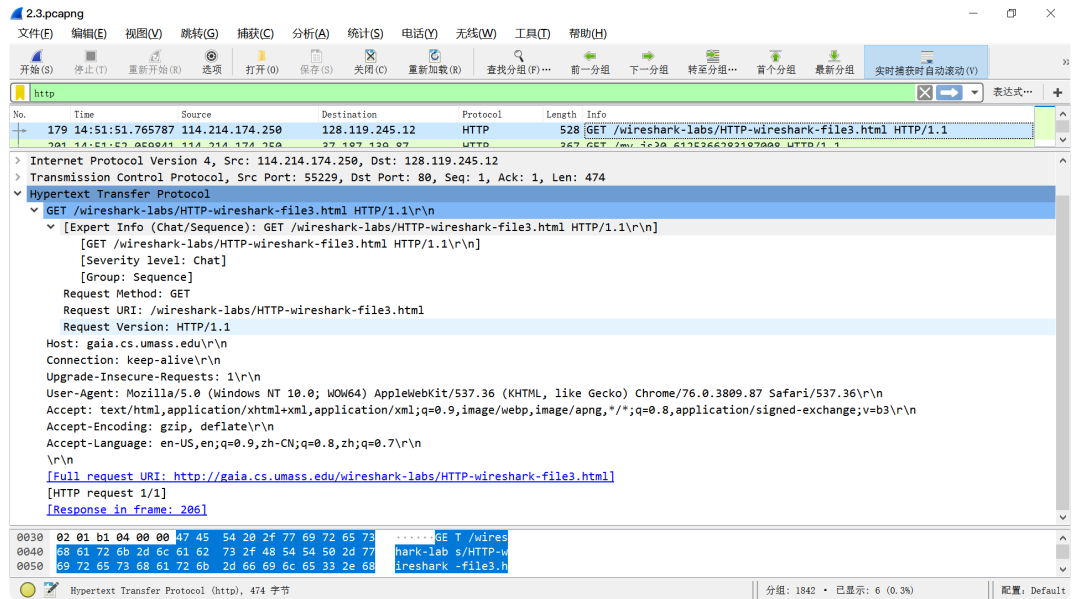
4. 捕获如下分组

1. HTTP请求报文

```

1 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Upgrade-Insecure-Requests: 1\r\n
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
7 Accept-Encoding: gzip, deflate\r\n
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
9 \r\n

```



2. HTTP响应报文

```

1 HTTP/1.1 200 OK\r\n
2 Date: Mon, 23 Sep 2019 06:51:50 GMT\r\n
3 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
4 Last-Modified: Mon, 23 Sep 2019 05:59:01 GMT\r\n
5 ETag: "1194-593321dccac20"\r\n
6 Accept-Ranges: bytes\r\n
7 Content-Length: 4500\r\n
8 Keep-Alive: timeout=5, max=100\r\n
9 Connection: Keep-Alive\r\n
10 Content-Type: text/html; charset=UTF-8\r\n
11 \r\n

```

```

1 <html><head> \n
2 <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
3 \n
4 \n
5 <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
6 <p><br>\n
7 </p>\n
8 <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
9 <em>Amendments 1-10 of the Constitution</em>\n
10 </center>\n
11 \n

```

12 <p>The Conventions of a number of the States having, at the
time of adopting\n

13 the Constitution, expressed a desire, in order to prevent
misconstruction\n

14 or abuse of its powers, that further declaratory and
restrictive clauses\n

15 should be added, and as extending the ground of public
confidence in the\n

16 Government will best insure the beneficent ends of its
institution; </p><p> Resolved, by the Senate and House of
Representatives of the United\n

17 States of America, in Congress assembled, two-thirds of both
Houses concurring,\n

18 that the following articles be proposed to the Legislatures
of the several\n

19 States, as amendments to the Constitution of the United
States; all or any\n

20 of which articles, when ratified by three-fourths of the said
Legislatures,\n

21 to be valid to all intents and purposes as part of the said
Constitution,\n

22 namely: </p><p><h3>Amendment I</h3>
\n

23 \n

24 <p></p><p>Congress shall make no law respecting an
establishment of\n

25 religion, or prohibiting the free exercise thereof; or\n

26 abridging the freedom of speech, or of the press; or the\n

27 right of the people peaceably to assemble, and to petition\n

28 the government for a redress of grievances.\n

29 \n

30 </p><p><h3>Amendment II</h3>
\n

31 \n

32 <p></p><p>A well regulated militia, being necessary to the
security\n

33 of a free state, the right of the people to keep and bear\n

34 arms, shall not be infringed.\n

35 \n

36 </p><p><h3>Amendment III</h3>
\n

37 \n

38 <p></p><p>No soldier shall, in time of peace be quartered in
any house,\n

39 without the consent of the owner, nor in time of war, but\n

40 in a manner to be prescribed by law.\n

41 \n

42 </p><p><h3>Amendment IV</h3>
\n

43 \n

44 <p></p><p>The right of the people to be secure in their
persons, houses,\n

45 papers, and effects, against unreasonable searches and
seizures,\n

46 shall not be violated, and no warrants shall issue, but
upon\n

47 probable cause, supported by oath or affirmation, and\n

48 particularly describing the place to be searched, and the\n

49 persons or things to be seized.\n

50 \n

51 </p><p><h3>Amendment V</h3>
\n

52 \n

53 <p></p><p>No person shall be held to answer for a capital, or
otherwise\n

54 infamous crime, unless on a presentment or indictment of a
grand
55 jury, except in cases arising in the land or naval forces,
56 or in the militia, when in actual service in time of war
or public danger; nor shall any person be subject for the
57 same offense to be twice put in jeopardy of life or limb;
58 nor shall be compelled in any criminal case to be a witness
59 against himself, nor be deprived of life, liberty, or
60 property,
without due process of law; nor shall private property be
61 taken for public use, without just compensation.
62
63
64 **Amendment VI**

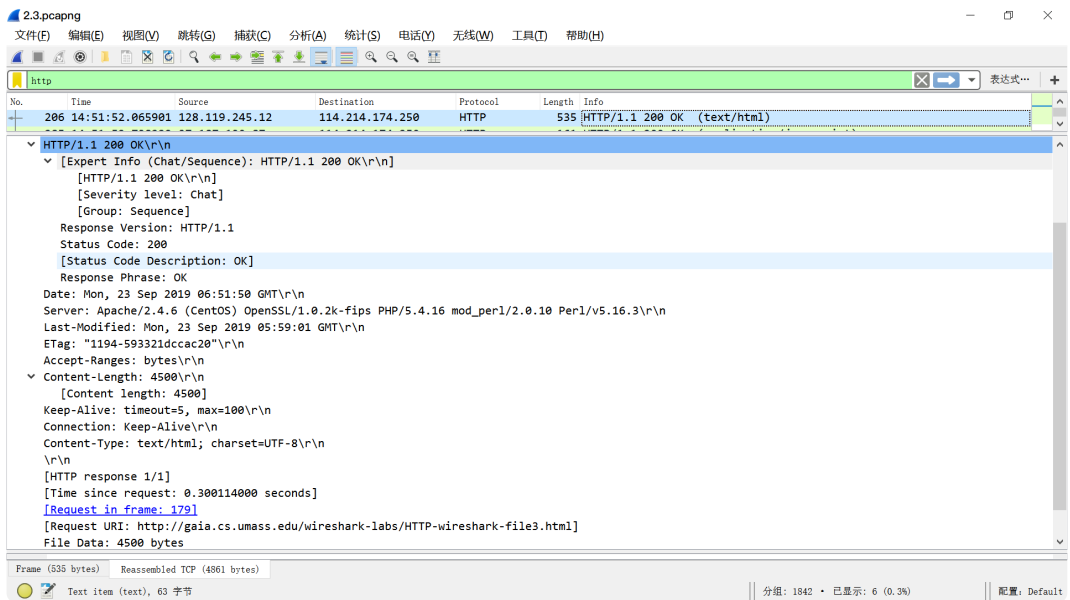
65
66 In all criminal prosecutions, the accused shall
enjoy the right
67 to a speedy and public trial, by an impartial jury of the
state
68 and district wherein the crime shall have been committed,
which
69 district shall have been previously ascertained by law, and
70 to be informed of the nature and cause of the accusation;
71 to be confronted with the witnesses against him; to have
72 compulsory process for obtaining witnesses in his favor,
73 and to have the assistance of counsel for his defense.
74
75 **Amendment VII**

76
77 In suits at common law, where the value in
controversy shall
78 exceed twenty dollars, the right of trial by jury shall be
79 preserved, and no fact tried by a jury, shall be otherwise
80 reexamined in any court of the United States, than
according
81 to the rules of the common law.
82
83 **Amendment VIII**

84
85 Excessive bail shall not be required, nor excessive
fines
86 imposed, nor cruel and unusual punishments inflicted.
87
88 **Amendment IX**

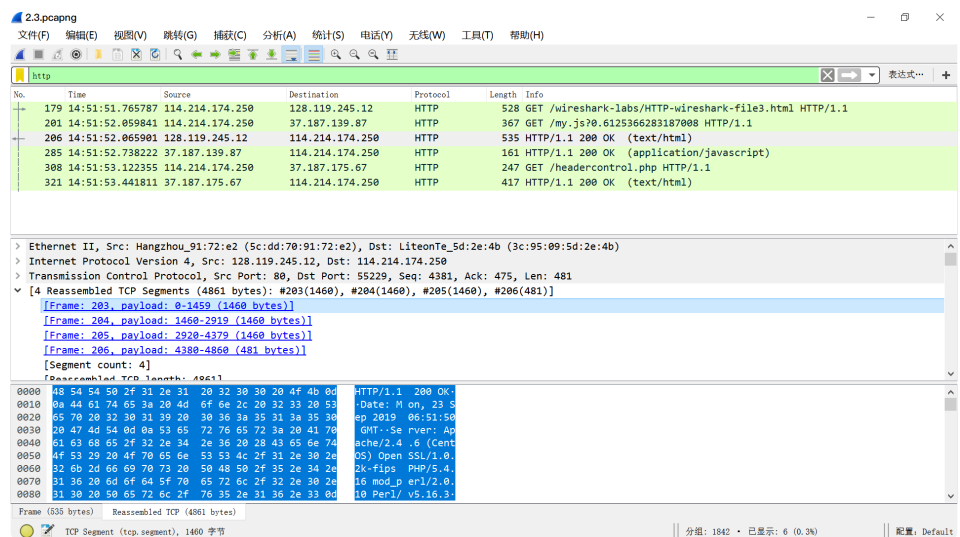
89
90 The enumeration in the Constitution, of certain
rights, shall
91 not be construed to deny or disparage others retained by the
people.
92
93 **Amendment X**

94
95
96 The powers not delegated to the United States by the
Constitution, nor prohibited
97 by it to the states, are reserved to the states
respectively, or to the people.
98



5. 阅读分组具体内容，对实验问题的回答如下

12. 浏览器发送了1个请求报文，在响应报文的第203、204、205与206分组中包含了相关内容



13. 在响应报文的第203分组中包含了状态码和与请求报文相关的状态短语

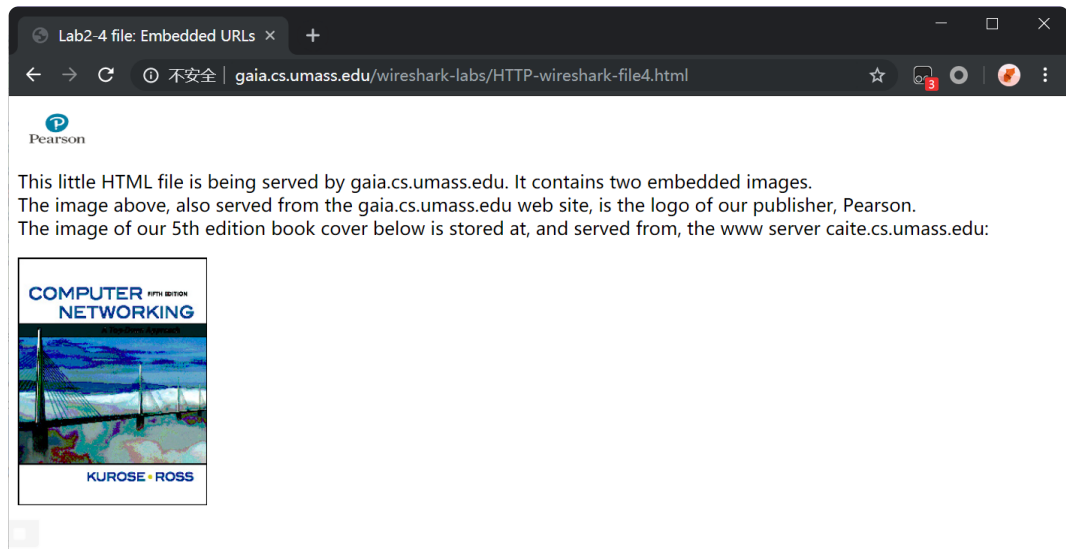
14. 状态码为 200 ，短语为 OK

15. 共计4861字节

嵌有对象的HTML文档

1. 清除浏览器缓存
2. 设置Wireshark捕获
3. 浏览给定网址

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



4. 捕获如下分组

1. HTTP请求报文

```
1 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Upgrade-Insecure-Requests: 1\r\n
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
7 Accept-Encoding: gzip, deflate\r\n
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
9 \r\n
```

2. HTTP响应报文

```
1 HTTP/1.1 200 OK\r\n
2 Date: Mon, 23 Sep 2019 13:45:01 GMT\r\n
3 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
4 Last-Modified: Mon, 23 Sep 2019 05:59:01 GMT\r\n
5 ETag: "2ca-593321dccfa41"\r\n
6 Accept-Ranges: bytes\r\n
7 Content-Length: 714\r\n
8 Keep-Alive: timeout=5, max=100\r\n
9 Connection: Keep-Alive\r\n
10 Content-Type: text/html; charset=UTF-8\r\n
11 \r\n
```

```
1 <html>\n
2 <head>\n
3 <title>Lab2-4 file: Embedded URLs</title>\n
4 <meta http-equiv="Content-Type" content="text/html;\n
charset=iso-8859-1">\n
5 </head>\n
```

```

6 | \n
7 | <body bgcolor="#FFFFFF" text="#000000">\n
8 |     \n
9 |     <p>\n
10 |          </p>\n
12 |     <p>This little HTML file is being served by
13 | gaia.cs.umass.edu. \n
14 |         It contains two embedded images. <br> The image above,
15 | also served from the \n
16 |         gaia.cs.umass.edu web site, is the logo of our publisher,
17 | Pearson. <br>\n
18 |         The image of our 5th edition book cover below is stored
19 | at, and served from, the www server caite.cs.umass.edu:</p>\n
20 |     <p align="left"></p>\n
23 | </body>\n
24 | </html>\n

```

3. HTTP请求报文

```

1 | GET /pearson.png HTTP/1.1\r\n
2 | Host: gaia.cs.umass.edu\r\n
3 | Connection: keep-alive\r\n
4 | User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
5 | (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 | Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
7 | Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
8 | file4.html\r\n
9 | Accept-Encoding: gzip, deflate\r\n
10 | Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
11 | \r\n

```

4. HTTP请求报文

```

1 | GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
2 | Host: manic.cs.umass.edu\r\n
3 | Connection: keep-alive\r\n
4 | User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
5 | (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 | Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
7 | Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-
8 | file4.html\r\n
9 | Accept-Encoding: gzip, deflate\r\n
10 | Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
11 | \r\n

```

5. HTTP响应报文

```
1 | HTTP/1.1 200 OK\r\n
2 | Date: Mon, 23 Sep 2019 13:45:02 GMT\r\n
3 | 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
4 | Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
5 | ETag: "cc3-539645c7flee7"\r\n
6 | Accept-Ranges: bytes\r\n
7 | Content-Length: 3267\r\n
8 | Keep-Alive: timeout=5, max=99\r\n
9 | Connection: Keep-Alive\r\n
10 | Content-Type: image/png\r\n
11 | \r\n
```

5. 阅读分组具体内容，对实验问题的回答如下

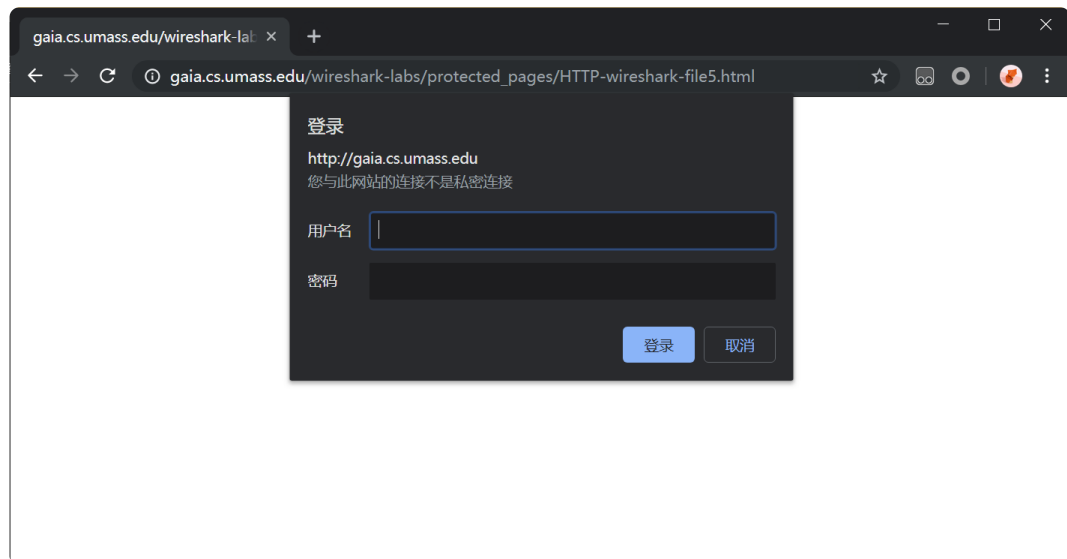
16. 浏览器发送了3个请求报文，都是向128.119.245.12发送的

17. 由于两个响应报文并非同时，因此浏览器是依序下载这两张图片的

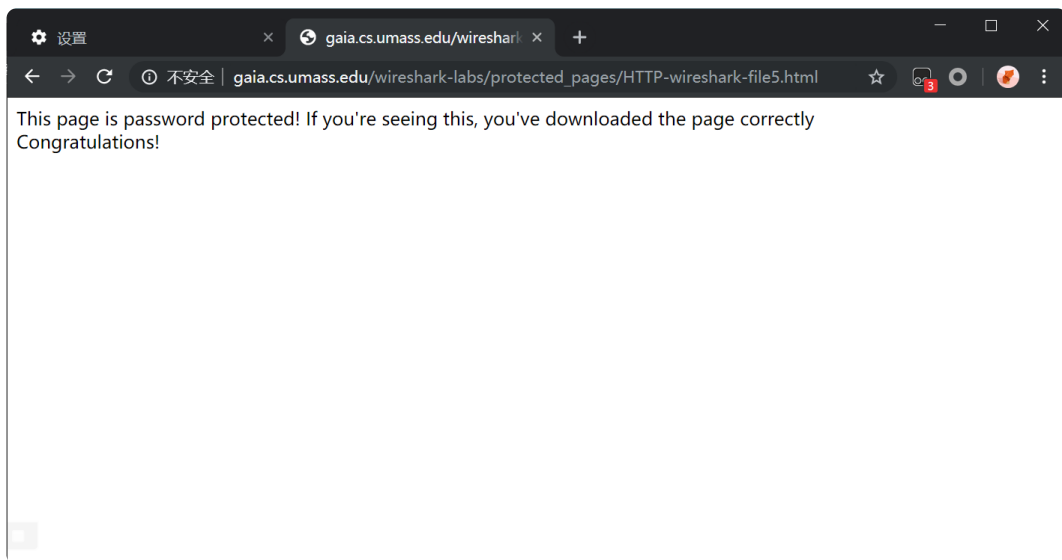
HTTP授权

1. 清除浏览器缓存
2. 设置Wireshark捕获
3. 浏览给定网址

<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file5.html>



4. 键入用户名 **wireshark-students** 与密码 **network**



5. 捕获如下分组

1. HTTP请求报文

```
1 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
  HTTP/1.1\r\n
2 Host: gaia.cs.umass.edu\r\n
3 Connection: keep-alive\r\n
4 Upgrade-Insecure-Requests: 1\r\n
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/76.0.3809.87 Safari/537.36\r\n
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
7 Accept-Encoding: gzip, deflate\r\n
8 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
9 \r\n
```

2. HTTP响应报文

```
1 HTTP/1.1 401 Unauthorized\r\n
2 Date: Mon, 23 Sep 2019 15:32:01 GMT\r\n
3 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
4 WWW-Authenticate: Basic realm="wireshark-students only"\r\n
5 Content-Length: 381\r\n
6 Keep-Alive: timeout=5, max=100\r\n
7 Connection: Keep-Alive\r\n
8 Content-Type: text/html; charset=iso-8859-1\r\n
9 \r\n
```

```

1 | <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
2 | <html><head>\n
3 |   <title>401 Unauthorized</title>\n
4 | </head><body>\n
5 |   <h1>Unauthorized</h1>\n
6 |   <p>This server could not verify that you\n
7 |     are authorized to access the document\n
8 |     requested. Either you supplied the wrong\n
9 |     credentials (e.g., bad password), or your\n
10 |    browser doesn't understand how to supply\n
11 |    the credentials required.</p>\n
12 | </body></html>\n

```

3. HTTP请求报文

```

1 | GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
   HTTP/1.1\r\n
2 | Host: gaia.cs.umass.edu\r\n
3 | Connection: keep-alive\r\n
4 | Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
5 | Credentials: wireshark-students:network
6 | Upgrade-Insecure-Requests: 1\r\n
7 | User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/76.0.3809.87
   Safari/537.36\r\n
8 | Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
   mage/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
9 | Accept-Encoding: gzip, deflate\r\n
10 | Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
11 | \r\n

```

4. HTTP响应报文

```

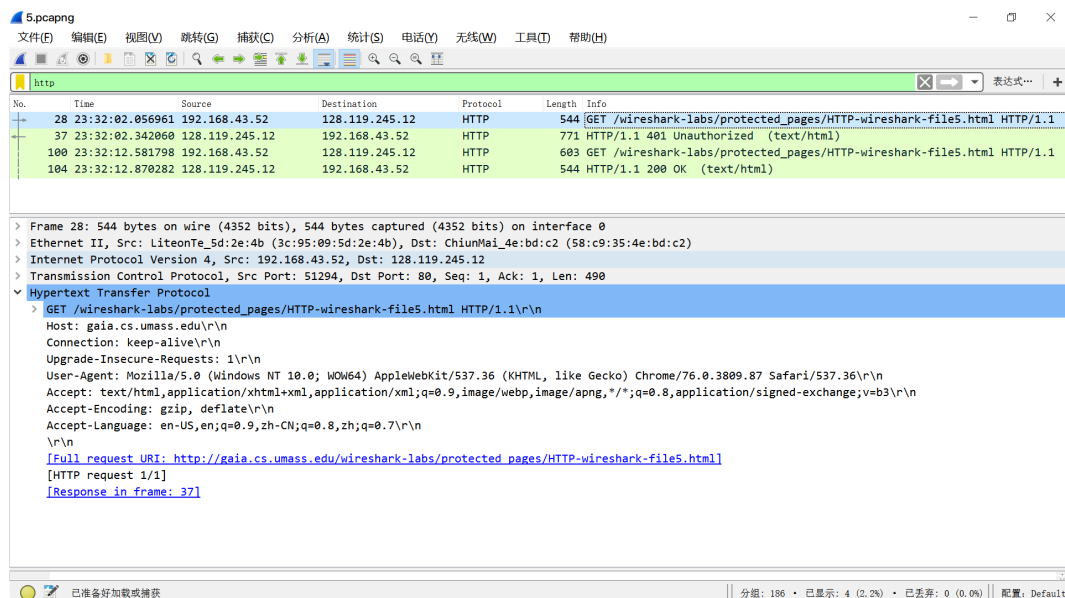
1 | HTTP/1.1 200 OK\r\n
2 | Date: Mon, 23 Sep 2019 15:32:12 GMT\r\n
3 | Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
   mod_perl/2.0.10 Perl/v5.16.3\r\n
4 | Last-Modified: Mon, 23 Sep 2019 05:59:01 GMT\r\n
5 | ETag: "84-593321dcd1d69"\r\n
6 | Accept-Ranges: bytes\r\n
7 | Content-Length: 132\r\n
8 | Keep-Alive: timeout=5, max=100\r\n
9 | Connection: Keep-Alive\r\n
10 | Content-Type: text/html; charset=UTF-8\r\n
11 | \r\n

```

```

1 | \n
2 | <html>\n
3 |   \n
4 |   This page is password protected! If you're seeing this, you've
   downloaded the page correctly <br>\n
5 |   Congratulations!\n
6 | </html>

```



6. 阅读分组具体内容，对实验问题的回答如下

18. 对于首次请求，服务器的响应为 **401 Unauthorized**，意为未授权

19. 第二次请求访问包含了如下的内容

```
1 | Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n
2 | Credentials: wireshark-students:network
```

提供了服务器要求的凭据

实验总结

本次实验主要研究了HTTP协议，通过捕获并分析包括条件响应、长文档、嵌入对象、授权等情况下的HTTP报文交互的具体内容，深入理解了HTTP的报文结构与有关字段的含义与功能，为之后向下学习网络结构提供了知识背景和基础。

附

本报告中出现的捕获分组文件以及相关截图可见 [GitHub@lyc0930](#)