计算机网络_实验2_HTTP

学号:PB20000219　姓名:李蔚林

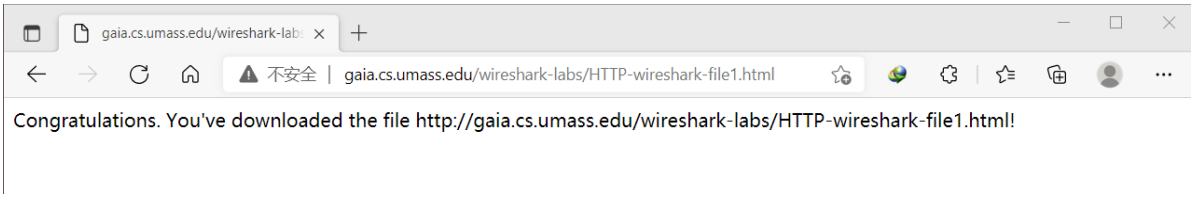
实验目的

1. 加强对Wireshark工具的理解,巩固其使用方法
2. 了解并学会分析HTTP协议,包括长文件,嵌入网页对象和加密网页

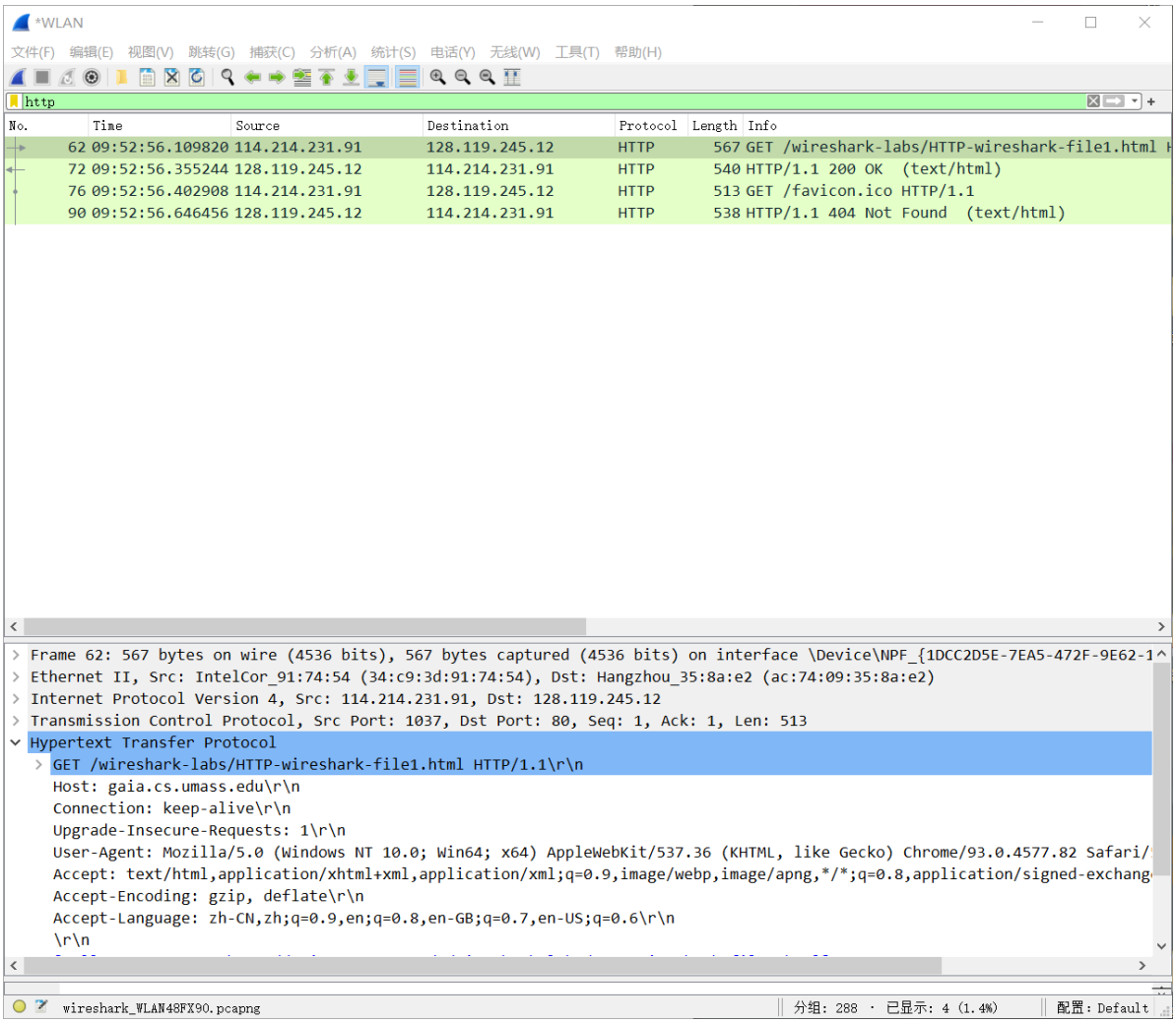
实验1_The Basic HTTP GET/response interaction

实验步骤

1. 打开浏览器,然后打开Wireshark工具
2. 一分钟后开始抓包并进入网址http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
3. 关闭捕捉



实验结果



问题回答

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

我的浏览器运行版本为HTTP1.1,服务器运行版本为HTTP1.1.

```
No.     Time               Source               Destination          Protocol Length Info
     62 09:52:56.109820    114.214.231.91       128.119.245.12       HTTP     567    GET /wireshark-labs/HTTP-wireshark-
file1.html HTTP/1.1
Frame 62: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1037, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

```
No.     Time               Source               Destination          Protocol Length Info
     72 09:52:56.355244    128.119.245.12       114.214.231.91       HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 72: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 1037, Seq: 1, Ack: 514, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Sep 2021 01:52:56 GMT\r\n
```

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

可以接受中文(zh-CN),英文(en,en-GB,en-US)

```
Frame 62: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1037, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 S
537.36 Edg/93.0.961.52\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    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
```

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

我的电脑的IP地址为:114.214.231.91,gaia.cs.umass.edu的服务器的地址为128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
62	09:52:56.109820	114.214.231.91	128.119.245.12	HTTP	567	GET /wireshark-labs/HTTP-wireshark-fi
72	09:52:56.355244	128.119.245.12	114.214.231.91	HTTP	540	HTTP/1.1 200 OK (text/html)
76	09:52:56.402908	114.214.231.91	128.119.245.12	HTTP	513	GET /favicon.ico HTTP/1.1
90	09:52:56.646456	128.119.245.12	114.214.231.91	HTTP	538	HTTP/1.1 404 Not Found (text/html)

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

服务器返回200 OK代码

```
567 GET /wireshark-labs/HTTP-wireshark-fi
540 HTTP/1.1 200 OK  (text/html)
```

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

最后一次修改在:Thu,23 Sep 2021 05:59:02

```
No.     Time              Source              Destination         Protocol Length Info
     72 09:52:56.355244   128.119.245.12      114.214.231.91      HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 72: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 1037, Seq: 1, Ack: 514, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Sep 2021 01:52:56 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 23 Sep 2021 05:59:02 GMT\r\n
```

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

返回了128Byte的内容

```
    [Next response in frame: 90]
    [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)
```

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.

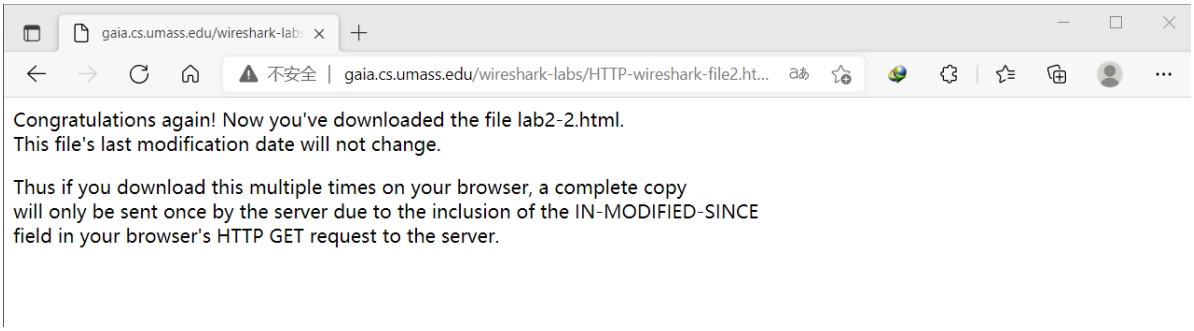
数据中有如下header,例如Accept-Language没有在packet-listing window显示.

```
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
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Sa
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
  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
```

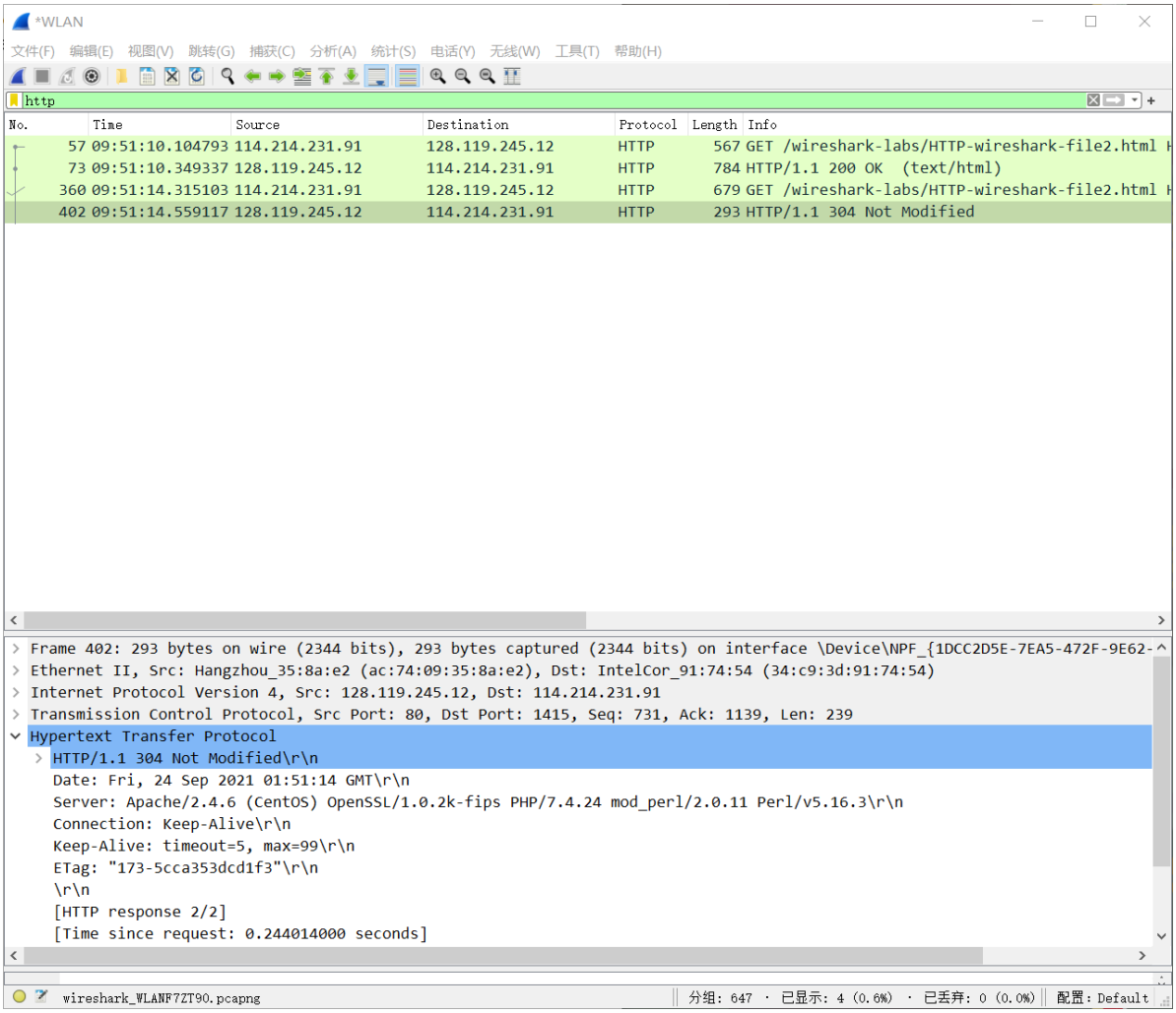
实验2_The HTTP CONDITIONAL GET/response interaction

实验步骤

1. 打开浏览器并确保已清除浏览器缓存.打开Wireshark工具
2. 打开网址http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
3. 迅速刷新网页或者重新输入相同的URL
4. 停止捕获,检索http项,可以看到有两个GET请求及其返回信息.



实验结果



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?

没有.

```
No.     Time               Source                Destination           Protocol Length Info
     57 09:51:10.104793    114.214.231.91        128.119.245.12        HTTP     567    GET /wireshark-labs/HTTP-wireshark-
file2.html HTTP/1.1
Frame 57: 567 bytes on wire (4536 bits), 567 bytes captured (4536 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1415, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file2.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 Gecko) Chrome/93.0.4577.82 Safari/
537.36 Edg/93.0.961.52\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    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
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 73]
    [Next request in frame: 360]
```

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

服务器返回了我想要的文件,从这里可以看到返回的text即为我们想要的结果

```
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Sep 2021 01:51:10 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\
    Last-Modified: Thu, 23 Sep 2021 05:59:02 GMT\r\n
    ETag: "173-5cca353dcd1f3"\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 1/2]
    [Time since request: 0.244544000 seconds]
    [Request in frame: 57]
    [Next request in frame: 360]
    [Next response in frame: 402]
    [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)
```

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?

有这个内容,跟在这个标题后面的是上一次得到的服务器修改该文件的时间: Thu, 23 Sep 2021 05:59:02

```
No.     Time                Source                Destination           Protocol Length Info
    360 09:51:14.315103     114.214.231.91        128.119.245.12        HTTP     679    GET /wireshark-labs/HTTP-wireshar
file2.html HTTP/1.1
Frame 360: 679 bytes on wire (5432 bits), 679 bytes captured (5432 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1415, Dst Port: 80, Seq: 514, Ack: 731, Len: 625
Hypertext Transfer Protocol
    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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Saf
537.36 Edg/93.0.961.52\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    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: "173-5cca353dcd1f3"\r\n
    If-Modified-Since: Thu, 23 Sep 2021 05:59:02 GMT\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.

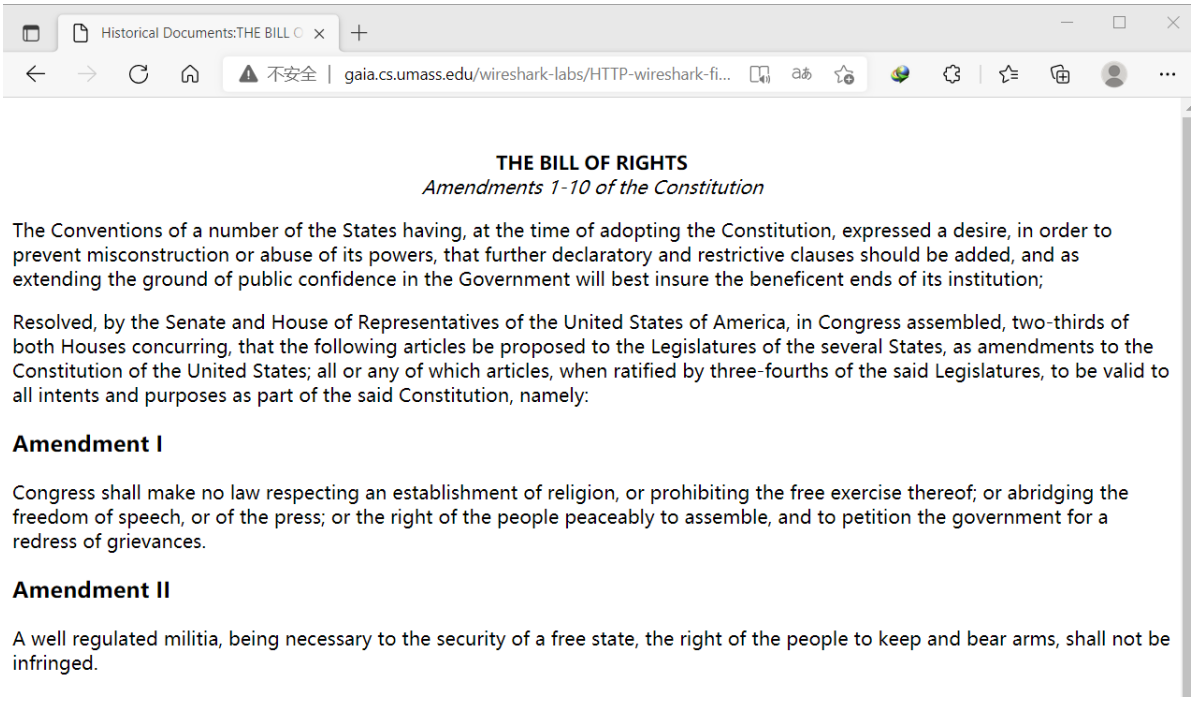
返回代码为 304 Not Modified. 服务器没有返回文件的内容,而是直接调用本地cache.因为自上一次访问时间较短,服务器未改变文件,所以返回304 Modified.

```
    [Response in frame: 402]
No.     Time                Source                Destination           Protocol Length Info
    402 09:51:14.559117     128.119.245.12        114.214.231.91        HTTP     293    HTTP/1.1 304 Not Modified
Frame 402: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 1415, Seq: 731, Ack: 1139, Len: 239
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 24 Sep 2021 01:51:14 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5cca353dcd1f3"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.244014000 seconds]
    [Prev request in frame: 57]
    [Prev response in frame: 73]
    [Request in frame: 360]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

实验3_Retrieving Long Documents

实验步骤

1. 打开浏览器并确保已清除浏览器缓存.打开Wireshark工具
2. 打开网址http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
3. 停止捕获,检索http项,可以看到GET请求和其返回信息.



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:

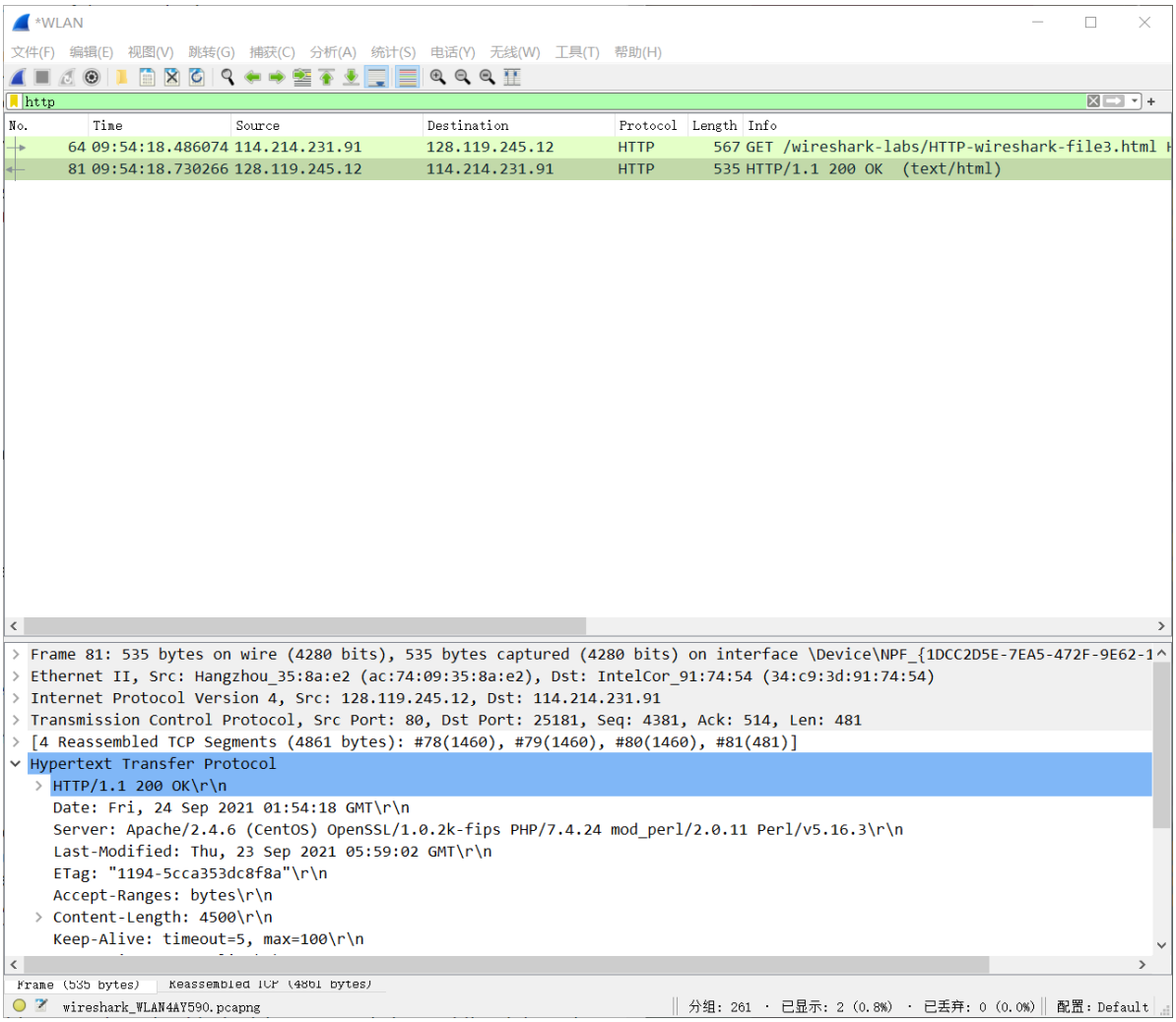
Amendment I

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.

实验结果



问题回答

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?

一共发送了1个GET request. packet number 81.

No.	Time	Source	Destination	Protocol	Length	Info
64	09:54:18.486074	114.214.231.91	128.119.245.12	HTTP	567	GET /wireshark-labs/HTTP-wireshark-file3.html H
81	09:54:18.730266	128.119.245.12	114.214.231.91	HTTP	535	HTTP/1.1 200 OK (text/html)

```
No.     Time                Source                Destination           Protocol Length Info
     81 09:54:18.730266     128.119.245.12        114.214.231.91        HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 81: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 25181, Seq: 4381, Ack: 514, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #78(1460), #79(1460), #80(1460), #81(481)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Sep 2021 01:54:18 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 23 Sep 2021 05:59:02 GMT\r\n
    ETag: "1194-5cca353dc8f8a"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\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: 0.244192000 seconds]
    [Request in frame: 64]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
```

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

如下图 packet No.81 包含status code: 200 OK.


```
No.     Time                Source                Destination           Protocol Length Info
     81 09:54:18.730266     128.119.245.12        114.214.231.91        HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 81: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 25181, Seq: 4381, Ack: 514, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #78(1460), #79(1460), #80(1460), #81(481)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 24 Sep 2021 01:54:18 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.24 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Thu, 23 Sep 2021 05:59:02 GMT\r\n
    ETag: "1194-5cca353dc8f8a"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 4500\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: 0.244192000 seconds]
    [Request in frame: 64]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
```


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?

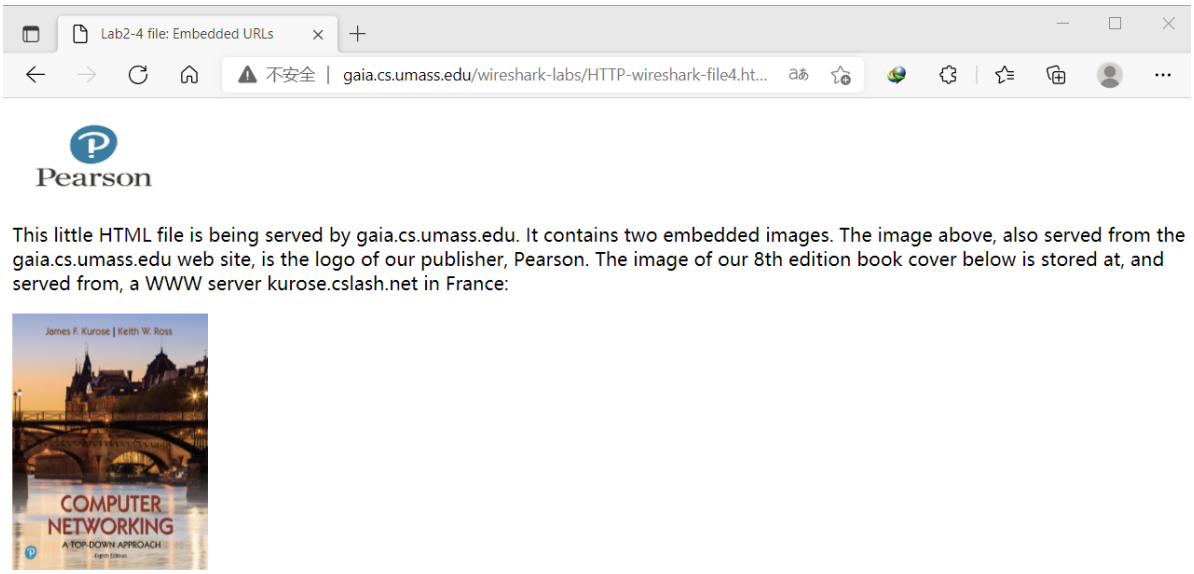
4个TCP segment 被用来传输单个HTTP response.

```
No.     Time                Source                Destination           Protocol Length Info
     81 09:54:18.730266     128.119.245.12        114.214.231.91        HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 81: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_91:74:54 (34:c9:3d:91:74:54)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.231.91
Transmission Control Protocol, Src Port: 80, Dst Port: 25181, Seq: 4381, Ack: 514, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #78(1460), #79(1460), #80(1460), #81(481)]
```

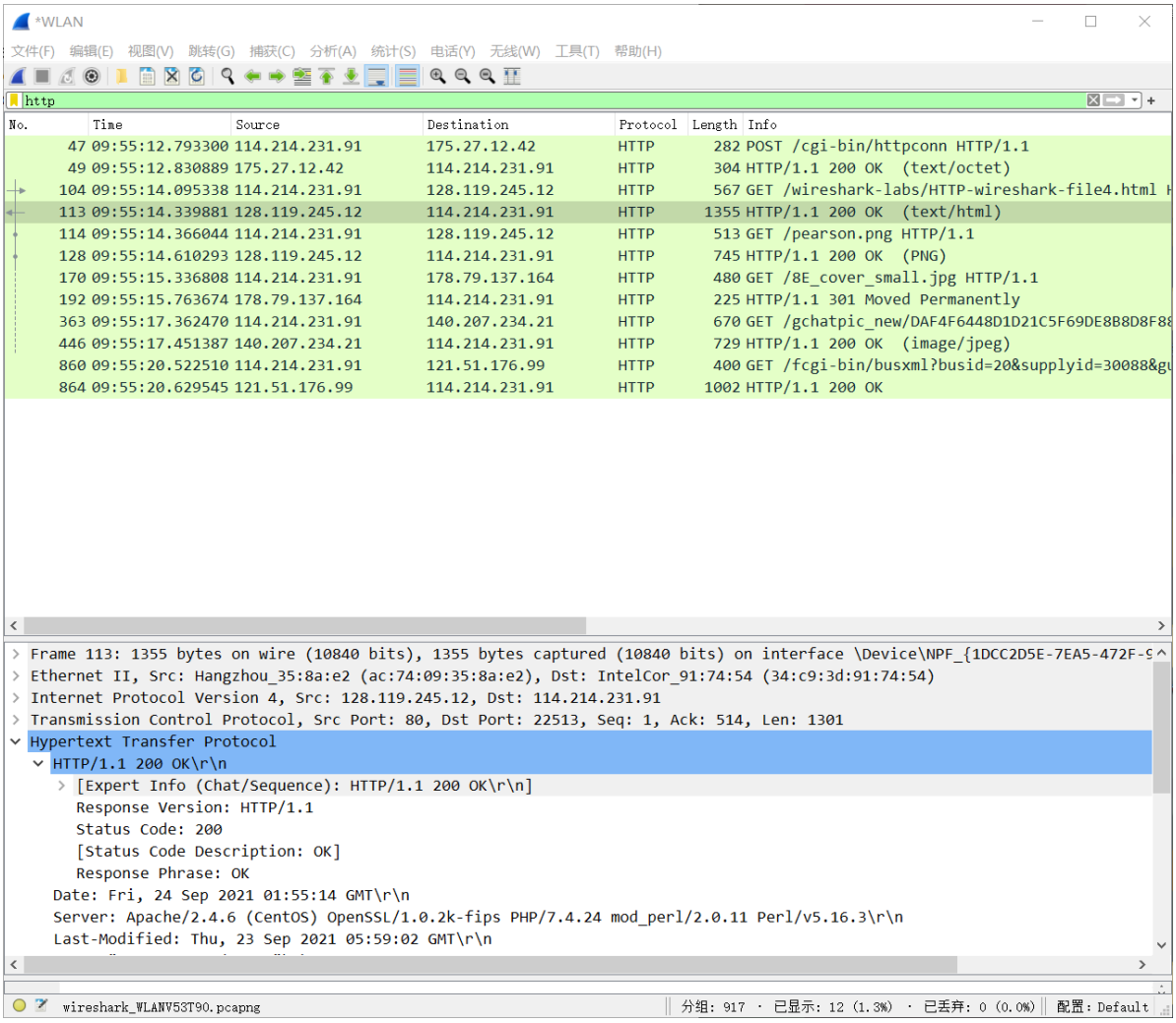
实验4_ HTML Documents with Embedded Objects

实验步骤

1. 打开浏览器并确保已清除浏览器缓存.打开Wireshark工具
2. 打开网址http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
3. 停止捕获,检索http项,可以看到GET请求和其返回信息.



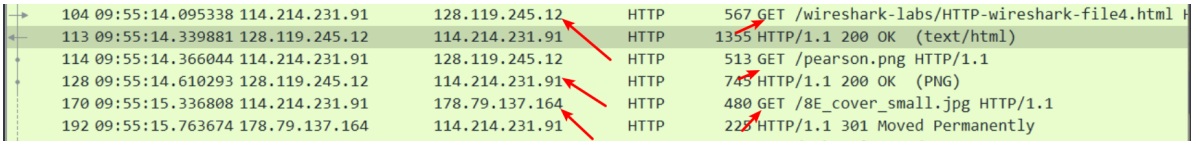
实验结果



问题回答

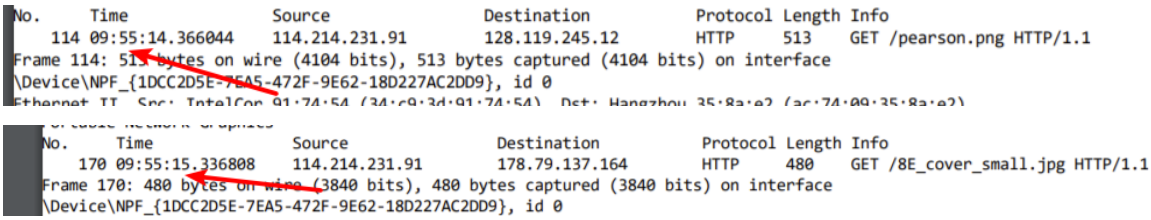
16.How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

发送了三个GET request. 前两个到128.119.245.12,后一个发送到178.79.137.164(据助教说是永久移动地址/重定向)



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.

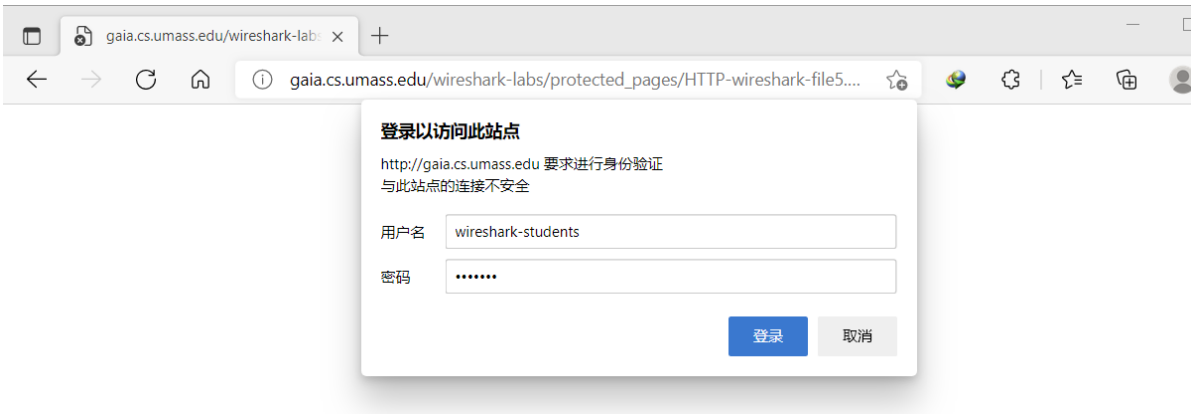
是先后下载的,包的发送时间有延迟,第一个是.366044发送的请求,第二个是.336808发送的请求

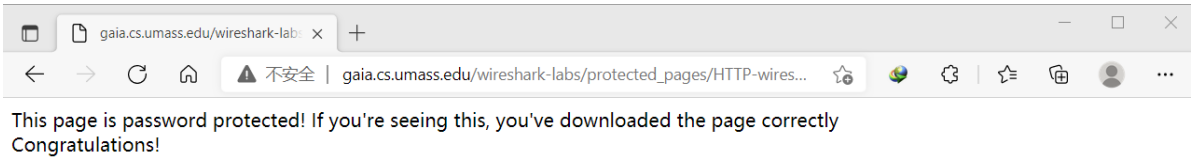


实验5_ HTTP Authentication

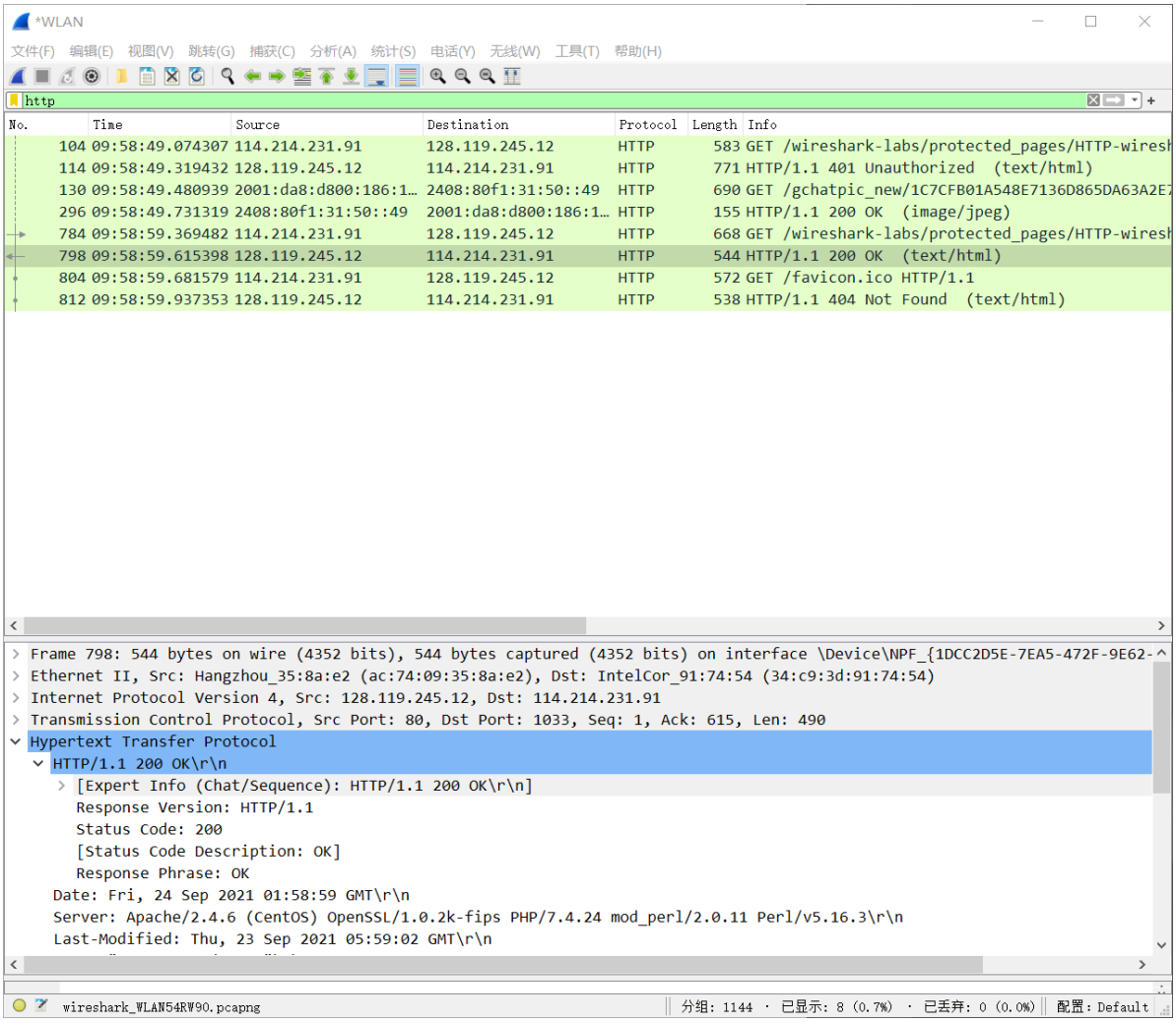
实验步骤

1. 打开浏览器并确保已清除浏览器缓存.打开Wireshark工具
2. 打开网址http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file5.html
3. 在新打开的界面窗口中输入用户名和密码
4. 停止捕获,检索http项,可以看到GET请求及其返回信息.





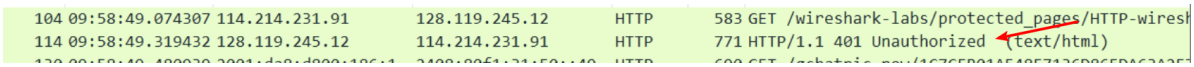
实验结果



问题回答

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?

多了Cache-Control 和 Authorization 两部分

```
No.     Time                Source              Destination         Protocol Length Info
    784 09:58:59.369482     114.214.231.91      128.119.245.12      HTTP     668    GET /wireshark-labs/protected_pages
HTTP-wireshark-file5.html HTTP/1.1
Frame 784: 668 bytes on wire (5344 bits), 668 bytes captured (5344 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1033, Dst Port: 80, Seq: 1, Ack: 1, Len: 614
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): 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
    Cache-Control: max-age=0\r\n
    Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
No.     Time                Source                Destination           Protocol Length Info
    104 09:58:49.074307     114.214.231.91        128.119.245.12        HTTP     583    GET /wireshark-labs/protected_pages
HTTP-wireshark-file5.html HTTP/1.1
Frame 104: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface
\Device\NPF_{1DCC2D5E-7EA5-472F-9E62-18D227AC2DD9}, id 0
Ethernet II, Src: IntelCor_91:74:54 (34:c9:3d:91:74:54), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
Internet Protocol Version 4, Src: 114.214.231.91, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 1029, Dst Port: 80, Seq: 1, Ack: 1, Len: 529
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safar
537.36 Edg/93.0.961.52\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
```

没有authorization

实验总结

本次实验中,我学习并巩固了HTTP协议的相关内容,同时复习了Wireshark工具的应用.在实验中遇到一些小问题并及时向助教咨询,在助教的帮助下完成了本次实验.