中国科学技术大学计算机学院

计算机网络实验报告

实验二

利用 Wireshark 观察 http 报文

学　　号：**JL19110004**

姓　　名：徐语林

专　　业：计算机科学与技术

指导老师：张信明

中国科学技术大学计算机学院

2020 年 **10** 月 **25** 日

一、　实验目的

1、　熟悉并掌握 wireshark 网络分析工具；

2、　捕获观察并分析 HTTP 报文结构；

二、　实验原理

Wireshark 是一种非常流行的网络封包分析软件，功能十分强大。可以截取各种网络封包，显示网络封包的各种详细信息。Wireshark 使用 Npcap 作为接口，直接与网卡进行数据报文交换，监听共享网络上传送的数据包

三、　实验条件

1、　硬件条件：一台 PC 机

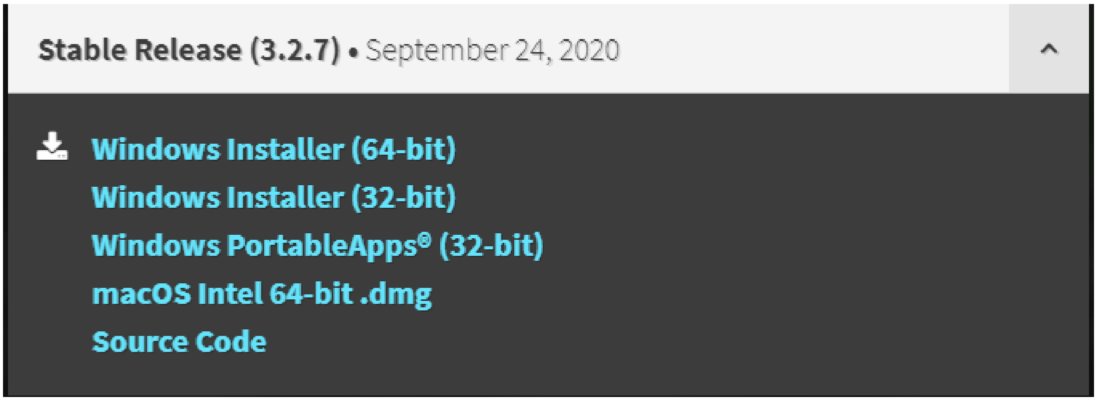
2、　软件条件：win10, wireshark 软件

四、　实验过程

1、　wireshark 的安装

按照助教给定的网址 https://www.wireshark.org/#download

根据自己的环境选择 wireshark 下载，如下图



Stable Release (3.2.7) • September 24, 2020

Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS Intel 64-bit .dmg
Source Code

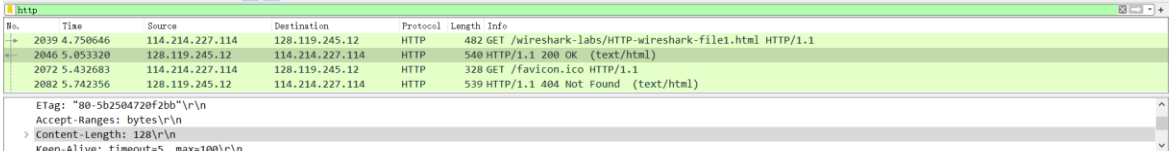
2、 利用 wireshark 来观察报文

（1）The Basic HTTP GET/response interaction

先打开 chrome 浏览器，将里面的缓存清空；再打开 wireshark；开始捕获的时候设置过滤为“http”；打开第一个网址：

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

稍等一小会儿停止捕获，得下图报文：



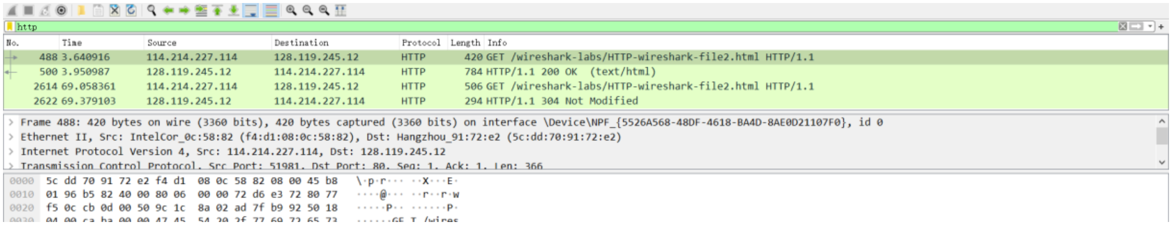
```
http
No.   Time      Source           Destination      Protocol Length Info
2039 4.750646  114.214.227.114  128.119.245.12   HTTP     482 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2046 5.053320  128.119.245.12   114.214.227.114  HTTP     540 HTTP/1.1 200 OK  (text/html)
2072 5.432683  114.214.227.114  128.119.245.12   HTTP     328 GET /favicon.ico HTTP/1.1
2082 5.742356  128.119.245.12   114.214.227.114  HTTP     539 HTTP/1.1 404 Not Found  (text/html)

    ETag: "80-5b2504720f2bb"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

（2）The HTTP CONDITIONAL GET/response interaction

首先清空缓存，重新打开 wireshark 进行报文的捕获，打开第二个网页：

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

然后快速进行一次刷新，停止捕获，如下图：



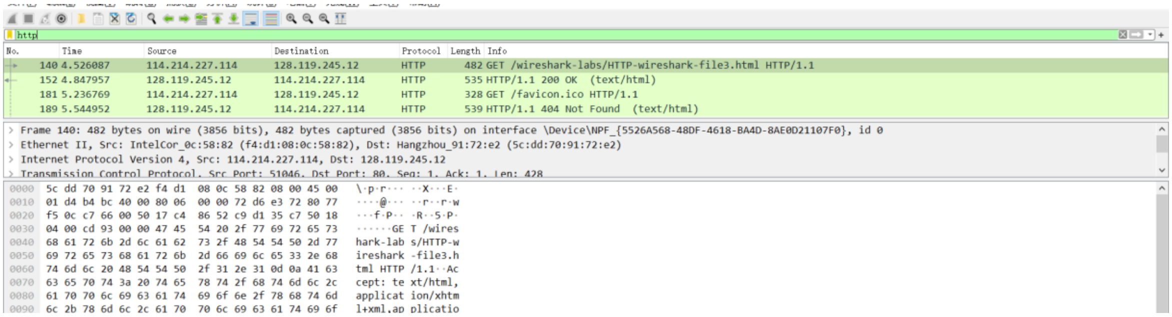
```
http
No.     Time        Source            Destination       Protocol  Length  Info
   488  3.640916    114.214.227.114   128.119.245.12    HTTP       420 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   500  3.950987    128.119.245.12    114.214.227.114   HTTP       784 HTTP/1.1 200 OK  (text/html)
  2614  69.058361   114.214.227.114   128.119.245.12    HTTP       506 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  2622  69.379103   128.119.245.12    114.214.227.114   HTTP       294 HTTP/1.1 304 Not Modified

> Frame 488: 420 bytes on wire (3360 bits), 420 bytes captured (3360 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.227.114, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51981, Dst Port: 80, Seq: 1, Ack: 1, Len: 366

0000  5c dd 70 91 72 e2 f4 d1  08 0c 58 82 08 00 45 b8   \·p·r··· ··X···E·
0010  01 96 b5 82 40 00 80 06  00 00 72 d6 e3 72 80 77   ····@··· ··r··r·w
0020  f5 0c cb 0d 00 50 9c 1c  8a 02 ad 7f b9 92 50 18   ·····P·· ······P·
0030  04 00 ca ba 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
```

（3）Retrieving Long Documents

清空浏览器缓存，打开 wireshark 开始捕获，并打开第三个网页：

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

稍等一小会儿停止捕获，得到如下图报文：



```
http
No.     Time        Source            Destination       Protocol  Length  Info
   140  4.526087    114.214.227.114   128.119.245.12    HTTP       482 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   152  4.847957    128.119.245.12    114.214.227.114   HTTP       535 HTTP/1.1 200 OK  (text/html)
   181  5.236769    114.214.227.114   128.119.245.12    HTTP       328 GET /favicon.ico HTTP/1.1
   189  5.544952    128.119.245.12    114.214.227.114   HTTP       539 HTTP/1.1 404 Not Found  (text/html)

> Frame 140: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.227.114, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51046, Dst Port: 80, Seq: 1, Ack: 1, Len: 428

0000  5c dd 70 91 72 e2 f4 d1  08 0c 58 82 08 00 45 00   \·p·r··· ··X···E·
0010  01 d4 b4 bc 40 00 80 06  00 00 72 d6 e3 72 80 77   ····@··· ··r··r·w
0020  f5 0c c7 66 00 50 17 c4  86 52 c9 d1 35 c7 50 18   ···f·P·· ·R··5·P·
0030  04 00 cd 93 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   tml HTTP /1.1··Ac
0070  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
0080  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
0090  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
```

（4）HTML Documents with Embedded Objects

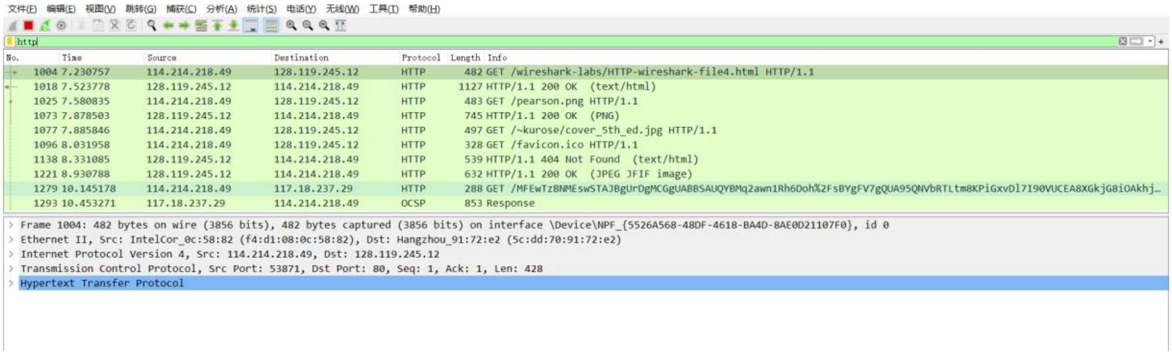
清空浏览器缓存，打开 wireshark 进行捕获报文，并打开第四个网页：

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

等到两张图片都加载完之后停止捕获，得到下图所示报文：

（5）HTTP Authentication

清空浏览器，打开 wireshark 开始捕获。并打开第五个网页：

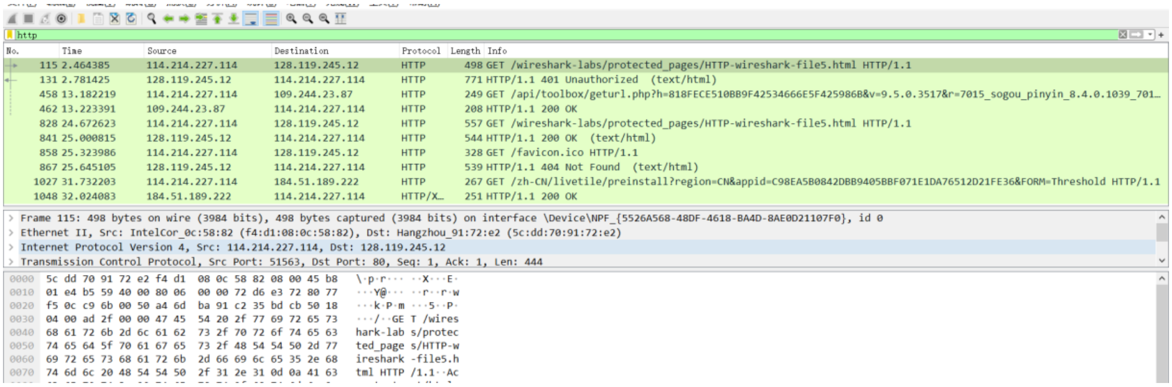

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http

```
No.     Time        Source           Destination      Protocol  Length  Info
   1004 7.230757    114.214.218.49   128.119.245.12   HTTP      482 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   1018 7.523778    128.119.245.12   114.214.218.49   HTTP      1127 HTTP/1.1 200 OK  (text/html)
   1025 7.580835    114.214.218.49   128.119.245.12   HTTP      483 GET /pearson.png HTTP/1.1
   1073 7.878503    128.119.245.12   114.214.218.49   HTTP      745 HTTP/1.1 200 OK  (PNG)
   1077 7.885846    114.214.218.49   128.119.245.12   HTTP      497 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
   1096 8.031958    114.214.218.49   128.119.245.12   HTTP      328 GET /favicon.ico HTTP/1.1
   1138 8.331085    128.119.245.12   114.214.218.49   HTTP      539 HTTP/1.1 404 Not Found  (text/html)
   1221 8.930788    128.119.245.12   114.214.218.49   HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
   1279 10.145178   114.214.218.49   117.18.237.29    HTTP      288 GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEA8XGkjG8iOAkhj…
   1293 10.453271   117.18.237.29    114.214.218.49   OCSP      853 Response
```

```
> Frame 1004: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.218.49, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53871, Dst Port: 80, Seq: 1, Ack: 1, Len: 428
> Hypertext Transfer Protocol
```

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

并输入实验介绍中给出的账号和密码，等到页面加载完毕后，停止捕获，得到如下图所示的报文：



```
No.     Time        Source           Destination      Protocol  Length  Info
    115 2.464385    114.214.227.114  128.119.245.12   HTTP      498 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    131 2.781425    128.119.245.12   114.214.227.114  HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
    458 13.182219   114.214.227.114  109.244.23.87    HTTP      249 GET /api/toolbox/geturl.php?h=818FECE510BB9F42534666E5F425986B&v=9.5.0.3517&r=7015_sogou_pinyin_8.4.0.1039_701…
    462 13.223391   109.244.23.87    114.214.227.114  HTTP      208 HTTP/1.1 200 OK
    828 24.672623   114.214.227.114  128.119.245.12   HTTP      557 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
    841 25.000815   128.119.245.12   114.214.227.114  HTTP      544 HTTP/1.1 200 OK  (text/html)
    858 25.323986   114.214.227.114  128.119.245.12   HTTP      328 GET /favicon.ico HTTP/1.1
    867 25.645105   128.119.245.12   114.214.227.114  HTTP      539 HTTP/1.1 404 Not Found  (text/html)
   1027 31.732203   114.214.227.114  184.51.189.222   HTTP      267 GET /zh-CN/livetile/preinstall?region=CN&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold HTTP/1.1
   1048 32.024083   184.51.189.222   114.214.227.114  HTTP/X…   251 HTTP/1.1 200 OK
```

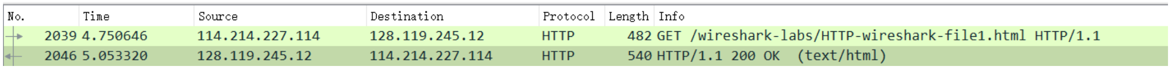
```
> Frame 115: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.227.114, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
```

```
0000  5c dd 70 91 72 e2 f4 d1  08 0c 58 82 08 00 45 b8   \·p·r··· ··X···E·
0010  01 e4 b5 59 40 00 80 06  00 00 72 d6 e3 72 80 77   ···Y@··· ··r··r·w
0020  f5 0c c9 6b 00 50 a4 6d  ba 91 c2 35 bd cb 50 18   ···k·P·m ···5··P·
0030  04 00 ad 2f 00 00 47 45  54 20 2f 77 69 72 65 73   ···/··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   tml HTTP /1.1··Ac
```

五、 结果分析

1. 关于五次 http 报文抓取的分析

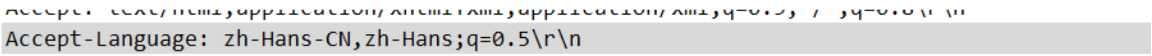
（1）Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



```
No.     Time        Source           Destination      Protocol  Length  Info
   2039 4.750646    114.214.227.114  128.119.245.12   HTTP      482 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   2046 5.053320    128.119.245.12   114.214.227.114  HTTP      540 HTTP/1.1 200 OK  (text/html)
```

都是 HTTP/1.1

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



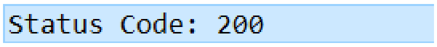
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
```

简体中文（大陆使用），简体中文

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

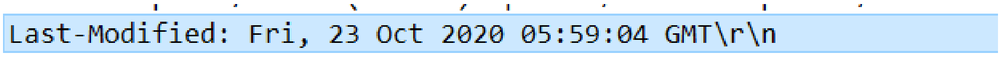
我的是 114.214.227.114；服务器的是 128.119.245.12

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



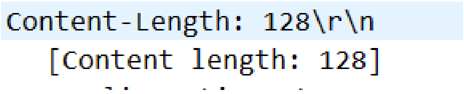
```
Status Code: 200
```

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



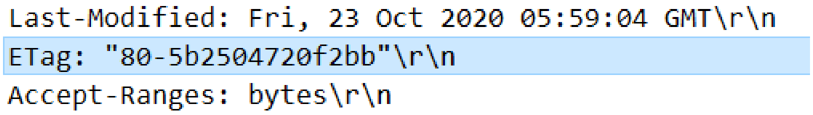
```
Last-Modified: Fri, 23 Oct 2020 05:59:04 GMT\r\n
```

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



```
Content-Length: 128\r\n
   [Content length: 128]
```

（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.

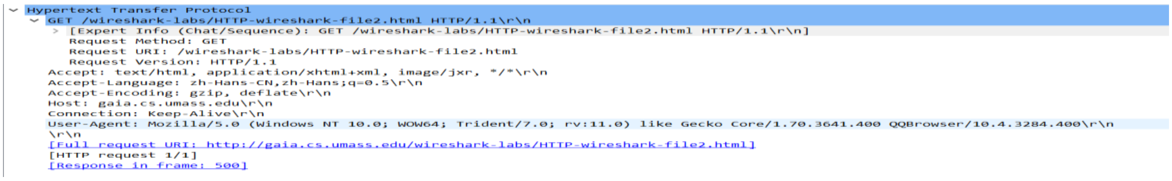


```
Last-Modified: Fri, 23 Oct 2020 05:59:04 GMT\r\n
ETag: "80-5b2504720f2bb"\r\n
Accept-Ranges: bytes\r\n
```

例如：Last-Modified.

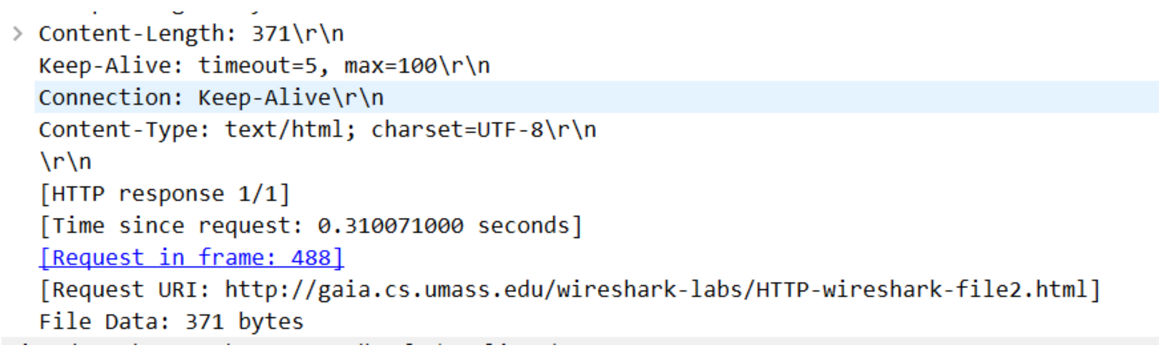
(8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

没有看见。

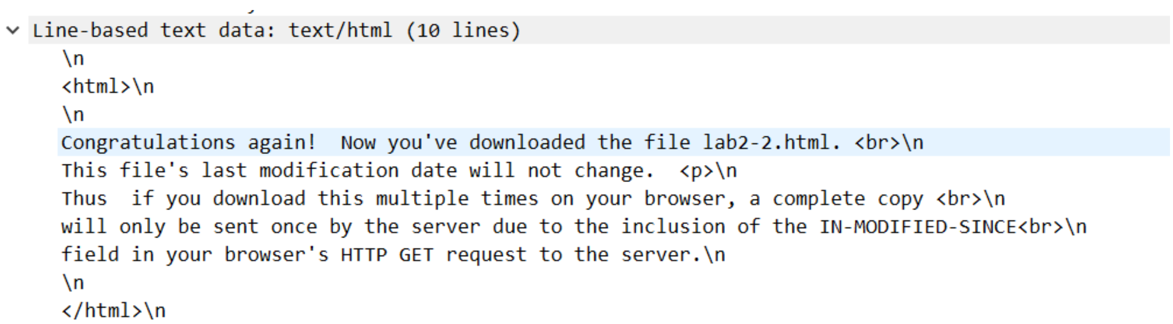


```
⌄ Hypertext Transfer Protocol
  ⌄ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
    Accept-Language: zh-Hans-CN,zh-Hans;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Core/1.70.3641.400 QQBrowser/10.4.3284.400\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
    [Response in frame: 500]
```

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



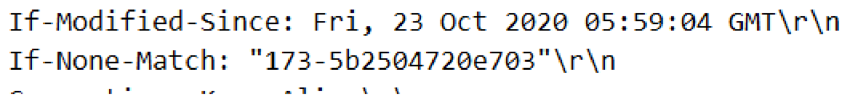
```
> Content-Length: 371\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.310071000 seconds]
  [Request in frame: 488]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 371 bytes
```



```
v 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
```

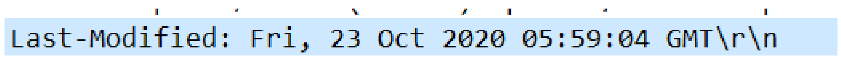
返回了文件内容。因为此报文中包含了文件内容的一些信息

（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?



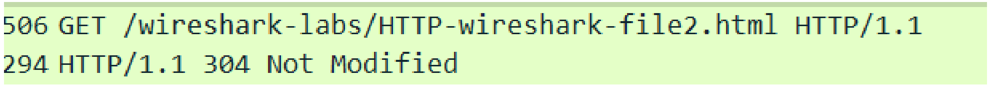
```
If-Modified-Since: Fri, 23 Oct 2020 05:59:04 GMT\r\n
If-None-Match: "173-5b2504720e703"\r\n
```

跟随着 Last-Modified 对应的时间：



```
Last-Modified: Fri, 23 Oct 2020 05:59:04 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.



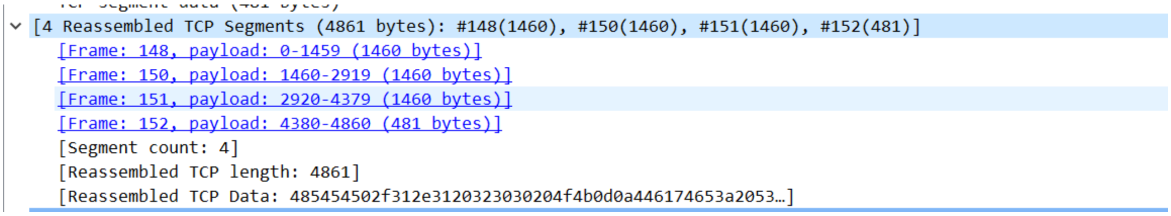
```
506 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
294 HTTP/1.1 304 Not Modified
```

是 304 Not Modified.没有显式地传一个文件的内容，因此此次报文并没有包含任何有关文件的信息

（12）How many HTTP GET request messages were sent by your browser?

1 个

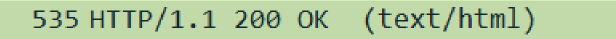
（13）How many data-containing TCP segments were needed to carry the single HTTP response?



```
    TCP segment data (481 bytes)
  [4 Reassembled TCP Segments (4861 bytes): #148(1460), #150(1460), #151(1460), #152(481)]
      [Frame: 148, payload: 0-1459 (1460 bytes)]
      [Frame: 150, payload: 1460-2919 (1460 bytes)]
      [Frame: 151, payload: 2920-4379 (1460 bytes)]
      [Frame: 152, payload: 4380-4860 (481 bytes)]
      [Segment count: 4]
      [Reassembled TCP length: 4861]
      [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053…]
```

4 个

（14）What is the status code and phrase associated with the response to the HTTP GET request?



```
535 HTTP/1.1 200 OK  (text/html)
```

（15）Are there any HTTP status lines in the transmitted data associated with a TCP-induced “Continuation”?

没有。在第三部分的 pdf 的介绍中明确的说明过此问题。

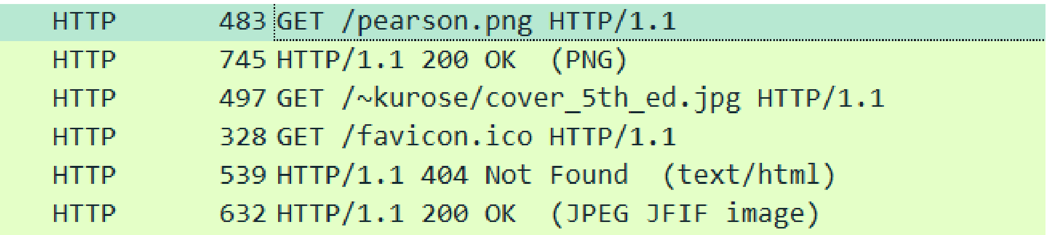
（16）How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

一共有五个。可以参见实验内容第四部分中给出的报文截图。

4 个发往 128.119.245.12,1 个发往 117.18.237.29

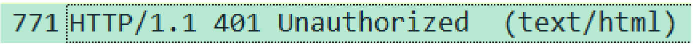
（17）Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

serially.因为发出了第一张图之后，等到了响应之后发出的第二张图片。



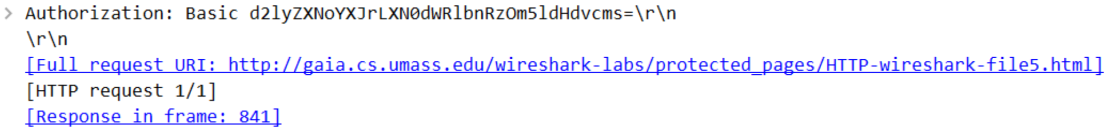
```
HTTP      483 GET /pearson.png HTTP/1.1
HTTP      745 HTTP/1.1 200 OK  (PNG)
HTTP      497 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
HTTP      328 GET /favicon.ico HTTP/1.1
HTTP      539 HTTP/1.1 404 Not Found  (text/html)
HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
```

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



```
771 HTTP/1.1 401 Unauthorized  (text/html)
```

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



```
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
  [HTTP request 1/1]
  [Response in frame: 841]
```

2.ppt 中的问题

分析 HTTP 中 get 和 post 请求方式的区别：

答：1.get 是不安全的，因为在传输过程中，数据被放在了请求的 URL 中；post 的所有操作对用户来说都是不可见的

2.get 传送的数据量较小，这主要是因为受 URL 长度的限制；post 传送的数据量较大，一般被默认为不受限制

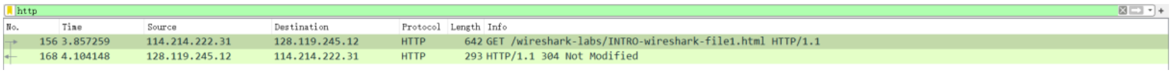
3.get 是从服务器上获取数据的，post 是向服务器传送数据的

3.<<Wireshark 简介>>对应的问题的回答：

1. List up to 10 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

ARP,TCP,ICMP,OICQ,DNS,DHCP,SSDP,MDNS,LLMNR,TCP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)



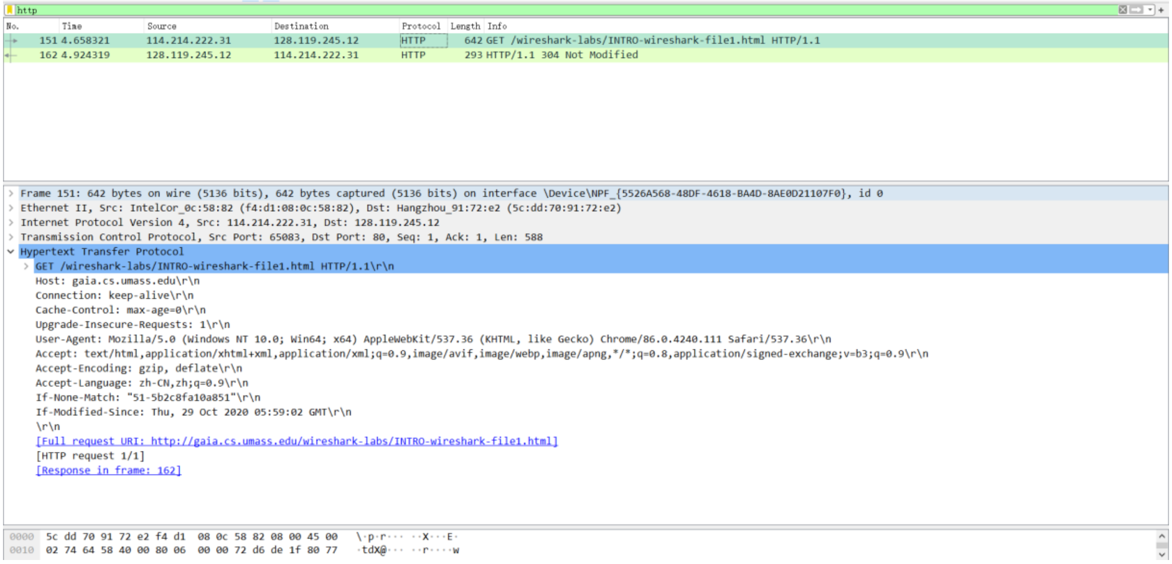
```
http
No.      Time       Source           Destination      Protocol Length Info
    156 3.857259   114.214.222.31   128.119.245.12   HTTP       642 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
    168 4.104148   128.119.245.12   114.214.222.31   HTTP       293 HTTP/1.1 304 Not Modified
```

0. 25s

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

128.119.245.12　114.214.222.31(本地)

4.第一条：

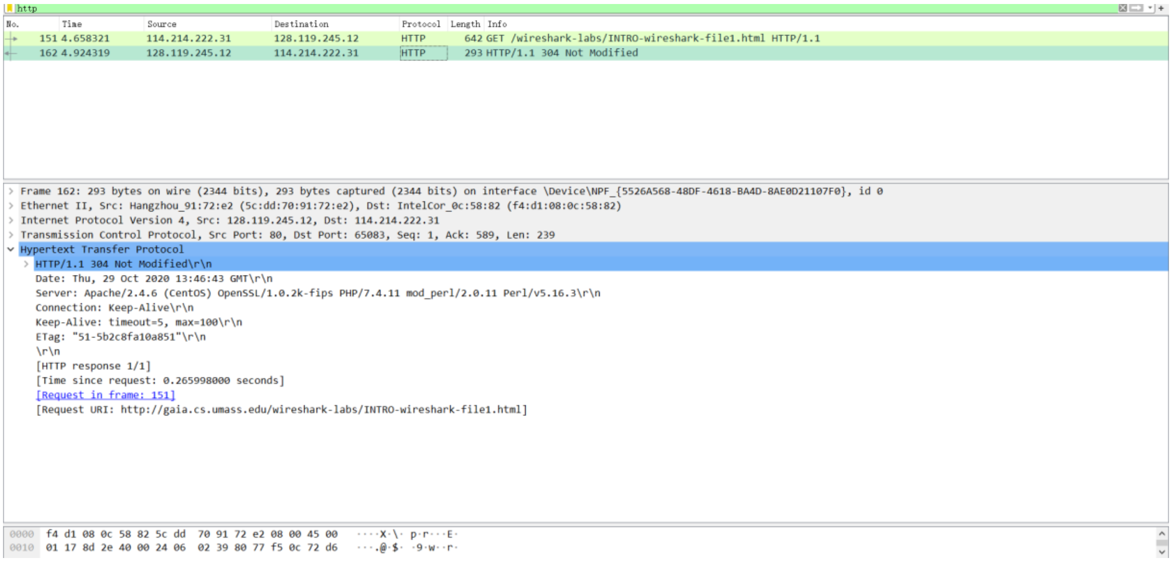


```
No.   Time      Source          Destination     Protocol Length Info
151 4.658321    114.214.222.31  128.119.245.12  HTTP     642 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
162 4.924319    128.119.245.12  114.214.222.31  HTTP     293 HTTP/1.1 304 Not Modified
```

```
> Frame 151: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: IntelCor_0c:58:82 (f4:d1:08:0c:58:82), Dst: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2)
> Internet Protocol Version 4, Src: 114.214.222.31, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65083, Dst Port: 80, Seq: 1, Ack: 1, Len: 588
v Hypertext Transfer Protocol
  > GET /wireshark-labs/INTRO-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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.111 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;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    If-None-Match: "51-5b2c8fa10a851"\r\n
    If-Modified-Since: Thu, 29 Oct 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 162]
```

```
0000  5c dd 70 91 72 e2 f4 d1  08 0c 58 82 08 00 45 00   \·p·r··· ··X···E·
0010  02 74 64 58 40 00 80 06  00 00 72 d6 de 1f 80 77   ·tdX@··· ··r····w
```

第二条：



```
No.   Time      Source          Destination     Protocol Length Info
151 4.658321    114.214.222.31  128.119.245.12  HTTP     642 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
162 4.924319    128.119.245.12  114.214.222.31  HTTP     293 HTTP/1.1 304 Not Modified
```

```
> Frame 162: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{5526A568-48DF-4618-BA4D-8AE0D21107F0}, id 0
> Ethernet II, Src: Hangzhou_91:72:e2 (5c:dd:70:91:72:e2), Dst: IntelCor_0c:58:82 (f4:d1:08:0c:58:82)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 114.214.222.31
> Transmission Control Protocol, Src Port: 80, Dst Port: 65083, Seq: 1, Ack: 589, Len: 239
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Thu, 29 Oct 2020 13:46:43 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-5b2c8fa10a851"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.265998000 seconds]
    [Request in frame: 151]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

```
0000  f4 d1 08 0c 58 82 5c dd  70 91 72 e2 08 00 45 00   ····X·\· p·r···E·
0010  01 17 8d 2e 40 00 24 06  02 39 80 77 f5 0c 72 d6   ···.@·$· ·9·w··r·
```