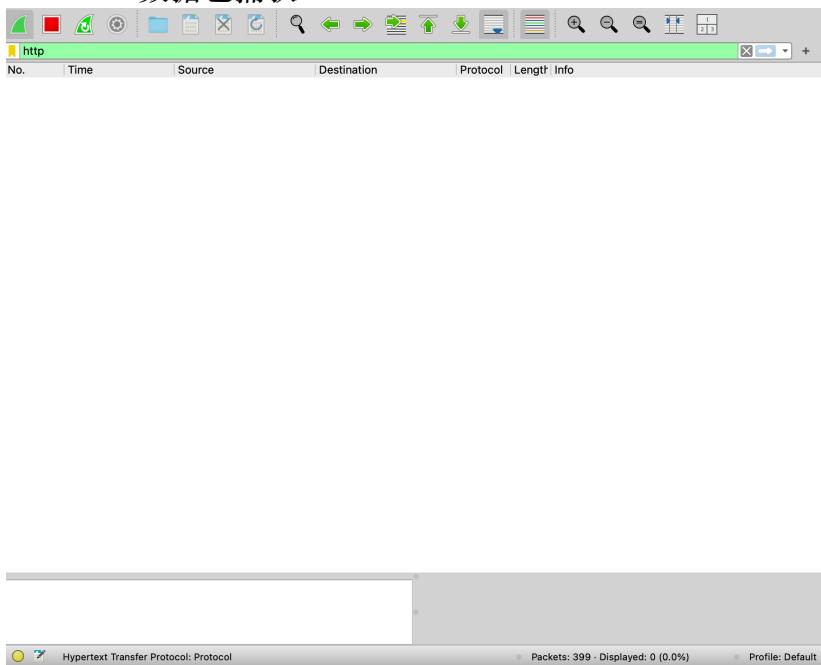


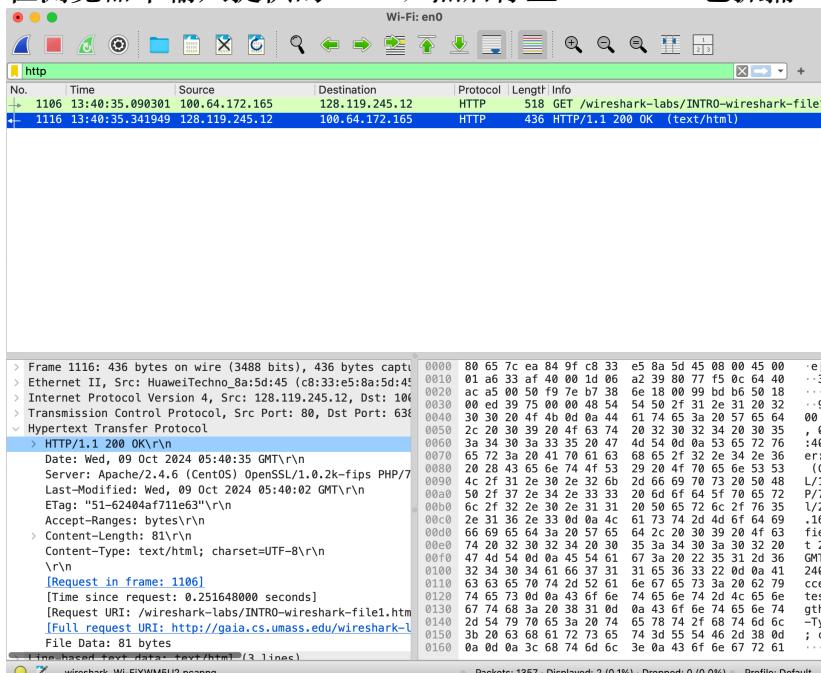
The Basic HTTP GET/response interaction

实验步骤

1. 启动 Chrome 浏览器。
2. 启动 Wireshark 数据包嗅探器，在 display-filter-specification 窗口中输入“http”，静待1分半钟后开始 Wireshark 数据包捕获。



3. 在浏览器中输入提供的 URL，然后停止 wireshark 包抓捕。



问题回答

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

浏览器运行的是 HTTP version 1.1；HTTP 版本是 Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips

PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3

```
> HTTP/1.1 200 OK\r\n
  Response Version: HTTP/1.1
  Status Code: 200
  [Status Code Description: OK]
  Response Phrase: OK
  Date: Wed, 09 Oct 2024 05:40:35 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: Wed, 09 Oct 2024 05:40:02 GMT\r\n
  ETag: "51-62404af711e63"\r\n
  Accept-Ranges: bytes\r\n
```

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

如图,是 zh-CN:

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
```

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

如下图:

我的 IP:100.64.172.165

服务器IP: 128.119.245.12

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

如下图

返回 200 OK

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

```
> Frame 1106: 436 bytes on wire (3488 bits), 436 bytes captured (3488 bits) on interface en0, id 0
> Ethernet II, Src: HuaweiTechno_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: Apple_ea:84:9f (80:65:7c:ea:84:9f)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.172.165
> Transmission Control Protocol, Src Port: 80, Dst Port: 63870, Seq: 1, Ack: 465, Len: 382
  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: Wed, 09 Oct 2024 05:40:35 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: Wed, 09 Oct 2024 05:40:02 GMT\r\n
      ETag: "51-62404af711e63"\r\n
      Accept-Ranges: bytes\r\n
      Content-Length: 81\r\n
      Content-Type: text/html; charset=UTF-8\r\n
      \r\n
      [Request in frame: 1106]
      [Time since request: 0.251648000 seconds]
      [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
      File Data: 81 bytes
  Line-based text data: text/html (3 lines)
```

如上图: Wed, 09 Oct 2024 05:40:02 GMT

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

```
> Content-Length: 81\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [Request in frame: 1106]
  [Time since request: 0.251648000 seconds]
  [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
  File Data: 81 bytes
```

如上图: 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.

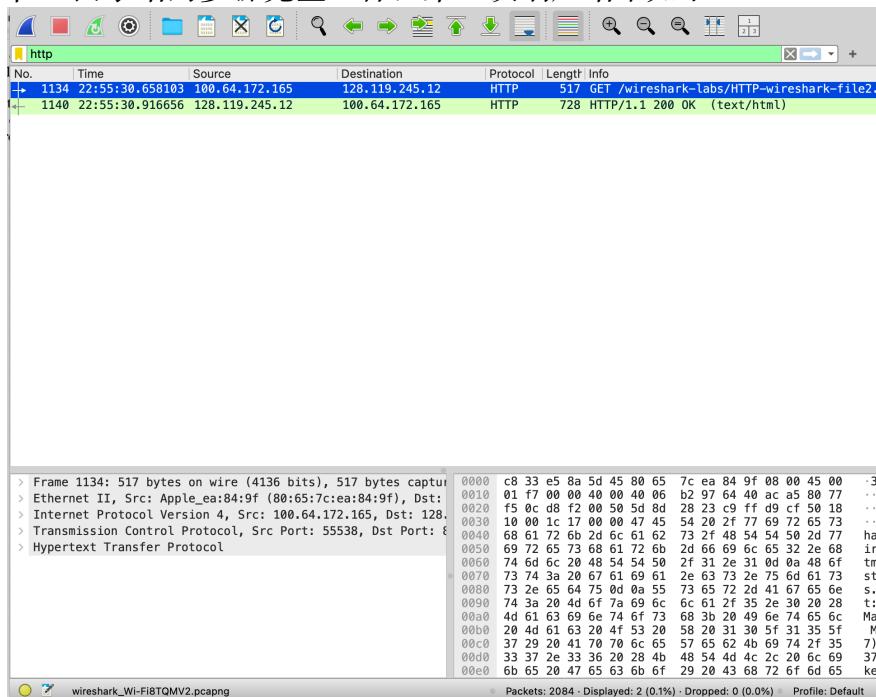
没有；如下图：

```
0000 c8 33 e5 8a 5d 45 80 65 7c ea 84 9f 08 00 45 00 -3...]E·e | ···· E·
0010 01 f8 00 00 40 00 40 06 b2 96 64 40 ac a5 80 77 ····@·@· ··@··w
0020 f5 0c f9 7e 00 50 00 99 bb e6 b7 38 6e 18 50 18 ...~·P···8n·P·
0030 10 00 51 df 00 00 47 45 54 20 2f 77 69 72 65 73 ··Q·GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 49 4e 54 52 4f 2d hark-lab s/INTRO-
0050 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e wireshar k-file1.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1·H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
0080 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age
0090 6e 74 3a 20 4d 6f 7a 69 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0
00a0 28 4d 61 63 69 6e 74 6f 73 68 3b 20 49 6e 74 65 (Macintosh; Inte
00b0 6c 20 4d 61 63 20 4f 53 20 58 20 31 30 5f 31 35 l Mac OS X 10.15
00c0 5f 37 29 20 41 70 70 6c 65 57 65 62 4b 69 74 2f _7) Appl eWebKit/
00d0 35 33 37 2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 537.36 (KHTML, l
00e0 69 6b 65 20 47 65 63 6b 6f 29 20 43 68 72 6f 6d ike Gecko) Chrom
00f0 65 2f 31 32 39 2e 30 2e 30 2e 30 53 61 66 61 e/129.0. 0.0 Safa
0100 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 ri/537.3 6.. Accep
0110 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/ html,app
0120 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication /xhtml+xml
0130 6d 6c 62 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 ,appl ication/x
0140 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 ml;q=0.9 ,image/a
0150 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 vif,imag e/webp,i
0160 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d mage/apn g,*/*;q=
0170 30 2e 38 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 0.8,appl ication/
0180 73 69 67 6e 65 64 2d 65 78 63 68 61 6e 67 65 3b signed-e xchange;
0190 76 3d 62 33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 v=b3;q=0 .7.. Acce
01a0 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 pt-Encod ing: gzi
01b0 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 63 65 p, defla te.. Acce
01c0 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 7a 68 2d pt-Langu age: zh-
01d0 43 4e 2c 7a 68 3b 71 3d 30 2e 39 2c 65 6e 3b 71 CN,zh;q= 0.9,en;q
01e0 3d 30 2e 38 0d 0a 55 70 67 72 61 64 65 2d 49 6e =0.8.. Up grade-In
01f0 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a secure-R equests:
0200 20 31 0d 0a 0d 0a 1....
```

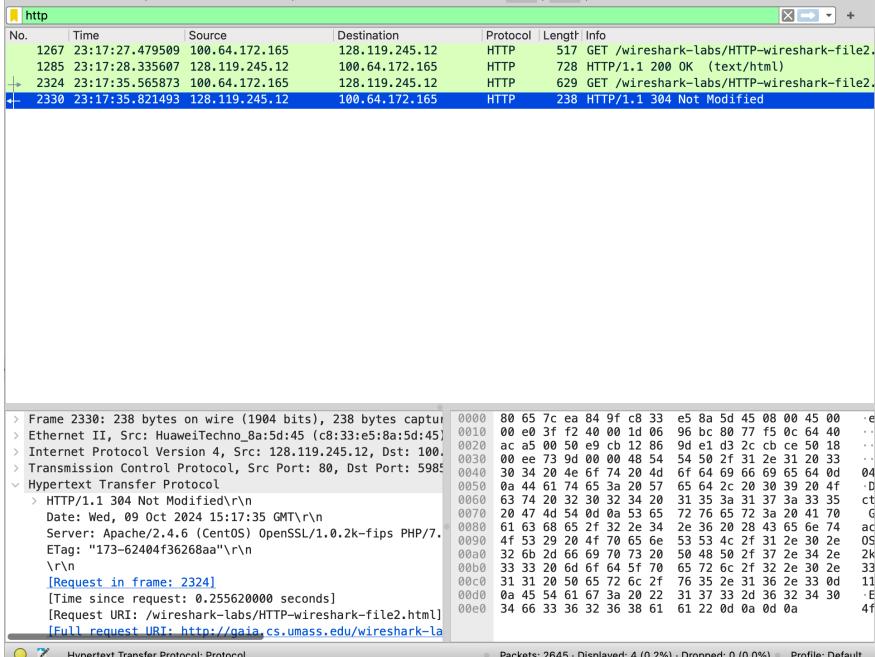
The HTTP CONDITIONAL GET/response interaction

实验步骤

和上面小结的步骤完全一样，第一次响应结果如下：



第二次如下:



问题回答

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?

```
✓ 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
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Request in frame: 2324]
    [Time since request: 0.255620000 seconds]
    [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

如上图,并没有发现。

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

有, 返回了一段 HTML 标记码, 包括了网页的文本。如下图:

```
✓ 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. <br>\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
```

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，它指示的是时间信息，这个时间与网页最后一次修改时间一致。

```
> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Host: gai.a.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.125 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
Cache-Control: max-age=0\r\n
If-Modified-Since: Wed, 09 Oct 2024 05:59:02 GMT\r\n
If-None-Match: "173-62404f36268aa"\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
```

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.

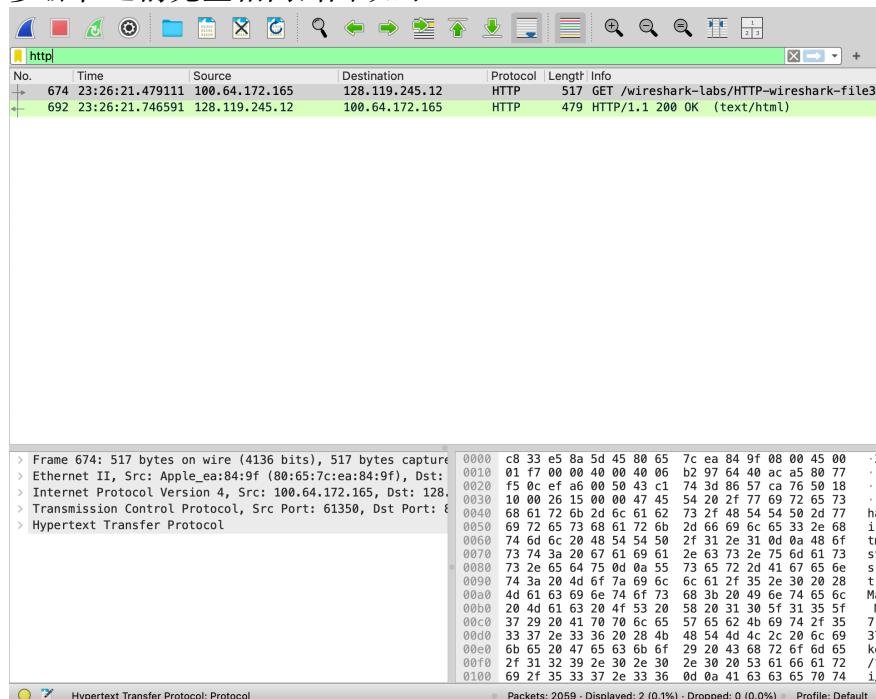
1267 23:17:27.479509 100.64.172.165	128.119.245.12	HTTP	517 GET /wireshark-labs/HTTP-wireshark-file2
1285 23:17:28.335607 128.119.245.12	100.64.172.165	HTTP	728 HTTP/1.1 200 OK (text/html)
2324 23:17:35.565873 100.64.172.165	128.119.245.12	HTTP	629 GET /wireshark-labs/HTTP-wireshark-file2
2330 23:17:35.821493 128.119.245.12	100.64.172.165	HTTP	238 HTTP/1.1 304 Not Modified

它返回了 304 状态码，这是因为如果客户端发送了一个带条件的GET 请求且该请求已被允许，而文档的内容（自上次访问以来或者根据请求的条件）并没有改变。

Retrieving Long Documents

实验步骤

步骤和之前完全相同,结果如下:



问题解答

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?

一共一个:

+ 674 23:26:21.479111 100.64.172.165	128.119.245.12	HTTP	517 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
- 692 23:26:21.746591 128.119.245.12	100.64.172.165	HTTP	479 HTTP/1.1 200 OK (text/html)

在 linked-based text data 这个包里面:

```
Line-based text data: text/html (98 lines)
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
<p><br>\n
</p></p><center><b>THE BILL OF RIGHTS</b><br>\n
<em>Amendments 1-10 of the Constitution</em>\n
</center>\n
\n
<p>The Conventions of a number of the States having, at the time of adopting\n
the Constitution, expressed a desire, in order to prevent misconstruction\n
or abuse of its powers, that further declaratory and restrictive clauses\n
should be added, and as extending the ground of public confidence in the\n
Government will best insure the beneficent ends of its institution; </p><p> Resolved,\n
States of America, in Congress assembled, two-thirds of both Houses concurring,\n
that the following articles be proposed to the Legislatures of the several\n
States, as amendments to the Constitution of the United States; all or any\n
of which articles, when ratified by three-fourths of the said Legislatures,\n
to be valid to all intents and purposes as part of the said Constitution,\n
namely: </p><p><a name="1"><strong><h3>Amendment I</h3></strong></a>\n
\n
<p></p><p>Congress shall make no law respecting an establishment of\n
religion, or prohibiting the free exercise thereof; or\n
abridging the freedom of speech, or of the press; or the\n
right of the people peaceably to assemble, and to petition\n
the government for a redress of grievances.\n
\n
</p><p><a name="2"><strong><h3>Amendment II</h3></strong></a>\n
\n
```

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

692 23:26:21.746591 128.119.245.12 100.64.172.165 HTTP 479 HTTP/1.1 200 OK (text/html)

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

200 OK, 表示请求成功，信息在返回的报文里

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

大概需要 5 个，如下图：

687 23:26:21.743487 100.64.172.165 128.119.245.12	TCP	65	[TCP ACKed unseen segment] 1050 -> 52807 [ACK] Seq=1 Ack=2 Len=0 TSeq=13363401313 TSecr=0
688 23:26:21.743487 100.64.172.165 128.119.245.12	TCP	68	89 -> 52807 [ACK] Seq=2 Ack=3 Len=0 TSeq=13363401313 TSecr=0
689 23:26:21.743487 100.64.172.165 128.119.245.12	TCP	1514	88 -> 61350 [ACK] Seq=3 Ack=464 Win=38336 Len=1460 [TCP PDU reassembled in 692]
690 23:26:21.746589 128.119.245.12 100.64.172.165	TCP	1514	88 -> 61350 [ACK] Seq=1461 Ack=464 Win=38336 Len=1460 [TCP PDU reassembled in 692]
691 23:26:21.746599 128.119.245.12 100.64.172.165	TCP	1514	88 -> 61350 [ACK] Seq=2921 Ack=464 Win=38336 Len=1460 [TCP PDU reassembled in 692]
692 23:26:21.746591 128.119.245.12 100.64.172.165	HTTP	479	HTTP/1.1 200 OK (text/html)

HTML Documents with Embedded Objects

实验步骤

结果如下：

No.	Time	Source	Destination	Protocol	Length	Info
981	23:37:04.838749	100.64.172.165	128.119.245.12	HTTP	517	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
985	23:37:05.094768	128.119.245.12	100.64.172.165	HTTP	1299	HTTP/1.1 200 OK (text/html)
987	23:37:05.153480	100.64.172.165	128.119.245.12	HTTP	463	GET /pearson.png HTTP/1.1
996	23:37:05.408654	128.119.245.12	100.64.172.165	HTTP	698	HTTP/1.1 200 OK (PNG)
1019	23:37:06.560704	100.64.172.165	178.79.137.164	HTTP	442	GET /BE_cover_small.jpg HTTP/1.1
1305	23:37:06.872550	178.79.137.164	100.64.172.165	HTTP	237	HTTP/1.1 301 Moved Permanently

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

一共发送了 3 个 HTTP GET 请求消息，这些 GET 请求发送到 128.119.245.12。

No.	Time	Source	Destination	Protocol	Length	Info
981	23:37:04.838749	100.64.172.165	128.119.245.12	HTTP	517	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
985	23:37:05.094768	128.119.245.12	100.64.172.165	HTTP	1299	HTTP/1.1 200 OK (text/html)
987	23:37:05.153480	100.64.172.165	128.119.245.12	HTTP	463	GET /pearson.png HTTP/1.1
996	23:37:05.408654	128.119.245.12	100.64.172.165	HTTP	698	HTTP/1.1 200 OK (PNG)
1019	23:37:06.560704	100.64.172.165	178.79.137.164	HTTP	442	GET /BE_cover_small.jpg HTTP/1.1
1305	23:37:06.872550	178.79.137.164	100.64.172.165	HTTP	237	HTTP/1.1 301 Moved Permanently

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.

串行下载，因为在第一张图片被下载完毕之后再开始下载第二张。

No.	Time	Source	Destination	Protocol	Length	Info
981	23:37:04.838749	100.64.172.165	128.119.245.12	HTTP	517	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
985	23:37:05.004768	128.119.245.12	100.64.172.165	HTTP	1299	HTTP/1.1 200 OK (text/html)
987	23:37:05.153468	100.64.172.165	128.119.245.12	HTTP	463	GET /pearson.png HTTP/1.1
996	23:37:05.408654	128.119.245.12	100.64.172.165	HTTP	698	HTTP/1.1 200 OK (PNG)
1019	23:37:06.560704	100.64.172.165	178.79.137.164	HTTP	442	GET /BE_cover_small.jpg HTTP/1.1
1305	23:37:06.872558	178.79.137.164	100.64.172.165	HTTP	237	HTTP/1.1 301 Moved Permanently

HTTP Authentication

实验步骤

最后结果为下图：

No.	Time	Source	Destination	Protocol	Length	Info
1297	23:43:15.723485	100.64.172.165	128.119.245.12	HTTP	541	GET /wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html HTTP/1.1
1373	23:43:45.983657	128.119.245.12	100.64.172.165	HTTP	715	HTTP/1.1 401 Unauthorized (text/html)
2634	23:43:56.237178	100.64.172.165	128.119.245.12	HTTP	606	GET /wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html HTTP/1.1
340	23:44:06.409003	128.119.245.12	100.64.172.165	HTTP	715	HTTP/1.1 401 Unauthorized (text/html)
5789	23:44:36.427908	100.64.172.165	128.119.245.12	HTTP	631	GET /wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html HTTP/1.1
6791	23:44:38.488332	128.119.245.12	100.64.172.165	HTTP	538	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 Unauthorized,该状态码表示用户没有访问权限，需要进行身份认证。

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

> Frame 1373: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface en0
> Ethernet II, Src: HuaweiTechno_8a:5d:45 (c8:33:e5:8a:5d:45), Dst: Apple_ea:84:9f (80:65:7c)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 100.64.172.165
> Transmission Control Protocol, Src Port: 80, Dst Port: 64192, Seq: 1, Ack: 488, Len: 661
<< Hypertext Transfer Protocol
> HTTP/1.1 401 Unauthorized\r\n
Date: Wed, 09 Oct 2024 15:43:46 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
WWW-Authenticate: Basic realm="wireshark-students only"\r\n
> Content-Length: 381\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
\r\n\r\n
[Request in frame: 1297]
[Time since request: 0.260172000 seconds]
[Request URI: /wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html]
File Data: 381 bytes
<< Line-based text data: text/html (12 lines)
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
<html><head>\n
<title>401 Unauthorized</title>\n
</head><body>\n
<h1>Unauthorized</h1>\n
<p>This server could not verify that you\n
are authorized to access the document\n
requested. Either you supplied the wrong\n
credentials (e.g., bad password), or your\n
browser doesn't understand how to supply\n
the credentials required.</p>\n
</body></html>\n

```
> Frame 6786: 626 bytes on wire (5008 bits), 626 bytes captured (5008 bits) on interface en0
> Ethernet II, Src: Apple_ea:84:9f (80:65:7c:ea:84:9f), Dst: HuaweiTechno_8a:5d:45 (c8:33:e5)
> Internet Protocol Version 4, Src: 100.64.172.165, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64351, Dst Port: 80, Seq: 1, Ack: 1, Len: 572
  Hypertext Transfer Protocol
    > GET /wireshark-labs/protected_pages/HTTP-wireshark%EF%BF%BEfile5.html HTTP/1.1\r\n
      Host: gaia.cs.umass.edu\r\n
      User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.147 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\r\n
      Accept-Encoding: gzip, deflate\r\n
      Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
    < Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRz0m5ldHdvcms=\r\n
      Credentials: wireshark-students:network\r\n
      Cache-Control: max-age=0\r\n
      Upgrade-Insecure-Requests: 1\r\n
      \r\n
      [Response in frame: 6791]
      [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresha
```

多了 Authorization 和 Credentials 字段，即用于网页提交用户名和密码。